FACULTAD DE GOBIERNO
UNIVERSIDAD DE CHILE

AGENCIA DE PROTECCIÓN DE DATOS PERSONALES
Oportunidades y desafíos respecto a las recomendaciones OCDE

AFE para optar al grado de Magíster en Gobierno y Gerencia Pública

CATALINA JAVIERA PINTO IRIBARREN

Profesor Guía:

PAULINA VERGARA SAAVEDRA

Santiago de Chile, año 2024

Resumen

Esta investigación examina la Agencia de Protección de Datos Personales en Chile propuesta dentro del Proyecto de ley que busca regular la protección y tratamiento de los datos personales, y se estudió conforme los principios que resguardan la información privada de la OCDE. Lo anterior, a través de un enfoque cualitativo, comparando la normativa propuesta, las recomendaciones internacionales y el testimonio de expertas, expertos y actores claves de la materia, se obtuvo un panorama amplio y detallado de la situación actual de la protección de datos en Chile y su propuesta de mejora.

Dentro de los hallazgos se observan oportunidades claras para la puesta en marcha de esta nueva institución, pero también se revelan desafíos importantes para cumplir con los principios internacionales y lograr una legislación capaz de adaptarse a la rápida evolución tecnológica. Este documento propone cuatro recomendaciones para la implementación de la Agencia y su proyecto de ley, incluyendo la autonomía, la adaptabilidad, la educación y concientización y la comunicación efectiva. Estas medidas ayudaran a la Agencia de Protección de Datos para ser eficiente, ya que es vital contar con una autoridad de control para para salvaguardar los derechos digitales en el contexto chileno.

Abstract

This investigation examines the Agency for Personal Data Protection in Chile proposed in the bill that seeks to regulate the protection and treatment of personal data, which was investigated in accordance with the OECD's principles that protect private information. This was carried out using a qualitative approach, comparing the proposed regulation with international recommendations and the testimony of experts and key actors in the field. A detailed overview of the current situation of data protection in Chile was obtained, along with a proposal for improvements.

Among the findings, clear opportunities were observed for the implementation of this new institution; however, important challenges were also revealed in order to comply with international principles and achieve legislation capable of adapting to rapid technological evolution.

This paper proposes four recommendations for the implementation of the Agency and its draft legislation, including autonomy, adaptability, education and awareness, and effective communication. These measures will help the Agency for Personal Data Protection to be effective, as it is vital to have an institutionality that safeguards digital rights in the Chilean context.

Palabras claves

Datos personales – Privacidad – Protección – Datos – Información – Institucionalidad – Autoridad de Control

FACULTAD DE GOBIERNO
UNIVERSIDAD DE CHILE

Tabla de contenido

Tabla de Abreviaturas

Abreviatura	Significado
AAIP	Agencia de Acceso a la Información Pública de Argentina
AFE	Actividad Formativa Equivalente
AG	Asamblea General de las Naciones Unidas
APDP	Agencia de Protección de Datos Personales de Chile
BCN	Biblioteca del Congreso Nacional de Chile
CDEP	Comité de Política de Economía Digital
CEPAL	Comisión Económica para América Latina y el Caribe
CPLT	Consejo para la Transparencia
DDHH	Derechos Humanos
DUDH	Declaración Universal de los Derechos Humanos
GPEN	Red Global de Aplicación de la Privacidad de la OCDE
HRC	Comité de Derechos Humanos de la ONU
ICO	Information Commissioner's Office de Reino Unido
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de datos Personales de México
MVM	Modelo de Vertientes Múltiples de Kingdon
OCDE	Organización para la Cooperación y el Desarrollo Económico
OEA	Organización de los Estados Americanos
OIM	Organización Internacional para la Migración
OIT	Organización Internacional del Trabajo
ONG	Organización No Gubernamental
ONU	Organización de las Naciones Unidas
RGPD	Reglamento General de Protección de Datos de la UE
RM	Región Metropolitana
SEGPRES	Secretaría General de la Presidencia
SEREMI	Secretaria Regional Ministerial
SERNAC	Servicio Nacional del Consumidor
UE	Unión Europea

Introducción

Una vez decretado el confinamiento en marzo del año 2020, a causa de la pandemia mundial desatada por el virus SARS-Cov-2, el uso de aplicaciones aumentó de 18 a 22 horas semanales (Montes, 2020). Así mismo, otro análisis realizado evidenció que a junio del 2020 aumentó en un 45% el tráfico de datos de red fija a comparación de marzo de ese mismo año, pasando de 27.080.374 a 39.368.413 GB, además de visibilizar que entre marzo y mayo del primer año de pandemia hubo un aumento del 122,5% en el tráfico de internet a comparación del mismo periodo en el año 2019 (Mundo en Línea, 2020).

La compañía de telecomunicaciones nacional ENTEL realizó el mismo análisis durante 2021 y 2022 identificando que al terminar el primer año de pandemia se utilizaron 996.205.229 GB de datos a nivel nacional, mientras durante el segundo año la cifra aumentó en un 23% llegando a 1.332.398.841 GB (Entel, 2022). Lo anterior, se explica bajo la situación sanitaria que se extendió lo suficiente para obligar a gran parte de los habitantes de Chile, como del mundo entero, a reformar su modalidad de estudio, trabajo y/o recreación, entre otras actividades, y llevarla al mundo digital, aumentando considerablemente el uso del internet y aparatos electrónicos, con el objetivo de continuar con una nueva cotidianidad, la cual se vivió tras pantallas.

Con tal aumento de tráfico de datos, se produjeron distintos delitos cibernéticos que constituyeron un peligro para las instituciones públicas y privadas, además de a la ciudadanía. El primero que causó bastante revuelo fue el ataque al cual se enfrentó el Banco Estado, siendo la entidad bancaria que alberga el dinero de la mayoría de los chilenos, en donde gracias a delincuentes infiltrados en la página web de la institución se bloqueó el acceso de los empleados a sus sistemas de trabajo, provocando una detención en la jornada laboral y la atención al público (Fossa y Solís, 2020).

Aunque esta situación no tuvo mayores consecuencias, lo relevante de este caso, es que logró visibilizar otras situaciones alarmantes que desde el 2018 vienen afectando a distintos usuarios, como la clonación de tarjetas, phishing (suplantación de identidad), robo de información personal, estafas, entre otras. Una de las más preocupantes fue el hackeo a la aplicación móvil del Banco Estado, situación que durante junio del 2020 dejó a varios usuarios sin poder realizar transacciones, movimientos e incluso a muchos les desapareció su dinero por horas, imposibilitándolos de hacer uso de este. Aun así, las autoridades del banco decidieron bajarle el perfil a esta situación para calmar a sus beneficiarios, siendo que en paralelo a estas declaraciones se llevaron a cabo las querellas pertinentes para comenzar con las investigaciones y llegar a los responsables (Fossa y Solís, 2020).

Durante octubre del año 2019 Gobierno Digital, plataforma dependiente de la Secretaría General de la Presidencia (Segpres), se vio afectada por el robo de una base de datos asociada al sistema de Claves Únicas, en donde se cree que se obtuvieron la totalidad de contraseñas con las cuales miles de chilenos, chilenas y residentes en Chile, gestionan múltiples trámites con información delicada. Aun así, no se confirmó desde las autoridades cuáles fueron las consecuencias de esta filtración, ni las diligencias realizadas para llegar a los responsables, mucho menos se indicaron las medidas que se tomarían para mejorar los sistemas de seguridad. La única acción que se identificó por parte del Gobierno, fue el envío de una circular en donde se recomendaba modificar la clave para evitar posibles filtraciones, dejando la responsabilidad en manos de cada usuario (Núñez, 2020).

Como último caso a mencionar, en noviembre del 2020 el conglomerado internacional Cencosud sufrió un secuestro virtual afectando a sus sucursales en Argentina, Brasil, Colombia, Perú y Chile, este ataque cibernético se vio materializado en pérdidas millonarias para la empresa, pero también en la filtración de nombres, números de documentos, números telefónicos, direcciones y más datos personales de los usuarios de estas tiendas. Esta situación se torna más grave aún, al momento en que las autoridades de esta compañía negaron la veracidad de este ataque, aludiendo a que era una “fake news” más, afirmación que se

desmoronó tras investigaciones en los distintos países afectados, y en donde el periódico online "El Desconcierto" logró llegar a la base de datos filtrada comprobando de primera fuente que dentro de ese archivo había información de chilenos y chilenas (Datos Protegidos, 2020).

Lo relevante de estos casos es que todos tienen en común la nula respuesta por parte de los dirigentes, de las distintas empresas e instituciones afectadas, con respecto a la advertencia hacia sus usuarios y/o clientes sobre las consecuencias que estas filtraciones podrían tener directa e indirectamente en ellos. Lo anterior, entendiendo que la información no es algo material que pueda ser recuperado, ya que estos datos pueden ser copiados, divulgados y/o difundidos por canales que muchas veces son desconocidos para la población en general, lo cual aumenta si esto es por un medio intangible como lo es internet. Pero a su vez, tampoco desde la población se exige un cuidado mayor por sus propios datos, demostrando la ignorancia de las personas frente al valor de su información personal.

El Servicio Nacional del Consumidor (SERNAC) en el año 2022, en el marco del día Internacional de la Protección de Datos Personales, lanzó los resultados de una encuesta realizada con el objetivo de *"identificar el conocimiento, los cuidados y el interés que tienen los consumidores respecto al tratamiento de sus datos personales en los sitios webs"* (SERNAC, 2022), encuesta que evidenció que aunque el 72% de los encuestados reconoce estar muy o extremadamente preocupados de que sus datos sean recopilados en internet, pero solo el 4,1% declara que siempre lee las políticas de privacidad de las páginas webs que visita, lo que solo confirma el fenómeno que los expertos han determinado como la "paradoja de la privacidad", que tal y como lo describe esta entidad, explica el fenómeno de que los individuos son conscientes y están preocupados por su privacidad, pero que también están dispuestos a entregar información a cambio de alguna recompensa (SERNAC, 2022).

Recompensa que muchas veces no tiene un retorno que equipare el valor de los datos entregados, pero que el alto nivel de desconocimiento de la población en general provoca que

estos pongan a libre disposición información que para empresas, organizaciones y/o asociaciones son útiles y aprovechan a su conveniencia.

Es por esto que se vuelve relevante estudiar la realidad chilena respecto a la protección de datos personales, sobre todo considerando que el proyecto de ley que busca regularizar está problemática, se encuentra dentro de una de sus últimas etapas de discusión y se han logrado consensos luego de 7 años en el Congreso. Como también es importante considerar que a nivel mundial, muchos países ya cuentan con una concientización importante frente al tratamiento de esta información y como proteger a los usuarios, y como también existen compromisos internacionales en esta materia que se encuentran pendientes por parte de Chile.

Marco Teórico y revisión de la literatura

Lindblom, dentro de su texto "El proceso de elaboración de políticas públicas", nos señala que hay dos cuestiones que sobresalen dentro de la política gubernamental, las cuáles se centran principalmente en la eficacia de la solución de problemas y en el nivel de respuesta del "control popular", respecto al primer concepto hace referencia de cómo se enfrenta un gobierno frente a los problemas de la nación, si lo hace de forma consciente utilizando las distintas ciencias sociales, si se acompaña de expertos, o si dentro de este mismo debaten o cuestionan las políticas públicas existentes e implementadas, agregando que aun así, si se cumpliera lo anterior, siguen existiendo problemáticas que al parecer no cuentan con una solución definitiva. En cuanto al control popular, lo menciona haciendo énfasis en cómo las personas participan, o no, en la formulación de las políticas públicas. Si es suficiente que haya una mayor participación popular dentro del gobierno, y si realmente influyen los ciudadanos o solo inciden las elites, como también si las elecciones son definitorias dentro de este proceso, pero también si fuera así, porque dentro de una sociedad democrática se siguen tolerando ciertas problemáticas (Lindblom, 1991).

El proceso de creación de una política pública es relevante para poder analizar una propuesta, por lo que lo que plantea Lindblom, nos sitúa en cómo hay dos claras influencias para comenzar la resolución de problemas en el ámbito público, en donde también nos propone que existen fases dentro de este proceso, en específico nombra lo propuesto por Harold Lass-wel en 1962, quien considera siete pasos dentro de la creación de una política pública; Información, Recomendación, Prescripción, Invocación, Aplicación, Valoración y Término (Lindblom, 1991).

Por su parte Charles O. Jones, descompone el proceso de forma secuencial en cinco fases; las cuáles comienzan con la identificación del problema, el cual demanda una solución y se encuentra dentro de la agenda de alguna autoridad pública, continua con la formulación de las soluciones, en donde se analizan y formulan las posibles respuestas, con el objetivo de conseguir el respaldo de una autoridad pública que pueda tomar la decisión y convertir la propuesta en una política legitima, luego se espera la ejecución del programa, en donde se ejecuta la propuesta en terreno, para terminar con la acción, a través de una evaluación de los resultados que se obtuvieron de la política (Jones, 1970).

Dentro de la corriente definida como de las políticas o la policy, se plantea las múltiples y distintas alternativas y/o mecanismos de acción que la autoridad política pueden considerar apropiada para resolver el problema que aqueja al grupo social. Aquí, es relevante la influencia de los emprendedores sobre actores decisores de las políticas, pues los primeros transforman la definición del problema para que sea acorde a los valores y creencias de los formuladores de políticas (Zahariadis, 2007) y que, en consecuencia, estos últimos decidan la alternativa más cercana a sus valores y de los emprendedores.

Otra corriente, específicamente la del problema, del modelo de vertientes múltiples (MVM) planteada por Kingdon (Domínguez, 2009) explica que existen problemas que logran ser captados por la autoridad competente o los tomadores de decisión para que se formulen y analicen posibles soluciones. Esto a través de cuatro formas: en que las indicadores actuales

demuestran un problema existente y que debe atenderse; la conclusión de nuevos estudios sobre el fenómeno del problema; la retroalimentación de programas o políticas que demuestran alguna otra falla que pueda ser atendida o, la ocurrencia de algún evento o crisis que ponga en la palestra pública algún problema. Kingdon hace énfasis en la diferencia entre las condiciones y los problemas, en esta línea el autor establece que las condiciones pueden llegar a ser problemas y como también pueden tener una mejor chance de llegar a la agenda, en la medida que las personas crean que deba hacerse algo para cambiar esa condición (Kingdon, 1995)

Es así como explican los distintos autores, la solución de problemas y a su vez la creación de políticas públicas que buscan resolver obstáculos que nacen con la identificación, reconocimiento y/o definición de una falencia presente en la sociedad, la cual puede tomar relevancia de distintas maneras pero que de alguna u otra forma se posiciona con el objetivo de tener una respuesta que posibilite la mejora a esta dificultad.

La privacidad

Una dificultad que se discute hace siglos es la separación de los espacios públicos sobre los espacios privados, reconociendo que al hablar de espacios no se trata solo de territorio, sí no más bien de la dicotomía público-privada que define Bobbio (1985), pero que observaremos a través de lo descrito por Nora Rabotnikof en su texto "El Espacio Público: Caracterizaciones teóricas y expectativas políticas" (1997) que enfrenta distintas perspectivas sobre lo que es público y lo que es privado. La autora parte señalando que la disputa entre estos dos conceptos inicia en el área jurídica, pero que finalmente se extiende a lo económico, a lo moral y a lo político. A su vez, identifica como desde la edad media, varios autores consideraban que tanto el derecho público, como el derecho privado compartían espacios, dentro de la prestación de deberes militares, los pactos de enfeudamiento y la tributación.

Por su parte, Norberto Bobbio (1985) reconoce como esta dicotomía se subordina una con la otra, ya que la definición del interés público determina y se contrapone a la del interés privado, y ocurre lo mismo al revés. Este autor también considera como estos espacios limitan el del otro, indicando que *"la esfera pública llega hasta donde comienza la esfera privada y viceversa"* (p. 13), lo que nos permite inferir que aunque estos espacios conviven, deben mantener sus límites definidos para respectar sus intereses.

Así y todo, Rabotnikof aclara como desde el origen de esta controversia existieron tres grandes sentidos asociados a esta dicotomía, los cuáles fueron enfrentados a sus opuestos para explicar este debate. En primer lugar se contrapuso lo colectivo frente a lo individual, y se reconoció, desde la época de la polis griega, como las cuestiones comunes se resolvían a plena luz del día y frente a todos, legitimándose como un espacio abierto al pueblo, el cual prohibía que una vez resuelto los asuntos comunes, estos no podían ser modificados de forma individual por pactos entre privados. En segundo lugar, se enfrentó lo abierto contra lo cerrado, y se expuso la existencia de espacios de uso común, libres y abiertos (como lo puede ser un mercado o una plaza), pero también la existencia de lugares cerrados y limitados (como una casa), a su vez se agregó como el feudalismo y el patrimonialismo se reconocen como una de las etapas de la privatización del poder público, en donde un espacio público (y abierto) pasa a ser propiedad de uno, o unos pocos, y estos pueden limitar su acceso (o cerrarlo). Y, en tercer lugar, se contrasta lo visible frente lo oculto o secreto, y lo ejemplifica en el medievo, en donde la máxima era que las resoluciones jurídicas debían ser conocidas por todos, pero que también existían límites, y ciertos temas se consideraban confidenciales, (Rabotnikof, 1997).

El desarrollo de las sociedades más modernas y la aparición del mercado, mantuvieron esta dicotomía, pero se fueron desarrollando aún más sus diferencias y lo público se terminó asociando con el ejercicio del poder colectivo-coactivo y al servicio estatal, como a todo lo que tiene que ver con el interés general, mientras que por su parte, lo privado se identificó con lo económico, lo moral y lo religioso, pasando a ser el espacio de los intereses personales

y la propia conciencia (Rabotnikof, 1997). Sobre este último concepto, Thomas Hobbes (1640) asocia a la conciencia como la opinión privada, y se establece una separación entre lo interno y lo externo, considerando que de forma personal cada quien decide que mantiene en lo profundo y que enseña a la superficie.

Siglos más tarde de lo establecido por Hobbes, Samuel D. Warren y Louis D. Brandeis, toman el concepto de privacidad dentro de su texto "The right to privacy" (1890) para hacer un llamado a la protección de la información personal a consecuencia de la intromisión de la prensa en la vida privada de las personas (Warren y Brandeis, 1890), a su vez y dentro de este texto utilizan la frase "the right to be let alone", que en español podría ser traducida como "el derecho a ser dejado en paz", concepto que Sparkes enlaza con lo planteado por Thomas M Cooley, quien más que considerarlo como una definición de privacidad, lo estudia como una característica o principio del derecho que esperan se reconozca en relación a la privacidad, ya que aunque la intromisión a esta misma no cause un daño físico, sí puede generar un perjuicio psicológico directo, es por esto que Cooley, al igual que Warren y Brandeis, lo consideran como una responsabilidad superior, a nivel legal, del cual deben hacerse cargo las autoridades (Sparkes, 1981).

Por su parte Jonathan López-Torres, incluye, sobre la frase "the right to be let alone", la relación que los autores hacen con el "derecho a la privacidad", ya que aclaran que sin una adecuada protección a este último derecho, no se puede asegurar el derecho al disfrute de la vida ni a la inmunidad (López-Torres, 2014), lo que los hace aclarar que dentro de los cambios que se van presenciando en la sociedad, se deben ir reconociendo nuevos derechos, dentro de los cuáles se debería considerar el derecho a la privacidad y el derecho a la protección de la información personal (Warren y Brandeis, 1890). Lo anterior lo refuerza Carlos Romeo, quien usando el termino intimidad como sinónimo de privacidad, lo considera como una necesidad insoslayable, que apoyándose en la famosa frase nombrada al inicio de este párrafo, debe considerarse ya como un derecho inherente de las personas y por ende un derecho fundamental, ya que transciende al ejercicio de otros derechos públicos o privados (Romeo, 1994a).

Uno de los primeros documentos, a nivel internacional, en dar luces de la protección al derecho a la privacidad es la Declaración Universal de los Derechos Humanos (DUDH), aunque lo hace de manera indirecta la Asamblea General de las Naciones Unidas (AG) establece en el artículo 12 (1948) 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.

Con el pasar de los años, distintas organizaciones de corte internacional, comenzaron a incluir indicios, que más allá de solo proteger la privacidad, se iban acercando a lo que hoy conocemos como la protección de los datos personales. Dentro del texto "Antecedentes internacionales en materia de privacidad y protección de datos personales" de Jonathan López-Torres (2014), se crea una breve línea de tiempo del avance en la protección de este derecho a nivel internacional, la cual parte con la Declaración Universal de Derechos Humanos de la ONU, y continua en el mismo año con la Declaración Americana de los Derechos y Deberes del Hombre de la Organización de Estados Americanos (OEA), en donde es su artículo quinto se establece la protección a la honra, la reputación personal y la vida privada y familiar (Organización de los Estados Americanos [OEA], 1948). Luego en 1950 se aprueba el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, también conocido como "Convenio Europeo de Derechos Humanos", el cual proclama el derecho al respeto a la vida privada y familiar, indicando que esto incluye su domicilio y correspondencia, a su vez agrega que las autoridades públicas no podrán entrometerse en el ejercicio de este derecho a menos que sea necesario para la protección de la seguridad nacional o pública, o para *"el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la mora, o la protección de los derechos y las libertades de los demás"* (European Court of Human Rights, 1950, p. 11).

López-Torres continua nombrando como en el año 1966 se adopta el Pacto Internacional de Derechos Civiles y Políticos por parte de la AG en donde en su artículo 17, casi de forma exacta repite lo estipulado en el artículo 12 de la Declaración Universal de Derechos Humanos, potenciando la idea de la protección a la vida privada y a la protección legal en contra la injerencia sobre ella por parte de terceros, y en 1969 la OEA aprueba la Convención Americana de Derechos Humanas, en donde bajo el mismo espíritu de los anteriores artículos nombrados, se invita a proteger la honra y la dignidad, incluyendo que dentro de la vida privada de las personas nadie debería entrometerse de forma arbitraria y a su vez también reconocen el derecho a la protección legal contra los ataques a las injerencias dentro de la vida privada (OEA, 1969).

Es así como desde estos primeros indicios sobre la protección a la privacidad se han evidenciado nuevas necesidades humanas, nuevas amenazas y distintas formas de agresión a las libertades personales, dando como resultado nuevos desafíos sobre la protección de los derechos humanos. A pesar de lo anterior, y tal como lo señala Antonio-Enrique Pérez Luño, no significa que las primeras declaraciones protectoras de este tópico dejen de ser útiles, sí no que es una señal para *"ampliar y actualizar su contenido"* (p. 154), entendiendo que estas declaraciones tienen un componente histórico y evolutivo, el cual según el autor ha determinado la aparición de sucesivas "generaciones" de derechos, y en específico reconoce tres; la primera, la cual protegió a los derechos de defensa, que resguardan las libertades de los individuos (la autoeliminación y la imposibilidad de la intromisión de los poderes públicos en la esfera privada), la segunda, que asegura los derechos de participación, que atañen a los derechos económicos, sociales y culturales (que necesitan una política pública activa de los poderes del estado) y la tercera, que es la que actualmente se está engendrando, la considera como una respuesta a la degradación que están sufriendo las dos primeras generaciones de derechos por la "contaminación de las libertades" en consecuencia al uso masivo de las nuevas tecnologías (Pérez, 1992).

