UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO
DEPARTAMENTO DE DERECHO COMERCIAL

# PROYECTO DE LEY QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES: ANÁLISIS Y PROPUESTAS A LA LUZ DEL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

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

AUTOR: DIEGO ALONSO LISONI CARO

PROFESOR GUÍA: CLAUDIO MAGLIONA MARKOVICTH

Santiago de Chile
Diciembre 2020

*A mis padres, Germania y Claudio, y a mi hermano Lucas, que hicieron posible un trabajo que parecía ciencia ficción.*

*"'You were right' said the Master impressed by the neatness of Korovyov's work, 'when you said: no documents, no person. So that means I don't exist since I don't have any documents'"*

— Mikhail Bulgakov, The Master and Margarita

*"It seems to me, Golan, that the advance of civilization is nothing but an exercise in the limiting of privacy."*

— Isaac Asimov, Foundation's Edge

**ÍNDICE**

**RESUMEN**

El presente ensayo tiene por objetivo defender y proponer la consagración legal expresa del Principio de Responsabilidad Proactiva, conocido internacionalmente como "*Accountability Principle*", en el marco normativo en materia de protección de datos personales que se encuentra en discusión en Chile, esto es, el "Proyecto de Ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales" (Boletines 11.144-07 y 11.092-07, refundidos). El antedicho principio constituye el eje vertebrador del sistema de responsabilidad y cumplimiento establecido en el estándar internacional en materia de protección de datos personales, representado por el "Reglamento General de Protección de Datos" de la Unión Europea, y es en base a este sistema de cumplimiento que el proyecto de ley realiza una propuesta que recoge, en su mayoría, la serie de medidas y herramientas que le permiten al responsable y encargado del tratamiento de datos personales demostrar proactiva y preventivamente el debido cumplimiento a la normativa y garantizar el respeto por los derechos y libertades de los titulares de datos personales.

Por ello, constituye uno de los objetivos específicos de este trabajo explicar y reseñar el origen y desarrollo doctrinal que ha recibido en el ámbito internacional el Principio de Responsabilidad Proactiva, haciendo referencia al tratamiento que ha obtenido de parte de la OCDE y la Unión Europea. Consiguientemente, se analizará el sistema de cumplimiento propuesto por el proyecto de ley, que incluye una evaluación pormenorizada de las medidas de cumplimiento, haciendo paralelos con la regulación internacional y realizando las propuestas técnicas que permitan mantener una lectura y entendimiento armónicos de la futura normativa. Así, se justificará la consagración explícita del principio y su implementación interpretativa, en virtud de los objetivos y valores que busca alcanzar este nuevo marco normativo en materia de cumplimiento.

**Palabras claves**: Protección de Datos Personales; Sistema de Cumplimiento; Principio de Responsabilidad Proactiva; *Compliance;* Regulación.

## INTRODUCCIÓN

En el mundo moderno, los efectos de la globalización y el progreso tecnológico han calado profundamente en la vida cotidiana de todas las personas: aquello que alguna vez se acercaba a la ciencia ficción actualmente está al alcance de las manos, se encuentra en los bolsillos, en las casas y e incluso en los lugares más inesperados.

Así, dentro de la nueva realidad que ofrece el siglo XXI, los avances de la tecnología han ido de la mano con nuevos riesgos y amenazas a bienes jurídicos como la seguridad y la privacidad de todas las personas. Ahí dónde antes existía una sensación de seguridad hoy hay cámaras o programas que recogen información y analizan los hábitos de los consumidores incluso luego de que estos disfruten de una buena comida en la comodidad de su hogar.

No obstante aquello, este nuevo mundo de posibilidades trae consigo un gran número de beneficios: podemos acceder más rápida y fácilmente a cualquier tipo de información, servicios o productos que en ningún otro momento en la historia de la humanidad, lo que a su vez ha generado la creación de nuevos puestos de trabajo y profundizado en la especialización educativa de carreras y estudios de postgrado en la mayoría de los centros educativos y universidades del mundo, con el objetivo de crear los profesionales que la sociedad necesita y necesitará en un futuro no muy lejano.

En ese sentido, el desarrollo de la civilización hoy en día se sostiene sobre enormes cimientos constituidos por la utilización del "*Big Data"*, *"Blockchain"*, Inteligencia Artificial, "*Machine Learning"*, entre otras nuevas tecnologías, que permiten el desarrollo y crecimiento exponencial de grandes multinacionales y empresas a lo largo y ancho del globo, como también de gobiernos, autoridades y servicios públicos. Así, la información se ha convertido, de a poco, en la moneda de cambio y el bien más preciado para garantizar y propiciar el intercambio económico de servicios y productos, al mismo tiempo que se cumplen los objetivos de desarrollo sostenible de las naciones.

Sin embargo, estos cambios han ocurrido de forma extraordinariamente veloz, por lo que ha sido difícil para los Estados el garantizar que estos nuevos cimientos no hagan sucumbir los pilares fundamentales que mantienen a flote a la sociedad y la legitimidad de los gobiernos, pilares constituidos por el respeto a los derechos humanos y libertades de todas las personas,

Debido a ello, y gracias a los enormes esfuerzos por parte de organizaciones internacionales y distintos países que han identificado esta problemática, se han implementado actualizaciones normativas y regulatorias con el fin de equilibrar el libre flujo de la información

y el desarrollo de la economía digital[1] con el respeto a los derechos fundamentales, como el de la privacidad, y libertades de las personas.

Estas actualizaciones regulatorias, como el "Reglamento General de Protección de Datos"[2] de la Unión Europea (en adelante "RGPD" o el "Reglamento"), han tenido un impacto global en la delimitación y homogenización de una serie de conceptos jurídicos claves, con el objetivo de desarrollar un marco normativo en materia de protección de datos personales.

Así, para iniciar el desarrollo de este ensayo, es necesario referirse brevemente a varios de estos términos y conceptos esenciales, debido que serán utilizados a lo largo de este indistintamente, es decir, sin ser objetos centrales del análisis que se propondrá en el presente trabajo.

Por ello, y para efectos teóricos, se entenderá por datos personales toda información sobre una persona física identificada o identificable, directa o indirectamente, a partir de identificadores como su nombre, número de identificación, localización, identidad física, fisiológica, genética, cultural, entre otros.[3]

A su vez, el tratamiento de datos personales, o simplemente tratamiento, se comprenderá como cualquier operación o conjunto de operaciones o procedimientos técnicos, automatizados o no, que permitan la recolección, procesamiento, almacenamiento, comunicación, transmisión o uso de datos personales o conjuntos de datos personales.[4]

Por responsable del tratamiento o responsable, se comprenderá a la persona, entidad, autoridad, servicio u organismo que, por sí mismo o junto con otros, determine los fines y medios del tratamiento de los datos personales.[5]

En último lugar, encargado del tratamiento o encargado referirá a la persona, entidad, autoridad, servicio u organismo que trate datos personales por cuenta del responsable, definido anteriormente.[6]

---

[1] RUDGARD, Sian. *Origins and Historical Context of Data Protection Law*. En: INTERNATIONAL ASSOCIATION OF PRIVACY PROFFESIONALS (IAPP), *European Data Protection: Law and Practice.* Ed: Eduardo Ustaran, 2018, pp. 30.
[2] UNIÓN EUROPEA (UE). *Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE*. Diario Oficial de la Unión Europea, 27 de Abril de 2016. Disponible en español en: https://bit.ly/2BFSyqV.
[3] Ibid., pp. 33. Artículo 4 numeral 1.
[4] Loc. Cit., Artículo 4 numeral 2.
[5] Loc. Cit., Artículo 4 numeral 7.
[6] Loc. Cit., Artículo 4 numeral 8.

Teniendo en consideración estos avances normativos, Chile no ha querido quedarse atrás en la carrera contra el tiempo para desarrollar las condiciones y contexto adecuados que permitirían impulsar el desarrollo y exportación internacional de la economía digital del país, y enfrentar los nuevos desafíos que trae consigo el uso de las nuevas tecnologías tanto por el sector público como privado, especialmente en materia de protección de datos personales.

Al igual que en el resto del mundo, los ciudadanos chilenos cada vez más se encuentran con la posibilidad de acceder a los beneficios que trae consigo la utilización de estas tecnologías. Esta sociedad digital sin fronteras ha permitido mejorar la calidad de vida de los chilenos, reduciendo la denominada brecha digital a través del uso sostenido de las "Tecnologías de la Información y Comunicación" (TICs), lo que especialmente se ha traducido en la utilización masiva del Internet, cuyo uso ha visto un incremento, desde el año 2013 al 2020, de 22 puntos porcentuales, logrando que el año 2020 un 80% de la población en Chile tenga acceso a esta tecnología.[7]

En ese sentido, aunque Chile fue pionero en la región en la década de los noventa con la entrada en vigor de la Ley N°19.628 "Sobre Protección de la Vida Privada"[8], la falta de actualización de esta normativa en materia de protección de datos personales, debido a la inexistencia de un enfoque centrado en los derechos y libertades de las personas[9], ha convertido esta cuestión en una problemática de prioritaria resolución a vista del Estado.

Lo anteriormente comentado se ve reforzado por la existencia de múltiples proyectos de ley, presentados y discutidos a lo largo de los años[10], que buscaban reformar la antedicha normativa. Por su parte, desde el año 2015 se viene desarrollando la "Agenda Digital 2020", que dentro de su hoja de ruta contempla la creación e implementación de un eje centrado en los derechos para el desarrollo digital, y que considera un marco normativo adecuado para el entorno digital.[11]

---

[7] LEÓN, Ricardo y MEZA, Sebastián. *Brecha en el uso de internet: Desigualdad digital en el 2020.* Fundación País Digital: Centro de Estudios Digitales. 2020, pp. 5-14. Disponible en: https://bit.ly/3nlLceM

[8] CHILE, Ley N°19.628, *Sobre Protección de la Vida Privada*. Diario Oficial de la República de Chile, Santiago de Chile, 28 de Agosto de 1999.

[9] ÁLVAREZ VALENZUELA, Daniel. *La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa.* Revista Chilena de Derecho y Tecnología. 9(1), 2020, pp. 2.

[10] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. *Proyectos de Modificación Ley N°19.628*. BCN/Ley Chile [en línea] Disponible en: https://bit.ly/3a7f5eQ. Se han presentado más de 40 proyectos de modificación a la ley N°19.628 desde su entrada en vigor.

