Facultad de Ciencias Sociales

Departamento de Política y Gobierno

Comparativa entre la normativa de Protección de Datos Personales en Chile y el Reglamento General de Datos de la Unión Europea.

Tesina para optar al Grado de Licenciado en Administración Pública

Autor: Fabián Catalán Segura

Profesor Guía**:** Sebastián Elgueta

Santiago, Chile

2022

TABLA DE CONTENIDO

INDICE DE TABLAS

GLOSARIO:

TICS	**Tecnologías de Información y Comunicación**
TI	**Tecnologías de Información**
TC	**Tecnologías de Comunicación**
ONU	**Organización de las Naciones Unidas**
Datenschutzgesetz	**Ley de Protección de Datos en alemán**
UE	**Unión Europea**
CdE	**Consejo de Europa**
CEDH	**Consejo Europeo de Derechos Humanos**
RGPD	**Reglamento general de Protección de Datos**
CCE	**Comunidades Europeas**
SEPD	**Supervisor Europeo de Protección de Datos**
TJUE	**Tribunal de Justicia de la Unión Europea**
ATELMO	**Asociación Chilena de Telefonía Móvil**
MTT	**Ministerio de Transporte y Telecomunicaciones**
CPLT	**Consejo para la Transparencia**
DPD	**Delegada o Delegado de Protección de Datos**

RESUMEN:

La tecnología y la capacidad para procesar datos personales se ha desarrollado a una velocidad acelerada en el mundo globalizado en el que se inserta Chile, sin embargo este avance requiere estar acompañado de una normativa que contenga las competencias para adaptarse a nuevas formas de interacción digital, al mismo tiempo que proteja los derechos de los ciudadanos. El presente trabajo busca reconocer el contexto en el que se encuentra Chile a la fecha y los desafíos que debe enfrentar para proteger los datos personales de las personas naturales. Situación estudiada en base a la normativa vigente en Chile, comparada con la experiencia de la Unión Europea, que es considerada el estándar mundial en la materia. Como resultado se encontraron cuatro dimensiones que son vitales para una regulación sólida y eficaz, las cuales actualmente no están presentes en la legislación vigente, o no tienen en cuenta características que se consideran relevantes para su debida protección.

ABSTRACT

The technology and the capacity to process personal data has developed at an accelerated speed in the globalized world in which Chile is inserted, however, this progress needs to be accompanied by regulations that contain the skills to adapt to new forms of digital interaction that at the same time protect the rights of citizens. The present work seeks to recognize the context in which Chile finds itself to date and the challenges it must face to protect the personal data of natural persons. Situation studied based on the regulations in force in Chile, compared with the experience of the European Union, which is considered the world standard in the matter. As a result, four dimensions were found that are vital for a solid and effective regulation, which are currently not present in the current legislation, or do not consider characteristics that are considered relevant for their due protection.

1 INTRODUCCIÓN

En la actualidad, hemos sido participes y testigos de un movimiento revolucionario, determinado por el crecimiento exponencial en la capacidad de acceso que tienen las personas a las "*Tecnologías de Información y Comunicación" (*TICS). Que se pueden reconocer como "las tecnologías que se necesitan para la gestión y transformación de la información, muy en particular con el uso de ordenadores y programas que permiten crear, modificar, almacenar, proteger y recuperar esa información" (Sánchez, 2008, p.156), en este sentido son sistemas que se encuentran integrados al ámbito de la información con la capacidad de tratarla y/o comunicarla, con un fin que se encuentre adecuadamente fundado.

Las TICS, se pueden dividir en dos dimensiones, las "*Tecnologías de la Comunicación*" (TC) dedicadas a posibilitar un rápido flujo de información mediante diversos dispositivos que hacen posible a la comunicación globalizada. Mientras que las *"Tecnologías de la Información"* (TI) son "caracterizadas por la digitalización de las tecnologías de registros de contenidos (informática, de las comunicaciones, telemática y de las interfaces)" (ONU en Sánchez, p.156).

Gracias a estas características es que en los últimos años se les puede atribuir el ser un tema relevante en Chile, más aún debido a que en contexto de pandemia se ha presentado un acelerado avance en la actualización de la información y la capacidad de plataformas gubernamentales, gracias a que sirven tanto como medio para intermediar entre los requerimientos de los ciudadanos, como responder a estos y facilitar la transparencia de información respecto a la situación nacional. Sin embargo en agendas de transformación digital se han divisado dilemas, con respecto en la forma en que estas pueden abordar una debida relación y protección con los datos tratados, del cómo convertirlos en recursos valiosos para la toma de decisiones y mejora de los servicios e incluso la forma en como regular a la industria que hoy en día ya domina como utilizar las ventajas de los datos en sus servicios, es decir, el mercado privado.

Como mencione con anterioridad existe una relación bastante normalizada en la sociedad actual, pero que ha encendido alarmas de alerta en organizaciones de cooperación internacional que concuerdan en el hecho de que las tecnologías son cada vez más dependientes de la información. Causando una situación crítica en donde las principales desarrolladoras de hardware, software o incluso que bancos de datos posean incentivos que contribuyen a que las nuevas tecnologías tengan cada vez mayor capacidad de tratar cantidades masivas de información que incluso tiene características propias de una persona física, pero que se encuentran como materia prima en lo que reconoceremos como datos.

Aunque para el gobierno de Chile la necesidad de modernizar el aparato del Estado a manera de adaptarse a las crecientes y dinámicas necesidades de la sociedad no sea un tema novedoso, lo cierto es que la instalación de los derechos de tercera generación si lo son. Razón por la cual incluso para países desarrollados es imperante fomentar el acoger ideas tales como, reestructurar la función de los derechos, los alcances de estos y el adaptarlos a las preocupaciones mundiales de los últimos años para que los Estados sean capaces de brindar una adecuada calidad de vida a los ciudadanos.

Entre estos derechos de 3º generación, encontramos a el "derecho de protección de datos personales", el cual ha significado un gran estudio sobre la normativa vigente, que evidencia como estas requieren de cambios estructurales en la forma en la que se deben articular y coordinar con el Estado para proteger, cumplir y respetar este derecho de manera apropiada. Por lo que primeramente se revisará en profundidad su historia normativa, en sus primeras apariciones en normativas internacionales, como también su implementación y discusión en nuestro país, luego se recopilaran los aportes de instituciones europeas e investigaciones de autores académicos en el área de derechos internacionales y protección y regulación de datos personales.

Todos estos aportes académicos e institucionales se comprenderán como recursos esenciales para comprender la situación actual que se tiene respecto a este derecho, que desafíos representa para la administración chilena y en qué dirección se corresponde orientarse. Por estos motivos se recurrirá en igual medida a una comparación objetiva de la normativa chilena vigente con el estándar que nos brinda la experiencia internacional de la Unión Europea (UE), que es reconocida como el sector donde se ha obtenido mayor avance en cuanto a tratar los límites y alcances de este novedoso derecho.

2 PROBLEMATIZACIÓN

2.1 Experiencia Internacional en Protección de Datos Personales:

Para continuar, es relevante repasar la historia y experiencia internacional sobre protección de datos personales, la cual tiene su origen como derecho fundamental en la Declaración Universal de Derechos Humanos de 1948, no obstante se debe aclarar que esta fue pactada en un contexto donde los sistemas de automatización no eran sino más que ideas. En el cual el derecho de protección de datos no se encuentra debidamente explicito, sino que, como bien lo titula este apartado se reconoce como el primer antecedente de este derecho ya que por más de dos décadas este derecho se encontraría dentro del derecho a la privacidad, asunto que se rescata en el artículo N° 12 donde se señala que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (Naciones Unidas, 2015; p.26).

No es hasta el 12 de octubre, en el año 1970, cuando Alemania se destacaba como el primer país en aprobar y publicar una ley en donde se trataría directamente la materia de protección de datos, que se denominó como "*Datenschutzgesetz"*, esta como ordenamiento busca brindar una adecuada protección a los datos de las personas del Estado de "Land Hessen". Es considerable este evento ya que por primera vez en la historia se apreciaba la oportunidad de que los documentos se procesen o estén en camino a ser procesados por sistemas automatizados.

Mas aún fue en esta instancia que se reconoció como menester, una normativa que proteja los resultados del tratamiento de los datos personales, ante autoridades, entidades públicas o empresas privadas, Según el Gesetz- und Verordnungsblatt (1970) se debe integrar especiales determinaciones en el tercer sector enunciado anteriormente, en vista de que al recoger los datos, estos adquieren la responsabilidad de determinar, reenviar y procesar datos, razones que deben establecerse con un fin único. Además de que deben asegurar que estos documentos no sean vistos o utilizados por personal no autorizado o idóneo, de lo contrario el mismo ordenamiento señala que los datos residentes en estos deben ser destruidos.

Esta tendencia seria seguida de cerca e inicialmente por Suecia en 1973, cinco años después por Noruega con la Ley Nº48, de 9 de junio de 1978, sobre registros de datos personales, pero se debe destacar a Francia con su Ley Nº78-17, de 6 de enero de 1978, sobre informática, ficheros y libertades. Puesto que en su búsqueda por el resguardo de los datos se integró como una legislación destinada a regular conductas consideradas potencialmente peligrosas en el procesamiento de datos, según señala la Doctora Monique Lions el "desarrollo de la informática, especialmente en el sector público, engendró el temor de que el conjunto de los ciudadanos estuviese "inscrito en tarjeta" en beneficio de los poderes públicos y de las organizaciones económicas" (Lions, 1994; p.441). Otro hecho relevante mencionado por la autora es que esta Ley que se originó por voluntad del poder ejecutivo, es decir, el Presidente Valéry Giscard d'Estaing fue quien creó una Comisión de doce miembros, con el objetivo de elaborar "medidas tendientes a garantizar que el desarrollo de la informática en los sectores público, semipúblico y privado se realice dentro del respeto a la vida privada, las libertades individuales y las libertades públicas" (Lions, 1994; p.441).

Este nuevo apogeo que instauró la tecnología en la década de 1970 permitió que se reconociera el avance y relevancia que significaba la tecnología basada en información, hecho que tomo cuerpo cuando se observó una respuesta por parte de las administraciones europeas, las cuales como hemos revisado se enfocaron en el diseño e implementación de normas destinadas a regular los datos de las personas que eran recolectados y tratados por procesos automatizados del sector privado y público. Adicionalmente otra muestra de esto se vislumbra cuando "el Comité de Ministros del Consejo de Europa adoptó diversas resoluciones en materia de protección de datos personales referidas al artículo 8 del CEDH"(UE, 2018; p.27), uno de los más importantes se firma en 1981, el denominado "Convenio 108" que según la Unión Europea se generó debido a una "creciente necesidad de contar con normas más detalladas para salvaguardar a las personas físicas"(UE, 2018; p.27), además esta misma entidad recalca que:

> se aplica a todo tratamiento de datos realizado por los sectores público y privado, incluidas las autoridades judiciales y los cuerpos de seguridad. Protege a las personas físicas contra los abusos que pueden llevarse a cabo en el tratamiento de datos personales, y busca, al mismo tiempo, regular los flujos transfronterizos de datos personales (UE, 2018; p.28).

Otros aportes que hacen de este un documento vigente hasta la actualidad, aunque con reformas en los años 2001 y 2012, son el integrar obligaciones jurídicamente vinculantes que en caso de no ser cumplidas de manera licita y leal, sentarían las bases para la prohibición de tratamiento de datos,

eso es debido a “falta de garantías jurídicas adecuadas” (UE, 2018; p.28). Incluso este instrumento provee limitaciones a este derecho, en caso de “intereses superiores” tales como la seguridad o defensa del estado, lo cual se traduce en que la libre circulación de los datos se vea limitada a causa de normativas que no proporcionan protecciones equivalentes.

No obstante existió un grave problema para los países miembros de la UE ya que “La libre circulación de bienes y servicios, capitales y personas en el mercado interior requería la libre circulación de datos, que no podía llevarse a cabo si los Estados miembros no podían confiar en un nivel elevado y uniforme de protección de los datos” (UE, 2018; p.33). Estas dificultades que producía el marco normativo vigente provocaron una inminente reforma en la legislación en materia de protección de datos personales, que significó años de diálogos y debates y dieron como resultado que en abril de 2016 el Consejo de Europa (CdE), la Unión Europea y el Parlamento Europeo en conjunto formaran a la “Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa”. Quienes elaboraron el denominado “Reglamento General de Protección de datos de la UE” en 2016, con la misión de elevar los niveles de protección de los datos personales y además sentar las bases para unificar dicho estándar en los países de la Comunidad Europea, respecto a esto el documento señala:

> Los principios y derechos esenciales del interesado que estaban recogidos en la Directiva sobre protección de datos. Además, introduce nuevas disposiciones que obligan a las organizaciones a aplicar la protección de los datos desde el diseño y por defecto, a nombrar un delegado de protección de datos en determinadas circunstancias, a respetar un nuevo derecho a la portabilidad de los datos y a atenerse al principio de responsabilidad proactiva (UE, 2018; pp.34-35).