Con respecto al reconocimiento de las tres generaciones de derechos humanos, Conde Ortiz coincide con lo planteado por Pérez Luño sobre la primera generación de DDHH, pero agrega sobre la segunda, la cual asegura la protección a los derechos económicos, sociales y culturales, que también en esta se produjo un encuentro entre el estado social de derechos y estado liberal de derechos, y sin dejar de lado, adscribe que la tercera generación es también la generación de la libertad informática, al cual considera como un nuevo derecho del ser humano, que debe ser protegido y garantizado respecto a la información personal y a su procesamiento en los bancos de datos (Conde, 2005).

Antonio-Enrique Pérez Luño sintetiza sus palabras indicando que el entendimiento general de los derechos humanos es reconocer que siempre evolucionaran y aparecerán nuevas necesidades en el marco de una sociedad democrática y libre. El autor también se refiere al aspecto utópico con el cual son plasmados los derechos humanos y sus sistemas de protección, pero como estos se anclan en verdades historias de libertad, proyectos emancipatorios y en como sí no fuera por estas experiencias, la historia perdería sus propios atributos de humanidad. Es por esto que propone que estos derechos deben ser plasmados y reconocidos por el marco jurídico nacional e internacional (Pérez, 1992).

Datos Personales

En relación al último concepto mencionado por Concepción Conde Ortiz, es importante definir que son los datos y como llegamos a tener bancos de datos. Thomas H. Davenport y Lawrence Prusak define a los datos como un conjunto de hechos discretos y objetivos sobre eventos, pero que estos por sí solos no dicen nada, ni sobre su propia importancia o relevancia, que sólo son capaces de describir una parte de lo sucedido, pero sin ningún juicio o interpretación. Aun así estos autores los consideran como la materia prima para la toma de decisiones, siendo un conjunto de datos bien estructurados un indicio de lo que se podría hacer y también porque son la materia prima para la creación de información, que a diferencia del dato, si tiene un significado, propósito y/o relevancia, ya que esta organizada de cierta

forma, que permite la entrega de un mensaje específico e intencionado, el cual depende directamente de quien la organice y con qué objetivo (Davenport y Prusak, 1998).

A la anterior definición se suman los autores del artículo "Follow the rainbow: a knowledge framework for new product introduction", los cuales describen el desarrollo de un marco de gestión del conocimiento para la introducción de nuevos productos, en donde nos indican que los datos son hechos objetivos, discretos y sin contexto, los cuales están codificados y describen y/o cuantifican eventos. Y por otro lado, la información es el conjunto de datos con una relevancia específica, que se le puede otorgar un contexto que la organice, como también se puede categorizar con un propósito particular (Herder et al, 2003).

Davenport y Prusak, nombran cinco formas de transformar o agregar valor a los datos para que estos entreguen cierta información; (1) Contextualizándolos, permitiéndoles conocer el propósito con el cual se recopilaron ciertos datos, (2) Categorizándolos, identificando las unidades de análisis de los componentes principales de los datos, (3) Calculándolos, considerando si estos fueron analizados de manera matemática o estadística, (4) Corrigiéndolos, eliminando los errores dentro del conjunto de datos, y (5) Condensándolos, al reunir y resumir los datos (Davenport y Prusak, 1998).

Lo anterior es apoyado por la visión planteada por Ganesh D. Bhatt, quien considera que la relación entre dato e información depende directamente del nivel de organización e interpretación, y describe esta relación ejemplificándola con una visita médica, en donde el doctor obtiene muchos datos del paciente, de los cuales solo algunos le servirán para poder interpretar qué enfermedad tiene, o identificar si necesita más información para dar un mejor diagnóstico (Bhatt, 2001), ya que también dentro de la visita recibe información que no será utilizada para identificar la dolencia, como es el nombre del paciente o su número de nacional de identificación.

Muchos autores muestran preocupación por los flujos de información que se pueden generar, los cuáles al almacenar altos niveles de información pasan a ser llamados bancos de datos y

aunque traen un progreso creciente y veloz para el desarrollo en diferentes áreas, también generan una gran amenaza, ya que al igual como plantearon Davenport y Prusak (1998), cuando la información se clasifica y ordena permite la entrega de un mensaje especifico y puede llegar a convertirse en *"una especie de Frankenstein en nuestro perjuicio"* (p. 111), Juan Antonio Travieso utiliza esta última frase para expresar una de sus principales preocupaciones en su texto "Protección de Datos Personales y Tecnología, en busca del paraíso", la cual es la falta de conocimiento de las personas que usan internet sobre la vigilancia a la que se encuentran expuestos, y como son las mismas personas las cuáles ponen a disposición su información personal, permitiendo que se trace un casi perfecto perfil de los usuarios, en donde es posible observar preferencias, creencias e intereses de todo tipo (Travieso, 2016).

Es por esto que Pérez Luño, recuerda que muchas veces se habla de una "sociedad de la información", en donde el ejercicio de los derechos humanos se desenvuelve en una cultura informática, que junto al desarrollo tecnológico han conllevado a la digitalización de múltiples actividades que, aunque facilitan, economizan y aceleran tramites, muchas veces se vuelven un proceso completamente informatizado que trabaja con datos fiscales y personales, a través del *"control electrónico de los documentos de identificación"* (Pérez, 1992, p. 155), provocando nuevos fenómenos de ataque a las libertades y derechos humanos, el autor lo ejemplifica con el registro que se genera a través de la compra de productos por medio del uso de tarjetas de crédito y la reserva online de viajes que indica los sitios por visitar, pero también en la actualidad, se pueden agregar ejemplos como; la descarga de ciertas aplicaciones que registran información de geolocalización, o aquellos programas que utilizan la biometría y podrían llegar a generar bases de datos con características físicas de sus usuarios, como también una situación mucho más cotidiana que es la revisión de distintos sitios webs, los cuáles a través de las cookies[1] pueden realizar un seguimiento de sus visitantes y sus las actividades dentro de su plataforma.

[1] Las cookies son datos que se guardan en el computador del usuario, lo anterior según Juan Lujan Mora, Doctor Ingeniero en Informática y Catedrático del Depto. de Lenguajes y Sistemas Informáticos de la Universidad de Alicante, se definen como *"un conjunto de datos que un navegador web almacena de forma automática en el computador de un usuario cuando visita una página web"* (2011).

Es así como los avances tecnológicos han permitido la captación y transmisión de información, muchas veces por el desconocimiento de los usuarios, pero también por el valor que han adquirido principalmente los datos personales, los cuáles se reconocen por contener información ligada a una persona física, a su intimidad y a su vida privada, tal y como lo señala Andoni Polo Roca (2021) y agrega como merecen una "especial protección", ya que es información que puede identificar o señalar a una persona en específico, como su nombre, su domicilio, su número de identificación personal, su correo electrónico, su número telefónico, como también pueden ser datos de carácter sensible, de los cuáles Concepción Conde Ortiz (2005) identifica a; la ideología, la afiliación sindical, la religión, las creencias, la salud, la vida sexual, y todo lo relativo a infracciones penales y administrativas. La divulgación, sin autorización o sin consentimiento informado, de los anteriores datos personales, sensibles o no, pone en peligro el entorno personal, social y profesional de las personas afectadas.

Sumado a lo anteriormente expuesto, distintas instituciones han sabido beneficiarse de la circulación de datos, y muchas veces de los datos personales de sus propios usuarios, como también de los posibles futuros usuarios, y ya los consideran parte de su inventario y como un instrumento imprescindible e indispensable dentro de sus procesos (Romeo, 1994b). Usufructúan esta información para tener una ventaja comparativa, sin considerar los daños, directos e indirectos, que pueden provocar en los dueños de los datos, ya que en el contexto de un mundo desarrollado, para Flavio Quezada (2012) quienes tienen el conocimiento e información, también tendrán el poder para recolectar, almacenar, unir y transmitir todo tipo de datos, podrán manejarlos, transformarlos y entregarles un valor agregado sí es que ese es su fin.

Davenport y Lawrence (1998) identificaron cuatro formas de transformar los datos para conseguir cierta información, lo que refuerza el poder que pueden a llegar a tener los datos, pero también como sí caen en las manos de entidades que cuentan con recursos para poder influenciar e incidir en la sociedad y su comportamiento adquiere un poder aún más

importante, ya que pueden llegar a concentrar tecnologías que ponen en peligro ciertas libertades de las personas, por lo que se propone establecer, a nivel constitucional, un límite (Quezada, 2012).

A los peligros identificados respecto al tráfico de datos e información, y como estos muchas veces contienen información privada, es que los espacios cibernéticos en los cuáles se mueven las grandes masas de datos son contextos muchas veces difusos, dinámicos y expansivos, en donde además de que las personas comparten información, se pierde el límite de la esfera pública y la privada (Romeo, 1994a), pero también se puede agregar que dentro de estos mismos espacios digitales, los usuarios muchas veces se ven obligados a romper este límite de su esfera privada para poder ser parte del mundo online, el cual te induce a entregar cierta información para poder navegar, acceder a ciertas plataformas o simplemente tener contacto con el resto de internautas.

Identificados solo algunos riesgos a los cuáles se ven expuestos los datos y la información que circula por distintos medios, en 1988 el Comité de los Derechos Humanos (HRC) de las Naciones Unidas hace referencia a la recopilación y registro de información personal en aparatos electrónicos y a la creación de bancos de datos. Se pronuncia por medio de su observación general N°16 hacia el Pacto Internacional de Derechos Civiles y Políticos, dentro de la cual exhorta a los estados miembros a reglamentar la recolección y uso de los datos personales, tanto por parte de entidades privadas y públicas. Dentro de este documento manifiesta distintas medidas que deberían ser aplicadas para proteger la información personal, más que nada refiriéndose a la vida privada, de las personas, con el objetivo de que esta información no llegue a ser utilizada sin previo consentimiento, y que esta solo sea manipulada bajo conocimiento de a quién pertenece. Específicamente invita a normar la recepción, la elaboración, el uso y los fines con los cuáles se manejan los datos personales, también establece el derecho de cada persona a verificar que datos se tienen almacenados y con qué fin los tienen guardados, quienes los tienen y el porqué, y a su vez contar con el derecho de solicitar que estos se eliminen y corrijan de ser necesario (Comité de los Derechos Humanos de las Naciones Unidas [HRC], 1988) .

Lo anterior es reconocido por López-Torres (2014) como el establecimiento de los derechos básicos que tienen todos sobre el tratamiento de su información personal y nombra el término del "derecho a la autodeterminación informativa" y que define como el derecho de cada persona a disponer sobre su información personal como le parezca correcto, teniendo en su poder la decisión de que compartir y que no. A este término también se refiere Concepción Conde Ortiz en su texto "La protección de datos personales" (2005), pero él lo sitúa en la realidad europea y como los distintos tratados y recomendaciones de organizaciones internacionales lograron formar en la ciudadanía la "conciencia europea sobre protección de datos", que finalmente habla sobre como la propiedad del dato personal esta totalmente arraigada al titular de esta información, y solo este *"tiene derecho a decidir quién, dónde, cuándo y cómo los presenta al exterior"* (Conde, 2005, p. 52).

En 1990, la Asamblea General de las Naciones Unidas aprueba los "Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales" siendo uno de los primeros antecedentes en materia de protección de datos personales y son las organizaciones gubernamentales, intergubernamentales y las no gubernamentales quienes finalmente aplican y observan estos principios dentro de sus respectivas competencias (López-Torres, 2014).

La reglamentación sobre los ficheros computarizados de datos personales incluyen el (1) principio de la licitud y lealtad en la recolección y almacenamiento de los datos, (2) el principio de exactitud, que busca mantener íntegros los datos recopilados para que sean verídicos, (3) el principio de finalidad, que establece el porqué del almacenamiento de aquel dato, (4) el principio de acceso de la persona interesada, que entrega el poder al dueño de los datos de corroborar la información que se tiene de él, (5) el principio a la no discriminación, que evita la segregación en el registro de los datos, (6) la facultad de establecer excepciones, que permitan resguardar la seguridad de los dueños de los datos, (7) el principio de seguridad que protege los almacenamientos de los datos, (8) el principio de control y sanciones, que a través de la designación de una autoridad, debe controlar el cumplimiento del resto de principios, (9) el principio de flujo de datos a través de las fronteras, cuando se traspasa

información entre estados y (10) el principio del campo de aplicación, que indica que todos los principios antes mencionados deben aplicarse en todos los ficheros que contienen datos, ya sean públicos o privados (Asamblea General de las Naciones Unidas [AG], 1990).

Otra entidad que ha tenido un papel importante frente a la protección de la información personal en el contexto internacional es la Organización para la Cooperación y el Desarrollo Económico (OCDE), quienes con objetivos e ideas ligadas al área comercial, han visto sus intereses sobrepuestos respecto a la utilización, cambio y administración de la información personal, principalmente dentro del comercio electrónico, medio por el cual y situándonos en la sociedad de la información en la cual vivimos, es utilizado de forma cotidiana, no siendo la única transacción en donde las personas entregan sus datos, ya que también existen los gobiernos electrónicos y tramites digitales, por solo nombrar algunas de las plataformas que permiten realizar trámites de forma online y más expedita, pero que generan un registro de datos personales, los cuáles se deben manejar resguardando la protección de los derechos humanos, considerando que aun así, no se debe dejar de potenciar el uso de las nuevas tecnologías y el derecho al desarrollo (López-Torres, 2014).

Es así como en 1980 la OCDE aprueba las "Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales" las cuáles buscaban homologar las normas en relación a esta temática entre los países miembros a través de la propuesta de estándares mínimos de protección de privacidad y sus libertades respecto a los datos personales, y a su vez potenciar la consideración de los intereses entre los estados para evitar las interferencias en los traspasos de datos (Organización para la Cooperación y el Desarrollo Económico [OCDE], 2013). Las anteriores orientaciones, fueron pensadas tanto en el área pública como en la privada, ya que principalmente buscaron resguardar la privacidad y las libertades individuales, y permitieron observar desde otra perspectiva al uso de los datos personales, no solo como un problema, sí no más bien como una oportunidad, pero que requería de una regulación para reglamentar su uso (López-Torres, 2014).

No fue hasta el 2007 que la OCDE público su siguiente documento sobre esta materia titulado "Recomendaciones del Consejo sobre cooperación transfronteriza en la aplicación de las leyes que protegen la privacidad", las cuáles con el objetivo de seguir con la mejora en la protección de la privacidad, incentivaba a la cooperación internacional entre autoridades responsables de la protección a la privacidad, como también a la colaboración interna de cada país entre autoridades que cubrieran materias a fin, como las legales. Y fue así como en 2011, a raíz del lanzamiento de la Red Global de Aplicación de la Privacidad (GPEN por sus siglas en ingles) en 2010, se lanza un Informe sobre la implementación de las recomendaciones de 2007, como un insumo para potenciar el anterior documento, y a su vez se pública un texto sobre el escenario actual de la privacidad y su evolución a 30 años del lanzamiento de las primeras directrices de la OCDE (OCDE, 2013).

Ya en 2013 se aprueba una nueva versión de las directrices que mandatan la "Protección de la Privacidad y los Flujos Transfronterizos de los Datos Personales" y un suplemento explicativo, siendo estos dos textos una actualización del documento publicado en 1980, con el objetivo de promover y facilitar los flujos transfronterizos de los datos personales, los tiempos, el estado de derecho y el resguardo a la privacidad como también a los derechos humanos relacionados y sus libertades (OCDE, 2013). Siendo su última manifestación formal sobre esta temática la "Declaración Sobre el Acceso de los Gobiernos a los Datos Personales en Poder de Entidades del Sector Privado", la cual se publicó en 2023 con el propósito de complementar los anteriores documentos a través de un acuerdo intergubernamental específicamente sobre el acceso legítimo de los gobiernos, sobre una base de valores comunes, al tratamiento de datos personales en poder de entidades del sector privado, con un fin único del orden público y la seguridad nacional (OCDE, 2023).

Del mismo modo en 2009, e inspirados por la Declaración y Pacto de la ONU en relación a la protección del derecho a la privacidad, la Organización Internacional para las Migraciones (OIM) fue pionera en la creación de normas internas para proteger los datos personales que ellos mismos manejaban, y lanzaron el "Manual de Protección de Datos de la OIM" (2010), el cual establece los principios de protección de datos para el tratamiento interno de la OIM,

resguardando la seguridad de la información de sus beneficiarios, con el objetivo de prevenir una intromisión innecesaria, abusiva y desproporcionada de los datos (OIM, s.f a), considerando que esta organización maneja datos sensibles de personas desarraigadas, desplazadas de forma interna, refugiados, migrantes y victimas de trata (OIM, s.f b).

A pesar de lo anterior y los múltiples tratados ya identificados, una de las iniciativas que estímulo a las naciones de forma particular a regularizar y reglamentar el tratamiento de los datos personales fue el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE) el cual entro en vigor el 2018 y aplica de forma directa a todos los países miembros (Unión Europea [UE], 2016). El RGPD llegó a robustecer lo establecido en la Carta de los Derechos Fundamentales de la Unión Europea (2009), dentro de la cual se garantiza de manera explícita y autónoma la protección de datos personales, aplicado a toda la UE por medio del rango de tratado constitucional (Benussi, 2020).

El Reglamento General de Protección de Datos, se gesta en una era tecnológica, y más que detener el tratamiento de los datos e información privada, busca regular su uso para que puedan seguir existiendo transferencias de información de forma segura y consciente, por lo que se establecen medidas y se busca que se adopten por quienes manejan los datos, pero que se cuide a los dueños de estos mismos, y que se priorice la intimidad de estos últimos por medio de un marco regulatorio (Rojas; López, 2018). Lo relevante de este nuevo reglamento se basa en la idea de implantar una norma única y que pueda ser suministrada de forma directa, resguardando los derechos de privacidad y seguridad de las personas dentro del ciberespacio y la ocupación de sus datos personales, es por esto que este documento aplica a todas las organizaciones situadas en Europa que tratan datos personales de los ciudadanos que ahí habitan, como también regula a las organizaciones fuera de la UE, pero que manejan datos de personas que viven en la Unión Europea y establece un sistema de certificación para que más países alrededor del mundo puedan formar parte de la transferencia de datos de manera segura, a través de un proceso de evaluación voluntaria que revisa que cumplan con estándares mínimos que resguarden los datos personales de sus habitantes como los de ellos

(Unión Europe [UE], 2016), a su vez permitiéndoles tener una relación positiva con las autoridades de control de los países europeos.

Situación en Chile

Una vez ya definidos los conceptos, identificados los posibles peligros y algunas soluciones, como también individualizadas las principales recomendaciones internacionales, en el marco de la protección de datos personales, es inconfundible que estamos frente a lo que Flavio Quezada reconoce como "problemas arquitectónicos"[2], los cuáles recomienda resolver a través de un adecuado desarrollo y anclaje constitucional, de forma de asumir la responsabilidad estatal por la protección de datos personales de forma íntegra y completa (Quezada, 2012).

Chile en 2018 consagra el derecho a la protección de los datos personales en la Constitución Política (Ley N°21.096, 2018), pero continua con una legislación sobre protección a la vida privada creada en la década de los noventa, la cual sigue siendo muy criticada ya que deja en manos del titular de los datos todo el proceso de protección de su información (costos y temporales) y sin una actualización al documento legal que responda al avance tecnológico y digital de este siglo.

Pablo Contreras, Pablo Trigo y Leonardo Ortiz, consideran que la legislación Chilena presenta un alto grado de dispersión y fragmentación en relación a su accionar y respuesta frente a situaciones que puedan perjudicar el goce al derecho de la protección de datos personales, el derecho a la autodeterminación informativa y el derecho a la privacidad, ya que dependiendo de la situación que se presente, existen distintos organismos públicos, que según sus competencias y disponibilidad, se podrían llegar a hacer cargo de la problemática, en donde la mayor parte de los casos (particulares) recae en los tribunales ordinarios de

[2] Flavio Quezada Rodríguez habla de este concepto en su texto "La protección de datos personales en la jurisprudencia del Tribunal Constitucional" (2012) pero en inglés "architectural problems", pero para efectos de facilitar el entendimiento se tradujo como problemas arquitectónicos.

justicia (Contreras et al, 2022). Lo anterior, deja claro que Chile no cuenta con una autoridad de control y/o una institución que se encargue de velar por la protección de estos derechos, ni tampoco que se encargue de fiscalizar el tratamiento de datos y mucho menos que pueda educar y concientizar respecto al valor de los datos personales.

Recalcando lo postulado por Juan Antonio Travieso, quien reconoce al conocimiento como una herramienta para la protección de los datos personales y el derecho a la privacidad, indicando que a través de la educación y su difusión se podrían garantizar los derechos humanos (Travieso, 2016). La gran pregunta es sí es responsabilidad de la sociedad auto educarse, o debe ser una entidad superior que se preocupe y tome cartas en el asunto respecto a esta problemática. Pese a lo anterior, Alberto Cerda reconoce como el contar con una autoridad de control facilitaría los medios para informar a los ciudadanos sobre sus derechos y asesorarlos, revisar y guiar la generación de protocolos para el tratamiento de datos, como también fiscalizar el cumplimiento de la normativa y sancionar de ser necesario (Cerda, 2012)

Los tres autores Contreras, Trigo y Ortiz, reconocen varias dificultades para Chile respecto a no contar con una autoridad especifica que se encargue de velar por la protección de datos personales, las cuales tienen directa relación a la postergación del goce legitimo del derecho a la autodeterminación informativa (como también a todos los derechos humanos relacionados a este tópico), reconocen que no se operativiza este derecho, ni se aplican los principios generales para su protección, no se generan mecanismos de prevención ni de sanción, y tampoco se puede generar una dedicación exclusiva, ni una supervisión especializada, como lo requiere este tema tan técnico, impidiendo que su aplicación se haga de manera independiente como lo requiere esta materia (Contreras et al, 2022).

Es así como se vuelve imprescindible que la legislación chilena tenga un proceso de actualización, el cual reconozca esta nueva generación de derechos humanos y sea capaz de responder a los requerimientos internacionales para tener un intercambio de datos personales de forma segura tanto para los tratantes, pero principalmente para los dueños de estos.

Diseño metodológico

En este apartado se presenta el enfoque de la investigación, así como la pregunta que guiará este estudio y los respectivos objetivos de la investigación.

PREGUNTA DE INVESTIGACIÓN

¿Cuáles son las oportunidades y desafíos de la creación de la Agencia Nacional de Protección de Datos Personales en Chile a partir de los principios de protección de datos personales planteados por la OCDE?