[11] GOBIERNO DE CHILE. *Agenda Digital 2020*. En Línea. Noviembre de 2015, pp. 12-19. Disponible en: https://bit.ly/3nhMLKn

En aquel contexto, el presente ensayo se propone analizar e interpretar, de manera crítica, el más reciente "Proyecto de Ley que regula la protección y el tratamiento de datos personales y crea la Agencia de Protección de Datos Personales" (Boletines N°11.144-07 y 11.092-07, refundidos, en adelante el "Proyecto de Ley"), con el objetivo general de proponer y defender la inclusión explícita del "Principio de Responsabilidad Proactiva", con el fin de reforzar y perfeccionar el sistema de cumplimiento que contemplará la futura legislación chilena, que permitirá garantizar los derechos y libertades de las personas en un contexto eminentemente digital.

Este principio se encuentra reconocido internacionalmente por la "Organización para la Cooperación y el Desarrollo Económico" (OCDE), de la cual Chile es parte desde el año 2010, y por el Reglamento de la Unión Europea, el que, al mismo tiempo, construye e innova un sistema de responsabilidad y cumplimiento que gravita en torno al mismo principio.[12]

Con ello en mente, este trabajo se estructurará en dos capítulos generales para tratar y desarrollar, de manera sintética y sistemática, los objetivos específicos que a continuación serán esbozados, y que permitirán en conjunto sostener la propuesta comentada anteriormente.

Se partirá por abordar en el primer capítulo, a modo de marco histórico y teórico, el origen y el desarrollo del Principio de Responsabilidad Proactiva (en adelante también denominado como el "Principio") en el contexto internacional, enfocado específicamente en cómo ha sido tratado por la OCDE, los países miembros de la Unión Europea y el RGDP.

Consecuentemente, el siguiente objetivo específico será identificar sumariamente el sistema de cumplimiento del RGDP y la batería de herramientas que ofrece para demostrar el debido cumplimiento a la normativa, con el propósito de destacar que el pilar que sostiene todo este sistema de cumplimiento es el Principio de Responsabilidad Proactiva.

En el segundo capítulo, se abordará el Proyecto de Ley y el contexto en el que fue presentado, haciendo énfasis en su necesidad, en el marco de los compromisos internacionales adoptados por Chile, su importancia y los objetivos que se busca alcanzar.

Luego, como objetivo específico, se analizará críticamente el sistema de cumplimiento propuesto por el Proyecto de Ley a la luz del Principio de Responsabilidad Proactiva, ya que

[12] MCMULLAN, Katie. *Legislative Framework*. En: INTERNATIONAL ASSOCIATION OF PRIVACY PROFFESIONALS (IAPP), *European Data Protection: Law and Practice*. Ed: Eduardo Ustaran, 2018, pp. 63.

se basa, como se dejará patente, en el sistema establecido por el RGDP. En ese sentido, se compararán sistemáticamente las normas contenidas en el Reglamento con las propuestas en el Proyecto de Ley.

De esta manera, y para finalizar, se sistematizará el análisis para sustentar la inclusión del Principio de Responsabilidad Proactiva en nuestro futuro ordenamiento. Especialmente en este segundo capítulo, se revisarán las innovaciones que se encuentran en el Proyecto de Ley en materia de cumplimiento y se propondrán las modificaciones que permitan, en suma, reforzar este sistema y otorgarle coherencia y practicidad a una materia que, como se verá, se está a tiempo todavía de perfeccionar.

## CAPÍTULO PRIMERO: EL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

### 1.1. ORIGEN

La primera vez que se incluyó el Principio de Responsabilidad Proactiva, en inglés conocido como "*Accountability Principle*", en materia de protección de datos, fue en las "Directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales"[13] de la OCDE, que se hicieron efectivas el 23 de Septiembre de 1980 (en adelante también denominadas como las "Directrices de 1980").

Aquella ocasión además representó la primera oportunidad en la que la comunidad internacional, de manera unánime, aglutinó en un solo texto los principios rectores y guías generales en materia de protección de datos personales, con el objetivo de homogeneizar las legislaciones de los diferentes países miembros, debido a las inquietudes que generaban las inconsistencias y competencias normativas internacionales que crecían en virtud de la aparición de nuevas tecnologías y tipos de tratamientos de datos personales.[14]

En ese sentido, se establecieron ocho principios básicos "*concisos, tecnológicamente neutrales, no vinculantes y escritos usando un lenguaje comúnmente entendible. Esto los hizo extraordinariamente adaptables a (…) las estructuras legales de los países implementadores, cambio social y ambiente tecnológico*"[15]. Entonces, las Directrices de 1980 establecieron un mínimo que permite evitar restricciones al libre fujo de la información entre los países miembros que las acatan.[16]

El Principio, establecido en el parágrafo 14 de las Directrices de 1980, establece lo siguiente:

> *"Sobre todo responsable del tratamiento debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente".*[17]

Este texto constituye el germen, en cuanto a contenido, del término "*Accountability*". Así, cumple un doble propósito: en primer lugar, sirve para identificar al responsable del tratamiento como la entidad que debería ser responsable de garantizar el cumplimiento de los principios y, en segundo lugar, alienta a los países miembros a establecer mecanismos que permitan dar

---

[13] ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. 1980. Disponible en: https://bit.ly/320wD8e.
[14] ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD). *The OECD Privacy Framework*. París: OECD Publishing. 2013. p. 69. Disponible en https://bit.ly/2Z4AS0N
[15] Ibid, pp. 76.
[16] Loc. Cit.
[17] OECD, 1980, op. cit., "*Accountability Principle Paragraph 14: A data controller should be accountable for complying with measures which give effect to the principles stated above"*. Traducción nuestra.

efectividad a los principios básicos establecidos y asegurar que el responsable responda en caso de que no cumpla con su deber[18].

No obstante lo anterior, el desarrollo de este principio, desde 1980 hasta nuestros días, ha supuesto a su vez algunos inconvenientes y problemas a la hora de determinar sus alcances y traducción, puesto que, tal como será tratado en los apartados subsiguientes, la sola lectura del término puede llevar a pensar que se trata de un principio de responsabilidad legal general, cuando en realidad en materia de datos personales y cumplimiento "*Accountability is not synonymous of responsibility*".[19]

En ese sentido, revisaremos el desarrollo de este principio, especialmente de la mano de la Unión Europea, para asentar una definición adecuada e interpretativa del mismo que nos permita continuar con el siguiente capítulo de este ensayo.

### 1.2. UNIÓN EUROPEA Y EL "GRUPO DE TRABAJO DEL ARTÍCULO 29"

El 24 de octubre del año 1995 entró a regir la Directiva 95/46/CE del Parlamento y el Consejo Europeo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante la "Directiva").[20]

La Unión Europea decidió establecer esta Directiva con el objetivo, en línea con las Directrices de 1980, de afrontar el aumento del uso del tratamiento de datos personales en los diferentes sectores de la actividad económica y social, a través del empleo de nuevas tecnologías de la información que facilitan el tratamiento e intercambio de dichos datos. Además, buscaba evitar que las diferencias entre los niveles de protección de los derechos y libertades de las personas entre los Estados miembros pudiese impedir la transmisión libre de estos datos entre las naciones, obstaculizando el desarrollo económico, la innovación y la libre competencia.[21]

---

[18] ALHADEFF, J., VAN ALSENOY, B. and DUMORTIER, J (DUMORTIER et al.). *The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions*. En: POSTIGO, H., NEYLAND, D., KROENER, I., Ilten, C., HEMPEL, L. and GUAGNIN, D. *Managing Privacy Through Accountability*. Basingstoke: Palgrave Macmillan. 2012, pp. 53.

[19] DE HERT, Paul. *Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights La.* En: POSTIGO, H., NEYLAND, D., KROENER, I., Ilten, C., HEMPEL, L. and GUAGNIN, D. *Managing Privacy Through Accountability*. Basingstoke: Palgrave Macmillan. 2012, pp. 199.

[20] UNIÓN EUROPEA (UE). *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva 95/46/CE)*. Diario Oficial de la Unión Europea, 24 de Octubre de 1995, Disponible en español en https://bit.ly/31RjZZr.

[21] UE., 1995, op. cit., pp. 1-2.

En ese sentido, optó por homogeneizar, hacer equivalente y coordinar los niveles de protección de los derechos y libertades de las personas, en el ámbito del tratamiento de los datos personales, entre los Estados miembros.[22]

De esta manera, en sus artículos 29 y 30, establece la creación de lo que se conocía como el "Grupo de Trabajo del Artículo 29" (en adelante "GT29"), al que se le dejó la tarea de interpretar y asesorar la implementación de la Directiva en toda la Unión Europea.[23] Con aquello en mente, comenzó sus actividades el año 1996 teniendo un carácter consultivo, independiente y experto en materia de protección de datos personales. Se compuso por un representante de la autoridad de protección de datos de cada Estado miembro de la Unión Europea, del Supervisor Europeo de Protección de Datos (SEPD) y un representante de la Comisión Europea (CE).