2.2 Normativa Vigente en Chile

En nuestro país, el proceso de concebir una ley de protección de datos personales comenzó a tomar fuerza en un contexto de regreso de la democracia en 1993 por el cual se vio favorecido, pasando a tomar especial relevancia al convertirse en un tema que se materializa concretamente en un proyecto de ley que se presentaría el día 5 de enero de 1993 a consideración del Senado en forma de moción parlamentaria que demostraría la iniciativa de la administración en turno y que se transformaría en el denominado “Proyecto de Ley sobre Protección Civil de la Vida Privada”.

En el documento se puede distinguir que este proyecto de ley tiene como principal objetivo el reforzar y "dar una adecuada protección al derecho a la privacidad de las personas, en el ámbito del Derecho Civil, ante a eventuales intromisiones ilegítimas. A diferencia de lo que sucede en otras naciones del mundo, nuestro país carece de una tradición legislativa en esta importantísima materia" (Cantuarias, 1993, Moción Parlamentaria en Sesión Parlamentaria; Legislatura 325), demostrando de esta manera que este documento nace de una necesidad de reconocer estos nuevos desafíos y adaptarse a normativas internacionales. Que se orientan igualmente por la "Declaración Universal de Derechos Humanos de 1948" y los artículos 5° y 19° de nuestra constitución de 1980, en donde se refiere a que la esfera de "vida privada" es un "derecho fundamental y por tanto es un derecho anterior y superior al Estado, además de ser una muestra de la importancia de reconocer los esfuerzos y experiencia de otras administraciones del globo.

Siguiendo esa línea es que el 16 de mayo de 1995, es que se desarrolla el "*Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento, Recaído en el Proyecto de Ley, en Primer Trámite Constitucional, sobre Protección de la Vida Privada de las Personas"*, que realiza observaciones que toman en cuenta a actores tales como la Asociación Chilena de Empresas de Tecnologías de Información, en donde se recomienda y expresa que la información de vida privada o íntima es "objetivo, acotado y universalmente aceptado. El individuo ha de ser el único propietario de su información íntima, y cuando deba o desee entregarla a terceros, le dará al receptor un derecho de uso, que en ningún caso será del tipo traslaticio de dominio" (Comisión de Constitución, 1995, Sesión 63; Legislatura 330).

Además se toma de manifiesto las influencias de experiencias internacionales como es el caso de España con la Ley orgánica Nº1, del 5 de mayo de 1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, la Legislación francesa, la ley sobre Informática, ficheros y libertades N° 78-17 de 1978 y la Ley Orgánica sobre tratamiento automatizado de los datos de carácter personal del 29 de octubre de 1992.

Otro aspecto no menos relevante que se divisa al leer este documento es que podemos distinguir como se considera que los datos personales son un recurso que puede transformarse en algo pernicioso en caso de no regularse, ya que se sostiene que los "antecedentes sobre ésta pueden organizarse por medios automatizados, mecánicos y manuales, como los conocidos ficheros de datos, y cualquiera de ellos puede constituir un arma potencial de la producción de daño" (Comisión de Constitución, 1995, Sesión 63; Legislatura 330).

Por último en este texto nos damos cuenta de que según el asesor jurídico, Sebastián Vial no puede definirse de manera tajante de los datos que pertenecen a la esfera pública, es decir de conocimiento general y los que encuentran residentes en la esfera privada, sin embargo se protegerían los hechos que afectan negativamente a la dignidad de una persona, a lo cual DICOM S.A incluyo anotaciones que fueron tomadas en cuenta por la Corte y se determinó que "existen antecedentes personales, como los comerciales y financieros de una persona, que interesan no sólo a su titular, sino también a quienes contratan con ellas y, por lo tanto, deben ser conocidos" (Comisión de Constitución, 1995, Sesión 63; Legislatura 330).

Es el 3 de septiembre del año 1997 cuando se presentaba el "*Segundo Informe de Comisión de Constitución"*, en el cual se determinaba que es beneficioso cambiar las perspectiva respecto a cómo asegurar y regular de manera eficiente y eficiente la vida privada de las personas considerando también la experiencia de Gran Bretaña con la Ley del 12 de julio de 1984, sobre protección de datos, por lo que según la Comisión encargada es imperante que el documento sea "dedicado a la protección de los datos personales de las personas, particularmente por la vía informática, ya que es evidente que uno de los más graves atentados contra la privacidad de los sujetos deriva del uso indiscriminado de la informática y de las computadoras" (Comisión de Constitución, 1997, Sesión 39; Legislatura 335), y de esta misma en esta sesión de debatieron y se configuraron 5 principios generales sobre los datos personales que se buscó plasmar en 5 títulos de la ley, los cuales son:

> La información individual dispersa es pública y la información organizada es reservada y quien autoriza es el legislador o quien sea facultado por los interesados. Los datos personales sólo pueden recolectarse por medios lícitos. Los datos personales sólo pueden recolectarse, procesarse, transmitirse y difundirse para la finalidad para la que, lícitamente, se hubieren recogido. Los antecedentes o hechos de la vida íntima o privada, que corresponden a la denominada "información sensible", son reservados, por lo que su publicidad requiere del consentimiento del afectado o estar autorizada expresamente por una ley excepcional. La ley puede, excepcionalmente, autorizar la desviación del fin para el cual se recolectó el dato, sólo con el fin de evitar una amenaza inminente al orden público o una violación grave de derechos de terceros, declaradas por una resolución judicial (Comisión de Constitución, 1997, Sesión 39; Legislatura 335).

Finalmente, el 28 de agosto de 1999, 18 días después de ser aprobada por el Congreso Nacional es cuando finalmente se pública la normativa denominada como Ley N° 19.628, sobre protección de la vida privada, que solucionaba este vacío normativo que existía en Chile respecto a otras normativas

de experiencia internacional que identificó el Senador Eugenio Cantuarias media década atrás. Sin embargo, esto no significaba que esta sería la versión final de la ley, ya que al revisar la Biblioteca Nacional del Congreso Nacional de Chile, se puede divisar que esta ha sufrido 5 modificaciones, la primera ocurrió el 13 de junio de 2002 mediante la ley 19.812, debido a que se incluyeron incisos al artículo N° 17 que protegían a los ciudadanos al contraer deudas con servicios básicos como "agua, electricidad, teléfono o gas" (Ley 19.812, 2002, art N° 1; inciso 3). Además de incluir en el artículo N°18 la prohibición de comunicar los "datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal" (Ley 19.812, 2002, art N° 1; inciso 4), de igual manera ocurre que es ilegítimo el comunicar datos de ciudadanos deudores "que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible" (Ley 19.812, 2002, art 1; inciso 4).

La segunda modificación de la ley se puede distinguir el 25 de octubre de 2010, a través de la ley 20.463 que modifica la ley N° 19.628 suspendiendo por el plazo que indica la información comercial de las personas cesantes, cambio legislativo impulsado por el Ministerio de Economía, Fomento y Turismo y la Subsecretaria de Economía y Empresas de Menor Tamaño, introduciendo al artículo 17 de la ley N° 19.628 que "Las entidades responsables que administren bancos de datos personales no podrán publicar o comunicar la información referida en el presente artículo, en especial los protestos y morosidades contenidas en él, cuando éstas se hayan originado durante el período de cesantía que afecte al deudor" (Ley 19.628, 2020, art 17; inciso 3)

Luego la tercera modificación la encontraríamos el 23 de julio de 2011, mediante la ley 20.521 que modifica la Ley N° 19,628, sobre protección de datos de carácter personal para garantizar que la información entregada a través de predictores de riesgo sea exacta, actualizada y veraz, este fue un cambio de menor envergadura ya que solo considero al artículo N°9 integrando que se "Prohíbese 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" (Ley 20.521, 2011; artículo único), donde se distingue que las empresas poseían el incentivo a generar bases de datos en las cuales consideraban aspectos que no eran meramente objetivos para relacionarse con las personas naturales o jurídicas, lo cual brinda una mirada de lo clave que es la labor de un documento legal y la importancia de irse adaptando en el tiempo.

Situación que se rescata nuevamente en su cuarta modificación el 17 de febrero de 2012, mediante la ley 20.575 que establece el principio de finalidad en el tratamiento de datos personales, que debió incluir al título III de la Ley 19.628 una aseveración respecto a la utilización de datos que se encuentren registrados y organizados donde se solicita respetar el principio de finalidad en el tratamiento de datos personales de carácter económico, financiero o bancario, que "será exclusivamente la evaluación de riesgo comercial y para el proceso de crédito", limitando así el tratamiento de datos personales para limitar el acceso de ciudadanos a actividades de la vida diaria, tales como "procesos de selección personal, admisión pre-escolar, escolar o de educación superior, atención médica de urgencia o postulación a un cargo público" (Ley 20.575, 2012; art N° 1).

Su quinta modificación se encuentra el 25 de agosto de 2020 donde se realizó un exhaustivo rediseño sobre las siglas y términos utilizados en el documento legal a manera de impedir vacíos o interpretaciones, además de regular la recolección de datos personales mediante encuestas, estudios de mercado o sondeos de opinión pública ya que se exige el "informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información. La comunicación de sus resultados debe omitir las señas que puedan permitir la identificación de las personas consultadas" (Ley 19.628, 2020, art N° 3).

Para terminar este recorrido de historia legislativa sobre la "vida privada" y la "protección de los datos personales" debemos entonces recurrir a la versión actual, que se encuentra vigente desde su publicación el día 26 de agosto de 2020, donde se realizó un nuevo aporte al artículo N° 17 anteriormente modificado, esta contempla el no poder comunicar el endeudamiento "con instituciones de educación superior de conformidad a las leyes números 18.591 y 19.287, ni aquellas adquiridas con bancos o instituciones financieras de conformidad a la ley N° 20.027, o en el marco de las líneas de financiamiento a estudiantes" (ley 19.628, 2020, art N° 17).

Este pequeño resumen de la historia legislativa de nuestro país nos deja entrever que una de las principales causas por la cual la Ley es modificada es debido a que si bien busca proteger a los datos personales y la dignidad de los ciudadanos, lo cierto es que se percibe un patrón en donde en la práctica no se considera grupos de empresas que interfieren y son vitales en la vida diaria de la sociedad chilena, refiriéndome de manera más clara al protegerlos de que bancos o empresas de servicios básicos sean capaces de comunicar información respectos a la conducta financiera y nivel de endeudamiento de los ciudadanos o estudiantes. Considerando además la forma en que se organiza el Estado, que desemboca en que la mayoría de estos servicios sean brindados por

empresas privadas, esto ya que podemos ver que en solucionar el primer aspecto hubo un periodo de 3 años y en caso del segundo punto es aún más preocupante ya que existió un periodo de 21 años para solucionar un problema que involucra a población no activa que aún no es parte de la cadena productiva del trabajo.

Otro factor que lleva a modificar la ley es el desconocimiento del cómo los datos personales pueden ser utilizados para restringir el acceso tanto a bienes como servicios, tampoco contempla tecnologías que utilizan "datos" como suministro en una red de aprendizaje reforzado, como es el caso de inteligencia artificial o la existencia masiva de bancos de datos con los que la industria de servicios actual no necesariamente necesita de datos "sensibles" o "personales" para interpretar o evaluar la conducta de un "grupo particular de la población" que es similar a un ciudadano específico.

3 PREGUNTA DE INVESTIGACIÓN

Reconocer cuales son las características de la sociedad actual no es una tarea sencilla, aunque como tema de discusión tiene su origen por lo general cuando se es consciente de incipientes noticias, conflictos o situaciones que afectan al entorno de una persona, pero es que, solo cuando se es capaz de realizar este cuestionamiento, es que se reconoce el motivador del nacimiento de las disciplinas denominadas como "ciencias sociales". Que a lo largo del tiempo adquieren como objetivo el estudiar el comportamiento de las sociedades y lograr establecer tanto patrones lógicos, como universales, aunque que generalmente se reconoce que al tener el concepto de "sociedad" como objeto de estudio, es también el cómo doctrina obtiene un aumento en la dificultad, ya que cuando se trata con esta materia, no se está tratando con una sustancia inmutable ni particular, sino más bien con una diversidad, tanto por el lugar en que se encuentran emplazadas las sociedades, como el espacio-tiempo en las que se les estudia o incluso aspectos como la cultura, economía o política que son inherentes en cualquier grupo de individuos. Aspectos que le dan a cada "sociedad" un sentido de "unicidad", y que desemboca en que para efectos de la investigación emplazada en entender un Chile dentro de una "era digital", se decidiera el adoptar y describir el concepto denominado como "sociedad actual".

Al razonar como describir este concepto se es testigo de tres categorías casuísticas, en primer lugar, que somos una sociedad que se encuentra en una constante evolución, en donde buscamos adaptarnos a necesidades cada vez más complejas, crecientes y dinámicas, cuestión que incluso nos da las causas por las cuales existen las instituciones y sistemas que tienen como objetivo dar una adecuada respuesta a estas. En segundo lugar está el reconocernos como una sociedad dedicada a la producción de servicios y bienes, que está ampliamente interconectada y es poseedora de un carácter interdependiente gracias a la extensión que han logrado los procesos de globalización en tratados y compromisos internacionales. En tercer lugar nos encontraríamos con la sociedad que no solo tiene disponible una cantidad de información nunca vista en la historia, sino que esta masa de información sigue creciendo tanto en volumen como en relevancia.