OPERACIONALIZACIÓN DE LAS VARIABLES:

OBJETIVO GENERAL

Analizar oportunidades y desafíos para la implementación de la Agencia Nacional de Protección de Datos Personales (APDP) que propone el Proyecto de Ley 11.144-07 que regula la protección y el tratamiento de Datos Personales en Chile, desde la primera moción en la Cámara del Senado (2017) hasta la actualidad, en relación a los principios de protección de datos de la OCDE.

OBJETIVOS ESPECÍFICOS

a) Individualizar y describir recomendaciones de organismos internacionales sobre la protección de los datos personales, en particular lo establecido por la OCDE[3].

[3] Específicamente para la descripción de recomendaciones internacionales se considerarán los principios establecidos por la Organización para la Cooperación y Desarrollo Económico (OCDE) en su Declaración sobre el acceso de los Gobiernos a los Datos Personales del Sector Privado del año 2023 y las Directrices de

b) Describir la situación actual con respecto a la protección de datos personales en Chile, de acuerdo a la opinión y perspectiva de personas expertas, y revisión de la bibliografía especializada.

c) Describir la institucionalidad y autoridad de control que propone el Proyecto de Ley 11.144-07, a partir de las recomendaciones de la OCDE.

d) Identificar las principales oportunidades y desafíos para la implementación del Proyecto de Ley 11.144-07, específicamente respecto a la Agencia de Protección de Datos Personales en Chile.

e) Formular recomendaciones para la implementación de la Agencia Nacional de Protección de Datos Personales en Chile del Proyecto de Ley 11.144-07.

En la siguiente tabla se presenta la operacionalización de las principales variables que, basadas en los objetivos de investigación, permiten construir las categorías de análisis de la presente investigación:

	Objetivo	Dimensión	Propiedades
a	Individualizar y describir recomendaciones de organismos internacionales sobre la protección de los datos personales, en particular lo establecido por la OCDE.	1) Declaración Universal de los Derechos Humanos de 1948 (DUDH). 2) Declaración Americana de los Derechos y Deberes del Hombre de 1948 (OEA). 3) Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales o "Convenio Europeo de Derechos Humanos" de 1950	Individualizar y describir las distintas recomendaciones internacionales sobre la protección de datos personales.

Privacidad de la OCDE sobre la protección de la privacidad y flujos transfronterizos de Datos Personales del año 2013.

		(European Coirt of Human Rights). 4) Convención Americana de Derechos Humanos de 1969 (OEA). 5) Directrices sobre la protección de la privacidad y flujos transfronterizos de datos personales de 1980 y 2013 (OCDE). 6) Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales de 1990 (ONU). 7) Recomendaciones del Consejo sobre cooperación transfronteriza en la aplicación de las leyes que protegen la privacidad de 2007 (OCDE). 8) Manuel de Protección de Datos de la OIM de 2009 (OIM). 9) Reglamento General de Protección de Datos: RGPD de 2018 (UE). 10) Declaración sobre el Acceso de los Gobiernos a los Datos Personales en Poder de las entidades del Sector Privado de 2023 (OCDE).	

b	Describir la situación actual con respecto a la protección de datos personales en Chile, de acuerdo a la opinión y perspectiva de personas expertas, y revisión de la bibliografía especializada.	1) Se realizaran entrevistas semiestructuras a expertos y personas ligadas a la protección de datos en Chile. 2) Se realizará una revisión temporal de las gestiones realizadas por el Estado de Chile en esta materia.	Describir el escenario actual de la protección de datos personales en Chile, para reconocer el panorama actual de este tópico en nuestro país.
c	Describir la institucionalidad y autoridad de control que propone el Proyecto de Ley 11.144-07, a partir de las recomendaciones de la OCDE.	1) Proyecto de Ley 11.144-07, en específico el Título VI "Autoridad de Control en materia de Protección de Datos Personales", en su última versión de 03 de enero de 2024. 2) Directrices sobre la protección de la privacidad y flujos transfronterizos de datos personales de 1980 y 2013 (OCDE). 3) Declaración sobre el Acceso de los Gobiernos a los Datos Personales en Poder de las entidades del Sector Privado de 2023 (OCDE).	Identificar y describir la autoridad de control que se busca instaurar en Chile.
d	Identificar las principales oportunidades y	Condiciones favorables y facilitadores en comparación a los rasgos obstaculizadores para la	Identificar y caracterizar

	desafíos para la implementación del Proyecto de Ley 11.144-07, específicamente respecto a la Agencia de Protección de Datos Personales en Chile.	implementación del Proyecto de Ley 11.144-07, específicamente respecto a la Agencia de Protección de Datos Personales en Chile.	condiciones facilitadores y Obstaculizadoras para la implementación del Proyecto de Ley 11.044-7, específicamente de la Agencia de Protección de Datos Personales en Chile.
e	Formular recomendaciones para la implementación de la Agencia Nacional de Protección de Datos Personales en Chile del Proyecto de Ley 11.144-07.	Condiciones de optimización que permitirían mejorar la implementación de la autoridad de control (Agencia Nacional de Protección de Datos Personales) del Proyecto de ley 11.144-07	Identificar oportunidades de mejora en el proceso de implementación del Proyecto de ley 11.144-07

ENFOQUE DE LA INVESTIGACIÓN

El tipo de enfoque que se utilizará a lo largo de la realización de esta tesis será cualitativo, ya que tal y como lo define el diccionario SAGE sobre métodos de investigación social, este tipo de investigación utiliza múltiples perspectivas teóricas, que permiten centrarse en los significados e interpretaciones, dentro de un contexto específico, de distintos fenómenos sociales (Sumner, 2006).

En este caso en particular se busca a través de un proceso inductivo indagar y definir las áreas de conocimiento que se han pronunciado respecto a su perspectiva con la protección de datos

personales. Lo anterior para comprender a cabalidad el estado de arte de esta temática, con el propósito de "comprender los significados que los individuos construyen" (Canedo, 2009). Y en base a eso identificar la importancia de la protección de estos y como el estado se enfrenta a esta problemática.

Una de las ventajas de este enfoque es que busca describir de manera holística, a través del análisis del proyecto de ley, junto a distintas interpretaciones de actores influyentes, con la intención de considerar el todo sin reducir a un estudio separado de sus partes, fundamentándose en una perspectiva interpretativa centrada en el entendimiento del significado de las acciones de los humanos y sus instituciones.

Tomando como ventaja que es un tema que aún se encuentra en discusión, se consideraran distintos puntos de vista que intentan proporcionar principios por los cuáles se deben regir las distintas autoridades para lograr un estándar mínimo frente a esta temática y como responder de manera responsable ante la ciudadanía.

TIPO DE INVESTIGACIÓN

El alcance de esta investigación es de tipo descriptivo e interpretativo, ya que se espera detallar y especificar las características, propiedades e implicancias de la propuesta para la creación de una nueva institución pública – Agencia de Protección de Datos Personales – establecida en el Proyecto de ley 11.144-07, en su última versión del 03 de enero de 2024.

El diseño corresponde a un estudio de caso, ya que se busca analizar en profundidad las oportunidades y desafíos para la implementación de la política pública de Protección de Datos Personales en Chile. Ya que se espera indagar a través de distintas fuentes bibliográficas, primarias y secundarias, como la nueva propuesta normativa, sobre la que se protegerán los datos personales, la cual no solo genera un nuevo documento legal, sí no que además se encargará de crear una institución que cumple el rol de autoridad de control responsable de hacer cumplir lo establecido por estos nuevos lineamientos.

Como plantea Díaz, Mendoza y Porras (2011), el estudio de caso retrata un momento específico, como lo será en este trabajo, en donde se estudiara la formulación del proyecto de ley sobre protección de datos personales, y sirve para relatar los distintos acontecimientos que han interferido en ella a través de la descripción y explicación de situación, de manera detallada, ya que aunque la unidad de análisis puede variar a lo largo del relato, los componentes se mantendrán y dependiendo de la calidad de la información se evidenciara la evolución.

Además, será necesario observar normativas internacionales, como los lineamientos establecidos por la OEA, OIM, ONU, y específicamente la OCDE, ya que se revisará lo establecido por esta última organización, específicamente en su Declaración sobre el acceso de los Gobiernos a los Datos Personales del Sector Privado del año 2023 y en las Directrices de Privacidad de la OCDE sobre la protección de la privacidad y flujos transfronterizos de Datos Personales del 2013, ya que estos identifican los estándares mínimos con los cuáles debería contar una regulación sobre protección de datos personales y en específico la autoridad de control.

A su vez, este tipo de investigación es útil para mostrar con precisión los ángulos o dimensiones de un fenómeno, suceso, comunidad, contexto o situación (Sampieri et al, 2014).

TÉCNICA DE RECOLECCIÓN DE DATOS

La ejecución de este estudio se llevará a cabo a través de un análisis de fuentes de información primarias, específicamente se recolectaran datos a través de una misma entrevistas semiestructuradas aplicada a distintas actores/as claves dentro del tema de protección de datos personales en Chile, las cuáles para facilitar y privilegiar la disponibilidad y ubicación de los y las entrevistadas se realizaron por video llamada.

En específico, se realizaron siete entrevistas a personas vinculadas, desde diversas áreas, al tema de protección de datos personales en Chile, a las cuáles se les aplico el mismo instrumento, el cual permitió evidenciar distintas opiniones y perspectivas sobre la situación actual de la protección de datos personales y la Agencia de Protección de Datos Personales y su futura implementación, considerando que luego de 7 años del ingreso del Boletín N°11.144-07 y N°11.092-07, el proyecto de ley finalmente se encuentra en revisión dentro de la Comisión Mixta para resolver los desacuerdos entre ambas cámaras y seguir su tramitación.

Se comenzó entrevistando a Daniel Pefaur Dendal, Sociólogo y Magister en Gobierno y Sociedad, quien lleva más de 11 años trabajando en el Consejo para la Transparencia, institución en la cual se ha desarrollado como Jefe de la Unidad de Inteligencia de Negocio, Jefe de Análisis e Innovación y actualmente se desempeña como Director de Estudios Subrogante, además ha tenido formación complementaria sobre Protección de Datos Personales. De igual modo, se entrevistó a Marcelo Drago Aguirre ex Presidente del Consejo Para la Transparencia (2017 – 2019), Abogado y Master en Administración pública, y quien además de desempeñar la docencia, también ha ocupado diversos cargos públicos como Gobernador Provincial de Cordillera, Asesor Legislativo y SEREMI de Vivienda y Urbanismo. A su vez, ha realizado labores de consultoría internacional, ligada a la gestión y políticas públicas para el Banco Interamericano de Desarrollo, la ONU, la CEPAL, y es vicepresidente de grupo del Grupo de Trabajo de Altos Oficiales en Integridad Pública de la OCDE.

Contar con sus testimonios fue útil para este trabajo, ya que entregaron una visión interna del Consejo Para la Transparencia respecto a la nueva autoridad de control de la protección de datos personales, considerando que, en el período en el que el CPLT sería la institución responsable de esta materia, ambos estaban dentro del Consejo y cuentan con experiencia técnica, por parte de Daniel, y una visión directiva desde el puesto de Marcelo.

También, bajo la misma modalidad, se entrevistó a tres Diputados, con distintas tendencias políticas, que participaron, en distintos niveles, en la discusión dentro de la Cámara Baja sobre el Boletín 11.144-07, específicamente se contactó a Boris Barrera Moreno diputado por el Distrito N°9 (segundo periodo), perteneciente al Partido Comunista e Ingeniero en Ejecución Industrial, y también a Luis Sánchez Ossa y a Leonardo Soto Ferrada, quienes además de ser parte de la discusión dentro de la Cámara de Diputados, son integrantes de la Comisión permanente de Constitución, Legislación, Justicia y Reglamento, dentro de la cual se discutió en detalle el proyecto de Ley y se elaboró el Oficio detallado con modificaciones de la Cámara revisora el cual llevo a tercer trámite constitucional a la iniciativa por crear un cuerpo legal que se preocupe de la protección de datos personales. Luis Sánchez es diputado por el Distrito N°7, pertenece al Partido Republicano es abogado y Magister en Derecho Regulatorio, fue Fiscal Regional (RM) del Ministerio de Obras Públicas y creó la plataforma de educación cívica "Charlas Constitucionales", y por su parte Leonardo Soto es diputado por el Distrito N°14 (tercer periodo), forma parte del Partido Socialista, es abogado y ha sido concejal en dos periodos dentro del Municipio de San Bernardo y fue candidato a alcalde por el mismo municipio.

Por último se aplicó la misma entrevista semi estructurada a una experta y un experto en esta materia, específicamente a Javiera Moreno Andrade, abogada y experta en el Reglamento Europeo de Protección de Datos y se encuentra en proceso de finalización de su magister en este reglamento, centrándose en la Agencia Española de Protección de Datos Personales, quien también se ha especializado en temas de derechos digitales, privacidad y datos personales y fue Coordinadora de litigios y Directora de la ONG Datos Protegidos hasta 2022. Y a Pablo Viollier Bonvin, abogado y LLM in Law and Digital Technologies, quien es especialista en derecho y tecnología, protección de datos personales y ciberseguridad, con múltiples publicaciones en estas temáticas, también trabajo como abogado de la ONG Datos Protegidos (2015-2020), es docente, co-investigador y fue Jefe de Ciberseguridad de la Corporación Santiago 2023.

Se considera la realización de entrevistas, ya que además de ser una de las formas más comunes y poderosas de conocer e interpretar a las personas (Fontana y Frey, 2005), es la técnica más apropiada y utilizada en las investigaciones cualitativas, siendo un instrumento útil para recolectar información fundamental que manejan los entrevistados, específicamente en su conocimiento de los contenidos y significados, pero junto a sus opiniones, actitudes y percepciones personales (Vargas, 2012), considerando, a su vez lo expuesto por Andrea Fontana y James Frey, quienes recuerdan que cada individuo o persona llega con su propia historia (social y política) y expectativas del mundo (Fontana y Frey, 2005).

Este instrumento, se reconoce como espontaneo, aunque en algunos casos se envíen las preguntas de forma previa a la realización de la entrevista (a solicitud del entrevistado), ya que las respuestas que se entreguen en el momento fluirán de manera espontánea según su visión y recuerdo, y se vuelve responsabilidad del entrevistador captar y comprender las respuestas, para posteriormente en la investigación reflejar lo que el participante pretendió anunciar e interpretar con responsabilidad sus palabras, bajo la confianza que entregó el interlocutor para la respectiva investigación. Dentro de este proceso no se puede olvidar el análisis posterior al dialogo, el cual debe contar con un registro para realizar una transcripción (total o parcial) de lo expuesto y así profundizar en lo ya conversado, y *"proteger y conservar la palabra"* (Fernández, 2001, p. 15).

Específicamente en esta investigación se consideró la entrevista semi estructurada, ya que al aplicarse a varias personas, provenientes de distintas áreas tanto formativas como laborales, podrían recogerse averiguaciones complementarias que no fueron preguntadas de forma directa, las cuáles podrían resultan enriquecedoras para el análisis posterior.

Identificación Entrevistados

N°	Nombre	Fecha realización entrevista
1	Daniel Pefaur Dendal	29 de junio de 2023

2	Luis Sánchez Ossa	12 de enero de 2024
3	Leonardo Soto Ferrada	16 de enero de 2024
4	Boris Barrera Moreno	17 de enero de 2024
5	Pablo Viollier Bonvin	17 de enero de 2024
6	Marcelo Drago Aguirre	19 de enero de 2024
7	Javiera Moreno Andrade	19 de enero de 2024

Contexto de la investigación

Protección de datos personales en Chile

En Latinoamérica, Chile destaca como uno de los países pioneros en normativa sobre el uso y protección de los datos personales, ya que fue el primer país de la región en legislar sobre esta materia en 1999 con la ley sobre protección de la vida privada, la cual regula el *"tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares"* (Ley Nº19.628, 1999, p. 1), velando por el buen uso de estos, lo anterior en una época en donde el dinamismo de las tecnologías digitales avanzaba a un ritmo diferente que en la actualidad.

Con el pasar de los años y junto a la consolidación de la era digital, han aumentado las tecnologías y el flujo de información, las cuales circulan a una mayor velocidad y por un sin fin de plataformas manejadas por distintos organismos y/o asociaciones a nivel mundial, las cuales tienen acceso a datos personales e información sensible, ya sea por la fragilidad de la seguridad de los infinitos sitios webs que existen, como también por medio del consentimiento entregado por cada usuario, quienes muchas veces, bajo el desconocimiento, apuro y/o desinterés, no tienen total discernimiento de los términos y condiciones en los cuáles serán usados sus datos al momento de presionar el botón aceptar, a lo anterior también se suma la poca capacidad de acción que tienen los gobiernos frente a este espacio intangible.

Lamentablemente, la normativa chilena no ha avanzado a la misma velocidad que las nuevas tecnologías, generando un peligro para los ciudadanos y una sobreexposición del uso de su información personal sin su total conocimiento. Es así como se ha vuelto prioritario y urgente la revisión y modificación de la legislación actual, ya que no existe una entidad clara que fiscalice esta materia, ni tampoco alguna institución que limite los tratamientos y difusión de estas grandes bases de datos (Cámara de Diputados Chile, 2016).

Es así como entre el año 2001 y 2012 se evidenciaron distintos intentos por modificar la ley N°19.628, los cuáles planteaban regular casos de autodeterminación informativa, el uso de tecnologías en el trabajo, el registro de ofensores sexuales, el monopolio de información comercial, el SPAM en los correos electrónicos y la creación de un registro de usuarios de cibercafés, todas relacionadas directamente al tratamiento de datos personales (Derechos Digitales, 2012). De los anteriores intentos, se crearon cinco leyes que efectivamente modificaron a la ley sobre protección de la vida privada, las cuáles prohibieron la entrega de información relacionada a; deudas contraídas con empresas públicas y privadas que proporcionen servicios básicos[4], protestos y morosidades comerciales de personas en período de cesantía[5], deudas con concesionarios de autopistas por el uso de su infraestructura[6] y adeudos asociados a servicios educacionales[7] y servicios y acciones de salud[8], como también establecieron el impedimento de realizar evaluaciones de riesgo comercial que no se basen en información puramente objetiva[9] (Ley N°20.521, 2022).

Durante el segundo gobierno de la Presidenta Michelle Bachelet, se promulgó la Agenda Digital 2020, la cual a través de cinco ejes claves buscaba trazar la ruta del desarrollo digital

[4] Ley N°19.812 Modifica la ley N°19.628, sobre protección de la vida privada (2002).
[5] Ley N°20.463 Modifica ley N°19.628, suspendiendo por el plazo que indica la información comercial de las personas cesantes (2010).
[6] Ley N°20.575 Establece el principio de finalidad en el tratamiento de datos personales (2012)
[7] Ley N°21.214 Modifica la ley N°19.628, sobre protección de la vida privada, con el objeto de prohibir que se informe sobre las deudas contraídas para financiar la educación en cualquiera de sus niveles (2020).
[8] Ley 21.504 Establece prohibición de informar deudas contraídas para financiar servicios y acciones de salud en la Ley N°19.628 (2022).
[9] Ley 20.521 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.

del país y en donde una de sus primeras medidas, incluida en el primer eje "Derechos para el Desarrollo Digital" se estableció la creación del proyecto de ley que proyectaba actualizar la normativa adecuándose a los requerimientos internacionales y dar respuesta a los estándares necesarios (Gobierno de Chile, 2015). Es importante señalar que durante este mismo año, 2015, Chile recibió una carta de advertencia por retraso en la modificación y actualización de su marco normativo, en relación a la protección de datos personales (Alonso, 2015).

Aun así, no fue hasta el 2017 que tras diversas situaciones de filtración de información y robos de bases de datos, esta temática volvió a posicionarse como relevante y tanto la presidencia[10] como la cámara del Senado[11] enviaron propuestas para modificar la ley Sobre protección de la vida privada, las cuales al tener bastantes puntos en común se tomó la decisión de refundirlas en un solo proyecto y dar inicio a las discusión en general y particular del primer informe (Senado, 2017). Desde ese año se encuentra en el Congreso el proyecto que busca regular la protección y el tratamiento de los datos personales y a su vez crear una agencia que se haga responsable de esta materia, de sus necesidades actuales y obligaciones futuras.

Uno de los acontecimientos más importantes que se presentó en paralelo al proceso de la discusión de la modificación de la ley N°19.628 (1999), fue que en junio de 2018 se consagró en la Constitución el derecho a la protección de los datos personales (Ley N°21.096, 2018), proceso que comenzó en 2014 luego de una moción presentada por la Comisión de Constitución, Justicia y Reglamento, la cual fundada por la falta de seguridad respecto al flujo de los datos e información y a la *"ausencia de una institucionalidad específica e independiente"* (Biblioteca del Congreso Nacional de Chile [BCN], 2018), la cual tuviera la facultad de velar por la protección de los derechos ligados al tratamiento de información personal, como también por la existencia de múltiples legislaciones alrededor del mundo que se estaban haciendo cargo de la protección y legislación en esta materia, siendo el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE) el más

[10] Boletín N°11.144-07
[11] Boletín N°11.092-07

elogiado por "fortalecer los derechos fundamentales de las personas en la era digital y facilitar la actividad económica" (Comisión Europea, 2018), generaron el clima propicio para poder establecer este derecho en la carta magna chilena.

Otro hecho internacional que motivó la consagración del derecho a la protección de datos personales en la Constitución, y a la revisión de la ley N°19.628, fue el ingreso en 2010 de Chile, como primer país Latinoamericano como miembro pleno, a la Organización para la Cooperación y el Desarrollo Económico (OCDE, 2010), institución que fue la primera en entregar lineamientos para las regulaciones locales en 1980 con sus "Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de los datos personales" (OCDE, 1980), documento que fue actualizado el año 2013 por el escrito denominado "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" el cual fue creado por el Comité de Política de Economía Digital (CDEP) con el fin de modernizar ciertos términos, pero también para instigar a los países miembros a aplicar las directrices OCDE en sus respectivos marcos jurídicos, bajo la continua necesidad de aunar los esfuerzos y estrategias nacionales y globales por proteger la privacidad (OCDE, 2013), sin dejar de promover la transferencia de información que simplifique el desarrollo económico.