El año 2009 el GT29, al responder una consulta de la Comisión Europea respecto a los nuevos desafíos en materia de protección de datos personales, propuso la inclusión del principio de Responsabilidad Proactiva y de mecanismos basados en rendición de cuentas[24] a la Directiva, con el objetivo de reforzar la efectividad del sistema de cumplimiento y aprovechar la oportunidad de innovar en este sentido, debido a que se diagnosticó que los responsables del tratamiento de datos e interesados no eran lo suficientemente cumplidores de sus obligaciones legales ni estas últimas se encontraban arraigadas en sus prácticas internas.[25]

Finalmente, en el año 2010, el GT29 dedicó toda una opinión al Principio de Responsabilidad Proactiva[26]. El objetivo fue discutir y proponer formalmente su inclusión, en vista de que los principios y obligaciones legales establecidos por la Directiva no encontraban asidero en prácticas y medidas concretas. De esta manera, la idea general era "*trasladar la protección de datos de la 'teoría a la práctica' y ayudar a las autoridades de protección de datos en sus tareas de supervisión y ejecución*".[27]

Establecidos los beneficios de incluir este principio, el GT29 realizó una aproximación a la estructura legal que debiese de presentar el mecanismo de cumplimiento basado en el mismo,

---

[22] Loc. Cit.
[23] BERNAL, Paul. *Internet Privacy Rights*. Cambridge: Cambridge University Press. 2014, pp. 124.
[24] ARTICLE 29 DATA PROTECTION WORKING PARTY (Art. 29WP). *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.* Bruselas, Bélgica, 2009, pp. 20, parágrafo 79. Disponible en https://bit.ly/2O6XE1Y.
[25] Ibid., pp. 19, parágrafo 74.
[26] ARTICLE 29 DATA PROTECTION WORKING PARTY (ART. 29WP). *Opinion 3/2010 on the principle of accountability*. Bruselas, Bélgica, 2010. Disponible en https://bit.ly/3gx4s4Q.
[27] Ibid., pp. 2.

que consideró herramientas ya presentes en la Directiva[28], el fomento de prácticas autorregulatorias[29], medidas que permitieran dar efectividad a los principios de protección de datos y la obligación de ser capaces de demostrar el cumplimiento de los mismos si la autoridad lo requiere, por parte de los responsables del tratamiento.[30]

Así, el GT29 procedió a proponer provisionalmente el siguiente texto para significar el Principio de Responsabilidad Proactiva:

> "*Artículo X – Implementación de los Principios de Protección de Datos*
> *1. El responsable implementará medidas apropiadas y efectivas para asegurar que se cumplan los principios y obligaciones establecidos en la Directiva.*
>
> *2. El responsable deberá demostrar el cumplimiento al párrafo 1 ante la solicitud de la autoridad supervisora".*[31]

Como se puede notar, el primer párrafo de la propuesta del GT29 es muy similar al principio establecido por las Directrices de 1980 de la OCDE. En ese sentido, su rol principal consiste en reforzar el hecho de que los responsables del tratamiento de datos son los encargados de implementar las medidas apropiadas para dar efectividad a los principios de la Directiva[32]. Por otro lado, el segundo párrafo pareciera deber su establecimiento a la influencia de otros cuerpos normativos, en los que además es necesario que el responsable, si desea demostrar cumplimiento, haya tomado antes las medidas apropiadas y preestablecidas para ello.[33]

Entonces, la técnica normativa del GT29 pareciera tomar dos enfoques. En primer lugar, no indica específicamente cuáles son las medidas que espera que el responsable de datos implemente, ya que posteriormente una lista no taxativa de dichas medidas sería otorgada por las autoridades de protección de datos o porque muchas de ellas ya se encontrarían o podrían ser establecidas en la Directiva[34], por lo que solo sería necesario hacer las modificaciones pertinentes para guiar la lectura de estas en el sistema de cumplimiento propuesto. En segundo lugar, el GT29 indica que dichas medidas[35] no en todos los casos podrían ser

---

[28] Ibid., pp. 5, parágrafo 13. Entre estas medidas complementarias encontramos "*privacy impact assessments in given cases or the appointment of data protection officers*".
[29] Ibid., pp. 6, parágrafo 14.
[30] Ibid., pp. 5, parágrafo 12.
[31] Ibid., pp.10, parágrafo 34. Traducción nuestra.
[32] DUMORTIER et al, 2012, op. cit., pp. 63.
[33] Ibid., pp. 58.
[34] ART. 29WP, 2010, op. cit., pp. 9, parágrafo 30.
[35] Ibid., pp. 11-12, parágrafo 41. *"The Article 29 Working Party considers that common accountability measures may include the following non-exhaustive list:*
• *Establishment of internal procedures prior to the creation of new personal data processing operations (internal review, assessment, etc);*

implementadas, puesto que son complementarias al principio, teniendo un carácter ilustrativo, y porque todo ello depende de los riesgos involucrados y los tipos de tratamientos y datos utilizados.[36]

Entre los marcos normativos y procesos que sirvieron como inspiración para el asentimiento de las acepciones propuestas por el GT29 podemos mencionar la *"Personal Information Protection and Electronic Documents Act"*[37] (PIPEDA), adoptada por el gobierno canadiense el año 2000, y que entre sus principios considera especialmente el de Responsabilidad Proactiva, estipulando de manera explícita que las organizaciones deben adoptar políticas y prácticas para dar efectividad a los demás principios contenidos en la normativa, además de establecer que la responsabilidad de la organización de cumplir con la normativa se mantiene aun cuando el procesamiento de los datos es llevado a cabo por un tercero, cuestión que tiene similitud con lo dispuesto por las Directrices de 1980.[38]

En el mismo sentido, la PIPEDA estableció un nuevo elemento que consagra, cómo se verá luego en este ensayo, la dimensión interna del Principio de Responsabilidad Proactiva, permitiéndole a los responsables designar una o más personas encargadas de rendir cuentas por el cumplimiento de los deberes y obligaciones de la organización, las que deben ejercer funciones tales como las de servir como punto de contacto con terceros interesados e implementar o supervisar las medidas que se adopten para cumplir con la normativa.[39]

En segundo lugar, el año 2009 se llevó a cabo la 31va "*International Conference of Data Protection and Privacy Commissioners*", conferencia hoy en día llamada "*Global Privacy*

---

*• Setting up written and binding data protection policies to be considered and applied to new data processing operations (e.g., compliance with data quality, notice, security principles, access, etc), which should be available to data subjects.*
*• Mapping of procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations,*
*• Appointment of a data protection officer and other individuals with responsibility for data protection;*
*• Offering adequate data protection, training and education to staff members. This should include those processing (or responsible for) the personal data (such as human resources directors) but also IT managers, developers and directors of business units. Sufficient resources should be allocated for privacy management, etc.*
*• Setting up of procedures to manage access, correction and deletion requests which should be transparent to data subjects;*
*• Establishment of an internal complaints handling mechanism;*
*• Setting up internal procedures for the effective management and reporting of security breaches;*
*• Performance of privacy impact assessments in specific circumstances;*
*• Implementation and supervision of verification procedures to ensure that all the measures not only exist on paper but that they are implemented and work in practice (internal or external audits, etc)."*

[36] Ibid., pp. 13, parágrafos 44 y 45.
[37] ESTADOS DE CANADÁ, *Personal Information Protection and Electronic Documents Act (PIPEDA).* 13 de Abril del 2000. Disponible en: https://bit.ly/2WbRG3M
[38] DUMORTIER et al., 2012, op. cit., pp. 55.
[39] DUMORTIER et al., 2012, op. cit., pp. 56.

*Assembly*"[40], cuyo objetivo fue llegar a un estándar mínimo global y promover la armonización legislativa y normativa en materia de protección de datos personales.[41]

En aquella oportunidad la conferencia se realizó en la ciudad de Madrid, España, y dio fruto a la denominada "Resolución de Madrid", que introdujo una propuesta conjunta para una redacción de estándares internacionales sobre la protección de la privacidad respecto al procesamiento de datos personales.[42]

Dentro de esta propuesta conjunta se establecieron una serie de principios rectores, entre ellos el de Responsabilidad Proactiva, que estatuyó lo siguiente:

> *"Sección 11. Principio de Responsabilidad Proactiva*
>
> *La persona responsable deberá:*
>
> *a. Tomar todas las medidas necesarias para cumplir con los principios y obligaciones establecidos en este Documento y en la legislación nacional aplicable, y*
>
> *b. Dotarse de aquellos mecanismos internos necesarios para demostrar dicho cumplimiento, tanto a los titulares de datos como a las autoridades de control en el ejercicio de sus competencias, según lo establecido en la sección 23."*[43]

Así, queda de manifiesto que esta concepción del Principio toma como base muchos de los elementos contenidos en las anteriores disposiciones y propuestas reseñadas. De todas maneras, cabe destacar la inclusión de la idea de que no solo se tiene que rendir cuentas a la autoridad de control, sino que también a los titulares de datos, cuestión que, a su vez, como se verá en el presente ensayo, es rescatada e implementada tanto en el Proyecto de Ley como en la legislación que actualmente rige a toda la Unión Europea.

Por si fuera poco, la "Resolución de Madrid" contempla, en su sección 22, el deber de los Estados de incentivar el establecimiento, por parte de los responsables que intervengan en cualquier etapa del procesamiento de datos personales, de medidas que promuevan proactivamente el cumplimiento de la legislación aplicable, entre las que explícitamente menciona la designación de oficiales de protección de datos, procedimientos para prevenir

---

[40] GLOBAL PRIVACY ASSEMBLY. *History of the Assembly*. [en línea]. Disponible en: https://bit.ly/2W8AqfI
[41] THE CIVIL SOCIETY, *The Madrid Privacy Declaration*. Madrid, España, 2009, pp. 2. Disponible en: https://bit.ly/3n9LOUC
[42] 31TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS (31TH ICDPPC), *The Madrid Resolution.* Madrid, España, 2009, pp. 1-5. Disponible en: https://bit.ly/3n86OLf
[43] Ibid., pp. 13. Traducción nuestra.

infracciones, programas de formación y educación interna en materia de protección de datos personales, realización de auditorías periódicas y transparentes, implementación de evaluaciones de impacto sobre privacidad y la adopción de acuerdos o medidas autorregulatorias.[44]

Finalmente, en el texto aprobado de la "Resolución de Madrid" se deja patente la diferencia entre los términos "*Accountability*" y "*Liability*". Este último concepto también es utilizado frecuentemente para significar lo que conocemos como responsabilidad legal o por daños[45], por lo que su uso en la resolución permite diferenciar claramente que se trata de conceptos que hacen referencia a cuestiones completamente distintas:

> *"(…) the processing of personal data in the public and private sector would be performed, in a more internationally uniform approach:*
>
> *d. implementing the principles of* ***accountability and liability****, even if the processing operations are carried out by service providers on behalf of the controller;"*[46]

En ese sentido, la propia "Resolución de Madrid" significa al principio de "*Liability*", ubicado en la sección 25, de la siguiente manera: "*la persona responsable será responsable por aquellos daños y/o perjuicios, tanto morales como materiales, que hubiese causado a los interesados como consecuencia de un tratamiento de datos de carácter personal que hubiese vulnerado la legislación aplicable en materia protección de datos (…)*"[47].

Lógicamente, si se tuviese que traducir lo aprobado por la resolución al español, sería necesario dejar en claro que se trata de dos tipos de responsabilidades diferentes por lo que, como se ha tratado hasta ahora, la acepción utilizada para significar el término "*Accountability Principle*" durante este ensayo, es decir, Principio de Responsabilidad Proactiva, cumple con dicha prerrogativa y permite zanjar las confusiones que pudiesen llegar a aparecer en lo que resta de este trabajo con los conceptos de responsabilidad legal o por daños en la normativa internacional, estos son, "*Responsibility*" o "*Liability*".