Es esta tercera característica la cual se destaca como un contexto clave del cual nace un dilema reciente para las administraciones del sector público, y lo cierto es que no pudo haber quedado en mejor posición, es decir, otras ocasiones en las cuales se ha repetido esta locación entre los autores y que da cuenta de nuestro avance como sociedad, es cuando se acuñan conceptos como el término de la "3º revolución industrial" que tuvo como principales aportes a la automatización y las tecnologías de información y comunicación (TICS) para dar paso a la "4º revolución industrial", trayendo consigo temas como la digitalización, el internet de las cosas, la nube, inteligencia artificial, etc.

Entonces el notable avance de la tecnología y la digitalización, son reconocidos como los nuevos referentes de la creación de procesos de innovación y herramientas que han demostrado tener la capacidad de transformarse en un arma de doble filo. Este fenómeno se debe a que en situaciones de esta índole, existe una suerte de dualidad, es decir, si esta innovación es adoptada por una administración eficiente e informada, entonces, los procesos de avance tecnológico tienden a convertirse en herramientas de apoyo esenciales de cara a mejorar el bienestar de la sociedad, como lo es el caso de las vacunas y las constantes investigaciones con las cuales se busca que los productos, servicios, medios, herramientas y entidades gubernamentales sean capaces de satisfacer las dinámicas y exigentes necesidades humanas.

Pero a la vez está disponible la posibilidad de que mediante estas innovaciones se busquen objetivos contrarios a los derechos fundamentales actuales, algunas consecuencias negativas de los pocos lineamientos normativos en el mundo digital actual son, primeramente la intervención e influencia arbitraria de grupos que poseen intereses particulares en los usuarios que usan regularmente

plataformas y dispositivos tecnológicos, divisándose a través de la programación de mensajes subliminales que permiten tanto el moldeamiento como el permear las distintas esferas, de índole social, política o económica, en segundo lugar se da el brindar un vació jurídico que incentive la creación de software destinado a realizar vigilancia sistemática a gran escala, causando tanto daños en la privacidad y vida privada de una población determinada, en tercer lugar estaría el no dar garantía del funcionamiento de los derechos fundamentales en el internet, tal y como si lo gozan las personas en la realidad, consecuencias consideradas graves y a las cuales cada vez podemos ir agregando una cantidad mucho más elevada que analizaremos más adelante.

Sin embargo, alejándonos de la teoría, se debe señalar que en la realidad no vamos a encontrarnos con lo que denominaríamos como "periodo de gracia" para el gobierno chileno y tampoco está disponible la oportunidad de esperar a que una herramienta novedosa sirva a fines ilegítimos que afecten tanto la integridad como la autonomía de sus ciudadanos para que el Estado reasuma su papel como ente regulador e intermediario, sino que se reconoce un sentido de urgencia, en donde existe la necesidad de intervenir en las nuevas tecnologías que contengan riesgos potenciales para las personas físicas.

Este es el motivador principal que ha llevado a esta investigación a centrarse en la "*Protección de Datos en Chile*", es un hecho innegable que se acepta de manera directa como las sociedades tienen a su disposición cada vez más cantidad de información o que incluso se esfuercen por adaptarse a paradigmas de automatización y digitalización, pero es imperante que Chile se haga la siguiente pregunta; ¿Qué desafíos se vinculan al tratamiento de datos personales para el sector público en Chile en la era digital?, cuya respuesta se aborda en esta investigación basada fundamentalmente en la experiencia internacional europea, que nos señala cuales son los requerimientos que debe tener un país para brindar protección en los datos personales de los ciudadanos.

Entonces, mediante esta investigación se busca aportar una perspectiva que fomente una revisión exhaustiva de la jurisprudencia vigente, mediante el esclarecimiento de la suficiencia de esta comparada a entidades que se auto reconocen como actores que van a la vanguardia en torno a la tendencia de los "derechos de protección de datos", además de reconocer cuales son los desafíos que deberán afrontar las administraciones gubernamentales en Chile respecto al tratamiento de los datos personales de sus ciudadanos.

Se considera vital que el primero en entender la importancia de la seguridad y uso responsable de los datos sea el mismo sector público, sirviendo de guía y de ejemplo para los distintos sectores

productivos, que hacen uso de disciplinas complejas como la “Inteligencia Artificial” (IA) o “Ciencias de Datos”, “Bancos de Bases de datos”, la “Nube”, etc. Las cuales no buscan reemplazar el razonamiento humano sino convertirse en un apoyo para la resolución y la automatización de “tareas cíclicas”, ya que, aunque las máquinas sean las que procesen los datos, no serán estas las encargadas de la toma de decisiones, es decir, son las autoridades competentes quienes deben fomentar el incluir al sector público como agente impulsor de un uso responsable y concordante con los derechos fundamentales de las avances de vanguardia, cosa que se logra a través de un equilibrio entre la innovación y la regulación.

4 OBJETO DE ESTUDIO:

Esta tesis tendrá como objetivo identificar qué problemáticas deberá a enfrentar el gobierno chileno con el fin de mejorar su desempeño en áreas como la eficiencia, eficacia y efectividad en procesos vinculados al tratamiento de datos y datos personales, entendiendo el nuevo paradigma global que suponen estos, es decir, como recursos primarios para las nuevas tecnologías en constante crecimiento como es el caso de las Bases de Datos, IA O Incluso Sistemas de “Smart city”,

Se investigara a los “datos personales” como un determinante clave para el avance del Estado chileno y la manera en que se deben adaptar las normativas y organizaciones que tenemos en la actualidad para la creación de una base altamente competente, que sentara beneficios a manera de poder fortalecer y proteger los derechos fundamentales de sus ciudadanos mediante la regulación este novedoso sector digital, teniendo como principal referente el estándar internacional, denominado como *“Reglamento General de Protección de Datos”* de la Unión Europea adoptado en 2016. Cuyo objetivo según la página web de la entidad es convertirse en una “medida esencial para fortalecer los derechos fundamentales de las personas en la era digital y facilitar la actividad económica, ya que aclara las normas aplicables a las empresas y los organismos públicos en el mercado único digital” (Comisión Europea, 2022).

5.1 Objetivo General:

Identificar los desafíos que brindan los datos personales en el mundo globalizado actual y determinar la suficiencia de la normativa legal vigente en Chile respecto a la materia de tratamiento de datos personales por el sector público y privado.

5.2 Objetivos Específicos:

1) Analizar la normativa legal vigente de la Unión Europea en materia de protección de datos personales.
2) Revisar la normativa legal vigente en Chile en materia de protección de datos personales.
3) Identificar los desafíos de la normativa Chile a partir del estándar de la Unión Europea sobre tratamiento de datos personales.

5 ESTADO DEL ARTE

Aunque hasta ahora en la investigación se ha hablado de la historia de los datos personales en la experiencia internacional y nacional, su importancia y razones por las cuales se considera esencial su regulación en las experiencias antes mencionadas, no se ha dejado en claro ¿qué es lo que se entiende como un dato en esta investigación?

Entonces lo que se entenderá como un dato, es cualquier información presente en la red, definición que parece resultar extensa, lo cierto es que lo es, pero no significa que sea errónea ya que si se acude a instituciones especializadas en la lengua, como lo es la RAE (2022), este concepto referirá a la "información dispuesta de manera adecuada para su tratamiento por una computadora", o incluso podemos vincular a los datos con lo que en la academia denomina como "huella digital". Concepto apto para describir las actividades realizadas de manera digital, que incluye movimientos como "lo que hacemos, dónde lo hacemos, adónde vamos, a quiénes conocemos, qué tenemos, qué nos gusta o cómo nos sentimos" (Buenadicha et al, 2019; p.6), eventos provocan la creación de nuevos datos, gracias a la interacción del ser humano en la red y que quedan almacenados en bases de datos o en la nube para un eventual tratamiento.

Además, se debe aclarar que un “dato” y un “dato personal” serán tratados desde aquí, como dos conceptos diferenciados, ya que el segundo tiene una condición peculiar, la cual es el contener un vínculo que hace posible el identificar a una persona o que “en dicha información se singulariza a la persona, aunque no se identifique, de manera que fuera posible averiguar quién es el interesado si se llevara a cabo una mayor investigación” (UE, 2018; p.101).

Esto significa que “comprenden información relativa a la vida privada de una persona, que también incluye sus actividades profesionales, así como información sobre su vida pública” (UE, 2018; p.99), de hecho según el Derecho de la UE los datos personales pueden ser originados a partir de información objetiva e incluso subjetiva, es decir características intrínsecas de una persona y consideraciones sobre el comportamiento de esta persona en diversos escenarios por individuos externos. Por lo que igualmente se considera como datos personales en la entidad internacional antes mencionada a “opiniones políticas, creencias religiosas y otras creencias, incluidas las filosóficas” (Ibid.), los “datos personales relativos a la salud, la vida sexual o la orientación sexual” (Ibid.) e incluso los “datos genéticos y datos biométricos tratados con el fin de identificar a una persona” (Ibid.).

Otro punto que le suma una barrera restrictiva a este derecho es que según el derecho de la UE “las personas físicas son las únicas beneficiarias de las normas de protección de datos y únicamente los seres vivos están protegidos por la legislación europea sobre protección de datos (RGPD, 2016, art N° 1). Situación que concuerda con la legislación chilena vigente modificada en 2020 que igualmente reconoce solo a las personas como entes de derecho, ya que señala que “refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual”. (Ley 19.628, 2020, art N° 2), otra aseveración importante en este ámbito es que cuando al fallecer la persona física en Chile, se señala lo siguiente:

> El Consejo ha establecido que una persona fallecida no es titular de datos personales a la luz de lo dispuesto en el artículo 2º, letra ñ) de la LPDP, al no tratarse de una persona natural. Su honra, sin embargo, se proyecta como un derecho propio de sus familiares, toda vez que su memoria constituye una prolongación de dicha personalidad, protegida y asegurada como parte de la honra de la familia (Consejo para la Transparencia, 2011; 10).

Por lo que si se trata un dato personal que contenga una vinculación directa o indirecta a una persona física natural que se encuentre en vida, entonces según tanto en el Derecho de la UE como en el de la CdE, pasaría a denominarse como un "Interesado". Es decir, que la legislación solo "refiere a la protección de las personas físicas en relación con el tratamiento de sus datos personales" (UE, 2018; p.97), aunque las personas jurídicas en los derechos internacionales mencionados al inicio del párrafo se les reconocen igualmente cierta gradualidad de protección, esto debido principalmente a que este tipo jurídico, puede adherirse o defenderse mediante el "El artículo 8 del CEDH comprende el derecho al respeto de la vida privada y familiar y también del domicilio y la correspondencia" (Ibid.)

Sin embargo, a estas definiciones se le suma la crítica de autores especializados en la temática de protección de datos, que hacen hincapié en que los estos, no se limitan a datos que adquiere un ciudadano al nacer en los aspectos determinado territorio, sino actualmente se deben extender a resguardar las interacciones que estas personas físicas realizan mediante sistemas automatizados o digitalizados, ya que según lo leído se señala que:

> Los identificadores únicos de computadores y teléfonos, como también los datos geolocalizados y los biométricos, constituyen datos personales y deben quedar sujetos a protección legal incluso cuando no se encuentran directamente asociados a un nombre propio. Si se busca compartirlos o abrirlos, será necesario definir un protocolo robusto de anonimización o seudonimización para evitar su mal uso o su empleo con fines distintos a los expresados cuando se los recolecto en su primera instancia (Buenadicha et al, 2019; p.13).

Desde la perspectiva de la región Latinoamericana, según la autora Romina Garrido (2013) menciona que existen características particulares al revisar el derecho de protección de datos, ya que se puede observar que "Pese a que los países que muestran un mayor crecimiento normativo en la materia han basado sus normas en el modelo europeo, no es posible desconocer que el desafío de la protección de los datos se presenta con particularidades" (p,5).

El primer desafío se sustenta en el hecho de que no existe una organización de cooperación Latinoamericana con alto poder de instaurar la temática dedicada a estudiar como resguardar este derecho como tal, en tanto el segundo obstáculo se relaciona a la "tardanza con que la tecnología penetra en la región" (Ibid.). Ya que como hemos revisado el auge de la protección de datos personales por la intromisión y amenaza que suponía la automatización de información comenzó en la década de los 70, s en la región de Europa, en la región no fue hasta 1997 que Chile basándose

en la experiencia de la legislación de Gran Bretaña de 1984, decidió reformar la "Ley de Protección de Vida Privada" a "Ley de Protección de Datos Personales". Lo que nos llevaría al tercer problema y que nos habla de que estos desafíos se encuentran interrelacionados, ya que en general en los países latinoamericanos existen casos como el de Chile donde solo existe la ley, pero no un sustento que salvaguarde el derecho de manera adecuada, estos " son Perú, con su Ley N° 29.733, de 2011; la Ley N° 8.968, de 2011, en Costa Rica; y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 2010, en México, por mencionar algunas" (p,8).