Respecto a los hitos importantes ocurridos dentro del proceso de discusión del proyecto de ley que insta por regular la protección y el tratamiento de los datos personales y la creación de la Agencia de Protección de Datos Personales en Chile (APDP), se encuentra la discusión de la autoridad de control que deberá tomar la responsabilidad de garantizar la protección de los datos personales. Lo anterior considerando que dentro del mensaje presidencial inicial, enviado en 2017 por Michelle Bachelet, se propuso la creación de una nueva institución especializada y de carácter técnico, que protegiera y fiscalizará el cumplimiento de esta nueva normativa (Boletín N°11.144-07, 2017). Sin embargo, al año siguiente, durante el segundo mandato del presidente Sebastián Piñera, desde el mismo poder ejecutivo se envió un Oficio que modificaba la autoridad encargada de la protección de datos personales y le entregaba estas facultades al Consejo para la Transparencia (CLPT), indicando que para cumplir con

estas nuevas funciones, esta institución deberá dividirse, consignando un área para el acceso a la información y otra para la protección de datos personales, las cuáles deberían trabajar en salas diferenciadas, y tendría que integrar a un quinto consejero, el cual, al igual que el resto del consejo, debería contar con dedicación exclusiva al cargo y no podría haber sido sancionado de forma previa por mal uso y tratamiento de datos personales, ni contar con intereses relacionados con el sector privado (Viollier, 2018).

La anterior decisión, enfatizo su origen en que el entregar nuevas funciones a una institución ya consolidada, como lo era el CPLT, implicaría menos burocracia que crear una nueva desde cero, como también comprometería menos recursos económicos. Este último argumento, también fue considerado por la ex presidenta Michelle Bachelet, ya que la entidad propuesta por su gobierno dependería de forma directa del Ministerio de Hacienda, generando un ahorro en su implementación. Esta decisión significó opiniones variadas, como la de Felipe Harboe, uno de los autores de la moción inicial, quien manifestó su preocupación respecto al riesgo que significaría entregarle la responsabilidad de la protección de datos a una entidad que se especializa en transparentar información, considerando a su vez que el Consejo trabaja fiscalizando instituciones públicas, y esta nueva responsabilidad implicaba trabajar en conjunto a entidades privadas, por lo que el ex senador estimaba como imperioso el contar con una agencia nueva y especializada (Leiva, 2018).

Aun así durante el año 2019 se logró la aprobación, por parte de la Comisión de Constitución, Legislación, Justicia y Reglamento, de la designación del Consejo para la Transparencia como la entidad encargada de velar por la protección de los datos personales en Chile, decisión dividida pero bien recibida por el entonces presidente de la institución Jorge Jaraquemada, quien indicó que estarían en condiciones de afrontar las nuevas funciones encomendadas, sin ver afectadas las labores actuales, agregando que en distintos países "*la autoridad de control y protección de datos personales debe actuar con independencia"* (Jaraquemada, 2019) y que el Consejo cumpliría con ese requisito (Cámara del Senado, 2019). Esta decisión fue aprobada un mes después del lanzamiento de la "Agenda de Modernización del Estado", la cual desde el gobierno de turno comprometió el avance de

este proyecto de ley, específicamente en las definiciones de las condiciones operacionales, junto a la creación de un marco institucional acorde a los estándares internacionales, haciendo hincapié en la importancia de contar con una autoridad de control que sea capaz de abordar los desafíos regulatorios y de fiscalización en esta materia (Gobierno de Chile, 2019).

Respecto a la compatibilidad de normar, fiscalizar y resguardar la protección de datos personales, junto a sostener la transparencia de la información en la Administración Pública, existen varios países que han utilizado esta fórmula. Un ejemplo es México, quien cuenta con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), el cual es un organismo autónomo con la misión de resguardar los derechos fundamentales de los ciudadanos mexicanos ligados a la información pública y la protección de datos personales (INAI, s.f.). Bajo una modalidad similar se encuentra Argentina con su Agencia de Acceso a la Información Pública (AAIP), que aunque su nombre no lo incluye, también es responsable de la protección de los datos personales, junto al monitoreo y desempeño de la transparencia en la gestión y el acceso a la información en el país vecino (Gobierno de Argentina, s.f.). Es importante mencionar como esta institución, durante el primer mes del presente año, recibió la revalidación del estatus como país adecuado para el libre flujo transfronterizo de datos personales, otorgado por la Unión Europea (Gobierno de Argentina, 2024). Como último ejemplo, aparece el Information Commissioner's Office (ICO), el cual es el organismo público de Reino Unido, que también se encarga de la Ley de Protección de Datos y la Ley de Libertad de la Información (Information Commissioner's Office [ICO], Sin Fecha).

Pese a lo proyectado por el lanzamiento de la agenda de modernización del gobierno del Presidente Piñera, durante el 2019 no se lograron mayores avances respecto al proyecto de ley, el cual según el historial de tramitación no se retomó hasta 2020 con la recepción de indicaciones en enero de ese mismo año, las cuáles fueron acogidas en marzo, con la entrega del segundo informe de la Comisión de Constitución, Legislación, Justicia y Reglamento, no obstante y considerando la crisis desatada por la pandemia mundial del virus SARS-Cov-2, el país se vio obligado a redestinar todos los esfuerzos y recursos al área de la salud, para

combatir el Covid-19 (atender los casos positivos y crear protocolos que previnieran el aumento incontrolable de casos), como también a enfrentar el aumento de la desocupación laboral (Organización Internacional del Trabajo [OIT], 2020), provocando una modificación de las prioridades a resolver por el gobierno de turno, ya que este evento imprevisto introdujo a Chile en una gran e inevitable crisis social, política y económica.

Lo anterior solo significo un obstáculo más dentro del largo camino que ha transitado la legislación en materia de protección de datos personales en Chile, la cual logro retomar su discusión en 2021, luego del primer llamado a suma urgencia a fines del año 2020, el cual se mantuvo hasta el mes de marzo, mes en el cual se llamó a urgencia simple, la que se mantuvo hasta octubre de 2021, cuando el Poder Ejecutivo ingreso una nueva indicación que dejaba fuera al CPLT y estableció la creación de la Agencia de Protección de Datos Personales, la cual sería una *"corporación autónoma de derecho público, de carácter técnico, descentralizado, con personalidad jurídica y patrimonio propio"* (Boletín de indicaciones N°183-369, 2021, p. 2), con el objetivo de proteger y fiscalizar el tratamiento de datos personales según lo establezca el proyecto de ley.

Es importante destacar que una de las discusiones más reiteradas, en el marco de la protección de datos personales, es quien será la autoridad de control que se hará cargo de velar por el correcto uso de la información privada, debido a que uno de los pocos consensos entre académicos y expertos en esta temática se encuentra en la ineludible necesidad de Chile por contar con una autoridad de control en un corto plazo, la cual se responsabilice de manera activa y no reactiva, como se han encargado los tribunales de justicia en la actualidad, recordando que los datos personales hoy en día constituyen un conjunto de información asociada a un valor económico transable (Álvarez, 2016), volviendo más atractivo su uso y tratamiento, aún más sí no existen normas, ya que posiciona a esta temática en una zona insegura.

A pesar de ello, no es hasta 2022 que el proyecto consigue la aprobación de la discusión particular y pasa a su segundo trámite constitucional en la cámara de diputados en donde se

mantiene 16 meses, dentro de los cuáles bajo un arduo trabajo dentro de la Comisión permanente de Constitución, Legislación, Justicia y Reglamento, la cual solo en su primer semestre tuvo más de 100 indicaciones, y en donde se generó una discusión muy nutritiva por parte de expertos y autoridades públicas, como también se consideraron experiencias ya instauradas en otros países, y se recogieron las recomendaciones de las organizaciones internacionales, las cuáles luego de arduas y extensas discusiones lograron converger en un Oficio, el cual fue despachado y presentado al Senado en mayo de 2023, pasando a tercer trámite constitucional (Senado, 2023).

El proyecto se mantuvo en esa etapa hasta enero de 2024, mes en el cual la Cámara del Senado entrego su documento respuesta con las observaciones, o más bien rechazos, al Oficio enviado por la cámara baja, por lo que al no tener un acuerdo mutuo, se pasó a la siguiente etapa, la cual es la revisión dentro de la Comisión Mixta (Senado, 2024b).

La Agencia de Protección de Datos Personales dentro del Proyecto de Ley

Respecto al proyecto de ley actual, y considerando la importancia que se le ha entregado a la autoridad de control de protección de datos personales, se resumirá lo que plantea la propuesta gubernamental respecto a la entidad que se hará responsable de la protección de la información personal, considerando el último texto comparado generado por la Cámara del Senado y publicado con fecha 03 de enero de 2024, dentro del cual se establece que esta institución será autónoma de derecho público, de carácter técnico, descentralizada, con personalidad jurídica y patrimonio propio, pero que se relacionará, a través del Ministerio de Economía, Fomento y Turismo, con el Presidente, y tendrá el objetivo de *"velar por la efectiva protección de los derechos que garantizan la vida privada de las personas y sus datos personales, de conformidad a lo establecido en la presente ley, y fiscalizar el cumplimiento de sus disposiciones"* (Senado, 2024a, p. 100).

Dentro de las funciones que tendrá la Agencia, es importante resaltar las siguientes:

1) Dictar normas generales e instrumentos que regulen el tratamiento de los datos personales.
2) Aplicar e interpretar de forma administrativa las disposiciones legales en materia de protección de datos.
3) Fiscalizar el cumplimiento de las disposiciones del proyecto de ley y todas las normativas asociadas, junto a la determinación de las infracciones en que se incurran
4) Determinar las infracciones y sancionar a quienes corresponda respeto a no cumplir con lo establecido en la ley en orden de la protección de datos personales.
5) Crear programas y proyectos que difundan y promocionen información para que las personas conozcan sus derechos en relación a los datos personales.
6) Proponer, ante quien corresponda, normas y reglamentos que actualicen a la normativa, y pueda cumplir con sus obligaciones, sobre el tratamiento de datos y uso de la información.
7) Asesorar técnicamente, cuando se requiera, a otras instituciones públicas, como también colaborar con estas mismas para implementar políticas públicas que resguarden la protección de los datos personales.
8) Suscribir convenios de cooperación y colaboración internacionales, nacionales, públicos y/o privados, que tengan competencias en esta área. Y participar con organismos internacionales.
9) Encargarse de certificar modelos de prevención de infracciones, sus cumplimientos y administrar el "Registro Nacional de Sanciones y Cumplimientos"[12].

Se espera que la Agencia este dirigida por el un consejo directivo, el cual deberá establecer normas internas, políticas de planificación y control, y formular propuestas de reformas. El consejo estará formado por un total de tres consejeros designados por el Presidente con

[12] El Registro Nacional de Sanciones y Cumplimientos estará encargado de mantener un catastro de todos los responsables de datos que hayan sido sancionados por incumplir la normativa, incluyendo su respectiva infracción, gravedad y sanción, como también debe registrar a los responsables que cuenten con modelos de prevención vigentes (Senado, 2024a).

acuerdo al Senado, respetando las inhabilidades e incompatibilidades establecidas en la ley. También la agencia deberá mantener una coordinación constante y reglamentada con el Consejo para la Transparencia, para evitar conflictos normativos (Senado, 2024a).

La deuda de Chile frente a la OCDE

Chile es parte de la Organización para la Cooperación y el Desarrollo Económico desde el año 2010, pero aun así continúan pendientes los esfuerzos por mejorar la legislación en protección de datos personales, siendo advertido por la entidad internacional respecto a su nulo perfeccionamiento en esta materia, llegando a ser uno de los pocos países pertenecientes a la OCDE en esta situación (Alonso, 2015).

Tras la recepción de la carta de advertencia de la OCDE al Ministerio de Economía, la Organización Datos Protegidos realizo un llamado a las autoridades para que por favor se levantará un proyecto de ley, el cual llevaban años anunciando, y que se aprobará con la celeridad necesaria en el Congreso (Datos Protegidos, 2015). Situación que lamentablemente no se cumplió y se evidencia en el relato sobre la legislación que se construyó en los apartados anteriores.

Se vuelve importante señalar, que al momento de ingresar como miembro pleno, Chile asume la obligación de implementar los acuerdos internacionales que establece la Organización para la Cooperación y el Desarrollo Económico, en este caso y en específico, los relacionados con la protección de los datos personales, como también de hacer parte dentro de su propia normativa a los principios reconocidas por la OCDE (Viollier, 2017).

Lo anterior, concretamente de los siguientes documentos:

1) **Directrices sobre la protección de la privacidad y flujos transfronterizos de datos personales de 2013.**[13]

Este documento creado en 1980 y actualizado en 2013, establece ocho (8) principios para aplicar a nivel nacional, en lo que respecta al tratamiento de datos personales, con el objetivo de promover y facilitar los flujos transfronterizos de los datos personales, cuidando los valores democráticos, el estado de derecho, los derechos humanos y sus libertades, junto a la privacidad de las personales.

El primer principio es denominado de "**Recolección limitada**" y busca establecer un margen, o normativa, para la recopilación de los datos personales, los cuáles deben ser obtenidos por medios lícitos y justos, con previo conocimiento y consentimiento del dueño de los datos. En segundo lugar aparece el principio de "**Calidad del dato**", estableciendo que cuando se usen los datos deben mantenerse tal cual como se recolectaron de forma precisa, completa y actual. El tercer principio corresponde al de "**Propósito específico**", el cual busca explicitar el fin con el que se recopila el dato, y el cuarto principio de "**Uso limitado**" condiciona su uso al cumplimiento de este objetivo. Como quinto principio se nombra al de "**Seguridad**", siendo el principio que imparte la noción de proteger los datos personales a través de medias razonables que prevean los riesgos de perdida, acceso no autorizado, destrucción, transformación y/o divulgación. El sexto principio sobre "**Accesibilidad**" implica la creación de una política general sobre el acceso a los datos personales, en el marco del desarrollo de prácticas que resguarden esta información, las cuáles también incluyan medios disponibles para conocer estas normativas y mantener un buen uso de los datos privados.

[13] Organización para la Cooperación y el Desarrollo Económico, Recommendation of the council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 10 de julio de 2013, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Como penúltimo principio se establece el de "**Participación individual**", el cual busca entregar el poder a los ciudadanos para poder confirmar que datos personales se encuentran en poder de ciertas instituciones, y que estas instituciones respondan de manera razonable, entendible y accesible, en cuanto a los costos asociados. El último y octavo principio establece la "**Responsabilidad**", la cual recae en el "data controller[14]", quien debe cumplir con los principios ya descritos.

2) Declaración sobre el Acceso de los Gobiernos a los Datos Personales en Poder de las entidades del Sector Privado de 2023. [15]

Esta declaración nace en la Conferencia a nivel ministerial del Comité de Política de Economía Digital (CDEP), la cual tenía como temática principal "Impulsar la recuperación a largo plazo y el crecimiento económico mediante la construcción de un futuro digital de confianza e inclusivo"(OCDE, 2023), por lo que este documento se considera como uno de los primeros acuerdos intergubernamentales con perspectivas comunes y generales que protejan la privacidad, las libertades y los derechos humanos, respecto al acceso de datos personales. Lo anterior con el objetivo de proteger la seguridad nacional y mantener el orden público (OCDE, 2023).

Dentro de este documento se promueven dos máximas, por un lado el acceso legítimo de los gobiernos sobre la base de los valores comunes, y por otro lado la confianza en los flujos transfronterizos, los cuáles se complementan para alcanzar el objetivo antes descrito.

Sobre el acceso legítimo de los estados a los datos, se establece que es responsabilidad de todos los países miembros resguardar a la ciudadanía a través de la prevención y detección de actividades delictivas que amenacen a la seguridad de sus datos personales y la protección

[14] El data controller es quien lleva el uso de los datos personales dentro de alguna institución, y se encarga de la recopilación, su almacenamiento, su procesamiento y su difusión (OCDE, 2013).
[15] Organización para la Cooperación y el Desarrollo Económico, Declaration on Gobernment Access to Personal Data Held by Private Sector Entities, 12 de febrero de 2023, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

de su privacidad, como también aquellos peligros que pasen a llevar los derechos humanos y sus libertades. Lo anterior, debe ser pensado en el cumplimiento de la legislación de cada nación, por lo que se espera que esto este reconocido en cada uno de los marcos jurídicos nacionales, para que los gobiernos tengan las facultades de acceder a los datos de forma legal y regularizada.

Respecto a la confianza en los flujos de datos fronterizos se establece que, los principios que se exponen en esta declaración son aplicables siempre y cuando los gobiernos tengan esto suscrito en su marco jurídico y requieran acceder a datos que se encuentran en poder de entidades del sector privado y de carácter internacional (dentro de su territorio nacional) con fines de orden público y de seguridad nacional. La aplicación de lo anterior, se debe adecuar a cada estado, ya que dependerá de la ley local, el contexto y las circunstancias del acceso solicitado.

El Comité , antes de nombrar los principios por los cuáles se debe entregar acceso a los datos en manos de entidades privadas, entrega tres importantes definiciones; en primer lugar define el concepto "Datos personales", concepto que hemos descrito en otros apartados de esta tesis pero que es relevante indicar como lo toma la Organización para la Cooperación y el Desarrollo Económico, siendo " cualquier información relativa a un individuo identificado o identificable" (OCDE, 2023)- En segundo lugar, define al marco jurídico como el conjunto de distintos documentos legales, como leyes nacionales, ordenes ejecutivas y judiciales, reglamentos administrativos, jurisprudencia y todos los instrumentos o requisitos jurídicos que resulten vinculantes, los cuales contengan obligaciones legales ligadas al derecho internacional y supranacional aplicables al país. Y por último, indica que las entidades del sector privado que se consideran en este artículo son los individuos y a las Organizaciones No Gubernamentales (ONG) sin fines de lucro.

La Declaración Sobre el Acceso de los Gobiernos a los Datos Personales en Poder de las Entidades del Sector Privado, establece siete (7) principios, los cuáles buscan respaldar la seguridad de los datos personales de la ciudadanía, los cuáles pueden estar en manos de

instituciones privadas, por lo que promueven el cuidado de estos por cada gobierno, motivando a que se integren estos postulados a sus respectivos procesos legislativos, siendo su primer principio la "**Base Legal**", dentro de la cual está el marco jurídico, el cual debería entregar las garantías idóneas para controlar el uso indebido y abusivo de los datos personales de su población, lo anterior estableciendo limitaciones y salvaguardias en relación al acceso gubernamental a esta información, tener claros los fines y condiciones, bajo las cuáles sea necesaria la participación gubernamental.

Bajo lo establecido en este mismo documento, la OCDE busca que prime la democracia, el Estado de derecho, la protección a los derechos humanos y la privacidad y las libertades de las personas, por lo que el segundo principio traducido al español como "**Objetivos Legítimos**" establece que el acceso de los gobiernos a los datos en poder de entidades privadas debe estar justamente respaldado por un motivo fundado que persiga un propósito específico y lecito, entendiéndose que la información recopilada será utilizada para el objetivo establecido y para nada más, manteniendo el imperio de la ley. Entendiendo además que todo acceso por parte de los gobiernos, debe realizarse sin reprimir ni perjudicar a las personas o a ciertos grupos minoritarios, resguardando que ciertos principios legales se antepongan como lo son el de proporcionalidad, racionalidad y necesidad, como también toda norma que proteja el acceso o uso indebido.

El tercer principio "**Aprobación previa**", indica que el marco jurídico de cada país debería establecer los requisitos y criterios para entregar acceso al Gobierno a los datos de particulares en manos de entidades privadas. Siendo estos requisitos revisados por una entidad que se encargue de revisar el cumplimiento y entregar la aprobación según corresponda, entendiendo que los criterios deben ser proporcionales al nivel de intromisión en la intimidad de los individuos, de sus derechos humanos y libertades, lo anterior considerando casos excepcionales de emergencia, que se deberían tipificar. A su vez, y según lo que plantea el cuarto principio sobre el "**Tratamiento de datos**", es que también deben establecerse procedimientos que aseguren el correcto uso de datos, como también controles internos que detecten, prevean y corrijan la posible pérdida de datos o accesos indebidos,

también la destrucción, mal uso, cambio o divulgación accidental o no autorizada de información, como también el reporte de estos casos a los organismos de supervisión correspondientes.

De no cumplirse el correcto tratamiento de los datos, se exhorta a las naciones a otorgar una "**Reparación**" (séptimo principio) de tipo judicial y no judicial, que logre evidenciar la infracción en la que se incurrió y enmendar a través de la prohibición del acceso, la eliminación de los datos mal usados, restableciendo la integridad de los datos e indemnizando a los afectados por daños y perjuicios.

Los anteriores movimientos deben ser de conocimiento público, por lo que desde la OCDE se invita a que cada estado presente informes periódicos desde el organismo de supervisión en donde se indique el cumplimiento de los requisitos de acceso por parte del gobierno, como también desde las entidades gubernamentales que hayan solicitado información se materialice un documento que sea de conocimiento público de los datos solicitados, siendo este el quinto principio de "**Transparencia**". Lo anterior, a menos que se establezca que por seguridad pública (o alguna otra razón) sea materia confidencial.

Como último principio se nombra al que en el documento corresponde al sexto de "**Supervisión**", ya que hace relevante al estar analizando la institución que se hará cargo de esta normativa en Chile. Este principio alienta a los países a contar con una supervisión imparcial y eficaz sobre esta temática, la cual bajo un marco jurídico docto garantice el correcto acceso a los datos por pate de los gobiernos. Es por esto que recomienda contar con un organismo con mandato individual e independiente, el cual cuente con las facultades suficientes para revisar, supervisar el cumplimiento del correcto tratamiento de datos. Esta organización debe ser capaz de investigar, averiguar y auditar al gobierno en sus procesos de accesos a datos para confirmar que se esté cumpliendo con la normativa y de no ser así que se cumpla con las funciones de reparación de ser necesarias y/o solicitadas por los particulares afectados.

Existen mecanismos para supervisión eficaz e imparcial que garantice que el acceso de los gobierno a los datos respecta el marco jurídico aplicable, a través de organismos (oficinas de cumplimiento internos, organismos jurisdiccionales, comisiones parlamentarias o legislativas y autoridades administrativas independientes), los cuáles actúan de acuerdo con sus mandatos individuales, y con las facultades suficientes que incluyen la capacidad de obtener y revisar información relevante, realizar investigaciones o averiguaciones, llevar a cabo auditorias , comprometerse con las entidades gubernamentales en materia de cumplimiento y atenuación y abordar el incumplimiento. Estos organismos también son quienes reciben los informes de incumplimiento, y fiscalizar así que se desde las entidades gubernamentales se rindan las cuentas correspondiente y que también se estén ejerciendo las funciones de reparación en respuesta de las quejas de los particulares (OCDE, 2023).

Estos documento, en especial los principios que establecen, se han posicionado como fundamentales en el tratamiento de datos personales y se han aplicado en la mayoría de sistemas y regímenes regulatorios dentro de los países miembros, para otorgarle seguridad a sus ciudadanos, priorizando el garantizar los derechos de las personas en el mundo digital (Benussi, 2020).

Análisis y resultados

Para el análisis de resultados se realizaron un total de siete entrevistas a personas vinculadas, desde diversas áreas al tema de protección de datos personales en Chile, a las cuáles se les aplicaron las mismas preguntas de manera semi estructurada, lo que permitió evidenciar distintas opiniones y perspectivas sobre la Agencia de Protección de Datos Personales y su futura implementación, considerando que luego de 7 años del ingreso del Boletín N°11.144-07 y N°11.092-07 (refundidos) (2017), el proyecto de ley finalmente se encuentra en revisión dentro de la Comisión Mixta para resolver los desacuerdos entre ambas cámaras y seguir su tramitación.