[44] 31TH ICDPPC, 2009, op. cit., pp. 24-25.
[45] DE HERT, Paul, 2012, op. cit., pp. 199.
[46] 31TH ICDPPC, 2009, pp. 31. El destacado es nuestro.
[47] Ibid., pp. 37. Traducción nuestra.

### 1.2.1. LAS DIRECTRICES SOBRE PRIVACIDAD DE LA OCDE DEL AÑO 2013

Las Directrices de 1980 de la OCDE fueron actualizadas y revisadas el año 2013, adoptándose el 11 de Julio de ese año su versión revisada[48] (en adelante también denominadas como las "Directrices del 2013").

Se realizó dicha revisión luego de que fuera solicitado por la Conferencia Ministerial de la OCDE del año 2008 en la Declaración de Seúl, con el objeto de evaluar las Directrices de 1980 a la luz de "*changing technologies, markets and user behaviour, and the growing importance of digital identities".*[49]

Así, entre los cambios introducidos, se pueden comentar dos de gran importancia. En primer lugar, se agregó todo un apartado tercero a las Directrices, justo después del Principio de Responsabilidad Proactiva, que estatuye su implementación[50]. De esta manera, se incorporan los "*Programas de Manejo de la Privacidad*"[51] como un compendio de medidas que permiten acreditar el debido cumplimiento a los principios básicos establecidos en las Directrices.

Algo a destacar respecto a este punto, en el que no se entrará en profundidad, es que este nuevo apartado justamente recoge el desarrollo e importancia que ha tenido, en los últimos años, el Principio de Responsabilidad Proactiva[52]. No es de extrañar entonces que inclusive, explícitamente, establezca como obligación[53] que el responsable de datos esté "*preparado para demostrar que su programa de manejo de la privacidad es apropiado*"[54] ante la solicitud de la respectiva autoridad. Similar técnica utilizó, como vimos anteriormente, el GT29.

En segundo lugar, las Directrices del 2013 introducen un nuevo concepto: la obligación de notificar las brechas de seguridad[55], tanto a las autoridades correspondientes como a las personas afectadas por las mismas. Este último punto será desarrollado con mayor detalle en los apartados subsiguientes de este ensayo.

---

[48] OECD, 2013, op. cit., pp. 11-37.
[49] Ibid., pp. 3.
[50] Ibid., pp. 16. Véase "*PART THREE. IMPLEMENTING ACCOUNTABILITY*"
[51] Ibid., pp. 23.
[52] Loc. cit.
[53] Ibid., pp. 16. Así lo indica el parágrafo 15 letra b) de las Directrices del 2013: "*Be prepared to demonstrate its privacy management programme as appropriate".* Traducción nuestra.
[54] Ibid., pp. 25.
[55] OECD, 2013, op. cit., pp. 3.

## 1.3. EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UE

El año 2016, la Unión Europea adoptó el Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se derogó la Directiva 95/46/CE. Además, a su entrada en vigor el 25 de mayo de 2018, el Comité Europeo de Protección de Datos (en adelante el "CEPD") pasó a reemplazar al GT29.

Desde el año 2016 al año 2018, las empresas y organizaciones tuvieron la oportunidad de utilizar esta marcha blanca para adecuar sus políticas al RGDP. Este además incluyó notables innovaciones, como que su esfera de aplicación se extendiera también a empresas fuera de la Unión Europea cumpliéndose con ciertas condiciones.[56]

Del mismo modo, y a diferencia de lo establecido en la Directiva, el RGPD consagra nuevos deberes y obligaciones que deben ser cumplidos no solo por el responsable del tratamiento, sino que también por el encargado del procesamiento de los datos personales, el que se arriesga a ser sancionado por incumplimientos de la normativa. En la misma línea, el encargado del tratamiento solo puede subcontratar a terceros para llevar a cabo actividades de procesamiento de datos únicamente con el consentimiento del responsable del tratamiento, cuestión que a su vez queda reforzada por una marcada lógica contractual, esencial para garantizar los derechos y libertades de los titulares de los datos personales y los principios y deberes impuestos por la normativa.[57]

En ese sentido, se trata de una normativa extremadamente compleja y ambiciosa, mucho más extensa que la anterior Directiva, ya que posee 173 recitales y 99 artículos, pero que comparte en variadas oportunidades los principios y valores que han caracterizado el desarrollo de esta materia en la Unión Europea, con un efecto, eso sí, mucho mayor a nivel internacional.[58]

Así, se ha convertido en el más alto estándar en materia de protección de datos personales, y ha sido y está siendo, como en el caso de Chile, un punto de referencia para la actualización y modernización de un sinnúmero de legislaciones relacionadas a esta materia alrededor del mundo.[59]

---

[56] FRIGERIO, Catalina. *Mecanismos De Regulación De Datos Personales: Una Mirada Desde El Análisis Económico Del Derecho*. Revista Chilena de Derecho y Tecnología 7(2): 2018, pp. 2. doi:10.5354/0719-2584.2018.50578.
[57] MCMULLAN, Katie, 2018, op. cit., pp. 63.
[58] Ibid., pp. 60.
[59] EUROPEAN COMMISSION (EC). *Commission Staff Working document accompanying the document: Communication from The Commission to the European Parliament and The Council: Data protection rules as a pillar*

Hace pocos meses, y luego de un poco más de dos años desde su entrada en vigor, la Comisión Europea ha publicado su informe de evaluación respecto a la aplicación del RGDP. Por ello, se deja de manifiesto que este "*ha cumplido la mayoría de sus objetivos, (…) ha creado un nuevo sistema europeo de gobernanza y control del cumplimiento (y) ha demostrado su flexibilidad para apoyar soluciones digitales en circunstancias imprevistas*".[60]

La importancia que tiene el RGPD para este ensayo es que crea, tal como fue referenciado, un sistema de cumplimiento. Este tipo de sistemas pueden estar basados "*tanto en la lógica del 'compliance' o en la lógica de 'rendición de cuentas*'"[61]. Así, y siguiendo la propuesta del GT29, este sistema se basa en aquel último factor, y tiene como eje vertebrador al Principio de Responsabilidad Proactiva, que se estatuye explícitamente en el RGPD en su artículo 5(2):

> "*El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 (Principios relativos al tratamiento) y capaz de demostrarlo*".[62]

Además, en su artículo 24(1), se desarrolla este principio de tres maneras:

- *"(El) responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento.*
- *Las medidas deberán estar basadas en virtud del riesgo (del tratamiento) y ser proporcionales.*
- *Dichas medidas se revisarán y actualizarán cuando sea necesario".*[63]

Nuevamente se puede constatar, tal como fue comentado anteriormente, que no se indican específicamente cuáles son las medidas que se espera el responsable implemente para demostrar su cumplimiento. De todas maneras, las diferentes autoridades de protección de datos de los países miembros de la Unión Europea y el propio CEPD, desde la adopción de este Reglamento, han estado constantemente creando y desarrollando guías, directrices y

---

*of citizens empowerment and EUs approach to digital transition - two years of application of the General Data Protection Regulation*. 2020a, pp. 20. Disponible en https://bit.ly/2CdjTjV.

[60]EUROPEAN COMMISSION (EC). *Informe de la Comisión: las normas de protección de datos de la UE empoderan a los ciudadanos y están adaptadas a la era digital*. European Union's Official Website. 2020b. Comunicado de prensa disponible en: https://bit.ly/2ZM6kAe.

[61] DE HERT, Paul., 2012, op. cit., pp. 199. Traducción nuestra.

[62] UE, 2016, op. cit., pp. 36.

[63] INFORMATION COMMISSIONER'S OFFICE (ICO). *Guide to the General Data Protection Regulation (GDPR)*. [en línea] 2019, pp. 170. Disponible en https://bit.ly/3fbFN5H.

herramientas que permiten hilar y explicar el sistema de medidas previstas por el propio RGPD.[64]

Además, los beneficios que trae la inclusión de este principio al RGPD no solo se limitan a conseguir un mejor y mayor cumplimiento legal de las obligaciones y principios estatuidos por este, sino que ofrece la oportunidad de demostrar, competitivamente, cómo los responsables de tratamiento respetan los derechos y la privacidad de los titulares de los datos, desarrollando y manteniendo la confianza depositada por estos en manos de los responsables.[65]

Entonces, de la lectura de los artículos antes referenciados, podemos definitivamente asentar la significación del Principio de Responsabilidad Proactiva. En ese sentido, el responsable del tratamiento de datos es el encargado del cumplimiento de los principios y obligaciones que emanan de estos, y además debe ser capaz de demostrarlo, adoptando todas aquellas medidas técnicas y organizativas necesarias.

Lo anterior supone una determinada conducta proactiva y preventiva (no reactiva) por parte del responsable, a miras de obtener evidencia tangible que permita probar que implementó, internamente y durante sus actividades, una aproximación organizada, rigurosa y segura respecto a la protección de los datos personales mediante la adopción de medidas proporcionales al tipo y fines del tratamiento que realiza o piensa realizar.[66]

De esta manera, el responsable de datos no solo sabe qué tiene que cumplir con la normativa, sino que además debe preguntarse ¿Cómo demuestro que cumplí con ella? Así, va a poder responder a esta última pregunta escogiendo, cumpliendo o implementando una batería de medidas y obligaciones que le van a permitir acreditar dicho cumplimiento frente a la autoridad correspondiente. Por consiguiente, al implementar estas medidas de manera preventiva y proactiva se cumple y refuerza uno de los objetivos más importantes en esta materia, y es que se evita que los riesgos de un determinado tipo de tratamiento de datos se materialicen, pudiendo afectar los derechos de los titulares de dichos datos.

Sin embargo, debe quedar claro que lo que se busca al incorporar un sistema de cumplimiento como este, en materia de protección de datos personales, va más allá de realizar un ejercicio de chequeo o verificación por parte del responsable, en el sentido de pensar, erróneamente,

---

[64] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *FACILITA RGPD: Herramienta de ayuda para empresas que realicen un tratamiento de datos personales de escaso riesgo para el cumplimiento del Reglamento General de Protección de Datos*. [en línea] s/f, Disponible en https://bit.ly/3gGDEiD.
[65] ICO, 2019, op. cit., pp. 169.
[66] Ibid., pp. 170.

que por el hecho de haber cumplido o utilizado todas las medidas disponibles se garantiza de verdad el cumplimiento a los deberes y principios establecidos en la normativa. Así, lo que se busca en el fondo es que las empresas y organizaciones demuestren que han internalizado y desarrollado una cultura de protección de datos personales en su ADN.[67]

Tomando en consideración lo anterior, y de forma ilustrativa, se pasará a nombrar cada una de las medidas más importantes que pueden implementarse en el sistema de cumplimiento del RGPD, con el objetivo de ser analizadas, explicadas y demostrar, durante el desarrollo del Capítulo 2 de este ensayo, que nuestro Proyecto de Ley se basa en este sistema y que este puede todavía ser perfeccionado.