Esta tercera problemática mencionada por la autora se sustenta cuando se señala que la Comisión Europea "ha reconocido que Andorra, Argentina, Canadá (organizaciones comerciales comprendidas en el ámbito de aplicación de la *Personal Information and Electronic Documents Act* o PIPEDA), Islas Feroe, Guernesey, Isla de Man, Israel, Jersey, Nueva Zelanda, Suiza y Uruguay garantizan una protección adecuada" (UE, 2018, p.289), es decir, solo dos países de la región cumplen los estándares de la región Europea, entre los cuales no encontramos a Chile.

Es entonces, que se puede hacer un punto de comparación de la panorámica de la región Latinoamérica con la experiencia o conflicto que estuvo presente en el continente europeo en la década pasada, debido a que no se encontraba instalado un documento legal de protección de datos personales, sino varias legislaciones, que podían o no contener las condiciones necesarias que aseguraran una adecuado resguardo a los datos a la hora de su recolección, tratamiento o uso, lo que genero consecuencias en cuanto a permitir un libre tráfico transfronterizo de datos personales en la región.

Además los Estados, al igual que en la actualidad en la región Latinoamericana, no contaban con la existencia de un órgano mediador que brinde y dote de un seguimiento activo al transferir datos de carácter sensible, por lo cual tanto los gobiernos como empresas de carácter privado tendieron a limitar la transferencia de estos, que por su naturaleza deben obedecer a intereses legítimos que no afecten al desarrollo de la democracia de una de las partes, pero que al no tener un estándar son capaces de generar externalidades negativas en el mercado y en las organizaciones de cooperación internacional.

Situación que como revisamos en los antecedentes cambiaría en 2001, cuando el Consejo de Europa (CdE) decidió la necesidad de modernizar el Convenio 108, que vendría a reconocer que, en el mundo globalizado actual, los rápidos avances tecnológicos significan nuevos dilemas para la protección de datos y que la normativa hasta 2001 debe adaptarse, retos que son nuevamente

recuperados por el Parlamento Europeo y el CdE (2016), para fundamentar la necesidad del RGPD, primeramente porque "La tecnología permite que tanto las empresas privadas como las autoridades utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades", en segundo lugar debido a que "Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial" y por qué "La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa".

Por lo que se decidió modificar el acuerdo para que formara parte de él la UE e incluso "se adoptó un Protocolo Adicional al Convenio 108 que introdujo disposiciones sobre los flujos de datos transfronterizos a los Estados no Partes, los denominados terceros países, y sobre la obligatoriedad de crear autoridades nacionales de control de la protección de los datos" (UE, 2020; p.29), además respecto a la circulación de los datos personales se señala que:

> Debe existir libre circulación de datos personales entre las Partes Contratantes del Convenio 108 modernizado. Sin embargo, se puede prohibir la transferencia si «existe un riego real y grave de que la transferencia a otra de las Partes pudiera conducir a evitar las disposiciones de la Convención» o si una de las partes «está obligada a ello por normas armonizadas de protección comunes a los Estados pertenecientes a una organización internacional regional (UE, 2018, p.284).

Otra característica que hace especial al Convenio 108, es que este documento legal, es jurídicamente vinculante, es decir que los Estados miembros del CdE y del Espacio Económico Europeo (EEE), más Uruguay, México y Argentina que son países no europeos invitados por el Comité de ministros del CdE, están obligados o comprometidos a cumplir con las disposiciones rectificadas en el convenio, en las cuales se considera clave:

> El control efectivo del cumplimiento de la normativa de protección de datos por parte de autoridades de control independientes en las Partes Contratantes se considera esencial para la aplicación práctica del Convenio. Con este fin, el Convenio modernizado subraya la necesidad de que se confieran a las autoridades de control competencias y atribuciones efectivas y que gocen de auténtica independencia en el cumplimiento de su misión (UE, 2018; p.30).

Por otro lado, otra problemática vigente se debe a la masificación de datos y datos sensibles en la red es que como pudimos distinguir en el apartado anterior los datos comenzaron a ser procesados por la tecnología alrededor en la década de los 70's, marcando el inició de un intenso debate que hasta el día de hoy no ha encontrado su punto final, este se puede resumir en una pregunta ¿Es el derecho a la protección de los datos personales un derecho fundamental?

Asunto que para la Organización de las Naciones Unidas (ONU), que se define como en "alerta" al significa avanzar en regular el uso de datos personales, es decir, como señala la misma Asamblea General en la resolución N° 68 que se encuentra:

> "Profundamente preocupada por los efectos negativos que pueden tener para el ejercicio y el goce de los derechos humanos la vigilancia y la interceptación de las comunicaciones, incluidas la vigilancia y la interceptación extraterritoriales de las comunicaciones y la recopilación de datos personales" (Asamblea General en Resolución 68/167, 2013; p.2)

Además señala que otras razones que le preocupan son el cómo la rapidez del desarrollo tecnológico "incrementa la capacidad de los gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos (Asamblea General en Resolución 68/167, 2013; p.1), dando entonces los lineamientos que llevan a la infracción y vulneración de un derecho fundamental, sin embargo, este derecho en riesgo potencial para las Naciones Unidas es tratado como materia del Derecho a la Privacidad que se encuentra sus bases en el artículo 12 de la "*Declaración Universal de Derechos Humanos*" y el artículo 17 del *"Pacto Internacional de Derechos Civiles y Políticos*", que esta entidad define como el derecho con el cual se vela porque:

> Nadie debe ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, y el derecho a la protección de la ley contra esas injerencias, y reconociendo que el ejercicio del derecho a la privacidad es importante para materializar el derecho a la libertad de expresión y para abrigar opiniones sin interferencias, y es una de las bases de una sociedad democrática (Asamblea General en Resolución 68/167, 2013; p.1)

En la misma línea, pero con diferencias claves, nos encontraríamos a la Unión Europea (UE), quien en 2018 liberó un documento denominado como *"Manual de legislación europea en materia de protección de datos"* con el cual busca "crear un estado de opinión y mejorar el conocimiento de las normas de protección de datos, especialmente entre los profesionales del derecho no especializados que tienen que abordar las cuestiones de protección de datos en su trabajo" (UE, 2018; p.3), debido a la vasta experiencia tanto de la misma entidad como de los países miembros y sus normativas en esta materia.

Sin embargo el punto de inflexión se encuentra en que esta institución reconoce a el derecho a la protección de datos como un "derecho fundamental distinto del derecho fundamental al respeto de la vida privada" (UE, 2018; p.21), esta aseveración viene dada debido a que según la UE el derecho al respeto de la vida privada consiste en prohibir en menor medida el alcance de lo moral

o de interés general, mientras que la "protección de los datos personales se considera un derecho moderno y activo, que establece un sistema con mecanismos de control para proteger a los ciudadanos cuando sus datos personales sean objeto de tratamiento" (UE, 2018, p.22). Además se señala que "afecta al tratamiento de todo tipo de datos y datos personales, sea cual sea la relación que tenga con la privacidad y sus efectos sobre ella" (UE, 2018, p.22), por lo cual este derecho de los datos puede pasar a llevar el derecho de la privacidad y por lo tanto involucra un mayor alcance que este último.

6 METODOLOGÍA

El diseño de investigación será No Experimental, ya que no se originará, ni se investigará una muestra determinada, sino que se realizará una recolección de información de la realidad en donde no se ha influido, que permita reconocer el fenómeno de la "Protección de Datos", categorizándolas en dimensiones que se utilizaran como insumo para la creación de una matriz comparativa entre la normativa legal ya existente de protección de datos de la Unión Europea y la normativa vigente en Chile. Entre las que destacan el "*Convenio 108"* del Consejo de Europa (CdE), el "*Reglamento general de protección de datos*" (RGPD) de la Unión Europea (UE) y la Ley N° 19.628 sobre "*Protección de la Vida Privada*".

Además la investigación será descriptiva, es decir no se buscará conocer las causas del problema, por el contrario se enfocará en la existencia de cuatro dimensiones que se consideran como desafíos para nuestro país, que considerando el "*Manual de Legislación Europea en Materia de Protección de Datos"* (2018). primeramente distinguiría la presencia de una *"Autoridad de Control Independiente"* en Chile*,* en segundo lugar nos encontraríamos la integración de la figura de *"Delegada o Delegado de Protección de Datos Personales",* en tercer lugar verificaremos el estado de *"Protección de Datos Personales desde el Diseño y por Defecto" y* finalmente revisaremos los *"Registros de Actividades u Operaciones en el Tratamiento de Datos Personales y Mecanismos de Rendición de Cuentas".*

Analizando cada una de estas Dimensiones de manera longitudinal o evolutiva ya que se revisará el objeto de estudio a partir de datos cualitativos y cuantitativos, para reconocer como estos han ido mutando a través del tiempo, hasta llegar a la situación actual.

7 HALLAZGOS

7.1 Autoridad de Control Independiente

Como se logra divisar en la tabla 1, Chile actualmente no es un país adherido al Convenio 108, lo que nos logra dar lineamientos de que este no contiene la capacidad de brindar una protección adecuada a los datos personales con la normativa vigente, considerando además que en la región ya se considera a tres países, es decir, Uruguay, Argentina y México como administraciones que logran regular de manera apropiada este derecho y brindan un elevado nivel de protección.

Tabla 1: Países Latinoamericanos invitados por el CdE a Convenio 108

País	Año de Adhesión a Convenio 108
Uruguay	2013
México	2018
Argentina	2019

Fuente: Elaboración propia a partir de información disponible en Buscar en la base de datos (coe.int) (Junio 2022)

En relación a lo mencionado anteriormente, hemos visto que un primer pilar para poder salvaguardar y garantizar una adecuada protección a los datos personales en Chile que son objeto de recolección, tratamiento y uso tanto por el sector privado como público sería el establecer una autoridad de control independiente, esta medida se encuentra contenida en el Convenio 108, la Directiva 95/46 y el RGDP del continente europeo, acentuando en que estas deben mantener facultades sobre el actuar y decidir “con total independencia en el desempeño de sus funciones y en el ejercicio de sus competencias” (UE, 2018; p.216).

Así mismo se menciona que cuando se integra el concepto de “independencia”, no significa que esta tenga atribuciones, funciones y recursos, sino que va aún más allá, es decir, el concepto de

independencia debe estar presente también en “la autoridad de control y de sus miembros, así como de su personal, frente a influencias externas directas o indirectas es fundamental para garantizar la objetividad plena en la toma de decisiones sobre protección de datos” (ibid.), situación que nos da a conocer que la independencia cubre el nivel estructural, pero también el de procesos y acciones más básicas de los miembros de esta.

Un ejemplo de la importancia de la independencia que debe tener la autoridad a cargo de la protección de los datos se puede encontrar en la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 2010, en donde la Comisión de las Comunidades Europeas (CCE) y el Supervisor Europeo de Protección de Datos (SEPD) acudieron a esta instancia para impugnar una reglamentación que permitía la vigilancia por parte de la administración de la República Federal de Alemania a una autoridades independientes de protección de datos, entonces en la solicitud al TJUE, se puede leer:

> Mediante su recurso, la Comisión de las Comunidades Europeas solicita al Tribunal de Justicia que declare que la República Federal de Alemania ha incumplido las obligaciones que le incumben en virtud del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, p. 31), al someter a la tutela del Estado a las autoridades de control competentes para vigilar en los diferentes Länder el tratamiento de datos personales en el sector no público, y al haber adaptado así incorrectamente su normativa nacional a la exigencia de «total independencia» de las autoridades encargadas de garantizar la protección de estos datos (Tribunal de Justicia de la Unión Europea, 2010, apartado 1)

Respecto a los motivos que configuran a esta situación como problemática y es necesario llegar a estas instancias la CCE y el SEPD, alegan que se debe a que como se ha mencionado, las disparidades en las legislaciones en dimensiones reglamentarias como administrativas sobre protección de datos “pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario” (Tribunal de Justicia de la Unión Europea, 2010, apartado 7), con esto en mente, no cumplir con la independencia en una autoridad de control contribuye a la generación de consecuencias a nivel económico, ya que se atenta con las características que hacen posible la libre competencia entre países con economías ampliamente vinculadas.