Situación Protección de Datos Personales en Chile

A los siete entrevistados se les consultó respecto a cómo observaban, en la actualidad y desde su labor, la situación de nuestro país sobre la protección de Datos Personales y todos coincidieron en que es necesario contar con mayor protección y regulación de los datos personales y mostraron preocupación respecto a lo rezagado que se encuentra Chile frente a la protección de datos personales, y que la existencia de la Ley N°19.628 (1999) sobre protección de la vida privada, es una ley que está desactualizada y no se adecua al avance tecnológico. Lo anterior, se identifica con lo que plantea Flavio Quezada en su texto "La protección de datos personajes en la jurisprudencia del Tribunal Constitucional" (2012), respecto a que estamos frente a "problemas arquitectónicos" y es necesario establecer un adecuado desarrollo y anclaje constitucional, para dar respuesta a esta problemática de forma íntegra y completa.

Aun así, Leonardo Soto (Entrevista N°3, 2024) y Marcelo Drago (Entrevista N°6, 2024) coincidieron en que incluso teniendo esta ley, nadie se encarga de su cumplimiento, salvo en algunos casos en los cuáles se le ha encomendado al Consejo Para la Transparencia hacerse responsable de situaciones específicas, en donde el Ex presidente del Consejo agrega que el cuidado de los datos personales se respeta un poco más en el sector público, ya que el CPLT se ha encargado de crear una serie de instrucciones generales, realizar auditorías e instrumentos de control y gestión, capacitar y orientar a los funcionarios públicos, permitiendo instaurar una cultura de protección a la información sensible dentro del aparato estatal (M. Drago, Entrevista N°6, 2024).

La situación plasmada por Marcelo Drago en su entrevista (2024), se condice con lo expuesto por los autores Contreras, Trigo y Ortiz (2022) respecto a cómo existe una fragmentación del sistema chileno para dar respuesta a la protección de datos personales, en donde no existe una autoridad que se encargue de esta materia de forma exclusiva, sino más bien y

dependiendo de la problemática, se encarga a algún organismo público para que busque alguna solución, perjudicando directamente el goce respecto al derecho sobre la privacidad.

Con respecto a la perspectiva de la protección de datos personales en el sector privado, gran parte de los entrevistados lo ven de forma negativa, ya que se desconoce cómo es el tratamiento de datos dentro de estas instituciones, cómo los manejan, cómo los consiguen y sí los comercializan. Sobre este último punto, Luis Sánchez en su entrevista (2024) no descarta la posibilidad de la venta de las bases de datos, a lo que se suma Boris Barrera (Entrevista N°4, 2024) quien resalta la importancia de los términos económicos dentro de los cuáles se manejan los datos, y se complementa con lo señalado en el contexto de esta investigación, respecto a cómo los datos personales en su conjunto pasan a ser *"un bien con valor económico que actualmente se transa en el mercado"* (Álvarez, 2016, p. 63).

Lo anterior, logra posicionar a ciertas instituciones por sobre otras, donde en la mayoría de casos los perjudicados son los usuarios y dueños de los datos, quienes al no tener total conocimiento del valor e importancia de su información quedan situados asimétricamente frente a empresas u organizaciones que tienen la capacidad tanto económica como técnica para recolectar sus datos, tratarlos y transferirlos, y no solo esto, como agrega Carlos Romeo, son capaces de beneficiarse de esta información que acumulan y utilizarla dentro de sus procesos internos (Romeo, 1994b).

Muchas instituciones y organizaciones con frecuencia ocupan mecanismos capciosos para conseguir el consentimiento y la entrega de datos por parte de las personas, con términos y condiciones que no leen, como lo evidencia la encuesta aplicada por el SERNAC en 2022 que evidencia como un 88,9% de las persona manifiesta que solo "algunas veces" o "nunca" leen la política de privacidad de los sitios webs que visitan (SERNAC, 2022). Pablo Viollier considera que las personas no leen estos documentos ya que están escritos en un lenguaje técnico y extenso, los cuáles establecen condiciones muchas veces abusivas, y que coinciden entre empresas que comparten rubro, siendo imposible para los individuos rechazar estas

condiciones sí quieren hacer uso de su página web o adquirir algún producto o servicio (Entrevista N°5, 2024).

Javiera Moreno (Entrevista N°7, 2024) agrega como también son estas compañías las que pueden llegar a ser infractoras de la ley, y a su vez del proyecto de ley de protección de datos personales, pero también son estas mismas las que tiene un mayor poder económico para defenderse frente a los tribunales en caso de recibir alguna demanda, ya que otra falencia de la ley actual, es que al presenciar un mal uso de datos personales o filtraciones, las personas de forma particular deben recurrir a la justicia civil, costear todos los gastos asociados a esta demanda y someterse a un proceso que muchas veces no es expedito. Lo anterior también es mencionado en el texto "Un Sistema Fragmentado: La protección sectorial de los datos personales" de Pablo Contreras, Pablo trigo y Leonardo Ortiz, en el cual exponen como al no contar con una autoridad de control en esta temática, el sistema se fragmenta y distintos organismos públicos se van haciendo cargo de la protección de datos personales en la medida de lo posible y los casos terminan en los tribunales ordinarios de justicia (Contreras et al, 2022).

Se vuelve importante también considerar lo señalado por Viollier (Entrevista N°5, 2024) respecto a la principal falta que él identifica respecto a la normativa actual, la cual es la falta de mecanismos de observancia que sean capaces de generar mecanismos para hacer efectiva la ley, lo que se complementa con lo expuesto por el Diputado Soto (Entrevista N°3, 2024) y Marcelo Drago (Entrevista N°6, 2024) quienes señalaron la falta de cumplimiento legal y normativo de la ley de protección de la vida privada, pero es el experto en ciberseguridad quien señala que *"la principal falencia de la ley es justamente el mecanismo de control"* (P.Viollier, Entrevista N°5, 2024), y es el primero en poner en discusión el tema de la autoridad de control que debe hacer efectiva la protección de datos personales, tal y como también lo plantean Contreras, Trigo y Ortiz, quienes aseguran que el no contar con una autoridad especifica que se encargue de velar por la protección de datos personales, retrasa el reconocimiento de este derecho fundamental, impide la exclusividad en esta materia y su aplicación efectiva (Contreras et al, 2022).

Importancia Agencia

Como ya se ha expuesto dentro de esta investigación, el mayor consenso dentro de la discusión respecto al resguardo de la privacidad y el cuidado de los datos personales, es la necesidad de contar con una autoridad y/o institución que cuente con las facultades necesarias para garantizar la protección de los datos personales, enfrentar los desafíos regulatorios y fiscalizar el cumplimiento de la ley, pero aun así dentro del proceso regulatorio que ha desarrollado Chile se ha discutido bastante sobre quién debería ocupar este lugar, tal cual se relató en el contexto, en donde se relató los distintos cambios que tuvo la autoridad.

Es por esto que se les consultó a los entrevistados, dentro del marco del Proyecto de ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, sí consideraban que la creación de esta institución pública era relevante dentro del proyecto de ley, a lo cual se repitieron respuestas en torno a lo necesario y relevante que era, a lo fundamental e ineludible de la institución, al nivel de urgencia de su instalación frente a la normativa internacional, como también una forma de proteger los derechos de los ciudadanos, tal y como se ha consagrado en distintos documentos internacionales de la ONU, de la Unión Europea, de la OIM, de la OEA y de la OCDE, principalmente.

Aun así, y tal como lo recalca el Diputado Leonardo Soto, la creación de una entidad que se encargue de la protección de datos personales en Chile es un compromiso pendiente que tiene el país con respecto a los foros internacionales (Entrevista N°3, 2024), recordando el llamado de atención que recibió Chile en el 2015 por parte de la OCDE, sobre su retraso en actualizar de la normativa de la privacidad (Alonso, 2015), que también es un hecho que incentivó a avanzar con la modificación de la Ley N°19.628, como también lo fue la puesta en marcha del Reglamento General de Protección de Datos Personales (RGPD) de la Unión Europea, el cual según el diputado Socialista es el modelo que está siguiendo Chile, en lo que se refiere a la gobernanza de los derechos y libertades que poseen las personas, junto a las obligaciones de las empresas y responsables del tratamiento de los datos (L. Soto, Entrevista N°3, 2024),

ya que tal y como plantea Benussi, el RGPD aparece para robustecer la legislación en el área de datos personales y unificar la normativa (Benussi, 2020).

Pablo Viollier, también nombra al Reglamento General de Protección de Datos como una guía para la actualización de la legislación sobre protección de datos personales en Chile, pero desde una perspectiva más utilitarista en el sentido de que sí el país cumple con ciertos niveles de autonomía y especialización, puede llegar a recibir la recomendación por parte de la UE y participar de forma resguardada del intercambio y envío de los datos personales que circulan en los países europeos y todos aquellos que también cuenten con esta certificación (Entrevista N°5, 2024), siendo Argentina y Uruguay, los únicos países latinoamericanos que cuentan con esta certificación (Agencia Española de Protección de Datos, s.f.)

Por parte de Marcelo Drago, y en relación a las experiencias internacionales, el señala cómo las distintas jurisdicciones demuestran que se requiere una agencia estatal que se ocupe de esta temática, ya que según el ex presidente del CPLT no es posible que las personas de forma individual tengan que encargarse de hacer valer sus derechos, y protegerlos (Entrevista N°6, 2024), como agrega Leonardo Soto quien considera que debe ser un órgano al servicio de los ciudadanos, en pro de sus libertades, el cual facilite el acceso a esta institución pública y logre recoger las consultas, planteamientos, controversias y resuelva, a través de una adecuada tramitación, los conflictos de naturaleza digital o jurídica que se presenten ante ella (Entrevista N°3, 2024). La anterior idea también es apoyada por Viollier, quien suma la noción de que esta institución debe entregar las herramientas necesarias para que los ciudadanos puedan apelar a nivel jurisdiccional sí así lo requieren (Entrevista N°5, 2024). Alberto Cerda, en su texto "Legislación sobre Protección de las Personas frente al Tratamiento de Datos Personales" confirma lo planteado por estos tres entrevistados y resume estas reflexiones indicando que el contar con esta autoridad, facilitaría la aplicación de las actividades antes descritas (Cerda, 2012)

Tanto el Diputado Leonardo Soto (Entrevista N°3, 2024) y el Experto Pablo Viollier (Entrevista N°5, 2024), nombran más funciones con las que debería contar la nueva Agencia,

y coinciden en que debe ser responsable de fiscalizar el cumplimiento de esta nueva normativa e interpretarla de ser necesario, como también actualizarla en el momento que surjan nuevas exigencias. Pero también el Diputado (Entrevista N°3, 2024) adscribe que es esta Agencia la que debe ser responsable de difundir la ley y otorgar sanciones severas a quienes infrinjan sus normas, lo que es compartido por Marcelo Drago (Entrevista N°6, 2024).

Es importante subrayar que tanto Daniel Pefaur (Entrevista N°1, 2023), Leonardo Soto (Entrevista N°3, 2024), Boris Barrera (Entrevista N°4, 2024), Pablo Viollier (Entrevista N°5, 2024) y Javiera Moreno (Entrevista N°7, 2024), coinciden en que el crear una nueva Agencia que garantice la protección de datos personales es el camino para que la implementación de este proyecto de ley sea expedito y exitoso, como también lo sea su respectiva regulación. El diputado Barrera agrega que se debe considerar, en la creación de la agencia, que sea una entidad autónoma (Entrevista N°4, 2024), en lo que coincide con el experto Pablo Viollier quien suma que debe ser altamente especializada, funcional y debe contar con autonomía presupuestaria, como también que sus directores deban ser electos por medio del Sistema de Alta Dirección Pública (SADP) (Entrevista N°5, 2024).

Lo anterior, respecto a la autonomía y tecnicismo de la agencia, se ajusta a la última versión del proyecto de ley, el cual establece que la Agencia de Protección de Datos Personales será una *"Corporación autónoma de derechos público, de carácter técnico, descentralizada, con personalidad jurídica y patrimonio propio"* (Cámara del Senado, 2024a, p. 100), pero no así a lo que respecto a la elección de los directores que formarán parte del Consejo Directivo de la Agencia que conducirá a esta institución, el cual será designado por el Presidente con acuerdo del Senado, solo se establece que se seleccionará de acuerdo a las normas que regulan los procesos del SADP, aquellos cargos con funciones directivas (Cámara del Senado, 2024a).

Por su parte Marcelo Drago (Entrevista N°6, 2024), según su experiencia dentro del Consejo para la Transparencia, valora la idea de contar con una Agencia, pero no necesariamente

comparte la idea de que tiene que crear desde cero, más bien considera que podría crearse dentro del CPLT, institución que él mismo señala que se encuentra en funcionamiento, cuenta con un aparataje administrativo consolidado y la experiencia suficiente para tomar está responsabilidad, pero aun así considera y declara que:

> esta ley no tendría ningún sentido sí no se crea la agencia y podemos hacer todos los cambios que se quiera al proyecto, pero sí eso no incluye una agencia con facultades sancionatorias para hacer cumplir la ley, nada de esto tiene sentido

Respecto a la facticidad de tomar esta nueva misión por parte del Consejo, Daniel Pefaur desde una mirada más técnica explica que se realizaron los cálculos en 2019, para estimar lo que significaría esta nueva función para el presupuesto de la institución y según las experiencias internacionales que mantenían estas dos responsabilidades juntas, se evidencio que los recursos debían ser mucho más de los estipulados para poder absorber esta demanda (Entrevista N°1, 2023).

En cuanto a la visión de Luis Sánchez, diputado del partido Republicano, sobre la importancia de la creación de la Agencia, apuntó que desde su bancada y a diferencia del resto de miembros de la comisión, no compartían la idea de crear una agencia completamente nueva, considerando que hay servicios públicos que ya están en funcionamiento y que podrían realizar el trabajo y abarcar esta responsabilidad, declarando que no se encuentran a favor de la expansión del estado y que existen otras prioridades, pero también agregando que en el momento en que dentro de la Comisión de Constitución se expuso la disponibilidad presupuestaria para esta institución, muchos expertos indicaron que era absolutamente insuficiente (Entrevista N°2, 2024).

La Agencia de Protección de Datos Personales a partir de los principios de la OCDE

En relación al reconocimiento de los principios que expone la OCDE dentro de (1) las Directrices sobre la protección de la privacidad y flujos transfronterizos de personales de 2013 y (2) la Declaración sobre el Acceso de los Gobiernos a los Datos Personales en Poder de las entidades del Sector Privado de 2023, se realizó una breve comparación para observar sí se acogieron a estos documentos internacionales al momento de formular la propuesta de autoridad de control e intentar materializar y llevar a la práctica las directrices y recomendaciones de la OCDE.

Para este análisis se consideró lo expuesto en entre los artículos N°30 y N°32 del Proyecto de Ley Boletín N°11144-07 y N°11092-07 (Refundidos), dentro de los cuáles se estipula el Titulo VI sobre la "Autoridad de Control en materia de Protección de Datos Personales".

Aun así es importante reconocer como dentro del Proyecto de ley, en su artículo N°3, se establecen ocho principios los cuáles deben regir el tratamiento de datos personales, los cuáles tiene una relación muy cercana a los ocho principios planteados en las Directrices sobre protección de la privacidad de la OCDE.

El proyecto de ley propone los principios de **Finalidad** (b)[16], **Calidad** (d), **Responsabilidad** (e), **Seguridad** (f) y el de **Transparencia e información** (g) (Senado, 2024a), los cuáles en sus propósitos principales cumplen con lo establecido en los principios de **Propósito específico** (3°)[17], **Calidad del dato** (2°), **Responsabilidad** (8°), **Seguridad** (5°), **Accesibilidad** (6°) (OCDE, 2013), respectivamente.

[16] Las letras al lado de cada principio dentro del Proyecto de Ley N°365, corresponde a la letra que esté mismo documento le asigna en la propuesta de ley.
[17] El número asignado a cada principio de las Directrices OCDE de 2013, corresponde al orden en el cual están expuestos dentro de este documento.

En relación a los principios expuestos en la Declaración de la OCDE 2023, el de **Objetivos legítimos** (II)[18] y **Transparencia** (V), comparten fundamentos con el principio de **Finalidad** (b) y **Transparencia e información** (g) del Proyecto de Ley.

También dentro del proyecto de ley se establece el principio de **Licitud y lealtad** (a), el cual busca limitar a los tratantes de datos, respecto a que los movimientos que realicen deben ser de manera licita y leal, apegándose a lo establecido en la normativa (Senado, 2024a), el que establece lo mismo que plantea la OCDE en su Declaración del año 2023, específico en su primer principio de Base Legal (I), que al igual que en la propuesta chilena, indica como todo este proceso debe estar resguardado bajo un marco legal, que establezca condiciones, limitaciones y fiscalización (OCDE, 2023). Pero que también, puede compararse con el primer principio de la OCDE de 2013, sobre **Recolección limitada**, el cual busca establecer parámetros para la recolección de esta información (OCDE, 2013), por lo que aunque no se relacionan fielmente entre ellos, sí buscan establecer un margen que fije hasta donde pueden realizar tratamiento de los datos recolectados. Pero también este último principio OCDE nombrado, puede vincularse con el principio de **Proporcionalidad** (c) del proyecto de ley, ya que este también establece límites frente a que, dentro del tratamiento, solo deben ocuparse los datos estrictamente necesarios y no más que esos (Senado, 2024a), el cual a su vez se parece al quinto principio de la OCDE de 2013 de **Uso limitado**, el cual establece que el uso del dato se debe establecer y respetar, como también su cuidado en razón a su no divulgación (OCDE, 2013).

Aunque no se ve una relación directa con el último principio que propone el proyecto de ley sobre la **Confidencialidad** (h), el cual busca que los tratantes de datos guarden secreto y confidencialidad sobre la información que manejan (Senado, 2024a), ni tampoco con el séptimo principio de **Participación individual** que establece la OCDE, sí se identifica un

[18] El número romano asignado a cada principio de la Declaración OCDE de 2023, corresponde al orden en el cual están expuestos dentro de este documento.

esfuerzo en general por alinearse con los estándares internacionales en esta materia (OCDE, 2023).

Además, la Agencia dentro de sus funciones establece que conforme a los principios establecidos en la ley deberá (a) "Dictar instrucciones y normas generales y obligatorias con el objetivo de regular las operaciones de tratamiento de datos personales", (d) "Determinar las infracciones e incumplimiento en que incurran quienes realicen tratamiento de datos personales, en sus operaciones de tratamiento de datos" e (i) "Prestar asistencia técnica, cuando le sea requerida (…), en la dictación y ejecución de las políticas y normas internas de estos organismos"[19] (Senado, 2024a, pp. 100-104), incluyendo de manera directa los principios de la OCDE en las responsabilidad de esta nueva institución.

Como también la Agencia, sería la institución que personificaría el principio de **Supervisión** (VI) que propone la OCDE en 2023, sobre los mecanismos que deben establecer los gobiernos para respectar los marcos jurídicos establecidos de manera imparcial y eficaz (OCDE, 2023).

Lo anterior, demuestra un esfuerzo claro por alinearse con los estándares internacionales en materia de protección de datos, en donde la Agencia sería la encargada de regular, supervisar y fiscalizar estos movimiento, y sería este servicio público el responsable de hacer efectivo el cumplimiento de estos principios.

Oportunidades y Desafíos para la Agencia de Protección de Datos en Chile

Tal y como ya se ha expuesto, la última versión del proyecto de ley que actualmente se encuentra en Comisión Mixta, establece la creación de la Agencia Nacional de Protección de Datos en Chile, por lo que se les consultó a los entrevistados cuáles serían, bajo sus perspectivas, las oportunidades y desafíos de la creación de la Agencia para la Protección de

[19] Las letras antes de las citas hacen referencia a la letra dentro del artículo N°30 bis que establece las funciones de la Agencia y las en lista.

Datos Personales en el marco de la puesta en marcha de la nueva normativa de protección de datos.

El mayor nivel de acuerdo, comenzando por las oportunidades identificadas, se presentó ante la posibilidad de tener un mayor control del tratamiento de los datos personales, como también la posibilidad de fiscalizar, y a su vez sancionar el mal uso de esta información. El Diputado Luis Sánchez, señala como el tener un mayor control del manejo de los datos en las diversas instituciones, ya sean públicas o privadas, permitirá regular la transacción de información y en lo inmediato disminuir los niveles de hostigamiento o SPAM que se recibe a través de llamadas, correos, mensajes de texto, entre otros (Entrevista N°2, 2024).

Con respecto al control se suma el Diputado Boris Barrera, señalando que una vez aprobada la creación de la Agencia, se podrá controlar y fiscalizar a todos aquellos que traten datos personales (Entrevista N°4, 2024), a lo que se suma Javiera Moreno, reconociendo la oportunidad que conlleva la fiscalización acerca de las sanciones, siendo estas últimas la consecuencia que se debe instaurar para evitar la infracción por parte de los tratantes de datos personales (Entrevista N°7, 2024).

Por su parte, Daniel Perfaur reconoce tres pilares fundamentales para el éxito en la instalación de la Agencia, los cuáles considera como oportunidades que tiene para su implementación, y son fiscalizar, garantizar y promover (Entrevista N°1, 2023), compartiendo fielmente lo expuesto por Barrera y Moreno sobre la fiscalización, pero introduciendo un concepto muy importante como lo es el "garantizar" el cual relaciona a la protección de los datos personales como un derecho, el cual en respuestas anteriores también se visibilizó (Entrevista N°4 y N°7, 2024). Lo anterior se condice a lo planteado por Warren y Brandeis en 1890, sobre la necesidad de reconocer los nuevos derechos a medida que la sociedad va cambiando (Warren y Brandeis, 1890)

El tercer pilar identificado por el Sociólogo Perfaur, habla sobre la posibilidad de la Agencia por concientizar sobre la importancia y el valor de los datos personales en la población

chilena, a través de la promoción, difusión y educación, invitando a las personas a identificar cuáles son sus datos personales y porque es relevante saber cómo y con quien los comparten (Entrevista N°1, 2023). A esto se suma la abogada especialista en datos personales Javiera Moreno (Entrevista N°7, 2024), indicando como el culturizar sobre la privacidad permitirá empoderar a los ciudadanos sobre el gran valor de su información personal y el conocimiento de que cuentan con mecanismos de protección, y podrá entregarles el valor para hacer efectivos sus derechos e interpelar ante la misma Agencia a las instituciones que pasen a llevar el uso de sus datos personales. Volviendo a lo estipulado por el autor Juan Antonio Travieso, quien comparte la visión de que a través de la educación es posible garantizar los derechos humanos y es la herramienta que se debe usar para la protección de los datos personales (Travieso, 2016).