Las medidas a las que hace referencia el RGPD se podrían resumir en las siguientes[68]:

- Registro de Actividades del Tratamiento
- Adopción de medidas de seguridad
- Obligación de notificar las brechas de seguridad
- Principio de protección de datos desde el diseño y por defecto
- Evaluaciones de Impacto
- Delegado de Protección de Datos
- Códigos de Conducta y Mecanismos de Certificación
- Uso de Cláusulas Contractuales Tipo

[67] POTHOS, Mary. *Accountability Requirements*. En: INTERNATIONAL ASSOCIATION OF PRIVACY PROFFESIONALS (IAPP), *European Data Protection: Law and Practice*. Ed: Eduardo Ustaran, 2018, pp. 205.
[68] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *Medidas de Cumplimiento*. [en línea] 27 de Febrero de 2020a, Disponible en: https://bit.ly/2Z7IkrU.

## CAPÍTULO SEGUNDO: EL PROYECTO DE LEY Y SU RELACIÓN CON EL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

El Proyecto de Ley ha sido elaborado tomando como base dos iniciativas, ambas del año 2017, que se han refundido en un solo texto. La primera de ellas correspondió a la Moción Parlamentaria (en adelante la "Moción") presentada por los Honorables Senadores Harboe, Araya, De Urresti, Espina y Larraín, sobre protección de datos personales[69], mientras que la segunda correspondió al Mensaje de S.E la Presidenta de la República (en adelante el "Mensaje"), que regula la protección y el tratamiento de datos personales y crea la Agencia de Protección de Datos Personales.[70]

Ambas iniciativas comparten un mismo objetivo y líneas generales[71], especialmente respecto a la importancia de que Chile adecúe sus niveles de protección de datos personales al estándar internacional, representado actualmente por las recomendaciones de la OCDE y el RGPD.

Además, durante la tramitación de ambas iniciativas en el Senado, el 16 de junio del año 2018, se publicó la Ley N°21.096, que elevó a garantía constitucional la protección de datos personales[72]. La antedicha consagración se dio gracias a la presentación de un proyecto de reforma constitucional el año 2014, iniciado en moción por los Honorables Senadores señores Harboe, Araya, Lagos, Larraín y Tuma, que pretendía consagrar el denominado derecho a la "autodeterminación informativa".[73]

Las razones que fundamentaron su presentación tienen ligación con el anhelo, desde la entrada en vigor de la Ley N°19.628, de actualizar el marco constitucional de derechos y garantías al estándar que se había llegado en países europeos como Alemania, España, Portugal y países latinoamericanos como Argentina, México, Brasil y Paraguay,[74] que vieron

[69] CHILE. Proyecto de ley sobre Protección de Datos Personales. Boletín N°11.092-07. Enero del 2017. Disponible en https://bit.ly/3iAuTbX.
[70] CHILE. Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N°11.144-07. Marzo del 2017. Disponible en https://bit.ly/3fb3knt.
[71] COMISIÓN CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO DEL SENADO (CCLJRS). *Primer Informe sobre el Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletines 11.144-07 y 11.092-07, refundidos)*. Marzo del 2018, pp. 5. Disponible en https://bit.ly/2CeD5hm.
[72] CHILE. Ley N°21.096, *Consagra el Derecho a la Protección de los Datos Personales*. Diario Oficial de la República de Chile, Santiago, Chile, 16 de Junio de 2018. Disponible en: https://bit.ly/3a7Z6NN
[73] CHILE. Proyecto de reforma constitucional que consagra el derecho a la protección de los datos personales. Boletín N°9.384-07. Junio de 2014. Disponible en: https://bit.ly/2IGXWxo
[74] COMISIÓN CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO DE LA CÁMARA DE DIPUTADOS (CCLJRD). *Segundo Informe recaído en el proyecto de reforma constitucional que consagra el derecho a la protección de los datos personales (Boletín 9.384-07).* Abril de 2018, pp. 9. Disponible en: https://bit.ly/3oI2DWZ

en el creciente uso de las tecnologías informáticas y digitales, tanto por el sector público como privado, y transferencias y procesamiento de información, la oportunidad de equilibrar y garantizar el libre flujo de la información, imprescindible para el desarrollo económico de cualquier sociedad moderna, con el resguardo de los derechos y libertades de los titulares de dichos datos.[75]

Así, el derecho a la "autodeterminación informativa" consiste en otorgarle a todas las personas el derecho a conocer quién tiene sus antecedentes, qué tipo de antecedentes posee, para qué los utilizan, con qué fines y cuáles son los ámbitos que limitan ese tratamiento de datos, derecho que tuvo como origen la ley del censo en Alemania el año 1983.[76]

Por ello, no es de extrañar que en nuestro Congreso Nacional, y producto de que la tramitación de esta iniciativa se vio prácticamente en paralelo y como complemento al Proyecto de Ley que nos compete, se haya celebrado y recomendado la inclusión constitucional de este derecho, especialmente si se toma en consideración que ya había sido objeto de discusión doctrinal, en el Tribunal Constitucional, el reconocimiento implícito del derecho a la protección de datos personales por su estrecha relación con el derecho a la protección de la vida privada.[77]

Gracias a este esfuerzo, actualmente el artículo 19 N°4 de la Constitución de 1980 asegura a todas las personas:

> *"El respeto y protección a la vida privada y a la honra de la persona y su familia,* ***y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley****;"*[78]

La antedicha concepción constitucional no es arbitraria, en el sentido de que dista bastante de lo que en un comienzo propuso la moción parlamentaria formalmente[79], aunque mantuvo lo que buscaba consagrar en el fondo. Lo anterior se explica por las múltiples indicaciones que recibió el proyecto de reforma constitucional, y que abrió debates respecto a, por ejemplo, si

---

[75] ÁLVAREZ VALENZUELA, Daniel, 2020, op. cit., pp. 2.
[76] CCLJRD, 2018, op. cit., pp. 7.
[77] CCLJRD, 2018, op. cit., pp. 9.
[78] CHILE. Constitución Política de la República de Chile, Diario Oficial de la República de Chile, Santiago, Chile, pp. 7. Disponible en: https://bit.ly/3oKneK6. El destacado es nuestro y resalta la reforma constitucional hecha por la Ley N°21.096 al artículo 19 N°4 de la Constitución.
[79] La moción parlamentaria propuso lo siguiente: "*Toda persona tiene derecho a la protección de sus datos personales y obtener su rectificación, complementación y cancelación, si estos fueren erróneos o afectaren sus derechos, como asimismo a manifestar su oposición, de acuerdo con las disposiciones establecidas en la ley. Su tratamiento sólo podrá hacerse por ley o con el consentimiento expreso del titular*". Boletín N°9.384-07, 2014, op. cit., pp. 6.

existía un derecho de propiedad sobre los datos personales, discusión que nos ayuda a interpretar lo contrario y a establecer, sin lugar a dudas, que se trata de un derecho integral y sistemáticamente autónomo, que le permite a cualquier persona el mantener el control sobre sus propios datos personales aun cuando estos hayan sido entregados a alguien para su tratamiento.[80]

Por otra parte, la técnica constitucional empleada deja entrever la estrecha relación que tuvo con la tramitación del Proyecto de Ley, ya que contiene sustancialmente una reserva legal especial, es decir, la regulación sobre la protección y el tratamiento de datos personales siempre debe adoptar la forma de una ley, excluyendo de esta manera mecanismos infralegales de regulación, y un mandato al legislador para que este determine las formas y condiciones de esta protección y tratamiento de los datos personales.[81]

Así, ambas iniciativas que componen el Proyecto de Ley comparten el diagnóstico de que la Ley N°19.628, sobre Protección a la Vida Privada, aunque fue pionera en la región en esta materia el año 1999 estableciendo una serie de principios y garantías, no está ahora a la altura de los cambios tecnológicos, las legislaciones internacionales, el aumento de la cantidad de datos tratados e intercambiados ni está enfocada en la protección de los derechos de las personas.[82]

Por otro lado, el ingreso de Chile a la OCDE el año 2010 significó el compromiso de su adecuación normativa y modificación de su marco legal en esta materia. Pero Chile no solo debe responder a las exigencias de la OCDE, ya que también es parte de la Organización de las Naciones Unidas (ONU), la Organización de los Estados Americanos (OEA), el Foro de Cooperación Económica Asia-Pacífico (*Asia-Pacific Economic Cooperation*, APEC) y la Red Iberoamericana de Protección de Datos, los que desde hace tiempo han establecido directrices o marcos generales regulatorios en materia de protección de la vida privada y tratamiento de datos personales.[83]

Inclusive, sigue rigiendo el acuerdo de Asociación entre la Unión Europea y Chile, del año 2003, el que estatuye en su Artículo 202 que "*Las Partes acuerdan otorgar un elevado nivel de protección al procesamiento de datos personales y de otra índole, compatible con las más*

[80] CCLJRD, 2018, op. cit., pp. 11.
[81] ÁLVAREZ VALENZUELA, D., 2020, op. cit., pp. 3.
[82] CCLJRS, 2018, op. cit., pp. 9 y 13.
[83] Ibid., pp. 156-157.

*altas normas internacionales*" [84]. Cabe destacar que la más alta norma internacional en la materia actualmente es el RGPD de la Unión Europea.[85]

Así, ambas iniciativas explícitamente reconocen que tienen como punto de referencia al RGPD y a las Directrices de 2013 de la OCDE. De esta manera, se incorporan un conjunto principios rectores[86], se mejoran y amplían el catálogo de definiciones y los derechos de las personas (como los derechos ARCO y de Portabilidad), se establecen procedimientos directos y un sistema de responsabilidad y cumplimiento que considera deberes y sanciones para los responsables del tratamiento de datos, además de nuevos estándares respecto al tratamiento de datos sensibles y categorías especiales de datos personales. Por último, el Mensaje crea además una autoridad de control encargada de velar por los derechos de las personas titulares de datos.[87]

Hoy en día, el Proyecto de Ley se encuentra en tramitación en la Comisión de Hacienda del Senado, luego de que la Comisión de Constitución, Legislación, Justicia y Reglamento (en adelante la "Comisión") emitiera su 2do informe habiendo finalizado su discusión en general y particular. Por lo tanto, se encuentra próximo a iniciar su 2do trámite Constitucional en la Cámara de Diputados.