Por lo que las autoridades de protección de datos deben ser independientes y ser implementadas de manera equivalente por todos los países miembros para no provocar una limitación del tráfico de los datos personales, situación que seguiremos revisando en el ejemplo de la CCE y el SEPD, quienes basaron su interpelación en lo siguiente:

> La exigencia de que las autoridades de control ejerzan sus funciones con «total independencia» debe interpretarse en el sentido de que dichas autoridades han de estar exentas de toda influencia, tanto si ésta es ejercida por otras autoridades como si es ajena a la Administración. Por ello, la tutela del Estado a la que están sometidas en Alemania las autoridades encargadas de controlar el respeto de la normativa en materia de protección de las personas físicas en lo que respecta al tratamiento de datos personales en el sector no público supone, en su opinión, incumplir dicha exigencia (Tribunal de Justicia de la Unión Europea, 2010, apartado 15)

Aunque la República Federal de Alemania se defendió, señalando que la expresión de total independencia de las autoridades de protección de datos personales es referida a "la independencia funcional de las autoridades de control, en el sentido de que éstas deben ser independientes del sector no público sujeto a su control y no deben estar expuestas a influencias externas" (Tribunal de Justicia de la Unión Europea, 2010, apartado 16), y que las autoridades de control emplazadas en los distintos estados federales con el objetivo de supervisar el tratamiento de datos personales "no constituye tal influencia externa, sino un mecanismo de vigilancia interna de la Administración, que llevan a cabo autoridades incardinadas en la misma estructura administrativa a la que pertenecen las autoridades de control y, como éstas, obligadas a cumplir los objetivos de la Directiva 95/46" (Ibid.)

Sin embargo, estas razones no lograron en resultado esperado, ya que para el TJUE los lineamientos estaban claros, en la legislación jurídicamente vinculante, por lo que el organismo dictaminaría lo siguiente:

> En contra de lo alegado por la República Federal de Alemania, nada indica que la exigencia de independencia se refiera exclusivamente a la relación entre las autoridades de control y los organismos sujetos a su control. Por el contrario, el término «independencia» viene reforzado por el adjetivo «total», lo que implica una facultad de decisión exenta de toda influencia externa a la autoridad de control, ya sea directa o indirecta (Tribunal de Justicia de la Unión Europea, 2010, apartado 19).

Analizando el contexto de nuestro país en esta materia nos encontraremos con que la entidad a cargo de la protección de los datos personales es en la actualidad el denominado" Consejo para la

Transparencia" (CPLT), entidad que por medio de la ley que lo funda, se le encarga la función de "Velar por el adecuado cumplimiento de la ley N° 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado" (Ley 20.285, 2020, art 33; letra m).

Aunque, no similar al caso alemán no se le puede considerar como una unidad de control independiente, a causa de que no contiene las características necesarias, es decir, independencia financiera, de recursos y de personal. Además, funda una encrucijada, que según la visión de autores, se señala que "Ambas leyes son contrapesos de una misma situación. Por una parte, cómo se deben tratar estos datos, los derechos de los titulares y las limitaciones al derecho de acceso cuando la información solicitada contiene datos personales de terceras personas" (Garrido, 2013; 19), es decir que esta entidad tiene como objetivo el cumplimiento de dos leyes con intereses contrapuestos, por un lado el CPLT debe procurar fomentar la transparencia y acceso a los datos personales y por el otro el salvaguardarlos a manera de no exponer datos personales cuando no se encuentren finalidades debidamente fundadas, problemática que es formada cuando no es posible reclamar o expresar que datos personales fueron necesariamente difundidos y cuales no, ya que la entidad encargada, de estas atribuciones es la misma pero respondiendo a dos objetivos estratégicos diferenciados.

Según la Fundación Datos Protegidos (2021), que el Consejo de Transparencia este a cargo de la protección de datos significa una situación "insostenible, especialmente considerando que ello implica ignorar el amplio desarrollo de la protección de datos personales, en particular respecto a los principios de finalidad, proporcionalidad y seguridad", esto debido a que se considera que al no ser una autoridad de control independiente a nivel administrativo estaría siendo influenciada por intereses que responden a necesidades del sector público chileno.

Situación que quedaría en evidencia el día 30 de abril de 2021, ya que la empresa "ATELMO" o "Asociación Chilena de Telefonía Móvil A.G." recurrió al CPLT para que este pueda "emitir pronunciamiento sobre el actuar de la Subsecretaría de Telecomunicaciones del Ministerio de Transporte y Telecomunicaciones (la "SUBTEL" o la "Subsecretaría"; y el "MTT"), en lo que se refiere al tratamiento de datos personales en materia de telecomunicaciones" (Consejo para la Transparencia, 2021; ofi N° 000127).

La cual en ese mismo año comprendía dos acciones que sentaban bases jurídicas peligrosas en la protección de datos personales, la primera de estas considera las "solicitudes que SUBTEL ha estado

efectuando a las empresas de telecomunicaciones del país para que le entreguen datos personales de sus clientes con el objetivo de llevar a cabo la "Encuesta de Satisfacción de Usuarios con los Servicios de Telecomunicaciones" (Ibid.), con las que la entidad "procedería no solo pedir la entrega datos de 15 millones de suscriptores, sino entregarlos a las empresas encuestadoras"(Datos Protegidos; 2021), y la segunda acción comprendería "Las disposiciones sobre tratamiento de datos personales y sensibles que establecen las normas que implementan la Ley N°21.046, que Establece la obligación de una velocidad mínima garantizada de acceso a internet" (Consejo para la Transparencia, 2021; ofi N° 000127), que genero los siguientes argumentos por parte de la asociación demandante:

> SUBTEL realizaría un tratamiento de datos sensibles, sin la habilitación legal expresa requerida. A dicho respecto indicó que el tratamiento solo puede ser realizado en la forma y condiciones que determine la ley, estando sujeto su procesamiento a una reserva legal especial, en circunstancias que la Ley N°21.046 solo le otorga a SUBTEL la atribución de utilizar la información de las mediciones de calidad recopilada por la OTI para la elaboración de informes comparativos, la que solo permitiría que la SUBTEL acceda a la información en términos agregados, y solo respecto a las mediciones de calidad.
>
> Respecto de los principios de finalidad, proporcionalidad, y seguridad, ATELMO señaló, con respecto al primero, que SUBTEL utilizará los datos obtenidos por el OTI para, entre otros fines, la elaboración y publicación de informes comparativos, lo cual es ambiguo y puede llevar a que SUBTEL amplíe la finalidad del tratamiento. En cuanto al principio de proporcionalidad, no se entiende que, si la única facultad otorgada a la SUBTEL es la realización de informes comparativos, esta tenga, a nivel reglamentario acceso en línea y en tiempo real a todos los datos del OTI. Finalmente, respecto del principio de seguridad, ATELMO estima que el Reglamento y la Norma Técnica no establecen los estándares pertinentes de seguridad (Consejo para la Transparencia, 2021, ofi N° 000127, p.3)

Descargos que no lograron interrumpir la planificación de la SUBTEL, ya que finalmente el Consejo de la Transparencia dictamino lo siguiente:

> Se puede concluir que el ejercicio de las competencias y facultades establecidas para SUBTEL, en pleno cumplimiento del mandato de reserva legal establecido en el artículo 19 N°4 de la Constitución Política, conforme lo establecido en la ley, en normas tales como aquellas relativas especialmente a "controlar y supervigilar el funcionamiento de los servicios de telecomunicaciones", "requerir antecedentes e informaciones a las concesionarias que sean necesarios", "proteger los derechos de los usuarios", y "adoptar decisiones de política pública en materia de telecomunicaciones", requiere necesaria e ineludiblemente, en el contexto de la ejecución de las Encuestas de Satisfacción de servicios públicos de telecomunicaciones y para poder contactar a los usuarios para ese fin; del acceso y tratamiento de los datos personales que han sido requeridos a las empresas de telecomunicaciones (Consejo para la Transparencia, 2021, ofi N° 000127, p.19)

Por lo tanto, si necesitamos que una autoridad de control independiente sea efectiva y eficaz en la protección de datos personales, es menester que se le brinden las herramientas necesarias y que estas se encuentren claramente demarcadas en una ley orgánica, ya que estos son los ordenamientos dedicados a proteger los derechos residentes en nuestra Constitución, así mismo, las acciones de los organismos públicos deben recurrir únicamente a atribuciones expresadas en una norma legal, respecto a lo que la UE señala algunas de las competencias básicas que debería considerar una autoridad de control en un país, aunque por temas de extensión solo se distinguirán en la tabla 2 a modo de ejemplificación, estas serían:

Tabla 2: Funciones de una Autoridad de Control de Protección de Datos

Asesorar a los responsables del tratamiento y a los interesados en todas las cuestiones relativas a la protección de datos
Autorizar cláusulas contractuales tipo, normas corporativas vinculantes o acuerdos administrativos
Investigar las operaciones de tratamiento e intervenir en caso necesario
Exigir la presentación de cualquier información pertinente para la supervisión de las actividades del responsable del tratamiento
Sancionar a los responsables del tratamiento con advertencias o apercibimientos y ordenar que se comuniquen a los interesados las violaciones de la seguridad de los datos personales
Ordenar la rectificación, el bloqueo, la supresión o la destrucción de los datos
Imponer una prohibición temporal o definitiva del tratamiento o imponer multas administrativas
Someter los asuntos a los órganos jurisdiccionales

Fuente: elaboración propia a partir de Manual de legislación europea en materia de protección de datos de 2018, paginas 219-220.

7.2 Delegada o Delegado de Protección de Datos

Una segunda dimensión que hace falta en nuestro país es la figura del delegado o delegada de Protección de Datos (DPD) , debido a que según la UE son “la «piedra angular de la responsabilidad proactiva», ya que facilitan el cumplimiento, al tiempo que actúan como intermediarios entre las autoridades de control, los interesados y la organización por la que han sido nombrados” (UE, 2018;

p.197), es decir, son quienes se encargan de brindar orientaciones a instituciones tanto del sector público como privado acerca de cómo cumplir y garantizar una adecuado tratamiento de los datos personales de su "personal, clientes, proveedores o cualquier otra persona (también conocida como sujetos de datos)"(UE;2020), conforme a lo señalado en las normativas de protección de datos personales.

Además, esta figura significa incluir una responsabilidad intrínseca para las entidades que recopilen o procesen datos personales, ya que se reconoce al DPD, como un agente que permite una consistente "rendición de cuentas a los responsables y encargados del tratamiento" (UE, 2018; p.197), porque también se reconoce, que debe existir un sentido de obligatoriedad de esta figura en casos en los cuales sea estrictamente necesario, respecto a este asunto la UE reconoce las siguientes situaciones:

> Cuando el tratamiento lo lleve a cabo una autoridad u organismo público, cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala, o cuando las actividades principales consistan en el tratamiento a gran escala de categorías especiales de datos personales relativos a condenas e infracciones penales (UE, 2018; p.198)

Se debe mencionar, que al analizar el contexto de Chile, se considera necesario que las normativas contemplen exigir que esta figura se encuentre presente tanto en entidades públicas como en empresas privadas que se encarguen del tratamiento o sean responsables de datos de su personal o de sus clientes. Aunque esto significa, que se deben encontrar sentadas las bases para que este cargo contemple un adecuado funcionamiento y monitoreo de las normativas de protección de datos, esto a causa de que este cargo precisa de condiciones que aseguren que este pueda llevar a cabo la función encomendada, respecto a este punto la UE señala lo siguiente:

> Para que los DPD puedan desempeñar sus funciones con eficacia, los responsables y encargados del tratamiento deberán facilitarles los recursos necesarios, incluidos recursos financieros, infraestructuras y equipos. También es obligatorio dar al DPD tiempo suficiente para desempeñar sus funciones y proporcionarle formación continua que le permita incrementar sus conocimientos (UE, 2018; p.199)

El o la DPD debe tener las herramientas suficientes que le permitan brindar lineamientos a la entidad, es decir, que incluso debe "tener la responsabilidad de administrar su propio presupuesto"(UE,2022), para realizar investigaciones respecto al tratamiento de datos y potenciales

irregularidades por lo que además, si hablamos de las entidades se debe proteger a la figura del DPD, debido a que este reconoce como una figura que al igual que una entidad de control no debe presentar influencias de su lugar de trabajo, las condiciones que sugiere la UE son:

> Los responsables y encargados del tratamiento deben garantizar que el DPD no reciba ninguna instrucción de la empresa en lo que respecta al desempeño de sus funciones relacionadas con la protección de datos, ni siquiera de las personas de más alto nivel directivo. Además, no debe ser despedido ni sancionado en modo alguno por desempeñar sus funciones (UE; 2018, 200)

Incluso en las recomendaciones de la UE (2022) se señala que para designar y despedir a un o una DPD se deben tener criterios prescritos objetivos y claros, donde la Autoridad de Control Independiente que es el órgano que le compete la contratación de este, debe velar por el conocimiento tanto en materia de protección de datos como en la institución en la cual se insertara. Otra recomendación relevante es el tiempo que este durara en el cargo, el cual debe extenderse por al menos 3-5 años, con derecho a reelección y la responsabilidad de conservar una cooperación directa y sostenida con la autoridad de control independiente de protección de datos, como lo que coloquialmente llamaríamos una "mano derecha" a lo cual se le atribuyen las siguientes tareas o responsabilidades:

Tabla 3: Responsabilidades de delegado de protección de datos

Garantizar que los responsables del tratamiento y los interesados estén informados sobre sus derechos, obligaciones y responsabilidades en materia de protección de datos y sensibilizar sobre ellos
Asesorar y recomendar a la institución sobre la interpretación o aplicación de las normas de protección de datos
Crear un registro de las operaciones de tratamiento dentro de la entidad y notificar a la ACI las que presenten riesgos específicos
Garantizar el cumplimiento de la protección de datos dentro de su institución y ayudar a esta última a ser responsable a este respecto
Atender consultas o quejas a solicitud de la institución, el controlador, otra(s) persona(s) o por iniciativa propia
Cooperar con la ACI (responder a sus solicitudes sobre investigaciones, tramitación de reclamaciones, inspecciones realizadas por la ACI, etc.)
Llamar la atención de la institución sobre cualquier incumplimiento de las normas de protección de datos aplicables

Fuente: Elaboración Propia a partir información disponible en: https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en (junio, 2022)

En esta área nuestro país este año ha presentado un antecedente debido a la pandemia de COVID-19 para distinguir la importancia que esta figura posee, ya que el 22 de enero de 2022 se publicó la Resolución 22 Ex del Ministerio del Interior y Seguridad Pública, la cual designa a un delegado de protección de datos personales en la División de Carabineros, para cumplir con los lineamientos de las leyes N° 19,628 sobre protección de datos personales y la ley N° 20.285 sobre acceso a la información pública, además de "El oficio Nº 35, de fecha 05.02.2021, del Director General (S) del Consejo para la Transparencia, en que, entre otras materias, solicita designación de delegado de datos personales" (Res N° 22 Ex; 2022).