La experta en protección de datos, ejemplifica lo anterior con el Servicio Nacional del Consumidor (SERNAC), ya que este servicio se ha posicionado como una entidad pública capaz de mediar entre las personas (consumidores) y las empresas (prestadores de servicios y/o bienes) ante situaciones en las cuáles se pasan a llevar los derechos de los consumidores, por lo que la población en general, sabe que ante un inconveniente en el proceso de compra o adquisición de un servicio puede recurrir al SERNAC para asesorarse y/o realizar el reclamo correspondiente, y conseguir una respuesta por parte del infractor. Por lo que Javiera reconoce la oportunidad de la nueva Agencia de ser el principal intermediario entre los ciudadanos y los tratantes de datos personales a través de la difusión y educación de sus principios, funciones y responsabilidades (J. Moreno, Entrevista N°7, 2024). Esto se ve reflejado en lo que se cuestiona Lindblom respecto al “control popular”, quien se cuestiona la importancia de la participación de las personas en el proceso de creación de una política pública, y se entiende que mientras haya un mayor nivel de participación, y en consecuencia, un mayor nivel de entendimiento, la política pública podrá ser más eficiente y considerada por la ciudadanía (Lindblom, 2991).

Otra oportunidad que se identifica por parte de Pablo Viollier es el iniciar desde cero, considerando que es una nueva institución, la Agencia de Protección de Datos Personales no

cuenta con una gestión previa, con actividades ya realizadas, ni con una inercia institucional preexistente, lo que a cuenta del abogado, le permitirá a la Agencia abordar esta difícil temática de forma tranquila sin la presión de mejorar una gestión anterior. El experto nombra como esto no hubiera sido posible de ser entregada esta responsabilidad al Consejo para la Transparencia, ya que podría empañar su buena evaluación, o también dificultar su ya asentada gestión, y utiliza la expresión "presente griego"[20] para referirse a lo que hubiera significado la APDP al integrarse al Consejo (Entrevista N°5, 2024).

Se destaca al Reglamento General de Protección de Datos de la Unión Europea como un documento que se ha posicionado alrededor del mundo, ya que ha impactado tanto en la administración pública, como en las entidades privadas, manteniendo su objetivo de proteger y regular el tratamiento de los datos personales, pero sin detener el intercambio de la información, tal y como lo señalan Rojas y López en su texto "El impacto del RGPD en el ámbito del control laboral y la era de la innovación" en 2018, lo que también reconocieron Leonardo Soto (Entrevista N°3, 2024) y Pablo Viollier (Entrevista N°5, 2024) los cuáles lo consideran la principal guía para nuestro país, dentro del proceso de garantizar el derecho a la privacidad.

Marcelo Drago se suma a esto, indicando como este documento ya cuenta con seis años de aplicación, los cuáles pueden orientar la implementación de la Agencia en Chile, agregando que nos encontramos en *"un futuro que ya pasó"* (M. Drago, Entrevista N°6, 2024), refiriéndose a que ya existe jurisprudencia en otros países, de las cuales se puede nutrir a la Agencia para responder a los casos que se presenten a nivel nacional, como también para adelantarnos e incluir en nuestra legislación y aplicación temáticas que en su momento no fueron abordadas por el RGPD o considerados en otras recomendaciones internacionales (Entrevista N°6, 2024).

[20] La expresión "presente griego" se utiliza para referirse a los regalos o presenten que traen más problemas que beneficios a quien son entregados, y Pablo Viollier lo utiliza para referirse lo que hubiera significado para el Consejo para la Transparencia el ingreso de la protección de datos a sus funciones y responsabilidades.

Aun así, lo anterior es demasiado complejo y Viollier lo identifica de inmediato como un desafío, el cual tiene que ver con lo disruptiva que es la tecnología y como el avance de esta misma requieren que el aparato estatal que se haga cargo de esta materia debe ser una institución dinámica, capaz de adaptarse rápidamente a la evolución de los nuevos medios digitales y las nuevas necesidades respecto al tráfico de datos personales. El experto en ciberseguridad nombra como la Agencia hubiera tenido distintas necesidades en una época pasada, en donde el uso del internet no era tan masivo, ni existían redes sociales, pero también como la regulación se deberá adaptar de manera fugaz a la Inteligencia Artificial y sus peligros, frente a la privacidad de las personas (Entrevista N°5, 2024). Se suma a esto el funcionario del CPLT, quien considera que la Agencia debe generar un modelo que no trabaje de forma lineal, sino que, aprovechando la tecnología disponible y sea capaz de mutar y absorber los desafíos venideros (D. Pefaur, Entrevista N°1, 2023). Boris Barrera, de forma semejante, reconoce como desafío para la Agencia el prevenir y anticiparse a nuevos delitos, nuevas formas de manejos de datos y no solo arreglar los problemas ya identificados, ya que el considera que al responsabilizarse solo de un tema específico, debería ser capaz de desarrollar mecanismos que le permitan a esta institución actuar de forma preventiva y no solo de manera reactiva (Entrevista N°4, 2024).

De forma complementaria, el ex Presidente del CPLT individualiza la oportunidad de que, al contar con países con jurisprudencia en la materia y años de implementación, se puede tomar esa experiencia previa y adaptarla a la realidad chilena y en específico en la implementación de la nueva institucionalidad de protección de datos personales (M. Drago, Entrevista N°6, 2024). A esto se suma la experta en el Reglamento General, Javiera Moreno Andrade, quien también considera importante tomar atención a otras experiencias, pero resalta la oportunidad que tiene Chile de generar un organismo especializado, que considere una organización interna con expertos en la materia y con una autoridad que tenga conocimiento y competencias técnicas en el área, lo que permitiría entregar una respuesta expedita y confiable ante una temática tan específica, pero a la vez tan común y cotidiana (Entrevista N°7, 2024).

Lo anterior, es reconocido como un desafío desde la perspectiva Marcelo Drago, ya que consideran que existe muy poca masa crítica sobre protección de datos en Chile, planteando el desafío de generar más expertos en la materia o atraerlos a trabajar en el sistema público (Entrevista N°6, 2024).

Y a su vez, Pablo Viollier tampoco considera como una oportunidad la idea de que la agencia se constituya sólo por expertos en protección de datos, ya que esto se vuelve un reto al considerar el presupuesto limitado con el cual se cuenta, el que además de costear la instalación de esta nueva entidad, debe financiar todos los insumos y materiales necesarios para el desempeño de las tareas de los funcionarios, lo anterior sin considerar que sí se piensa tener un aparataje institucional profesionalizado y especializado en esta temática, no bastará con tener a los mejores abogados, sí no que también se requerirán profesionales ligados a la informática y área digital, que sean capaces de levantar sistemas computacionales y expertos de última generación que estén calificados para identificar falencias y mejoras en los sistemas de almacenamientos de datos personales, como para que también puedan fiscalizar los sistemas de empresas como Google, Meta y Apple, por solo nombrar algunas de las grandes compañías internacionales que hacen uso y abuso de la información privada, a través de algoritmos, los cuáles el cuerpo técnico de la Agencia debería ser capaz de descifrar y manejar (Entrevista N°5, 2024).

Respeto al desafío económico evidenciado por Pablo Viollier, se adhiere Javiera Moreno, recordando que se generará una gran discusión en torno a la formulación y distribución presupuestaria de este nuevo servicios (entrevista N°7, 2024), y Daniel Pefaur reconoce que se requerirá de mucha creatividad y uso de tecnología para encontrar un diseño pertinente que se adecue a los limitados recursos con los cuales se contará para cumplir con la labor encomendada (Entrevista N°1, 2023).

En contraposición aparece el Diputado Luis Sánchez, quien se contrapone a lo inmediatamente antes expuesto, en relación al desafío presupuestario identificado, ya que el

político plantea que el verdadero desafío es cumplir con las responsabilidades y funciones de la APDP con los recursos humanos que ya están disponibles, lo cual sería factible siempre y cuando estos se aprovechen de manera eficiente, ya que bajo la mirada de Sánchez la administración pública cuenta con un gran presupuesto, el cual debería alcanzar para absorber esta nueva responsabilidad (Entrevista N°2, 2024).

Otro desafío identificado por el Diputado Luis Sánchez es la atención eficaz a la fiscalización y al control que debe haber por parte de la Agencia, poniendo en discusión el cómo será la organización interna que tendrá este servicio y cómo definirá sus procesos burocráticos (Entrevista N°2, 2024), por los cuáles también muestra preocupación Daniel Pefaur, quien expone como desafío el orden, la estructura y el modelo de la institución que se emplea alrededor de las funciones que se le han encomendado a la Agencia (Entrevista N°1, 2023).

Respecto al proceso de estructuración de la Agencia de Protección de Datos Personales es importante destacar el modelo de vertientes múltiples de Kingdon (1995), ya que este plantea como en la medida que las personas consideren que se debe realizar un cambio, las condiciones de la solución del problema mejoran, es por esto que dentro de la organización interna de la agencia y sus funciones deben incluir la educación y la difusión, ya que así se fortalecerá a la población y será capaz de exigir mejoras en lo que respecto a esta temática, siendo también un desafío identificado por Javiera Moreno, específicamente en lo que tiene que ver con el empoderar a la ciudadanía en este tópico (Entrevista N°7, 2024).

Recordando que uno de los mayores problemas es la falta de conocimiento por parte de las personas, sobre todo respecto al uso del internet, quienes al no manejar los conceptos, muchas veces ponen a disposición su información personal y no identifican el nivel de vigilancia que existe en los sitios webs, tal y como lo plantea el autor Juan Antonio Travieso en su texto “Protección de Datos Personales y Tecnología, en busca del paraíso” (2016).

Respecto a la estructura que tendrá la nueva institución, el experto Pablo Viollier, identifica un nuevo desafío, respecto a la dependencia de la Agencia de Protección de Datos, situando

el desafío en respetar la máxima de que sea una institución totalmente autónoma e independiente, que no dependa ni administrativa ni presupuestariamente de algún órgano público ya existente, para evitar futuros conflictos y posibles presiones, como también imposición de directrices (Entrevista N°5, 2024). Lo anterior, es prácticamente imposible, ya que la propuesta legislativa que se encuentra dentro de sus últimas etapas de tramitación, establece que esta institución se relacionará con el Presidente a través del Ministerio de Economía, Fomento y Turismo, quien además será la institución que dispondrá, mediante decreto supremo, de la aprobación de los estatutos de la Agencia, dentro de los cuales se establecerán las normas de funcionamiento de esta nueva institución, los cuales además deben ser enviados de forma previa al Presidente de la República, y el mismo procedimiento aplicará para las posibles modificaciones que sufran los estatutos. Sin considerar que, además la Agencia dependerá presupuestariamente del Ministerio, por lo menos, en su primer año de implementación (Senado, 2024a).

Es así, como esta institución deberá generar mecanismos de coordinación con distintas organizaciones, tanto públicas como privadas, destacando la relación que deberá mantener con el Consejo para la Transparencia, la cual preocupa a Daniel Pefaur (Entrevista N°1, 2023) y Leonardo Soto (Entrevista N°3, 2024), quienes coinciden que uno de los principales desafíos de la Agencia será no contradecirse con el Consejo, considerando que la visión de este último es *"liderar el resguardo de la transparencia y el derecho de acceso a la información en Chile con criterios de legalidad, oportunidad y responsabilidad"* (Consejo para la Transparencia, s.f.), y el objetivo con el cual se crea la Agencia de Protección de datos es el *"velar por la efectiva protección de los derechos que garantizan la vida privada de las personas y sus datos personales (...)"* (Senado, 2024a), los cuáles pueden llegar a enfrentarse ante situaciones en la cual no haya coincidencia y se requiera una entidad mediadora o mecanismos superiores de resolución.

El proyecto de ley (2024), en su artículo 31, incluye la Coordinación regulatoria con el Consejo para la Transparencia, y busca generar *"coordinación, cooperación y colaboración entre ambos órganos"* (Senado, 2024a, p. 117), en cuanto se presente la necesidad, de alguna

de las dos instituciones, de dictar una instrucción o norma de carácter general y obligatoria, la cual pueda tener efectos en los ámbitos de competencias de la otra, deberá remitir un informe para evitar posibles conflictos de norma.

Daniel Pefaur agrega que, un gran desafío para la Agencia será desarrollar el trabajo y la relación con el mundo privado (sobre el flujo que mantienen de datos personales), ya que como se destacó más arriba, a diferencia de las entidades privadas, en el sector público ya existe una noción de la protección de datos personales, en cambio en el sector privado se desconoce, ya que no existe una obligación para que ellos regulen sus tratamientos, aun así y para incidir, Daniel indica que el desafío más allá de fiscalizar, es el incidir en su comportamiento (Entrevista N°1, 2024). Javiera Moreno se une a lo expuesto por Daniel, ya que identifica que un desafío se encuentra en responsabilizar a las instituciones, a los proveedores y a las empresas, respecto al uso de información privada, e influir en ellas para lograr que adapten sus procesos y conseguir desde dentro un cambio en el tratamiento de los datos personales y en sus respectivos compliance[21]. Lo anterior además considerando que, principalmente para las empresas, los datos son un negocio (Entrevista N°7, 2024).

Un intento, dentro del proyecto de ley que crea la Agencia de Protección de Datos Personales, por incidir en el comportamiento de las instituciones tratante de datos personales, y su vez de designarles esta labor, es la creación de la figura del "Responsable de datos", figura que puede ejercer una persona natural o jurídica, pero que se vuelve la persona encargada de las decisiones respecto a los fines y medios con los cuales, y en los cuales, se trataran los datos personales que están en su posesión (Senado, 2024a), lo anterior con el objetivo de tener a quien imputar todas las acciones relacionadas con el uso de la información privada, y será quien tenga que dar cuenta, de ser necesario, ante la Agencia.

[21] El término "compliance", o en español "cumplimiento normativo", es definido como "*las normas para la lucha contra la corrupción en todas sus formas, el lavado de activos y el financiamiento del terrorismo. También se debe prestar atención a las cuestiones referidas a actividades de lobby, antimonopolio y protección de datos personales*" (Accifonte, 2019, p. 26).

A lo anterior se refiere Leonardo Soto (2024) en su entrevista, respecto a las posibles ventajas que, dentro de un proceso sancionatorio, las instituciones podrían llegar a tener, sí además de contar con un responsable de datos, demuestran trabajar con un modelo preventivo de cumplimiento de la normativa, en donde el responsable de datos no solo sea la cara visible en esta temática, sí no más bien supervise y guie a la empresa en la protección de datos personales, y así puedan optar a atenuantes e incluso a la eliminación de sanciones, lo que promovería el *"compliance en materia de protección de datos personales"* (L. Soto, Entrevista N°3, 2024). El incentivar la prevención, por sobre el castigo, lograría posicionar a la agencia como una entidad formadora, a la cual consultar respecto a la importancia de la protección de datos personales, y no generar un miedo respecto a los riesgos de la sobre exposición de la información privada (D. Pefaur, Entrevista N°1, 2023), como también para que, en el momento que se conozca o transparente el tráfico de datos, que es un desafío identificado por Boris Barrera, sirva para concientizar más que inquietar a la población (Entrevista N°4, 2024), siendo relevante aun así, que la Agencia se situé como una autoridad importante, la cual sea capaz de posicionarse frente a las empresas, fiscalizar sin miedo a una represalia y sancionar cuando se requiera, *"con multas que sean lo suficientemente ejemplificadoras"* (J. Moreno, Entrevista N°7, 2024).

Finalizando la individualización de desafíos para la Agencia de Protección de Datos Personales de Chile, se identifica la falta de jurisprudencia nacional para emplear por parte de esta nueva institución, ya que a pesar de que más arriba, Marcelo Drago consideró como una oportunidad el contar con jurisprudencia internacional, fueron varios entrevistados quienes se inquietaron ante esta carencia, donde el mismo expresidente del CPLT dejo en claro que puede tener un gran costo la curva de aprendizaje por partir desde cero (Entrevista N°6, 2024), y Pablo Viollier, tomándose de esto mismo, indica que el partir desde cero también implicará el crear y formar todos los criterios sin un modelo previo. Y dentro de esta misma línea el Diputado Leonardo Soto agrega que se deberán apegar a lo establecido en la ley y los distintos principios internacionales, y utilizarlos como fuentes de ley para los casos particulares y controversias que se produzcan, quedando como desafío para la agencia y sus

autoridades el ver los casos delicados, en los cuáles se deberá generar el criterio para interpretarlos de manera correcta y así ir generando jurisprudencia propia (Entrevista N°3, 2024).

Con el objetivo de sintetizar las oportunidades y desafíos identificados se elaboró una tabla resumen:

N°	OPORTUNIDADES	DESAFÍOS
1	Garantizar y promover el derecho a la protección de datos personales de las personas.	Coordinación y relación con stakeholders
2	Concientizar sobre la importancia y el valor de los datos personales en la población.	Organizar el funcionamiento interno de la Agencia.
3	Controlar, fiscalizar y sancionar el mal uso y tratamiento de los datos personales.	Generar un plan de prevención del mal uso de Datos Personales.
4	Iniciar desde cero.	Poseer un presupuesto limitado.
5	Contar con experiencia y jurisprudencia internacional previa.	Concientizar sobre la importancia y el valor de los datos personales en la población.
6	Organizar el funcionamiento interno de la Agencia.	Crear jurisprudencia a nivel nacional.
7	Generar un plan de prevención del mal uso de Datos Personales.	Transparentar situación actual sobre el tratamiento de Datos Personales.
8		Controlar, fiscalizar y sancionar el mal uso y tratamiento de los datos personales
9		Iniciar desde cero.
10		Falta de expertos

Conclusiones y propuestas

La presente investigación, también conocida como AFE, abordo de manera integral el contexto chileno respecto a la protección de datos personales, y en específico sobre la propuesta de la autoridad de control que se propone instaurar con el Proyecto de Ley (Boletín N°11.144-07), el cual además busca actualizar la vigente ley sobre Protección de la Vida Privada, y poder dar cumplimiento a las exigencias internacionales respecto a la protección de la información de las personas.

El objetivo principal de este trabajo fue "analizar oportunidades y desafíos para la implementación de la Agencia Nacional de Protección de Datos Personales (APDP) que propone el Proyecto de Ley 11.144-07 que regula la protección y el tratamiento de Datos Personales en Chile, desde la primera moción en la Cámara del Senado (2017) hasta la actualidad, en relación a los principios de protección de datos de la OCDE"

La investigación se realizó con un enfoque analítico y comparativo, bajo un enfoque estrictamente cualitativo, ya que se privilegió la experticia de actores y expertos relevantes en esta temática, con el fin de poder analizar la propuesta que se encuentra en discusión en el Congreso. Considerando a su vez que los distintos punto de vista estudiados, permiten plasmar distintas perspectivas, lo que fue útil para contraponer sus ideas y poder identificar las dificultades y/u obstáculos presentes en el Proyecto de Ley.

Por otro lado, se examinaron de manera detallada múltiples documentos normativos, legislativos y periodísticos, como también convenios y recomendaciones internacionales ligados a la protección de datos personales, dentro de los cuáles el central fue el citado Proyecto de ley, en tercer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales redactado por la Cámara de Senado de Chile, junto a las Directrices sobre la protección de la privacidad y flujos transfronterizos de personales de 2013 y la Declaración sobre el Acceso de los

Gobiernos a los Datos Personales en Poder de las entidades del Sector Privado de 2023, ambos documentos de la OCDE.

El enfoque de esta investigación, al ser de tipo descriptivo e interpretativo, permitió pesquisar las características, propiedades e implicancias de los anteriores documentos y evidenciar elementos claves, para valorarlos respecto de los principios internacionales establecidos por la Organización para la Cooperación para el Desarrollo Económico, su alineación ante estos y lo demandado por la situación actual respecto al uso de tecnologías digitales, las cuáles ponen en peligro el uso de los datos de la personas y el cuidado del derecho a la autodeterminación informativa, sí es que no se cuenta con una normativa que regule estas transferencias. A su vez, el realizar este trabajo bajo este tipo de investigación, fue útil para identificar con precisión las diferentes dimensiones de esta temática, frente a la ciudadanía.

La metodología utilizada permitió un análisis profundo y sistemático, a través de un abordaje riguroso, el cual fue esencial para la recolección de testimonios a través de las entrevistas realizadas y se permitió generar recomendaciones informadas y reconocer la importancia de estas temáticas, que por su naturaleza se desarrollan en un campo totalmente dinámico y de constante cambio, a una velocidad muchas veces mayor a la capacidad de respuesta normativa e institucional.

El proyecto de ley de Chile, que aún se encuentra en discusión en el Congreso Nacional, refleja un esfuerzo consciente por alinear las prácticas nacionales con los estándares internacionales establecidos por la OCDE, los cuales destacan la importancia de la privacidad de los datos personales y la concientización sobre su tratamiento. Lo anterior desde el establecimiento de principios como el límite en la recolección de información, la determinación de su uso y su propósito, asimismo la mantención en la calidad y veracidad del dato, como también la seguridad, accesibilidad y responsabilidad dentro del procesamiento de la información.

Este esfuerzo, a su vez, da respuesta a la tendencia universal por el empoderamiento de las personas sobre su información personal, lo que además de mejorar la protección, genera una concientización y educación sobre los derechos de los datos personales y su valor. Por lo que la educación, junto a la sensibilización y la humanización de esta temática, se vuelven desafíos claves para la efectividad del marco legal, ya que sí contamos con una ciudadanía educada en sus derechos y obligaciones, contamos con una ciudadanía capaz de trabajar por el cuidado de su información ante las entidades tratantes, como ante la misma Agencia, permitiendo que este proyecto de ley se situé como relevante y no como otra regulación más.

Por otro lado, y reconociendo que estos principios están pensados en todo tipo de instituciones, públicas y privadas, de cualquier tamaño y de todos los rubros, la OCDE en 2023 suma siete nuevos principios, los cuáles se centran en regularizar el tratamiento de datos personales entre instituciones públicas y privadas, ya que como se discutió dentro de esta investigación, existen varios limites en esta relación y en sus respetivos modelos de funcionamiento, pero aun así es evidente y sobre todo en esta materia, que deben realizarse esfuerzos por mantener un nivel de cooperación y coordinación entre ambos sectores, para hacer efectivo el resguardo de este derecho. Lo anterior, se refleja dentro del proyecto de ley, el cual muestra indicios de desarrollar sistemas de colaboración y concientización para lograr cooperación desde el sector privado, pero también incluye las medidas de seguridad apropiadas y proporcionales respecto al tratamiento de datos personales. Como también incluye la definición clara de los objetivos con los cuáles se pueden realizar procesamiento de los datos, requisitos para la aprobación previa y los principios por los cuáles se regirá la ley.