No obstante todo lo anterior, debido a que el Proyecto de Ley se elaboró discutiendo en conjunto y en particular ambas iniciativas descritas, tomando como punto de partida al Mensaje[88] del ejecutivo, se pasó por alto el hecho de que no se consagró explícitamente el Principio de Responsabilidad Proactiva, alrededor del cual fue construido el sistema de responsabilidad y cumplimiento propuesto.

Así, al ponerse en consideración particular el Principio de Responsabilidad Proactiva (*Accountability Principle*) en la Comisión, se tuvieron a la vista las propuestas de ambas iniciativas, siendo aconsejado por el grupo de asesores parlamentarios que se aprobara el texto del ejecutivo[89], ya que fue el punto de partida en la discusión, quedando de esta forma consagrado el artículo 3 letra e) del Proyecto:

---

[84] CHILE. MINISTERIO DE RELACIONES EXTERIORES. *Decreto Supremo N°28 que promulga el Acuerdo por el que se establece una Asociación entre la República de Chile, por una parte, y la Comunidad Europea y sus estados miembros, por la otra, sus anexos, declaraciones conjuntas y la corrección introducida al articulo 40 del Anexo III, en su versión en español*. 2003. Disponible en https://bit.ly/2VWl12t.
[85] CCLJRS, 2018, op. cit., pp. 157.
[86] Los principios rectores son el de licitud del tratamiento, de finalidad, de proporcionalidad, de calidad, de responsabilidad, de seguridad, de transparencia y el principio de confidencialidad.
[87] CCLJRS, 2018, op. cit., pp. 9-10 y 14-20.
[88] Ibid., pp. 207.
[89] Ibid., pp. 250-251.

*"Quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes de conformidad a la ley".*[90]

Queda patente de la sola lectura de su texto y luego de haber estudiado el desarrollo de este principio en el anterior capítulo, que existió un error terminológico a la hora de presentar la propuesta por parte del ejecutivo, el que considera solamente un principio de responsabilidad legal general (*Responsability*). Por el otro lado, la Moción Parlamentaria propuso lo siguiente en su artículo 8 letra f):

*"Responsabilidad y rendición de cuentas: El responsable del tratamiento será responsable del cumplimiento de la presente ley,* ***debiendo ser capaz de demostrarlo****".*[91]

Lamentablemente, dicho texto fue desechado por la Comisión sin mayor discusión. No obstante, deja en claro que la propuesta de la Moción está acorde o es, mejor dicho, más cercana al estándar internacional sobre el que se supone ambas iniciativas fueron construidas (el RGPD). Sin embargo, la tramitación en particular lógicamente no se detuvo, por lo que se dejará patente en lo que resta de este capítulo que el sistema de cumplimiento y responsabilidad propuesto por el Proyecto está basado, casi íntegramente, en el establecido por el RGPD que, como fue explicado *ut supra,* contempla una serie de medidas complementarias destinadas a demostrar el debido cumplimiento al Principio de Responsabilidad Proactiva, sobre el que gira todo el sistema y que el Proyecto, actualmente, no consagra.

Entonces, se pasará a revisar el sistema de cumplimiento propuesto hoy en día por el Proyecto, analizando crítica y sintéticamente las medidas que contempla haciendo una comparación a lo establecido por el RGPD, con el objetivo específico de realizar las propuestas y modificaciones pertinentes que le doten de coherencia y sistematicidad al mismo, y con el objetivo general de defender la inclusión explícita del Principio de Responsabilidad Proactiva.

[90] COMISIÓN CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO DEL SENADO (CCLJRS). *Comparado Primer Trámite Constitucional: 2do Informe sobre el Proyecto de Ley que modifica la ley 19.628, con el fin de regular la protección y el tratamiento de los datos personales (Boletines 11.144-07 y 11.092-07, refundidos)*. 2020a, pp. 18. Disponible en https://bit.ly/2CbKpKy.
[91] CCLJRS, 2018, op. cit, pp. 250. El destacado es nuestro.

## 2.1. SISTEMA DE CUMPLIMIENTO: MEDIDAS CONTEMPLADAS EN EL PROYECTO DE LEY Y EL RGPD

### 2.1.1. PRINCIPIO DE PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

El deber de protección de datos desde el diseño y por defecto (en adelante "PDdDI" y "PDpDE", respectivamente) es uno de los principios complementarios al Principio de Responsabilidad Proactiva más importantes.[92] Actualmente se encuentra estatuido en el marco del Título II, Párrafo Primero, "sobre deberes y obligaciones del responsable" del Proyecto de Ley, específicamente en su artículo 14 quáter[93], gracias a la indicación N°98 presentada por el Honorable Senador Harboe.[94]

La inclusión de este principio está en línea con lo establecido en el Artículo 25 del RGPD[95] y lo recoge casi en su totalidad, aumentando el estándar del Proyecto en esta materia. De esta manera, se logra compatibilizar los derechos de las personas titulares de datos y el libre flujo de dichos datos.

Al igual que en el artículo 25(1) del RGPD, el primer párrafo del artículo 14 quáter define lo que se entiende por PDdDI. En síntesis, considera que es deber del responsable el implementar "*las medidas técnicas y organizativas apropiadas con anterioridad y durante el tratamiento de datos con el fin de cumplir los principios del tratamiento de datos y los derechos del titular*"[96] establecidos en el Proyecto.

Además, dichas medidas deben considerar "*el estado de la técnica, los costos de implementación y la naturaleza, ámbito, contexto y fines del tratamiento de datos, así como los riesgos*"[97]. Como puede entreverse, este principio tiene mucha similitud con el Principio de Responsabilidad Proactiva estatuido por el RGPD, e inclusive pudieran llegar a confundirse.

---

[92] ICO, 2019, op. cit., pp. 171 y AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *Medidas de protección de datos desde el diseño y por defecto.* [en línea] 27 de Febrero de 2020b, Disponible en https://bit.ly/38zpQ6Y.
[93] CCLJRS, 2020a, op. cit., pp. 56.
[94] Boletín de indicaciones formuladas durante la discusión en general del proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletín de Indicaciones). 2018, pp. 20-21. Disponible en https://bit.ly/2Oi7yxT.
[95] UE, 2016, op. cit., pp. 48.
[96] CCLJRS, 2020a, op. cit., pp. 56.
[97] Loc. cit.

Sin embargo, la idea de la PDdDI existe desde hace más de 20 años y se ha trabajado en ella bajo la terminología de "privacidad desde el diseño", concepto desarrollado por la Comisionada de protección de datos de Ontario, Ann Cavoukian, en la década de los 90.[98]

Por ello, la definición de PDdDI implica que se realice una aproximación basada en los riesgos y en el Principio de Responsabilidad Proactiva que permita implementar estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (sea este un *hardware*, *software*, un sistema o servicio determinados), entendiéndose lo anterior como todas las etapas por la que atraviesa este, incluidas su concepción, desarrollo, producción, operación, mantenimiento y retirada.[99]

De todas maneras, es necesario que se interprete la idea anterior de la siguiente manera: la PDdDI se materializa en el deber de implementar medidas que permiten dar efectividad a los principios básicos y dar cumplimiento a las obligaciones de los responsables, por lo que refuerza al Principio de Responsabilidad Proactiva desde una mirada preventiva y proactiva, es decir, comparten objetivos.[100] Además, la PDdDI tiene como principio fundacional el de anticiparse a los eventos que afecten a la privacidad antes de que sucedan, lo que implica que todo sistema, proceso o infraestructura que vaya a utilizar datos personales debe ser concebido y diseñado, *a priori,* identificando los posibles riesgos a los derechos y libertades de los titulares de datos personales para minimizarlos y evitar que se materialicen en daños tangibles.[101]

La PDdDI ha sido considerada una "*buena práctica de aproximación al diseño de nuevos productos, sistemas y procesos que usan datos personales*",[102] integrando esta mirada preventiva en la estructura y actividades internas de las empresas u organizaciones, es decir, busca en el fondo "*que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto*".[103]

Una de las medidas que se pueden adoptar al respecto, y que ejemplifica el RGPD, es la seudoanonimización temprana de los datos personales, que permite que estos no puedan atribuirse a una persona sin utilizar información adicional, reemplazando los datos

[98] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *Guía de Privacidad desde el Diseño*. [en línea] [Archivo PDF] 2019a, pp. 5. Disponible en: https://bit.ly/341tmpH
[99] AEPD, 2019, op. cit., pp. 6.
[100] EUROPEAN DATA PROTECTION BOARD (EDPB). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. [en línea] Versión 2.0, 2020a, pp. 5. Disponible en https://bit.ly/3qGu2KF
[101] AEPD, 2019, op. cit., pp. 7.
[102] ICO, 2019, op. cit., pp. 171. Traducción nuestra.
[103] AEPD, 2020b, op. cit.

identificadores con datos ficticios y realistas que no pueden irrogarse a un determinado individuo, cumpliéndose así los principios de confidencialidad y minimización de datos. No obstante lo anterior, permite algunas formas de re-identificación, pero al mismo tiempo, reduce el vínculo de estos datos con la identidad original del titular a través de, por ejemplo, la encriptación de dichos datos.[104]

La aproximación que permite realizar la PDdDI, al igual que la PDpDE, ayuda a cumplir las obligaciones de los responsables al dejar documentado las decisiones que toma a través de, por ejemplo, las Evaluaciones de Impacto, medida que sirve a su vez para demostrar el debido cumplimiento al Principio de Responsabilidad Proactiva[105] y que será analizada más adelante. Dicha documentación se debe dar con un enfoque "*privacy design thinking*", sustentado anteriormente por una evaluación de los riesgos a los derechos y libertades de los titulares de datos como elemento integral de cualquier nueva iniciativa de tratamiento.[106]

En el mismo sentido, y para garantizar la privacidad durante todo el ciclo de vida del proyecto u objeto, se deben analizar las operaciones implicadas en cada una de las etapas de su desarrollo e implementar medidas tales como la clasificación y organización de los datos y actividades del tratamiento en base a perfiles de acceso, la k-anonimidad,[107] el cifrado por defecto de modo que el estado de los datos en caso de robo, destrucción o pérdida sea ilegible y la destrucción segura y garantizada de la información al final de su ciclo de vida.[108]