En donde se resuelve que se designa al "Coronel (J) Heriberto Andrés Navarro Vásquez de dotación de la Contraloría General de Carabineros, como Delegado de Protección de Datos Personales de Carabineros de Chile, en carácter de titular, quien en ejercicio de esta designación dependerá directamente del Contralor General de Carabineros de Chile" (Ibid.). Aunque claro no cumple con ser una figura independiente, por otro lado si posee algunas de las condiciones necesarias para desempeñar de manera óptima sus funciones, estas serían, la coordinación con la autoridad de protección de datos y facilitar el acceso a la información de tratamiento de datos en la entidad, esto se refleja en las siguientes aclaraciones del resuelvo de la resolución ya mencionada:

> Establécese que al Oficial Superior (J) designado por el presente acto, le corresponderá servir de enlace institucional con el Consejo para la Transparencia y con otros órganos y servicios de la Administración Pública en materias propias de la ley Nº 19.628, "Sobre Protección de la Vida Privada"; proponer, coordinar y cautelar el cumplimiento de la Política de protección de datos personales y de privacidad de los mismos, que dicte Carabineros de Chile; informar y asesorar a los responsables y/o encargados del tratamiento de datos y en general, a la totalidad del personal institucional, en materia de protección de datos personales.
>
> Ordénase que el Delegado de Protección de Datos Personales deberá mantener una permanente coordinación con el encargado de ciberseguridad de Carabineros de Chile, sobre la aplicación, implementación y seguimiento de las medidas de seguridad relacionadas con la protección de datos personales; especialmente, en lo que respecta de los encargados de tratamiento de datos, a requerir informes de evaluación sobre la situación de protección y privacidad de los datos, como en la coordinación de las notificaciones relacionadas con brechas de seguridad, tanto con las autoridades competentes y/o titulares de los datos, cuando procediere.
>
> Precísase que todo estamento institucional deberá prestar plena colaboración al Oficial Superior (J) designado como Delegado de Protección de Datos Personales, para el cumplimiento de su cometido, y que toda nueva normativa interna que se refiera a datos personales ha de ajustarse a la Política de protección que se dicte. (Resolución N°22 Ex, 2022)

7.3 Protección de Datos Personales desde el Diseño y por Defecto

Este punto refleja dos aspectos diferenciados, la primera, se trata de del diseño, cuyo enfoque contempla el preparar las condiciones para el surgimiento de una nueva cultura para las entidades que procesan datos y las tecnologías utilizadas para estos propósitos, ya que, al momento de diseñar planes, proyectos, programas o políticas públicas, se considera necesario el adoptar interrogantes tales como, "Do we really need to collect these data? Is there a way to have the same functionality without collecting them?" (EDRi, s.f; p.12). Es decir, que para la European Digital Rights, es de suma importancia que desde el inicio de las acciones del Estado para la provisión de bienes y servicios se razone en torno a como estos pueden beneficiar o perjudicar a la privacidad y protección de datos personales de las y los interesados.

Mientras que la segunda, se refiriere a cómo los datos deben tener una base normativa que considere los principios de los datos personales, además de garantizar que efectivamente las autoridades a cargo de la protección posean los lineamientos para delimitar cuando una entidad ha hecho un tratamiento indebido de los datos de las y los interesados, para así posteriormente determinar un grado de sanción acorde a determinadas acciones, para profundizar este segundo aspecto se señala que:

> Dada la engorrosa y compleja naturaleza técnica de muchas políticas de protección de la privacidad y los datos. La carga no debe recaer en las personas: no debe esperarse que tengan los conocimientos y la experiencia necesarios para comprender la complejidad de los servicios y dispositivos que usan. Siempre que sea posible, deberán gozar del más elevado nivel de protección de forma predeterminada (Privacy Internacional, 2018; 86)

Siendo entonces estos dos aspectos los que podemos entender como los causantes de la existencia de siete principios claves que se encuentran en las legislaciones estándar de protección de datos, tales como el RGDP y el Convenio 108. Estos entonces se reconocen como esenciales o como el "punto de partida de otras disposiciones más detalladas en artículos posteriores del Reglamento" (UE, 2018; p.132), por lo cual es relevante repasar cada uno de estos, conociendo tanto sus características, como su capacidad de responder como una herramienta o marco de referencia, acerca de cómo se debe realizar un adecuado tratamiento de datos personales.

El primero que encontraríamos, es el "*Principio de Licitud, Lealtad y Transparencia*", aunque se reconoce como un principio que para cumplirse considera 3 aspectos, con respecto a la licitud tiene definición en el artículo N°6, del RGDP 2016/ 679, donde se señala como principal aporte señala la necesidad de que el tratamiento de cualquier dato de carácter personal debe tener como condición previa el consentimiento expreso del o la interesada en ya sea para un fin o ya sea varios fines especificados, otras condiciones consideran que para ser licito el tratamiento es que se considere como una condición en la ejecución de un contrato del cual el interesado o interesada es parte, que sea una obligación legal para el responsable del tratamiento, o bien que los poderes públicos le confieran el poder a un responsable de tratamiento orientados por el interés público o intereses legítimos en donde los derechos y libertades de la o el interesado prevalezcan y no sean pasados a llevar.

Respecto a la lealtad, considera la relación que mantiene el responsable del tratamiento con el interesado, respecto a este la UE señala.

> Los responsables del tratamiento deben notificar a los interesados y al público en general que tratarán los datos de manera lícita y transparente y deben ser capaces de demostrar que las operaciones de tratamiento cumplen las disposiciones del RGPD. Las operaciones de tratamiento no deben realizarse en secreto y los interesados deben ser conocedores de los riesgos potenciales. Además, los responsables del tratamiento, en la medida de lo posible, deberán actuar de manera que se cumplan los deseos del interesado sin dilaciones (UE, 2018; p.135)

Mientras que el último aspecto cubre la transparencia, que es definida como los canales y mecanismos por lo cual el encargado del tratamiento de datos debe mantener actualizado al interesado en la manera en que se han utilizado, ya sea que este a la disposición la información o si se realizó una petición para acceder a esta.

Un segundo principio, es el "*Principio de Finalidad*", que busca limitar los usos secundarios de un dato personal, es decir, un uso secundario ocurre cuando un dato recolectado es utilizado para un uso que inicialmente no estaba presupuestado, por lo que involucra que todo tratamiento de datos debe realizarse con un fin único o bien, con fines compatibles con el inicial, es decir que no se puede recolectar un dato que sirva potencialmente en un futuro, pero que no considera una finalidad para la entidad en el momento de recolección.

Entonces las finalidades deben ser expresadas de manera "explícita, especificada y legítima" (UE, 2018; p.140), conforme a que el RGDP, usa un concepto denominado como "compatibilidad de

finalidad", es decir que "Cada nueva finalidad del tratamiento de datos que no sea compatible con la original deberá tener su propio fundamento jurídico y no podrá basarse en el hecho de que los datos fueran inicialmente obtenidos o tratados para otra finalidad legítima" (Ibid.). Sin embargo en el artículo N° 5 del RGDP 2016/ 679 se señala que "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" (letra b).

El tercer principio, es el "*Principio de Minimización de los Datos*", el cual según la UE (2018) supone directa relación con la privacidad, por lo que considera procedimientos en los que se busca "evitar todo uso de datos personales o aplicar medidas que reduzcan la capacidad para atribuir datos a un interesado" (p,143), entre uno de estos procedimientos, se presenta a la "seudonimización", la cual es una herramienta que permite que los datos personales recolectados mantengan un mayor nivel de privacidad.

Un ejemplo de cómo se ve un dato seudonimizado es que el sujeto bky#74 tiene 2 mascotas, un perro y un gato, debido a que el sujeto o persona física no es propiamente reconocible por otra persona sin poseer una "llave" que tendría el responsable del tratamiento de los datos personales, esto en línea con que los datos personales deben ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados" (RGDP/ 679, 2016, articulo N° 5; letra c).

El cuarto, es el *"Principio de Exactitud de los Datos*", que trata acerca de que los datos deben de ser "exactos y, si fuera necesario, actualizados; se adoptarán 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" (RGDP/ 679, 2016, articulo N° 5; letra d), es decir, que los responsables del tratamiento de los datos deben realizar una verificación periódica de los datos y que antes de utilizar información sensible deben disponer de medidas que de la misma forma garanticen "con una certeza razonable, que los datos son exactos y están actualizados" (UE, 2018; p.145), aunque también se considera que existen casos en los que la normativa del país prohíba la actualización de datos particulares, "puesto que la finalidad de dicha conservación es principalmente documentar los acontecimientos, a modo de «instantánea» histórica"(UE, 2018;146).

En quinto lugar encontraríamos al "*Principio de Limitación del Plazo de Conservación*", vinculado a los plazos definidos con respecto a la finalidad de tratamiento de un dato, ya que estos estipulan un cierto periodo en el cual es dato de un interesado para un fin especificado, además de contribuir

directamente a la privacidad de una persona ya que los datos de esta son suprimidos pasado el tiempo, excepto en condiciones especiales de archivo científico , respecto a este principio la UE también señala:

> Deben ser «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». Por lo tanto, los datos deberán ser suprimidos o anonimizados cuando se hayan cumplido dichos fines. Con este fin, «el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica», a fin de asegurarse de que no se conserven los datos durante más tiempo del necesario (UE, 2018; 147)

Un sexto principio, es el "*Principio de Seguridad*", que tiene directa relación con el principio de "principio de minimización de datos" visto anteriormente, ya que este igualmente vela por la privacidad con la que se puede acceder a las personas físicas mediante los datos personales que son tratados, respecto a esta situación el RGPD señala que:

> El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. (RGDP/ 679, 2016; articulo N° 25)

Este principio entonces comprende medios de verificación, los cuales pueden ser "La adhesión a un código de conducta aprobado o a un mecanismo de certificación aprobado" (UE,2018; p.151), otras medidas que se recomiendan son "la conservación de los datos en un entorno físico seguro, la limitación del control de acceso mediante sistemas de inicio de sesión que consten de varios niveles y la protección de la comunicación de los datos con métodos criptográficos robustos" (Ibid.)

El ultimo principio y uno de los más relevantes, es el de "*Responsabilidad Proactiva*", en el cual podemos observar la importancia de las dos dimensiones anteriores, es decir la Autoridad de Control Independiente y el o la delegada de protección de datos, ya que son estos los que deben "aplicar medidas técnicas y organizativas adecuadas" (UE, 2018; p.153). Observando de este modo que según el artículo 5° del RGDP se encargan de hacer efectivos los demás principios, es decir, que como se ha dicho anteriormente registran el rendimiento de cuentas de como se ha realizado el tratamiento de datos, lo que nos lleva a una característica esencial de este principio, que no

considera al responsable del tratamiento de los datos, sino directamente a las entidades del sector público.

Sin embargo cuando revisamos la normativa vigente en Chile, nos encontramos con que la situación de los 7 principios que recomendados por la experiencia europea se encuentra en un estado bastante variado, es decir, existen múltiples amparos para algunos principios, pero otros ni siquiera están integrados, lo cual se revisara a modo de resumen en la siguiente tabla 4:

Tabla 4: Principios de los Datos y Ley 19.628 sobre "Protección de la Vida Privada"

Principios	Apariciones en Ley N° 19.628 sobre "Protección de la Vida Privada"	Artículos de Ley N° 19.628 sobre "Protección de la Vida Privada"
Principio de Finalidad	9	3, 4, 5, 9, 10, 17, 20, 22, 24
Principio de Limitación de Plazo de Conservación	3	6,18,19
Principio de Exactitud de los datos	3	2, 6, 12
Principio de Licitud, Lealtad y Transparencia	3	3, 4, 10
Principio de Seguridad de los Datos	2	7, 11
Principio de Minimización de Datos	1	2
Principio de Responsabilidad Proactiva	0	

Fuente: Elaboración propia a partir de información disponible en: http://bcn.cl/31r0j

Para la realización de la tabla se ha realizado una revisión exhaustiva, en donde se tomó en cuenta como lo descrito en la normativa chilena se relacionaba a las características propias revisadas de cada uno de los principios.