Respecto a la Agencia

La configuración y puesta en marcha de la Agencia de Protección de Datos Personales en Chile representa un paso significativo hacia el fortalecimiento de la privacidad y la seguridad de la información privada y personal de los ciudadanos chilenos, como de todos aquellos que

viven en el país y quienes lo visitan. Es un hito crucial para el proceso del proyecto de ley, que busca actualizar la ley sobre protección de la vida privada, poder contar con la autoridad de control, la cual expertos y autoridades señalan como indispensable en el proceso de protección de la información, y es esencial para conseguir un procesamiento responsable y seguro de los datos personales y sensibles, así como lo plantean las recomendaciones internacionales, bajo un estándar nacional coherente y armonizado.

La Agencia propuesta tendrá la capacidad, no solo de monitorear la aplicación de la ley, sí no también fiscalizar y sancionar a los posibles infractores y establecer una regulación eficiente y transparente, la cual concentre las solicitudes, reclamos y disputas de los ciudadanos, lo que permitirá garantizar una aplicación uniforme y rigurosa de la ley y generar una jurisprudencia propia pertinente a la realidad chilena, que facilitará construir un entorno de confianza y seguridad para los ciudadanos, ciudadanas y responsables de datos. Lo anterior, cumpliendo su objetivo principal el cual es mejorar la protección de los datos personales de las personas, junto a al ejercicio de sus derechos.

La investigación revelo, que sí bien hay un camino prometedor hacia la conformación de la Agencia y la adopción de sus principios, también emergen desafíos significativos. Estos incluyen la autonomía y eficacia de la Agencia, equilibrar la protección de datos con otros derechos e intereses públicos y adaptar las prácticas de protección de datos a un panorama tecnológico en rápida evolución. Si estos desafíos no se abordan adecuadamente podrían comprometer el éxito de esta política pública y la confianza de la ciudadanía en el sistema.

Esta investigación fue elaborada con el objetivo de contribuir a la discusión sobre la protección de los datos personales en Chile, dejando abierto el debate más allá de lo jurídico y centrado en lo administrativo e institucional que se materializa a través de la Agencia de Protección de Datos Personales, pero también incorporando en la discusión el enfoque de los Derechos Humanos, en este caso la necesidad de consagrar y proteger nuevos derechos que se van emergiendo con la evolución contante de las personas como de las tecnologías.

La creación de una nueva institucionalidad estatal es constituye desafíos complejos, los cuáles van ligados al proceso de implementación y adaptación, pero que sí se reconocen de forma oportuna pueden garantizar el mejoramiento significativo de la realidad actual y en este caso respecto a la protección de los datos personales. Aun así, el hecho de identificar desafíos claros, no significa que no existan múltiples oportunidades estratégicas para comenzar desde la aprobación de la ley a avanzar en el cuidado de la privacidad y la seguridad de los datos, como lo es guiarse por los estándares internacionales y tomar las experiencias previas para poder adelantarse a temáticas emergentes, que en un futuro influirán en esta materia. Por lo que sí se toman estas oportunidades desafiantes pueden tener un impacto positivo y duradero en la sociedad chilena.

La Agencia y su éxito dependen de la implementación práctica y de su continua evolución, por lo que sí su gestión permite asegurar los principios de protección de datos personales como realidades funcionales, y no solo como ideales, Chile puede llegar a posicionarse nuevamente como un país avanzado en esta temática y garantizar el derecho a la privacidad y autodeterminación informativa de todas y todos los ciudadanos.

Sin duda a futuro se requerirá la evaluación del funcionamiento de está institucionalidad que permita medir y evaluar su nivel de respuesta ante esta problemática, como también se vuelve relevante e interesante observar la interacción que tendrá con las tecnologías emergentes como el big data o la inteligencia artificial, especialmente lo atingente a aspectos éticos del uso de estas tecnologías en el día a día de la ciudanía.

Recomendaciones:

A continuación se materializa un listado que resume las recomendaciones que se proponen, a partir de esta investigación, para tener una exitosa implementación de la Agencia de protección de datos personales, las cuáles permite maximizar las oportunidades y recoger los desafíos y así lograr que se reconozca a Chile como un país seguro dentro de esta temática:

1) **Robustecer la autonomía de la Agencia:** reconociendo que en el papel tiene cierto nivel de independencia, es importante considerar lo expuesto respecto a los posibles conflictos de interés que pueden generarse con el Ministerio de Económica, como también con el resto de instituciones públicas, por lo que es esencial orientar el trabajo de la Agencia a implementar mecanismo de gobernanza transparente, instaurar procesos claros y justos para la selección y nombramiento de sus autoridades y miembros, como también garantizar un presupuesto acorde a las necesidades de esta institución, que le permita funcionar de manera efectiva y autónoma.
2) **Adaptabilidad tecnológica y técnica:** con el objetivo de mantener una normativa vigente, relevante y efectiva, es necesario que la Agencia y su marco legal sean constantemente revisados y actualizados, junto al equipo que conforma a la institución, los cuáles deben ser capacitados continuamente, para dar respuesta a la evolución digital.
3) **Educación, concientización y difusión:** es importante generar una cultura alrededor de la protección de datos personales y asegurar que la ciudadanía y las distintas organizaciones, comprendan la importancia y el valor de su información privada, como también conozcan sus derechos asociados y sus obligaciones respecto a la nueva legislación. Es por esto que se vuelve estrictamente necesario crear campañas y/o instancias de sensibilización, pensadas en los distintos niveles, para que se logre una concientización integral a nivel nacional.
4) **Creación de canales de comunicación efectivos:** dentro de una realidad tecnológica y digital, la Agencia debe ser capaz de instaurar medios de comunicación directos y eficaces, para las personas (dueñas de sus datos), como para las entidades que manejan datos personales, lo anterior con el objetivo de mantener un dialogo y feedback constante, para la colaboración y conocimiento de lo que está pasando, como también para resolver dudas y conflictos, y entregar las herramientas suficientes para hacer uso de la información de manera segura y consciente.

Bibliografía

Accifonte, A. (2019). Compliance en América Latina. Programa de Contaduría Pública; Sesión invitados Contextos internacionales. Pp 23-39. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/9106/Compliance-AulaContable5.pdf?sequence=1&isAllowed=y

Agencia Española de Protección de Datos. (s.f). ¿Qué países consideran con un nivel adecuado a efectos del artículo 45 del RGPD?. Transferencias internacionales. Transferencias internacionales, BCR y Códigos de Conducta. Preguntas frecuentes. https://www.aepd.es/preguntas-frecuentes/6-transferencias-internacionales-bcr-codigos-de-conducta/1-transferencias-internacionales/FAQ-0605-que-paises-se-consideran-con-un-nivel-adecuado-a-efectos-del-articulo-45-del-rgpd

Alonso, C. (23 de julio de 2015). OCDE envía carta de advertencia a Chile por retraso en protección de datos personales. *Pulso - La Tercera.* https://www.latercera.com/pulso/ocde-envia-carta-de-advertencia-a-chile-por-retraso-en-proteccion-de-datos-personales/

Álvarez, D. (2016). Acceso a la Información Pública y Protección de Datos Personales. ¿Puede el Consejo para la Transparencia ser la Autoridad de Control en Materia de Protección de Datos?. *Revista de Derecho Universidad Católica del Norte, 23*(1), 51-79. https://www.scielo.cl/pdf/rducn/v23n1/art03.pdf

Asamblea General de las Naciones Unidas [AG]. (1990). *Principios rectores para la reglamentación de los ficheros computadorizados de datos personales*. Resolución 45/95. http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf

Bhatt, G. (2001). Knowledge management in organizations: examining the interaction between technologies, techniques, and people. *Journal of Knowledge Management, 5*(1), 68-75. https://doi.org/10.1108/13673270110384419

Benussi, C. (2020). Obligaciones de seguridad en el tratamiento de datos personales en Chile: escenario actual y desafíos regulatorios pendientes. *Revista chilena de derecho y tecnología*. Vol.1 No.9 https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000100227#fn93

Biblioteca del Congreso Nacional de Chile [BCN]. (2018*). Historia de la Ley N°21.096 Consagra el derecho a protección de datos personales.* https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/vista-expandida/7551/#h1_1_1

Bobbio, N. (1985) Estado, Gobierno y Sociedad, Por una teoría general de la política. *Fondo de Cultura Económica.*

Boletín de indicaciones N°183-369. (2021). Formula indicaciones al Proyecto de Ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de protección de datos personales (Boletines N° 11.144-07 y 11.092-07, refundidos).

Boletín N°11.992-07. (2017). Proyecto de ley, iniciado en moción de los Honorables Senadores señores Harboe, Araya, De Urresti, Espina y Larraín, sobre protección de datos personales.

Boletín N°11.144-07. (2017). Proyecto de ley, iniciado en mensaje de S. E. la Presidenta de la República, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Mensaje N°001-365.

Canedo, S. (2009). *Contribución al estudio del aprendizaje de las ciencias experimentales en la educación infantil: cambio conceptual y construcción de modelos científicos precursores.* [Tesis doctoral. Universidad de Barcelona] Repositorio Dipòsit Digital de la Universitat de Barcelona. https://www.tdx.cat/bitstream/handle/10803/1321/03.SPCI_CAPITULO_III.pdf;jsessi

Cámara de Diputados de Chile. (2016). *Evaluación de la ley Nº19.628 Protección de la Vida Privada*. Comisión evaluación de la ley/OCDE Cámara de diputados Chile. Departamento de Evaluación de la Ley.

Cámara del Senado de Chile. (2019). *Comisión aprueba que Consejo para la Transparencia se haga cargo de la protección de datos personales*. https://www.senado.cl/comision-aprueba-que-consejo-para-la-transparencia-se-haga-cargo-de-la/senado/2019-08-05/181431.html

Cerda, A. (2012). Legislación sobre Protección de las Personas frente al Tratamiento de Datos Personales.

Comisión Europea. (2018). La protección de datos en la UE. *Protección de datos*. [en línea] https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es [Consulta: 15 de enero de 2024].

Comité de los Derechos Humanos de las Naciones Unidas [OACDH]. (1988). *Observación General N°16, Comentarios generales adoptados por Comité de los Derechos Humanos, Artículo 17 – Derecho a la intimidad, 32° período de sesiones, U.N. Doc. HRI/GEN/1/Rev.7 al 162*. http://hrlibrary.umn.edu/hrcommittee/Sgencom16.html

Conde, C. (2005). *La protección de Datos Personales: Un derechos autónomo con base en los conceptos de intimidad y privacidad*. Editorial DYKNSON.

Contreras, P. et al (2022). Un sistema fragmentado: La protección sectorial de los datos personales en Chile. Revista de Derecho Administrativo Económico, No. 35, pp. 35-64.

Datos Protegidos. (18 de mayo de 2015). OCDE: la deuda de Chile con la protección de los datos personales. *Noticias.* https://datosprotegidos.org/ocde-la-deuda-de-chile-con-la-proteccion-de-los-datos-personales/

Datos Protegidos. (2 de diciembre de 2020). Especialistas denuncian abandono del Estado en ciberseguridad. *Ciberseguridad.* https://datosprotegidos.org/especialistas-denuncian-abandono-del-estado-en-ciberseguridad

Datos Protegidos. (4 de diciembre de 2020). Hackeo a Cencosud: Fundación Datos Protegidos comprueba filtración que la compañía insiste en desmentir. *Ciberseguridad*. https://datosprotegidos.org/hackeo-a-cencosud-fundacion-datos-protegidos-comprueba-filtracion-que-la-compania-insiste-en-desmentir/

Davenport, T. & Prusak, L. (1998). Working Knowledge: How Organizations Manage What They Know. Harvard *Business School Press*. https://www.researchgate.net/publication/229099904_Working_Knowledge_How_Organizations_Manage_What_They_Know

Díaz, S. et al(2011). Una guía para la elaboración de estudios de caso. *Razón y Palabra* (75). https://www.redalyc.org/articulo.oa?id=199518706040

Domínguez, C. (2009). Ventanas de oportunidad y coaliciones de política pública: el caso del proyecto para un nuevo aeropuerto en la ciudad de México desde una perspectiva histórica. *Secuencia* (79), 63-88.

Entel. (2022). *Tráfico de datos aumentó 34% a nivel nacional durante 2021*. https://entel.modyocdn.com/uploads/bc2e5dfb-b961-41f5-9682-c670f6d2b063/original/COM_General_de_tra_fico_de_datos.pdf

Espinosa, M. (10 de marzo de 2021). *Herramientas digitales orientadas a la investigación en ciencias sociales y humanidades: criterios para su selección*. Hypotheses. https://bdcv.hypotheses.org/3606

Espuny, M. (2020). *Introducción al análisis digital: qué es y cómo se hace*. Agencia COMMA. https://agenciacomma.com/analisis-de-datos/analisis-digital-que-es-y-como-se-hace/

European Court of Human Rights. (1950). Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales. *Tribunal Europeo de Derechos Humanos.* https://www.echr.coe.int/documents/d/echr/convention_spa

Fernández, R. (2001). La entrevista en la Investigación cualitativa. *Revista Pensamiento Actual*, 2(3), 14-21.

Fontana, A. & Frey, J. (2005). The Interview: From Neutral Stance to Political Invovement. http://www.cl.aoyama.ac.jp/~dias/pdfs/interview.pdf

Fossa, L. & Solís, C. (10 de septiembre de 2020). Querella confirma que Banco Estado ya había sufrido grave ataque cibernético en junio. *Interferencia*. https://interferencia.cl/articulos/querella-confirma-que-bancoestado-ya-habia-sufrido-grave-ataque-cibernetico-en-junio

Gálvez, C. (9 de junio de 2018). Banco de Chile confirma que ataque informático de mayo robó US $10 millones. *Emol.* https://www.emol.com/noticias/Economia/2018/06/09/909234/Banco-de-Chile-confirma-que-ataque-informatico-de-mayo-robo-US-10-millones.html

García, M. et al (2018). *Ciberseguridad: un enfoque desde la ciencia de los datos.* Editorial Universidad Icesi. https://repository.icesi.edu.co/biblioteca_digital/bitstream/10906/84046/3/navarro_ciberseguridad_ciencia_2018.pdf

Gobierno de Chile. (2015). *Agenda Digital 2020. Chile Digital para Tod@s*. https://www.alejandrobarros.com/wp-content/uploads/old/Agenda_Digital_2015-2020_Bachelet_.pdf

Gobierno de Chile. (2017). *Política Nacional de Ciberseguridad.* Comité Interministerial sobre Ciberseguridad.

Gobierno de Chile. (2019). Agenda de Modernización del Estado. Presidencia, Ministerio de Hacienda y Ministerio Secretaría General de la Presidencia.

Gobierno de Argentina. (s.f.). *AAIP: Monitoreamos el desempeño de la transparencia en la gestión, el acceso a la información y la protección de datos personales.* [en línea] https://www.argentina.gob.ar/aaip [consultado : 15 de enero de 2024].

Gobierno de Argentina. (15 de enero de 2024). Argentina logró la nueva adecuación por parte de la Unión Europea para el flujo internacional de datos personales. [En línea] https://www.argentina.gob.ar/noticias/argentina-logro-la-nueva-adecuacion-por-parte-de-la-union-europea-para-el-flujo

Herder, P. et al (2003). Follow the rainbow: knowledge management framework for new product introduction. *Journal of Knowledge Management, 7*(3). https://doi.org/10.1108/13673270310485668

Hernández, A. (2017). *Ciberseguridad y Confianza en el ámbito digital*. ICE. *El Cambio Digital en la Economía, un Proceso Disruptivo N.º 837.* http://www.revistasice.com/index.php/ICE/article/view/1946/1946.

Hobbes, T. (1640). Elements of law, natural and politic: part I, Human nature, part II, De corpore politico; with Three lives Oxford; New York; Oxford University Press.

Information Commissioner's Office [ICO]. (s.f). Who we are. *About the ICO.* https://ico.org.uk/about-the-ico/who-we-are/
[Consultado: 25 de enero de 2024]

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos [INAI]. (s.f.). ¿Qué es el INAI?. *Conócenos*. [en línea] https://home.inai.org.mx/?page_id=1626 [consultado: 15 de enero de 2024].

Jones, C. (1970). *An Introduction to the study of Public Policy*. Belmont, Duxbury Press.

Kingdon. (1995). *Agendas, alternatives and public policies.*

Laswell, H. (1962). *The public interest.* En The Public Interest edition C.F. Friendruch (vol. 5). Atherton Press.

Leiva, M. (9 de julio 2018). Parlamentarios y privados discrepan por Ley de Datos. [en línea]. *La Tercera*. https://www.latercera.com/pulso/noticia/parlamentarios-privados-discrepan-ley-datos/235786/ [Consultado: 12 de enero de 2024].

Ley 19628. (1999). Sobre la protección de la vida privada.

Ley 19628. (2002). Modifica la ley N°19.628, Sobre protección de la vida privada

Ley 20463 (2010). Modifica ley N°19628, suspendiendo por el plazo que indica la información comercial de las personas cesantes.

Ley 20521 (2011). Modifica ley N°19628, sobre protección de datos de carácter personal para garantizar que la información entregada a través de predictores de riesgo sea exacta, actualizada y veraz.

Ley 20575 (2012). Establece el principio de finalidad en el tratamiento de datos personales.

Ley 21096. (2018). Consagra el derecho a protección de los datos personales.

Ley 21214. (2020). Modifica la ley N°19.628, Sobre protección de la vida privada, con el objeto de prohibir que se informe sobre las deudas contraídas para financiar la educación en cualquiera de sus niveles.

Ley 21504. (2022). Establece prohibición de informar deudas contraídas para financiar servicios y acciones de salud en Ley N°19.628

Ley 19628 (2022). Sobre Protección de la Vida Privada: Modificaciones

Lindblom, C. (1991). *El proceso de elaboración de políticas públicas*. MAP.

López-Torres, J. (2014). Antecedentes Internacionales en Materia de Privacidad y Protección de Datos Personales. EAFIT *Journal International Law 5*(2). https://publicaciones.eafit.edu.co/index.php/ejil/article/view/2849/2616

Lujan, J [@SergioLujanMora]. (2011). Cookies: ¿Qué son y para qué sirven? [Video]. YouTube. https://www.youtube.com/watch?v=8LaTgXMhgtE

Microjuris. (2018). *Ley N.º 21.096 consagra constitucionalmente el Derecho a la Protección de datos personales.* Inteligencia Jurídica. https://aldiachile.microjuris.com/2018/06/18/ley-no-21-096-consagra-el-derecho-a-la-proteccion-de-datos-personales/.

Montes, C. (24 de abril de 2020). De 18 a 22 horas semanales: el fuerte aumento de uso de aplicaciones de los chilenos. Revista Qué Pasa. *La Tercera*. https://www.latercera.com/que-pasa/noticia/de-18-a-22-horas-semanales-el-fuerte-aumento-de-uso-de-aplicaciones-de-los-chilenos/CKTPYU4FHBDLDIH6BO7KGCGGFE/

Mundo en Línea. (6 de agosto de 2020). En cuarentena, el 65% del uso de Internet en Chile es para streaming y videos. *Destacados*. https://mundoenlinea.cl/2020/08/06/en-cuarentena-el-65-del-uso-de-internet-en-chile-es-para-streaming-y-videos/

North, C. (1993). Instituciones. Poner la Editorial http://ebour.com.ar/pdfs/Instituciones,%20de%20Douglass%20North.pdf

Núñez, M. (14 de octubre de 2020). Denunciaron que hackers robaron las Claves Únicas de todos los chilenos desde Gobierno Digital. *ADN*. https://www.adnradio.cl/nacional/2020/10/14/denunciaron-que-hackers-robaron-las-claves-unicas-de-todos-los-chilenos-desde-gobierno-digital.html

Organización de las Naciones Unidas [ONU]. (1948). *Declaración Universal de los Derechos Humanos*. https://www.un.org/es/about-us/universal-declaration-of-human-rights

Organización de los Estados Americanos [OEA]. (1948). *Declaración Americana de los derechos y Deberes del Hombre*. IX Conferencia Internacional Americana. https://www.oas.org/es/cidh/mandato/basicos/declaracion.asp

Organización de los Estados Americanos [OEA]. (1978). Convención Americana sobre Derechos Humanos (Pacto de San José). Convención Americana sobre Derechos Humanos. Gaceta Oficial N° 9460. Secretaría General OEA (Instrumento Original y Ratificaciones). *Serie sobre Tratados OEA N°36 – Reg. ONU 27/08/1979 N°17955*. https://www.oas.org/dil/esp/1969_Convención_Americana_sobre_Derechos_Humanos.pdf

ONG Derechos Digitales. (2012). *Proyecto de ley que introduce modificaciones a la Ley N°19.628, sobre protección de la vida privada y protección de datos de carácter personal (Boletín N°8143-03). Minuta de discusión.* https://www.derechosdigitales.org/wp-content/uploads/comentariosdd-datos.pdf

Organización Internacional del Trabajo [OIT]. (23 de noviembre de 2020). Chile: efectos de la pandemia generaron consecuencias sin precedentes en el mundo del trabajo. *Noticias* https://www.ilo.org/santiago/sala-de-prensa/WCMS_761927/lang--es/index.htm

Organización Internacional para las Migraciones [OIM]. (s.f. a). Protección de Datos. https://www.iom.int/es/proteccion-de-datos [Consulta: 26 de enero de 2024].

Organización Internacional para las Migraciones [OIM]. (s.f. b). Nuestro Trabajo. https://www.iom.int/es/nuestro-trabajo [Consulta: 26 de enero de 2024].

Organización para la Cooperación y Desarrollo Económico [OCDE]. (1980). *Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales*. http://www.oas.org/es/sla/ddi/docs/directrices_ocde_privacidad.pdf

Organización para la Cooperación y Desarrollo Económico [OCDE]. (2010). *Chile, primer país sudamericano miembro de la OCDE*. https://www.oecd.org/espanol/chileprimerpaissudamericanomiembrodelaocde.htm [consulta: 15 de enero de 2024].

Organización para la Cooperación y el Desarrollo Económico [OCDE]. (2013). *The OECD Privacy Framework*. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Organización para la Cooperación y el Desarrollo Económico [OCDE]. (2023). *Declaration on Government Access to Personal Data Held by Private Sector Entities. OECD/Legal/0487*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

Pérez, A. (1992). Del habeas Corpus al Habeas Data. Informática y derecho: *Revista Iberoamericana de derecho informático*, (1), 153-161 https://dialnet.unirioja.es/descarga/articulo/4482974.pdf

Prosser, W. (1960). Privacy. *California Law Review, 48*(3).

Polo, A. (2021). Datos, datos, datos: El dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos. Estudios de Deusto. http://dx.doi.org/10.18543/ed-69(1)-2021pp211-240

Quezada, F. (2012). La protección de datos personales en la jurisprudencia del Tribunal Constitucional. Revista Chilena de Derecho y Tecnología, 1(1).

https://revistaderechopublico.uchile.cl/index.php/RDPU/article/view/35417/37101

Rabotnikof, N. (1997). El Espacio Público: Caracterizaciones teóricas expectativas políticas.