Finalmente, cabe destacar que el cumplimiento de la PDdDI es solamente aplicable al responsable del tratamiento. No obstante lo anterior, este cumplimiento se proyecta a otras entidades que participan de las actividades del tratamiento, como lo serían los proveedores y prestadores de servicios y desarrolladores o fabricantes de productos, aplicaciones y dispositivos, ya que el responsable debe diligentemente, y en virtud del Principio de Responsabilidad Proactiva, escoger a aquellas organizaciones y encargados que puedan

[104] ŠTARCHOŇ, Peter y PIKULÍK, Tomáš. *GDPR principles in Data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones.* Procedia Computer Science. Vol. 151, 2019., p. 306. DOI 10.1016/j.procs.2019.04.043.
[105] ICO, 2019, op. cit., pp. 187.
[106] AEPD, 2019, op. cit., pp. 8.
[107] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), *La K-anonimidad como medida de privacidad*, 2019b, pp. 3. Disponible en: https://bit.ly/3gAFRNY La AEPD define a este concepto de la siguiente manera: *"La k-anonimidad es una propiedad de los datos anonimizados que permite cuantificar hasta qué punto se preserva la anonimidad de los sujetos presentes en un conjunto de datos en el que se han eliminado los identificadores. Dicho de otro modo, es una medida del riesgo de que agentes externos puedan obtener información de carácter personal a partir de datos anonimizados*"
[108] AEPD, 2019a, op. cit., pp. 9.

garantizar el cumplimiento de la normativa y especialmente la protección de datos personales desde el diseño y por defecto.[109]

Por otro lado, la PDpDE está establecida en el párrafo segundo del artículo 14 quáter del Proyecto, al igual que en el artículo 25(2) del RGPD. En síntesis, indica que el responsable debe implementar "*las medidas técnicas y organizativas para garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales que sean necesarios para los fines específicos y determinados del tratamiento*".[110]

Lo anterior hace referencia a las decisiones que toma el responsable respecto a determinadas opciones durante el proceso que, por defecto, en determinados softwares, programas computacionales o dispositivos[111], ajustan la cantidad de "*datos recogidos, la extensión del tratamiento, el plazo de conservación de los datos y su accesibilidad*".[112]

Supone entonces que el responsable debe evaluar y asegurar, con anterioridad, que solo los datos necesarios para el tipo y fines del tratamiento sean utilizados, impidiendo de esta manera que dichos datos sean accesibles a un grupo indeterminado de personas.[113] Debe tenerse especial consideración respecto de aquellas personas que trabajan en la misma organización o se relacionan con ella, como prestadores de servicios de software o procesamiento de datos, evitando y minimizando el cruce de información innecesaria entre los distintos tratamientos que se realizan.[114]

En resumen, la inclusión de ambos principios constituye un gran avance en el Proyecto de Ley, pero su reciente introducción deja entrever una falta de certeza respecto a cómo pueden implementarse las medidas que permitan dar cumplimiento a estos deberes ya que, por ejemplo, el Proyecto actualmente no consagra explícitamente las Evaluaciones de Impacto[115], las que fueron desechadas antes de la presentación de la indicación del Honorable Senador Harboe.

Por otro lado, a diferencia del RGPD, el texto del artículo 14 quáter del Proyecto de Ley no menciona ni ejemplifica cuáles son las medidas que se pueden adoptar, por lo que sería prudente que se incluyeran ejemplos de medidas concretas (como la seudoanonimización,

[109] Ibid., pp. 11-12.
[110] CCLJRS, 2020a, op. cit., pp 56.
[111] EDPB, 2020a, op. cit., pp. 11.
[112] CCLJRS, 2020a, op. cit. pp. 57.
[113] EDPB, 2020a, op. cit., pp. 11.
[114] Ibid., pp. 29-30.
[115] CCLJRS, 2018, op. cit., pp. 331.

Evaluaciones de Impacto o Mecanismos de Certificación) que permitan acreditar el debido cumplimiento a estos deberes. De esta manera, lo que debiese de hacerse es guiar la lectura del sistema tomando como referencia el texto de la Ley.

En el fondo, la inclusión de estos deberes sin un marco claro de medidas y sin, por supuesto, el Principio de Responsabilidad Proactiva, termina por restarle efectividad y certeza al sistema de cumplimiento, perdiéndose una gran oportunidad de reforzar los deberes de los responsables y ofrecerles, al mismo tiempo, medidas efectivas que les permitan acreditar y entender sus obligaciones con la sola lectura de la normativa.

### 2.1.2. ADOPCIÓN DE MEDIDAS DE SEGURIDAD Y NOTIFICACIÓN DE LAS BRECHAS DE SEGURIDAD

La ciberseguridad a nivel global y regional ha tomado un papel preponderante en la agenda pública, no solo para elevar sus niveles en el sector público, por ejemplo, en materia de Gobierno Digital, sino que para asegurar el desenvolvimiento de la creciente actividad digital y el comercio electrónico.

Así, más allá de la excepcionalidad de la pandemia de la Covid-19, la preocupación por la ciberseguridad se estaba dando incluso anteriormente. Por ejemplo, el "Reporte de Riesgos Globales 2020" del Foro Económico Mundial (WEF, por sus siglas en inglés), tomando como base que más de la mitad de la población mundial tiene acceso a internet y que prácticamente 1 millón de personas, diariamente, se está integrando a esta tecnología, estableció que los riesgos de ciberataques a infraestructura crítica y el robo de datos están dentro de los 10 principales riesgos con mayor probabilidad de ocurrir.[116]

En esta línea, recientemente el "Reporte de Ciberseguridad 2020" del Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA) da cuenta de una creciente capacidad en materia de ciberseguridad en Latino América y el Caribe desde el año 2016.[117]

Este reporte utiliza el "Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones" (CMM, por sus siglas en inglés), que sigue un enfoque integral que entiende esta capacidad dentro de cinco dimensiones: i) Política y Estrategia; ii) Cultura y Sociedad; (iii)

[116] WORLD ECONOMIC FORUM (WEF). *The Global Risks Report 2020.* Suiza, 15 de Enero de 2020, pp. 63-67. Disponible en: https://bit.ly/348zrAL

[117] BANCO INTERAMERICANO DE DESARROLLO Y ORGANIZACIÓN DE ESTADOS AMERICANOS (BID y OEA). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*, 2020, pp. 17. http://dx.doi.org/10.18235/0002513

Educación, Capacitación y Habilidades; (iv) Marcos Legales y Regulatorios, y v) Estándares, Organizaciones y Tecnología.[118] Desarrollado por el Centro Global de Capacidad en Seguridad Cibernética (GCSCC, por sus siglas en inglés), de la Universidad de Oxford, busca ofrecer una evaluación del nivel de ciberseguridad de un país, asignándole una etapa específica, existiendo de esta manera cinco etapas de madurez para cada una de las dimensiones, que van desde la más básica (inicial) hasta la más avanzada (dinámica).[119]

La importancia de este reporte radica en que deja patente la relevancia de que exista una única política nacional de ciberseguridad y una sólida institucionalidad que pueda dar curso y efectividad a esta materia de manera estratégica, ya que países con esas características obtienen resultados positivos en ciberseguridad.[120] Lo anterior va de la mano con una creciente necesidad de garantizar la confianza digital, a medida que Latino América avanza hacia la economía digital.[121]

De esta manera, Chile ha dado importantes pasos ya que presentó el año 2017 su "Estrategia Nacional de Ciberseguridad" y además, el año 2018, en virtud de su "Política Nacional de Ciberseguridad" se nombró a un asesor presidencial en esta materia, reestructurando la Subsecretaría del Interior para llevar a cabo la Política a través de la Unidad de Coordinación de Ciberseguridad.[122]

Sin embargo, el marco normativo de Chile se encuentra, como se sabe, en actualización. Importante es destacar que en la dimensión "Marcos Legales y Regulatorios" del CMM, en el subcomponente de "Legislación sobre Protección de Datos", Chile alcanzó la etapa N°3 "consolidado", producto del ingreso y tramitación del Proyecto de Ley en cuestión. No obstante aquello, sigue en espera que se presente el "proyecto de Ley Marco de Ciberseguridad", que estaba agendando para finales de 2019, y que permitiría establecer una institucionalidad permanente que vele por la implementación y efectividad de la seguridad cibernética en Chile.[123]

Por tanto, no se puede hablar de protección de datos personales sin hablar de ciberseguridad. Se trata de materias altamente interrelacionadas en las que Chile se encuentra trabajando prácticamente en paralelo, lo que a su vez conlleva una serie de ventajas ecosistémicas. Así,

[118] Ibid., pp. 20.
[119] BID y OEA, 2020, op. cit., pp. 42.
[120] Ibid., pp. 21.
[121] Ibid., pp. 29
[122] Ibid., pp. 75.
[123] Ibid., pp. 76-78.

es imprescindible que en un primer lugar, el Proyecto de Ley sobre Protección de Datos Personales sea aprobado en el Congreso, en vista y considerando que el ecosistema regulatorio chileno en estas materias se encuentra extremadamente atrasado y, no menos importante, estaría constituyendo las bases necesarias para luego discutir y generar un ecosistema regulatorio en materia de ciberseguridad armónico, más aun si consideramos que Chile se enfrenta a un proceso constituyente[124] en donde la propia Constitución Política de la República debe ser parte de este nuevo ecosistema regulatorio.[125]

Así lo ha recomendado la propia Unión Europea en su reciente "*2020 E-Government Survey*", donde destaca la importancia de que los gobiernos establezcan un sistema institucional que sostenga e implemente el ecosistema regulatorio relativo a ciberseguridad, protección de datos personales e inclusive legislación en relación con materias tales como Inteligencia Artificial[126], en la que también Chile se encuentra trabajando.

Por ello, y para comenzar el análisis del Proyecto en materia de ciberseguridad, no es de extrañar que, al igual que en el artículo 32 del RGPD[127], el Proyecto de Ley contemple en su artículo 14 quinquies[128] el deber del responsable de adoptar medidas de seguridad en el tratamiento de datos.

En primer lugar, establece que el responsable debe tomar las "*medidas necesarias para resguardar el cumplimiento del principio de seguridad*"[129], pero tomando en consideración el avance de la tecnología, sus costos y la proporcionalidad respecto a los fines y características del tratamiento, tanto como los riesgos involucrados.