El principio de finalidad apareció 9 veces, sin embargo esto se produce de una forma desagregada en la legislación, es decir, el articulo N°3 trata acerca de la finalidad de los datos recolectados en

encuestas, estudios de mercado o sondeos de opinión pública, mientras que en el artículo N° 4 se encuentran las finalidades de los datos de fuentes accesibles al público, mientras que el articulo N°5, 9, 10, 17, 20 regulan los usos secundarios de los datos personales, el articulo N° 22 responde a la institución que vele por un registro de responsables de tratamiento de datos y la finalidad, mientras que el articulo N° 24 trata acerca del caso específico de datos en recetas médicas, análisis y exámenes de laboratorio, pero aun así este principio es que contiene una mejor presencia y se acerca a los estándares del RGPD, ya que se observa explicitud en las finalidades expresadas y el criterio de compatibilidad de finalidades con cada fundamento jurídico correspondiente.

Mientras que el principio de plazo de limitación del plazo conservación, se puede observar 3 veces y responde a tendencias observadas en los antecedentes de la investigación, ya que las versiones modificadas de la ley, buscaban proteger a distintos sectores de la población que al principio no se consideró de manera tal, concretamente en los articulo N° 6 y 19 que se encargan de señalar que los datos en conservación de datos de personas en situación de morosidad deben ser eliminados una vez que se pierda el fundamento legal, mientras que el articulo N° fija un plazo de 5 años en deudores de servicios básicos como luz, agua, gas y teléfono.

El Principio de exactitud de los datos, aparece 3 veces presente en el documento legal, a pesar de que en todos los artículos se relate el cómo el dato no debe tener características erróneas, inexactas, equívocas o incompletas, la realidad es que la modificación o eliminación debe ser exigida por la persona natural afectada, además que no plantea a los responsables el hacer una verificación periódica o asegurarse si los datos que poseen están propiamente actualizados, situación que deja en evidencia un sentido de poco compromiso en las instituciones públicas en la exigencia de este principio como tal.

Si seguimos revisando el principio de licitud, lealtad y transparencia también aparece 3 veces en la ley, se consideró a los artículos N° 3 y 10, aunque el primero haya sido revisado anteriormente en la finalidad, ya que considera el consentimiento para comenzar los procesos de recolección de datos, mientras que el articulo N° 4, mantiene la misma relación. Sin embargo este artículo denota una perspectiva desactualizada de cómo proteger este principio ya que comprende a responsables de datos que consigan una autorización por escrito del titular de manera informada, lo cual no considera propiamente a plataformas digitales, en las cuales observa que los términos y condiciones no son fácilmente compresibles y estos se aceptan más bien como personalidades jurídicas con fines propios, lo cual se puede considerar ambiguo.

El principio de seguridad de los datos solo conserva dos apariciones, que tienen la capacidad de atribuir responsabilidades de cuidado a responsables de tratamiento de datos personales, pero no considera mecanismos por los cuales corroborar que esto suceda en la realidad y tampoco considera

orientaciones en los cuales se busque proteger a la persona identificable en los bancos, bases y registros de datos, características clave de este principio según la UE.

Mientras que ligado al punto anterior el principio de minimización de datos solo se puede encontrar solo una vez, en el artículo N° 2 en la letra e, respecto al tratamiento de datos estadísticos, lo cual no logra dar la debida protección considerando los usos potenciales de los datos personales. A pesar de esto tiene más presencia que uno de los principios más importantes de la UE, el de responsabilidad proactiva que se considera el pilar para los principios anteriores, situación esperada debido a que Chile no tiene presencia de una autoridad de control independiente de protección de datos o a la figura de delegado en la misma materia.

7.4 Registros de Actividades u Operaciones en el Tratamiento de Datos Personales y Mecanismos de Rendición de Cuentas

En esta última dimensión, se debe aclarar que se integra considerando el contexto nacional de Chile y las recomendaciones de la UE en torno a la protección en el tratamiento de datos personales, entre los que se encontraríamos el principio de la responsabilidad proactiva, principio de seguridad y el principio de lealtad, licitud y transparencia de los datos personales, que para funcionar de manera apropiada requieren de la integración de una autoridad de control independiente y a él o la delegada de protección de datos. Sin embargo, la sustancia del actuar de estos agentes no se encuentra en su mera existencia, sino que se encuentra en la capacidad de llevar a cabo mecanismos de rendición de cuentas, por lo cual es necesario comprender diversos métodos y acciones que se deben llevar a cabo en determinadas situaciones, entre las que se encuentran:

El Registro de actividades y tratamiento de datos personales, como concepto surge para “demostrar el cumplimiento y rendir cuentas” (UE, 2018; p.201), en materia de protección de datos personales ya que las empresas que sean responsables de estos procesos, ya sea en el sector privado o en el público deberían conservar una obligación legal en la que se documente y registre las actividades, es decir, obedece a la lógica de ¿cómo sabemos que un dato ya ha sido usado para una finalidad, si no se tienen los métodos para corroborarlo?. Por lo tanto se podría decir que para UE al tratar un dato personal, estaríamos haciendo uso de un recurso institucional y los recursos normalmente son controlados y protegidos en su uso, ya que esto refleja la responsabilidad que existe en la institución con estos, se generan auditorias, inspecciones y fiscalizaciones que tienen como “objeto garantizar

que, en caso de necesidad, las autoridades de control dispongan de la documentación necesaria para poder confirmar la licitud del tratamiento" (Ibid.)

En nuestro país este criterio no se encuentra amparado en la normativa vigente, sin embargo la información que deben o deberían presentar los responsables que tengan una cantidad igual o mayor a 250 empleados en los registros de tratamientos u operaciones sobre datos personales según la UE se observan en la tabla N° 5:

Tabla 5: Información contenida por un registro de actividades de tratamiento de datos personales

Nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable y del DPD
Los fines del tratamiento
Descripción de las categorías de interesados y de las categorías de datos personales objeto de tratamiento
Información sobre las categorías de destinatarios a quienes se comunicaron o se comunicarán los datos personales
Información sobre si se han realizado o se realizarán transferencias de datos personales a terceros países u organizaciones internacionales
Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos personales, así como una descripción general de las medidas técnicas adoptadas para garantizar la seguridad del tratamiento

Fuente elaboración propia a partir de información de Manual de legislación europea en materia de protección de datos (2018).

Otro mecanismo importante para procesos de rendición de cuenta es la Evaluación de Impacto, la cual se debe realizar antes de cada tratamiento y responde ante la aparición tanto de nuevas tecnologías, como de las capacidades crecientes que estas tienen para entablar diversas actividades y resultados con los datos personales que son tratados, debido a que la UE considera que mientras más grande sea la cantidad de datos que se trate, también se motivara a mayores riegos en la naturaleza y ámbito de tratamiento de los datos previamente consentidos por parte de los interesados.

Según la UE los responsables de tratamiento deben "identificar, gestionar y mitigar adecuadamente los riesgos de antemano, limitando notablemente la posibilidad de que el tratamiento tenga efectos negativos para los interesados" (UE, 2018;p.203), hechos que la entidad materializa en el RGPD

2016/679 en su artículo N° 35 que establece que una evaluación de impacto se debe aplicar cuando "sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas" (apartado N° 1), además en el mismo artículo se señala que esta evaluación será necesaria en los siguientes casos contenidos en la tabla N° 6

Tabla 6: Situaciones particulares en donde es necesaria la Evaluación de Impacto relativa a la protección de datos

Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar
Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10
Observación sistemática a gran escala de una zona de acceso público

Fuente: elaboración propia basado en información del apartado N° 3 del artículo 35 del RGPD 2016/679

Una tercera herramienta para la UE respecto a los responsables de tratamientos de datos personales son los códigos de Conducta, los cuales se comprenden como mecanismos especializados para los variados sectores industriales, tecnológicos, gubernamentales o de servicios, en los que la UE remarca que:

> Para los responsables y encargados del tratamiento, la creación de estos códigos puede mejorar en gran medida el cumplimiento y reforzar la aplicación de las normas de protección de datos de la UE. Los conocimientos especializados de los miembros del sector favorecerán que se encuentren soluciones que resulten prácticas y, por tanto, probablemente se apliquen. Reconociendo la importancia de estos códigos para la aplicación efectiva de la normativa de protección de datos (UE, 2018; p.205)

Es decir, que se puede observar a estos como una cooperación entre la figura del delegado de protección de datos personales y los sectores productivos, debido a que se busca reconocer como

proteger a los datos personales de un modo más particular, en donde se tome en cuenta la experiencia de las cadenas productivas vinculadas a la "recopilación de datos personales, la información que se ha de facilitar a los interesados y al público y el ejercicio de los derechos de los interesados" (Ibid.), siguiendo los términos del RGPD en torno a los principios que se deben proteger en los datos personales, además que la UE señala que las ventajas de implementar este tipo de códigos son:

> Directrices detalladas que adaptan los requisitos legales a sectores concretos y favorecen la transparencia de las actividades de tratamiento. Los responsables y encargados del tratamiento también pueden utilizar la adhesión a estos códigos como prueba palpable de que cumplen la normativa de la UE y como forma de reforzar su imagen pública en tanto que organizaciones que priorizan y se comprometen con la protección de datos en sus operaciones. Los códigos de conducta aprobados, junto con compromisos vinculantes y exigibles, pueden utilizarse como garantías adecuadas para la transferencia de datos a terceros países (UE, 2018; p.206)

Por último tendríamos a las certificaciones, las cuales se comprender como un medio adicional en el cual los responsables de tratamiento de datos personales pueden demostrar el cumplimiento a las normativas vigentes sobre protección de la materia. Estos se materializarían en *"Mecanismos de Certificación y Sellos y Marcas de Protección de Datos"* (UE, 2018; p.207), que son diseñados y emitidos por la autoridad de control independiente, en donde los responsables y encargados de tratamiento de datos personales podrán optar por participar en adherirse a las certificaciones existentes, entre los cuales se determinara si cumplen o no con la normativa, situación que será dictada por el delegado de protección de datos, este responde a una lógica de voluntariedad y cooperación, similar al caso revisado en los párrafos anteriores, sin embargo la UE remarca que "el hecho de que el responsable o encargado del tratamiento posea una certificación de este tipo no reduce sus obligaciones y responsabilidades de cumplimiento de todos los requisitos del Reglamento" (Ibid.).

8 PRINCIPALES RESULTADOS

A modo de resumen, en los puntos anteriores se analizaron a profundidad cuatro dimensiones con el objetivo de establecer una comparativa entre la normativa estándar de la Unión Europea en contraste con la situación de protección de datos personales de la legislación actual chilena,

resultando en que estas dimensiones tienen competencias interdependientes, que no se pueden considerar como excluyentes una de la otra, sino al contrario, mientras más dimensiones se encuentren sustentadas en sus respectivos fundamentos legales, mayor será la capacidad de los mecanismos para rendir cuentas y resguardo de datos personales en el país, además de que se observara un aumento en la eficacia y eficiencia de entidades y agentes que busquen proteger el derecho de protección de datos personales y vida privada de las personas.

De esta manera entonces se considera que la existencia de una "*Autoridad de Control Independiente*" es de suma importancia, sin embargo su creación debe velar por un carácter independiente a nivel de estructura, procesos, recursos e incluso de su personal a modo de evitar que existan influencias externas o intereses representados por la entidad. Ya que como consecuencia de esta esta se permite la existencia de la figura de "*Delegado o Delegada de protección de Datos*" y a la vez que son estos actores en conjunto quienes se encargan de hacer cumplir la normativas de protección de datos, mediante la "*Protección de Datos Personales desde el Diseño y por Defecto*", en donde se encuentran residentes siete principios.

Entre los cuales el "*Principio de Finalidad*", se destaca como el que tiene mayor presencia en la legislación actual en Chile, sin embargo en la misma línea existen tres principios con relativa presencia, entre los cuales se encuentran el *"Principio de Limitación de Plazo de Conservación", "Principio de Exactitud de los Datos" y el "Principio de Licitud, Lealtad y Transparencia",* en razón a que solo conservan 3 apariciones a lo largo de la "Ley N° 19.628 sobre Vida Privada", mientras que los tres principios restantes, que son el "Principio de Seguridad de los Datos", "Principio de Minimización de Datos" y el "Principio de Responsabilidad Proactiva", contienen una baja presencia, al solo aparecer de dos a ninguna vez, donde el caso más preocupante es la "responsabilidad proactiva", ya que se considera como el pilar para los procesos de rendición de cuentas y ejercicio o defensa del derecho de protección de datos personales.