Riofrío, J. (2014). La Cuarta Ola de Derechos Humanos: Los Derechos Digitales. *Revista Latinoamericana de Derechos Humanos, 25*(1).

Rojas, R. & López, D. (2018). El impacto del RGPD en el ámbito del control laboral y la era de la innovación. *Actualidad Civil No.5, Editorial Wolters Kluwer*. https://ecija.com/wp-content/uploads/2018/06/08_Raúl-y-Daniel-1.pdf

Romeo, C. (1994a). Interrogantes y lagunas jurídicas. Revista TELOS (Revista de Pensamiento, Sociedad y Tecnología), *37*. https://telos.fundaciontelefonica.com/archivo/numero037/interrogantes-y-lagunas-juridicas/?output=pdf

Romeo, C. (1994b). Infracciones Administrativas y Penales en Relación con la Protección de Datos. *Informativa y Derecho*, (6), 365-383. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj-5IPD2tODAxUaK7kGHd4GAA4QFnoECBoQAQ&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F248381.pdf&usg=AOvVaw0JxdMtBmPFi1wi_OjFJ5Ny&opi=89978449

Sampieri, R., Fernández, C. & Baptista, P. (2014). *Metodología de la investigación. Sexta edición.* McGraw Hill education.

Senado. (2017). *Tramitación Proyecto de Ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.* [en línea] https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07

Senado. (2023). *Tramitación Proyecto de Ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.* [en línea] https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07

Senado. (2024a). Informe de comisión de Constitución, Legislación, Justicia y Reglamento. Versión Comparado. Proyecto de ley, en tercer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de protección de datos personales. (Boletines N°S 11.144-07 y 11.092-07, refundidos).

Senado. (2024b). *Tramitación Proyecto de Ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.* [en línea] https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07

SERNAC. (2022). Casi la mitad de los consumidores admite nunca leer la política de privacidad de los sitios que visita. Noticias. Servicio Nacional del Consumidor. Recuperado el 25 de julio de 2022, de https://www.sernac.cl/portal/604/w3-article-64751.html

Sparkes, A. (1981). *The right to be let alone: a violation of "privacy".* ASLP Bulletin N° 20. http://classic.austlii.edu.au/au/journals/AUSocLegPhilB/1981/17.pdf

Sumner, M. (2006). Qualitative research. En: V. Jupp (Ed.). *The Sage Dictionary of Social Research Methods*. Sage. http://text-translator.com/wp-content/filesfa/Dic-of-Social-Research.pdf

Travieso, J. (2016). Protección de datos personales y tecnología. En busca del paraíso perdido. *Revista Tribuna Internacional, 5*(9).

Unión Europea [UE]. (2016). Reglamento general de protección de datos. (UE) 2016/679 https://www.boe.es/doue/2016/119/L00001-00088.pdf

Vargas, I. (2012). La entrevista en la investigación cualitativa: nuevas tendencias y retos. Revista Calidad en la Educación Superior Programa de Autoevaluación. Universidad Nacional de Costa Rica. Vol. 3, No. 1, pp. 119-139. https://dialnet.unirioja.es/servlet/articulo?codigo=3945773

Viales, R. & Juárez, J. (2007). Gobernabilidad democrática en América Central: una propuesta de análisis path dependence de carácter neo institucional a partir de la crítica de los planteamientos de J. Mahoney: El caso de El Salvador entre 1930 y 1960. *Diálogos Revista Electrónica de Historia, 8*(1), 26-43.

Viollier, P. (2017). El estado de la protección de datos personales en Chile. *Derechos Digitales.* https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

Viollier, P. (19 de julio de 2018). Avanza la tramitación de la ley de datos: lo bueno, lo malo y lo feo. Chile. *Derechos Digitales en internet.* https://www.derechosdigitales.org/12316/avanza-la-tramitacion-de-la-ley-de-datos-lo-bueno-lo-malo-y-lo-feo/

Warren, S. & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review, 4*(5). https://www.jstor.org/stable/1321160

Zahariadis, N. (2007). *El marco de las corrientes múltiples. Estructura, limitaciones, perspectivas.* En P. Sabatier (Ed), *Teorías del Proceso de las Políticas Públicas,* (2nd ed). Westview Press.

FACULTAD DE GOBIERNO
UNIVERSIDAD DE CHILE

Anexos.

FACULTAD DE
GOBIERNO
UNIVERSIDAD DE CHILE

CONSENTIMIENTO INFORMADO ENTREVISTAS MAGISTER EN GOBIERNO Y GERENCIA PÚBLICA

Yo _____, estoy siendo entrevistado/a en forma voluntaria por la estudiante regular del Magister en Gobierno y Gerencia Pública de la Facultad de Gobierno de la Universidad de Chile, Catalina Pinto Iribarren, en el marco de la investigación titulada: Agencia de Protección de Datos Personales, oportunidades y desafíos respecto a las recomendaciones OCDE.

Al participar entiendo que se me solicitará lo siguiente:

- Participar en una entrevista, en horario y lugar previamente convenido.
- La entrevista será grabada y transcrita para su posterior análisis.
- La transcripción de la entrevista se realizará solo con el fin de analizarla.
- Los resultados de la investigación serán presentados con fines académicos.
- El/ la investigador podrá acordar con su informante la confidencialidad o no confidencialidad de la identidad e institución.
- Usted podrá retirar su consentimiento de participar en la investigación sin previa justificación. Para ello tendrá que contactar con la/el investigador.

Nota: Tanto la identidad y el servicio, ministerio u organización al que pertenece el/la participante, así como la individualización de los/as entrevistados/as respecto a sus propias entrevistas, serán resguardadas con estricta confidencialidad.
En caso de que la/el investigador acuerde con el/la informante la no confidencialidad, debe marcar la siguiente cláusula (SÍ/NO).

SÍ Acepto que mi identidad y el nombre de la institución, a la cual pertenezco, no sean confidenciales y su detalle sea utilizado con fines académicos.

En caso de cualquier duda dirigirse a:

Comité Académico Magister en Gobierno y Gerencia Pública, Santa Lucía 240, Santiago, o a través de su Coordinadora, prof. Cecilia Osorio Gonnet, coordinacionmggp@gobierno.uchile.cl

Yo _____ comprendo los procedimientos arriba señalados, y comprendo mis derechos al participar en esta investigación. Mis preguntas han sido satisfactoriamente respondidas, y acepto participar en este estudio. Se me ha dado una copia de este formulario.

Firma del/de la participante: Fecha: 29 de junio de 2023

Yo, Catalina Pinto Iribarren he explicado los alcances de ser entrevistado/a para esta investigación, y he respondido a todas sus preguntas. Creo que él/ella comprende la información descrita en este documento y libremente consiente en participar.

Firma del/de la Investigador/a: Fecha: 29 de junio de 2023

FACULTAD DE
GOBIERNO
UNIVERSIDAD DE CHILE

CONSENTIMIENTO INFORMADO ENTREVISTAS MAGISTER EN GOBIERNO Y GERENCIA PÚBLICA

Yo_____, estoy siendo entrevistado en forma voluntaria por la estudiante regular del Magister en Gobierno y Gerencia Pública de la Facultad de Gobierno de la Universidad de Chile, Catalina Pinto Iribarren, en el marco de la investigación titulada: Agencia de Protección de Datos Personales, oportunidades y desafíos respecto a las recomendaciones OCDE.

Al participar entiendo que se me solicitará lo siguiente:

- Participar en una entrevista, en horario y lugar previamente convenido.
- La entrevista será grabada y transcrita para su posterior análisis.
- La transcripción de la entrevista se realizará solo con el fin de analizarla.
- Los resultados de la investigación serán presentados con fines académicos.
- El/ la investigador podrá acordar con su informante la confidencialidad o no confidencialidad de la identidad e institución.
- Usted podrá retirar su consentimiento de participar en la investigación sin previa justificación. Para ello tendrá que contactar con la/el investigador.

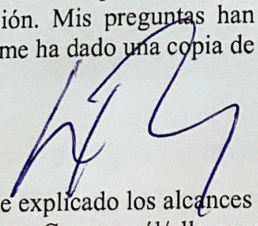
Nota: Tanto la identidad y el servicio, ministerio u organización al que pertenece el/la participante, así como la individualización de los/as entrevistados/as respecto a sus propias entrevistas, serán resguardadas con estricta confidencialidad.
En caso de que la/el investigador acuerde con el/la informante la no confidencialidad, debe marcar la siguiente cláusula (SÍ/NO).

_____ Acepto que mi identidad y el nombre de la institución, a la cual pertenezco, no sean confidenciales y su detalle sea utilizado con fines académicos.

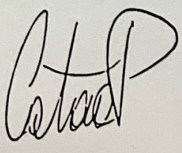
En caso de cualquier duda dirigirse a:

Comité Académico Magister en Gobierno y Gerencia Pública, Santa Lucía 240, Santiago, o a través de su Coordinadora, prof. Cecilia Osorio Gonnet, coordinacionmggp@gobierno.uchile.cl

Yo_____ comprendo los procedimientos arriba señalados, y comprendo mis derechos al participar en esta investigación. Mis preguntas han sido satisfactoriamente respondidas, y acepto participar en este estudio. Se me ha dado una copia de este formulario.

Firma del/de la participante:  Fecha: 12 de enero de 2024

Yo, Catalina Pinto Iribarren he explicado los alcances de ser entrevistado/a para esta investigación, y he respondido a todas sus preguntas. Creo que él/ella comprende la información descrita en este documento y libremente consiente en participar.

Firma del/de la Investigador/a:  Fecha: 12 de enero de 2024

FACULTAD DE GOBIERNO
UNIVERSIDAD DE CHILE

CONSENTIMIENTO INFORMADO ENTREVISTAS MAGISTER EN GOBIERNO Y GERENCIA PÚBLICA

Yo_____, estoy siendo entrevistado en forma voluntaria por la estudiante regular del Magister en Gobierno y Gerencia Pública de la Facultad de Gobierno de la Universidad de Chile, Catalina Pinto Iribarren, en el marco de la investigación titulada: Agencia de Protección de Datos Personales, oportunidades y desafíos respecto a las recomendaciones OCDE.

Al participar entiendo que se me solicitará lo siguiente:

- Participar en una entrevista, en horario y lugar previamente convenido.
- La entrevista será grabada y transcrita para su posterior análisis.
- La transcripción de la entrevista se realizará solo con el fin de analizarla.
- Los resultados de la investigación serán presentados con fines académicos.
- El/ la investigador podrá acordar con su informante la confidencialidad o no confidencialidad de la identidad e institución.
- Usted podrá retirar su consentimiento de participar en la investigación sin previa justificación. Para ello tendrá que contactar con la/el investigador.

Nota: Tanto la identidad y el servicio, ministerio u organización al que pertenece el/la participante, así como la individualización de los/as entrevistados/as respecto a sus propias entrevistas, serán resguardadas con estricta confidencialidad.
En caso de que la/el investigador acuerde con el/la informante la no confidencialidad, debe marcar la siguiente cláusula (SÍ/NO).

Yo, _____, Diputado de la República, Acepto que mi identidad y el nombre de la institución, a la cual pertenezco, no sean confidenciales y su detalle sea utilizado con fines académicos.

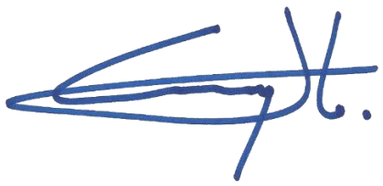
En caso de cualquier duda dirigirse a:

Comité Académico Magister en Gobierno y Gerencia Pública, Santa Lucía 240, Santiago, o a través de su Coordinadora, prof. Cecilia Osorio Gonnet, coordinacionmggp@gobierno.uchile.cl

Yo Leonardo Soto Ferrada comprendo los procedimientos arriba señalados, y comprendo mis derechos al participar en esta investigación. Mis preguntas han sido satisfactoriamente respondidas, y acepto participar en este estudio. Se me ha dado una copia de este formulario.

Firma del/de la participante:

Fecha: 16-01-2024



Yo, Catalina Pinto Iribarren he explicado los alcances de ser entrevistado/a para esta investigación, y he respondido a todas sus preguntas. Creo que él/ella comprende la información descrita en este documento y libremente consiente en participar.

Firma del/de la Investigador/a: 

Fecha: 16 de enero de 2024

FACULTAD DE
GOBIERNO
UNIVERSIDAD DE CHILE

CONSENTIMIENTO INFORMADO ENTREVISTAS MAGISTER EN GOBIERNO Y GERENCIA PÚBLICA

Yo_____, estoy siendo entrevistado en forma voluntaria por la estudiante regular del Magister en Gobierno y Gerencia Pública de la Facultad de Gobierno de la Universidad de Chile, Catalina Pinto Iribarren, en el marco de la investigación titulada: Agencia de Protección de Datos Personales, oportunidades y desafíos respecto a las recomendaciones OCDE.

Al participar entiendo que se me solicitará lo siguiente:

- Participar en una entrevista, en horario y lugar previamente convenido.
- La entrevista será grabada y transcrita para su posterior análisis.
- La transcripción de la entrevista se realizará solo con el fin de analizarla.
- Los resultados de la investigación serán presentados con fines académicos.
- El/ la investigador podrá acordar con su informante la confidencialidad o no confidencialidad de la identidad e institución.
- Usted podrá retirar su consentimiento de participar en la investigación sin previa justificación. Para ello tendrá que contactar con la/el investigador.

Nota: Tanto la identidad y el servicio, ministerio u organización al que pertenece el/la participante, así como la individualización de los/as entrevistados/as respecto a sus propias entrevistas, serán resguardadas con estricta confidencialidad.
En caso de que la/el investigador acuerde con el/la informante la no confidencialidad, debe marcar la siguiente cláusula (SÍ/NO).

_Si_____ Acepto que mi identidad y el nombre de la institución, a la cual pertenezco, no sean confidenciales y su detalle sea utilizado con fines académicos.

En caso de cualquier duda dirigirse a:

Comité Académico Magister en Gobierno y Gerencia Pública, Santa Lucía 240, Santiago, o a través de su Coordinadora, prof. Cecilia Osorio Gonnet, coordinacionmggp@gobierno.uchile.cl

Yo _____comprendo los procedimientos arriba señalados, y comprendo mis derechos al participar en esta investigación. Mis preguntas han sido satisfactoriamente respondidas, y acepto participar en este estudio. Se me ha dado una copia de este formulario.

Firma del/de la participante:  Fecha: 17-01-2024

Yo, Catalina Pinto Iribarren he explicado los alcances de ser entrevistado/a para esta investigación, y he respondido a todas sus preguntas. Creo que él/ella comprende la información descrita en este documento y libremente consiente en participar.

Firma del/de la Investigador/a:  Fecha: 17 de enero de 2024

FACULTAD DE
GOBIERNO
UNIVERSIDAD DE CHILE

CONSENTIMIENTO INFORMADO ENTREVISTAS MAGISTER EN GOBIERNO Y GERENCIA PÚBLICA

Yo [redacted], estoy siendo entrevistado en forma voluntaria por la estudiante regular del Magister en Gobierno y Gerencia Pública de la Facultad de Gobierno de la Universidad de Chile, Catalina Pinto Iribarren, en el marco de la investigación titulada: Agencia de Protección de Datos Personales, oportunidades y desafíos respecto a las recomendaciones OCDE.

Al participar entiendo que se me solicitará lo siguiente:

- Participar en una entrevista, en horario y lugar previamente convenido.
- La entrevista será grabada y transcrita para su posterior análisis.
- La transcripción de la entrevista se realizará solo con el fin de analizarla.
- Los resultados de la investigación serán presentados con fines académicos.
- El/ la investigador podrá acordar con su informante la confidencialidad o no confidencialidad de la identidad e institución.
- Usted podrá retirar su consentimiento de participar en la investigación sin previa justificación. Para ello tendrá que contactar con la/el investigador.

Nota: Tanto la identidad y el servicio, ministerio u organización al que pertenece el/la participante, así como la individualización de los/as entrevistados/as respecto a sus propias entrevistas, serán resguardadas con estricta confidencialidad.
En caso de que la/el investigador acuerde con el/la informante la no confidencialidad, debe marcar la siguiente cláusula (SÍ/NO).

Si Acepto que mi identidad y el nombre de la institución, a la cual pertenezco, no sean confidenciales y su detalle sea utilizado con fines académicos.

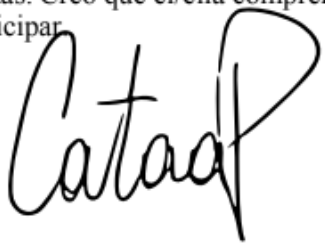
En caso de cualquier duda dirigirse a:

Comité Académico Magister en Gobierno y Gerencia Pública, Santa Lucía 240, Santiago, o a través de su Coordinadora, prof. Cecilia Osorio Gonnet, coordinacionmggp@gobierno.uchile.cl

Yo [redacted], comprendo los procedimientos arriba señalados, y comprendo mis derechos al participar en esta investigación. Mis preguntas han sido satisfactoriamente respondidas, y acepto participar en este estudio. Se me ha dado una copia de este formulario.

Firma del/de la participante:  Fecha: 17-01-2024

Yo, Catalina Pinto Iribarren he explicado los alcances de ser entrevistado/a para esta investigación, y he respondido a todas sus preguntas. Creo que él/ella comprende la información descrita en este documento y libremente consiente en participar.

Firma del/de la Investigador/a:  Fecha: 17 de enero de 2024

FACULTAD DE GOBIERNO
UNIVERSIDAD DE CHILE

CONSENTIMIENTO INFORMADO ENTREVISTAS MAGISTER EN GOBIERNO Y GERENCIA PÚBLICA

Yo , estoy siendo entrevistado en forma voluntaria por la estudiante regular del Magister en Gobierno y Gerencia Pública de la Facultad de Gobierno de la Universidad de Chile, Catalina Pinto Iribarren, en el marco de la investigación titulada: Agencia de Protección de Datos Personales, oportunidades y desafíos respecto a las recomendaciones OCDE.

Al participar entiendo que se me solicitará lo siguiente:

- Participar en una entrevista, en horario y lugar previamente convenido.
- La entrevista será grabada y transcrita para su posterior análisis.
- La transcripción de la entrevista se realizará solo con el fin de analizarla.
- Los resultados de la investigación serán presentados con fines académicos.
- El/ la investigador podrá acordar con su informante la confidencialidad o no confidencialidad de la identidad e institución.
- Usted podrá retirar su consentimiento de participar en la investigación sin previa justificación. Para ello tendrá que contactar con la/el investigador.

Nota: Tanto la identidad y el servicio, ministerio u organización al que pertenece el/la participante, así como la individualización de los/as entrevistados/as respecto a sus propias entrevistas, serán resguardadas con estricta confidencialidad.
En caso de que la/el investigador acuerde con el/la informante la no confidencialidad, debe marcar la siguiente cláusula (SÍ/NO).

X Acepto que mi identidad y el nombre de la institución, a la cual pertenezco, no sean confidenciales y su detalle sea utilizado con fines académicos.

En caso de cualquier duda dirigirse a:

Comité Académico Magister en Gobierno y Gerencia Pública, Santa Lucía 240, Santiago, o a través de su Coordinadora, prof. Cecilia Osorio Gonnet, coordinacionmggp@gobierno.uchile.cl

Yo comprendo los procedimientos arriba señalados, y comprendo mis derechos al participar en esta investigación. Mis preguntas han sido satisfactoriamente respondidas, y acepto participar en este estudio. Se me ha dado una copia de este formulario.

Firma del/de la participante: Firmado digitalmente por
Nombre de reconocimiento (DN): c=CL, st=METROPOLITANA DE SANTIAGO, l=SANTIAGO, o=ESTRATEGIA PUBLICA CONSULTORES SPA, ou=*,
email=
Fecha: 2024.01.19 12:26:04 -03'00'
Fecha: 19-01-2024

Yo, Catalina Pinto Iribarren he explicado los alcances de ser entrevistado/a para esta investigación, y he respondido a todas sus preguntas. Creo que él/ella comprende la información descrita en este documento y libremente consiente en participar.

Firma del/de la Investigador/a: Fecha: 19 de enero de 2024

FACULTAD DE
GOBIERNO
UNIVERSIDAD DE CHILE

CONSENTIMIENTO INFORMADO ENTREVISTAS MAGISTER EN GOBIERNO Y GERENCIA PÚBLICA

Yo [redacted], estoy siendo entrevistado en forma voluntaria por la estudiante regular del Magister en Gobierno y Gerencia Pública de la Facultad de Gobierno de la Universidad de Chile, Catalina Pinto Iribarren, en el marco de la investigación titulada: Agencia de Protección de Datos Personales, oportunidades y desafíos respecto a las recomendaciones OCDE.

Al participar entiendo que se me solicitará lo siguiente:

- Participar en una entrevista, en horario y lugar previamente convenido.
- La entrevista será grabada y transcrita para su posterior análisis.
- La transcripción de la entrevista se realizará solo con el fin de analizarla.
- Los resultados de la investigación serán presentados con fines académicos.
- El/ la investigador podrá acordar con su informante la confidencialidad o no confidencialidad de la identidad e institución.
- Usted podrá retirar su consentimiento de participar en la investigación sin previa justificación. Para ello tendrá que contactar con la/el investigador.

Nota: Tanto la identidad y el servicio, ministerio u organización al que pertenece el/la participante, así como la individualización de los/as entrevistados/as respecto a sus propias entrevistas, serán resguardadas con estricta confidencialidad.
En caso de que la/el investigador acuerde con el/la informante la no confidencialidad, debe marcar la siguiente cláusula (SÍ/NO).

SI Acepto que mi identidad y el nombre de la institución, a la cual pertenezco, no sean confidenciales y su detalle sea utilizado con fines académicos.

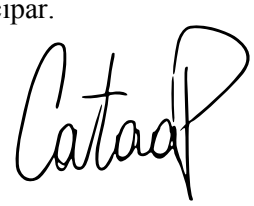
En caso de cualquier duda dirigirse a:

Comité Académico Magister en Gobierno y Gerencia Pública, Santa Lucía 240, Santiago, o a través de su Coordinadora, prof. Cecilia Osorio Gonnet, coordinacionmggp@gobierno.uchile.cl

Yo [redacted] comprendo los procedimientos arriba señalados, y comprendo mis derechos al participar en esta investigación. Mis preguntas han sido satisfactoriamente respondidas, y acepto participar en este estudio. Se me ha dado una copia de este formulario.

Firma del/de la participante: Fecha: 19-01-2024

Yo, Catalina Pinto Iribarren he explicado los alcances de ser entrevistado/a para esta investigación, y he respondido a todas sus preguntas. Creo que él/ella comprende la información descrita en este documento y libremente consiente en participar.

Firma del/de la Investigador/a:  Fecha: 19 de enero de 2024

Powered by ecert Firma electrónica avanzada [redacted]
2024.01.22 09:39:52 -0300