Mientras que en la dimensión denominada como "Registros de Actividades u Operaciones en el Tratamiento de Datos Personales y Mecanismos de Rendición de Cuentas", se revisó que existen mecanismos adicionales fomentan e incrementan los niveles de protección en los países de la Unión Europea. Donde se destaca las ventajas que contiene poseer integrado el registro de actividades de tratamiento de datos personales, ya que permiten al Delegado de Protección de Datos ejercer las competencias de las obligaciones legales tanto en sector público como privado, mediante la documentación y registro de actividades de tratamiento de datos personales.

La "*Evaluación de Impacto"* se considera otro medio, que tiene su aplicación antes de cada tratamiento con el objetivo de tener claridad, conocimiento y herramientas para controlar eventuales riesgos o consecuencias negativas que conserven determinados tratamientos para los interesados. Por último en este apartado analizamos a los "*Códigos de Conducta*" y *"Mecanismos de Certificación y Sellos y Marcas de Protección de Datos",* los cuales sirven como un espacio de intermediación positiva que reconoce los esfuerzos de los sectores que son responsables de tratar datos.

Todo lo mencionado anteriormente se expresa a modo de resumen en la tabla N° 7 , donde las dimensiones se configuran en 3 niveles de protección, en las cuales inicialmente encontraríamos al "*Nivel de Protección Alto*" que considera que se cumplan todas las características de la categoría en la normativa vigente del país, le seguiría el "Nivel de Protección Regular", donde aunque encontraríamos características de la categoría, aunque no las suficientes para proteger de adecuada manera a los datos personales, por último, en el tercer puesto encontraríamos al "Nivel de Protección Bajo", que comprende que las características de la categoría no se encontrarían recogidas en el texto legal vigente del país, se pueden observar de la siguiente manera:

Tabla 7: Comparación de Normativas de protección de datos entre Chile y la UE

	Niveles de Protección de los Datos Personales					
Dimensiones de Análisis	Unión Europea			República de Chile		
	Nivel de Protección Bajo	Nivel de Protección Regular	Nivel de Protección Alto	Nivel de Protección Bajo	Nivel de Protección Regular	Nivel de Protección Alto
Autoridad de Control Independiente			X	X		
Delegado de Protección de datos			X	X		
Protección de datos personales desde el Diseño y Defecto			X		x	
Registro de Actividades de Tratamiento			X	x		

Fuente: Elaboración Propia.

9 REFLEXIÓN

Para concluir, en la actualidad nos encontramos en un mundo cada vez más interconectado gracias a los procesos de globalización, donde las tecnologías de la información han tomado un papel muy importante en posicionarse, como herramientas que intervienen parte de la vida cotidiana de las personas, gracias tanto a las plataformas digitales o redes sociales, como también por dispositivos que con el tiempo han ido mejorando su capacidad de recopilar información de su uso.

Sin embargo esta relación entre la tecnología y la información plantea un reto para las administraciones del sector público, caso en el cual la Unión Europea se encuentra a la vanguardia gracias a esfuerzos en donde la Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, que mediante el RGPD se plantearon el promulgar una medida que permitiera tanto el fortalecer el derecho de protección de la vida privada y datos personales, considerado como emergente en las últimas décadas, pero que ya ha sido considerado como fundamental para las personas en la era digital, como también el generar las condiciones apropiadas orientadas a facilitar actividades económicas que sean responsables y coherentes en todos los países que sean considerados en calidad de firmantes como para rectificar.

Se considera entonces de suma importancia, el adaptar la Ley N° 19.628 sobre protección de la vida privada a los estándares internacionales, no solo para evitar problemas en la transmisión de datos personales en el mercado, sino también como un compromiso para resguardar los derechos que los ciudadanos tienen y que deben ser protegidos ahora incluso en el mundo digital.

Las administraciones no pueden quedarse en la presunción de que los ciudadanos ejercerán control de sus datos, sin una base normativa en la cual ampararse. Por lo que respondiendo a la pregunta de esta investigación los desafíos que se vinculan al tratamiento de datos personales para el sector público en Chile en la era digital, estaría en primer lugar el actualizar la normativa vigente para reconocer la alta relevancia que contiene el integrar tanto autoridades independientes que ejerzan competencias de responsabilidad proactiva, como mecanismos de registros de actividades de tratamiento y uso de datos, que a manera de herramientas para la toma de decisión, hacen posible determinar los grados de cumplimiento de las normativas. Son los agentes especializados y entendidos en el tema, quienes se deberían interponerse como un recurso de protección entre los responsables de tratamiento de datos y la ley, no los ciudadanos, los cuales muchas veces no disponen ni del tiempo, ni son conscientes de las problemáticas existentes en la materia.

Por lo que según la metodología seguida en la investigación se realizó una comparativa desde dos puntos, primero una revisión de la normativa europea y como se lograba brindar un elevado nivel de protección de datos personales en la Unión Europea, luego se realizó una exhaustiva revisión de la normativa chilena, como resultado se pudo comparar las dos normativas vigentes y determinar que los desafíos para Chile se pueden dividir en cuatro dimensiones debidamente delimitadas.

La primera es la creación de una "autoridad de control independiente" y la segunda es relacionado al cargo de "delegada o delegado de protección de datos personales", como entes institucionales que sirven como una "primera piedra" de lo que se conformaría como un sistema de protección de datos en el sector público, estos a su vez requieren de condiciones para su existencia, una se refiere a que se les debe reconocer como independientes en áreas como los recursos, infraestructura, información e incluso de personal.

Pero a su vez en tercer lugar se deben poseer límites claros definidos en una ley que considere aspectos claves por diseño y por defecto, incluso se señala de que estas entidades, con el tiempo deben tener como cuarto y ultimo objetivo de mediano plazo el poder integrar de manera armónica un registro de actividades de tratamiento de datos personales a responsables de datos personales, es decir, el sector público a modo de ejemplo, pero también el sector privado en donde las empresas superen o iguales la cifra de 250 empleados.

Ya que como hemos revisado en este trabajo los datos personales incluyen áreas bastante ampliadas, no solo son los datos personales el nombre, fecha de nacimiento, número verificador o información de contacto, sino también lo son las creencias, opiniones políticas, datos biométricos o genéticos, localización, orientación sexual e incluso actividades laborales, etc. Debido a la existencia de todas estas aristas es que se considera importante el adaptar la normativa vigente en Chile como manera proteger en la actualidad a la democracia y a los ciudadanos en todos los ámbitos de su vida personal.

10 REFERENCIAS

"Resolución 22 Exenta." Ley Chile. Santiago, Chile. 22 de enero de 2022. recuperado de: http://bcn.cl/2w8jo

"Resolución 68/167". Naciones Unidas, 21 de Enero 2014. Recuperado de A/RES/68/167 (undocs.org)

2018. (UE). "Manual de legislación europea en materia de protección de datos". junio 18, 2022, de Z-Library Sitio web: https://cl1lib.org/book/5436260/192caf

Cantuarias, E. (1993). *"Proyecto de Ley sobre Protección Civil de la Vida Privada".* marzo 26, 2022, de Biblioteca del Congreso Nacional de Chile Sitio web: https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/6814/

Comisión Europea. (2021). "*La protección de datos en la UE*". marzo 22, 2021, de Unión Europea Sitio web: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es

Consejo para la Transparencia (2021). "*Oficio N° 000127 sobre pronunciamiento a requerimiento de la Asociación Chilena de Telefonía Móvil A.G., sobre adecuación al ordenamiento jurídico de solicitud y tratamiento de datos personales efectuado por la Subsecretaría de Telecomunicaciones del Ministerio de Transporte y Telecomunicaciones".* Santiago, Chile. Recuperado de: Oficio.-Acoge-parcialmente-solicitud.pdf (consejotransparencia.cl)

Cunill N. (2009). "*La Modernización de la Gestión Pública en Chile y su impacto en el Proceso de la Descentralización*". Abril 21,2022, de FLACSO Sitio web: https://www2.congreso.gob.pe/sicr/cendocbib/con3_uibd.nsf/8F79160F42E2F0880525786A006616F6/$FILE/moder_gestion_publi_chile.pdf

Datos Protegidos. (2021). "*Contra el tratamiento abusivo y desleal de nuestra información personal: Sociedad civil por una autoridad autónoma de protección de datos personales en Chile*". mayo 10, 2021, de Datos Protegidos Sitio web: https://datosprotegidos.org/contra-el-tratamiento-abusivo-y-desleal-de-nuestra-informacion-personal-sociedad-civil-por-una-autoridad-autonoma-de-proteccion-de-datos-personales-en-chile/

Dirección Jurídica del Consejo para la Transparencia. (2011). "*Protección de Datos Personales*". Mayo 20, 2022, de Consejo para la Transparencia Sitio web: https://www.consejotransparencia.cl/wp-content/uploads/estudios/2018/01/proteccion_de_datos_web.pdf

Domínguez Álvarez, J. L. (2021). "*Inteligencia Artificial, derecho administrativo y protección de datos personales. Entre la dignidad de la persona y la eficacia administrativa*". *IUS ET SCIENTIA*, *7*(1), 304–326. https://doi.org/10.12795/IETSCIENTIA.2021.i01.16

EDRi. (s.f). "An Introduction to Data Protection". Junio 10, 2022, de European Digital Rights Sitio web: https://www.edri.org/files/paper06_datap.pdf

European Data Protection Supervisor. (2022). *"Data Protection Officer (DPO)".* mayo 10, 2022, de Unión Europea Sitio web: https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

Garrido, R. (2013). "*El Habeas data y la ley de protección de datos en Chile*". Mayo 20, 2022, de Escuela de Bibliotecología Sitio web: https://sitios.vtte.utem.cl/seriebibliotecologia/wp-content/uploads/sites/11/2018/05/Serie-N%C2%B0-83-Junio-2013El-Habeas-data-y-la-ley-de-proteccio%CC%81n-de-datos-en-Chile.pdf

Kelly. G, Melgan. G, Muers. S. (2000). *"Creating Public Value"*. Abril 22, 2022, de Academia.edu Sitio web: https://www.academia.edu/23693003/Creating_Public_Value_An_analytical_framework_for_public_service_reform

Ley N° 19.628. Ley Chile, Santiago, Chile, 26 de Agosto de 2020. Recuperado de http://bcn.cl/2m4rr

Ley N° 19.628. Ley Chile, Santiago, Chile, 28 de agosto de 1999. Recuperado de http://bcn.cl/2z64p

Ley N° 19.812. BCN, Santiago, Chile, 13 de Junio 2002. Recuperado de http://bcn.cl/2z64s

Ley N° 20.285. Ley Chile, Santiago, Chile, 1 de Marzo de 2020. Recuperado de http://bcn.cl/2lswp

Ley N° 20.463. Ley Chile, Santiago, Chile, 25 de Octubre de 2010. Recuperado de http://bcn.cl/32dtj

Ley N° 20.521.BCN, Santiago, Chile, 23 de Julio 2011. Recuperado de http://bcn.cl/2z64f

Ley N° 20.575. BCN, Santiago, Chile, 17 de Febrero 2012. Recuperado de http://bcn.cl/2z64l

Ley N° 21.214. BCN, Santiago, Chile, 28 de Febrero 2020. Recuperado de http://bcn.cl/2izxv

Lions, M. (1994). "*Obra jurídica*". México: Instituto de Investigaciones Jurídicas de la UNAM.

Naciones Unidas. (2015). "*Declaración Universal de los Derechos Humanos (DUDH)"*. Bélgica: Naciones Unidas.

Parlamento Alemán. (1970). *"Datenschutzgesetz. Gesetz- und Verordnungsblatt*", 625-628. Recuperado de http://starweb.hessen.de/cache/GVBL/1970/00041.pdf

Parlamento Europeo y Consejo de la Unión Europea (2016), "*Reglamento General de Protección de Datos 2016/ 679"*. Unión Europea. Recuperado de: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Privacy Internacional. (2018). "*Las Claves para Mejorar la Protección de Datos*". mayo 12, 2022, de Privacy Internacional Sitio web: https://privacyinternational.org/sites/default/files/2018-11/Gui%CC%81a%20de%20Proteccio%CC%81n%20de%20Datos%20Personales_web.pdf

Real Academia Española. (2022). "*Definición de Dato".* mayo 23, 2022, de RAE Sitio web: https://dle.rae.es/dato

Sánchez, E. (20 de noviembre de 2007). "*LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TIC) DESDE UNA PERSPECTIVA SOCIAL".* Revista Electrónica Educare, Vol. XII, Extraordinario, ISSN:1409-42-58, 2008, 151-162. Recuperado de: https://www.redalyc.org/pdf/1941/194114584020.pdf

Tribunal de Justicia Europeo. (2010). "Sentencia del Tribunal de Justicia (Gran Sala)". mayo 10, 2022, de InfoCuria Jurisprudencia Sitio web: https://curia.europa.eu/juris/document/document.jsf?docid=79752&text=&dir=&doclang=ES&part=1&occ=first&mode=DOC&pageIndex=0&cid=5084208