Además, estatuye que ante la ocurrencia de un incidente de seguridad, y ante la solicitud de la autoridad respectiva, "*corresponderá al responsable acreditar la existencia y funcionamiento de las medidas de seguridad adoptadas en base a los niveles de riesgos y a la tecnología disponible*"[130]. Es decir, estamos en presencia de una disposición que textualmente, al igual

---

[124] MOLINA, Paulina. *Plebiscito histórico en Chile: apruebo o rechazo, las opciones que tenían los chilenos en el referendo de cambio de Constitución.* BBC Mundo: News. [en línea] Octubre de 2020. Disponible en: https://bbc.in/346edmL

[125] LISONI, Diego. *Modernización y Transformación Digital del Estado: Desafíos, Oportunidades y Propuestas a la luz de la Crisis Sanitaria y el Estallido Social en Chile.* CAF- Banco de Desarrollo de América Latina, 2020, pp. 16. Disponible en: https://bit.ly/3afGE5A

[126] DEPARTAMENTO DE ASUNTOS ECONÓMICOS Y SOCIALES DE LA ORGANIZACIÓN DE NACIONES UNIDAS [ONU:DAES]. *United Nations E-Government Survey 2020*. [s.l.]: United Nations, 2020, pp. 190. Disponible en: https://bit.ly/3a9TzpQ

[127] UE, 2016, op. cit., pp. 51-52.

[128] CCLJRS, 2020a, op. cit., pp. 57.

[129] Loc. cit.

[130] Ibid., pp. 58.

que en el RGPD, previene que el responsable debe ser capaz de demostrar que efectivamente adoptó medidas de seguridad.

No cabe duda de que por medio de este deber se logra dar efectividad y materializar el principio de seguridad, establecido en el artículo 3 letra f) del Proyecto y que estatuye lo siguiente:

> *"Principio de seguridad. En el tratamiento de los datos personales, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza de los datos".*[131]

No obstante lo anterior, el Principio de Responsabilidad Proactiva permitiría reforzar y dotar de coherencia a la antedicha obligación, ya que por medio de este el responsable, si quiere demostrar cumplimiento a este deber, necesita primero haber tomado las medidas prestablecidas para aquello y que el Proyecto ya considera a medias, por lo que el estándar no aumenta, sino que simplemente se ve reforzado.

Por otro lado, el hecho de que solo se describan a las medidas como "necesarias" no permiten significar verdaderamente el tipo de medidas que se pueden o deben adoptar. En ese sentido, se sugiere que, tal como fue propuesto por el Honorable Senador Guillier en la indicación N°99, se hable de "*medidas técnicas y organizativas necesarias*"[132], ya que de esta manera se construye, de a poco, un sistema de cumplimiento que habla en los mismos términos en toda su extensión.

Es así como, en general, se puede afirmar que el Proyecto de Ley está a la altura en esta materia respecto al estándar internacional. De todas maneras, se deja entrever nuevamente que no existe una señalización o ejemplificación de las medidas que podrían considerarse como necesarias y eficaces para demostrar el debido cumplimiento al principio de seguridad. Por ejemplo, el RGPD en su artículo 32(1) literal a) propone la utilización de la seudoanonimización y el cifrado de datos, o la adhesión a códigos de conducta y mecanismos de certificación en su tercer apartado como medios para demostrar el cumplimiento a esta obligación. Además, se considera que la adopción de políticas de seguridad o la capacitación

[131] CCLJRS, 2020a, op. cit., pp. 18-19.
[132] Boletín de Indicaciones, 2018, op. cit., pp. 21.

del personal en ciberseguridad son medidas organizativas que permiten demostrar el debido cumplimiento al mismo.[133]

En segundo lugar, al igual que en los artículos 33 y 34 del RGPD[134], el Proyecto de Ley en su artículo 14 sexíes establece la obligación del responsable de datos de notificar las vulneraciones a las medidas de seguridad a la autoridad de control, es decir, al Consejo para la Transparencia y Protección de Datos Personales.[135]

Esta comunicación debe realizarse cuando estas vulneraciones "*ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no autorizados a dichos datos cuando exista un riesgo para los derechos y libertades de los titulares".* [136]

Además, el responsable y encargado del tratamiento deberán llevar un registro de dichas comunicaciones, que incluirá la descripción de la naturaleza de las vulneraciones, sus efectos, las categorías de datos, la cantidad de titulares afectados y, especialmente, las medidas adoptadas para gestionar las vulneraciones y evitar incidentes futuros. Cuando las vulneraciones refieran a categorías especiales de datos, como los datos sensibles, se deberán comunicar también a los titulares de dichos datos.[137]

Sin embargo, cabe destacar en este apartado un agujero en la técnica legislativa utilizada por el Legislador, ya que por un lado se solicita que se lleve un registro de este tipo de notificaciones, pero por el otro lado, el Proyecto no considera, tal como lo hace el RGPD, la obligación de llevar un registro de las actividades del tratamiento, que justamente es utilizado y es una medida imprescindible para materializar y organizar este tipo de medios de prueba.

Particularmente, se entiende que la vulneración ocasiona la destrucción de los datos personales cuando estos dejan de existir o no permiten que sean utilizados de ninguna forma por el responsable del tratamiento. Por su parte, las vulneraciones ocasionan la pérdida de datos personales cuando estos, aun cuando sigan existiendo, dejan de estar en manos o el control del responsable del tratamiento, o este último ha perdido acceso a ellos.[138]

---

[133] ICO, 2019, op. cit., pp. 230.
[134] UE, 2016, op. cit., pp. 52-53.
[135] CCLJRS, 2020a, op. cit., pp. 59.
[136] Loc. cit.
[137] Ibid., pp. 60.
[138] ARTICLE 29 DATA PROTECTION WORKING PARTY (ART. 29WP), *Guidelines on Personal data breach notification under Regulation 2016/679*. 2017a, Bruselas, Bélgica, pp. 7. Disponible en: https://bit.ly/3mmHal2

Por otro lado, es necesario clarificar que una brecha de seguridad es un tipo de incidente de seguridad, que solamente gatilla la obligación de notificación cuando tiene relación con datos personales. En esencia, mientras que toda brecha de seguridad es un tipo de incidente de seguridad, no necesariamente todos los incidentes de seguridad son brechas de seguridad de datos personales.[139]

Cabe destacar, a su vez, que se ha entendido que existen tres tipos de brechas de seguridad:

a) *"Vulneración de la confidencialidad de datos personales, donde hay una divulgación no autorizada o accidental de, o acceso a, datos personales.*
b) *Vulneración de la integridad de los datos personales, donde hay una alteración accidental o no autorizada de datos personales.*
c) *Vulneración de la disponibilidad de los datos personales*, *donde hay una pérdida de acceso accidental o no autorizada a, o destrucción de, datos personales*".[140]

Dependiendo de las circunstancias, puede darse el caso de que una brecha de seguridad reúna las características de los tres tipos anteriormente reseñados. Sin embargo, es importante destacar, respecto al tipo de vulneración de disponibilidad de datos personales, que ésta siempre se configurará cuando se pierda acceso total y permanente a los datos personales, lo que ocurriría, por ejemplo, si se perdiera la clave de desencriptación para desencriptar una determinada cantidad de datos o si el responsable no pudiese restaurar los datos personales desde un respaldo de estos datos o "*backup"*.[141]

A diferencia de lo anterior, determinar cuándo una vulneración temporal a la disponibilidad de los datos personales debe ser notificada es una cuestión más compleja. En ese sentido, un corte del suministro eléctrico podría ser considerado una brecha de seguridad si conlleva una pérdida de disponibilidad de datos relevante, pero no así una pérdida de disponibilidad ocasionada por el mantenimiento programado de los servidores del responsable o encargado del tratamiento. En cualquiera de estos casos, y frente a las dudas, es recomendable siempre dejar registro y documentar aquellas situaciones en orden de probar el debido cumplimiento a la normativa, en virtud del Principio de Responsabilidad Proactiva, ante la autoridad de control.[142]

[139] Loc. Cit.
[140] ART. 29 WP, 2017a, op. cit., pp. 7. Traducción nuestra.
[141] Ibid., pp. 8.
[142] Loc. Cit.

La importancia de esta obligación se ve justificada por las consecuencias negativas, tanto físicas, materiales o inmateriales, que puede llegar a acarrear una vulneración a las medidas de seguridad a los titulares de datos personales. Entre estas consecuencias podemos encontrar la limitación de los derechos de los titulares de datos, la pérdida de control sobre sus propios datos personales, discriminación, fraudes o robos de identidad, pérdidas financieras, daño a la honra y reputación o la pérdida de confidencialidad sobre datos personales vinculados al secreto profesional.[143]

Por ello, resulta lógico que dicha notificación se realice de la manera más expedita posible, y sin dilaciones indebidas, para evitar que se materialicen los riesgos y consecuencias negativas antes mencionadas. Sin embargo, el Proyecto no establece un plazo para efectuar la antedicha notificación, por lo que sería recomendable que, al igual como ocurre en el RGPD, el responsable o encargado comuniquen las brechas de seguridad dentro de las 72 horas de haber tomado conocimiento de éstas a la autoridad de control. De esta manera, la efectividad de la medida no se ve diluida y, además, cualquier tipo de atraso podría ser documentado y justificado ante la autoridad de control, de forma de excusar el mayor riesgo o daño al que se expuso a los titulares de datos personales.[144]

Este vacío del Proyecto relativo al plazo en el que se puede realizar la debida notificación, o su modalidad como ocurre en el RGPD[145], puede ser subsanado razonablemente, para evitar errores interpretativos de términos tan amplios como “sin dilaciones indebidas” y que además no tuvieron discusión en la Comisión, a través de su integración explícita en el Proyecto, una regulación reglamentaria del mismo o instrucciones de carácter obligatorio por parte del Consejo para la Transparencia y Protección de Datos Personales.

Finalmente, al deber de documentar las comunicaciones se le debe agregar como recomendación, en la práctica, la inclusión en los registros de todas aquellas brechas de seguridad no necesariamente notificables, en caso de que la autoridad de control las requiera y en concordancia con el Principio de Responsabilidad Proactiva.[146]

Aun cuando el Proyecto no establece el periodo durante el cual deben mantenerse los registros de las comunicaciones, se recomienda en la práctica que el responsable lo determine tomando en consideración, por ejemplo, si los antedichos registros contienen o no datos personales y

[143] ART. 29 WP, 2017a, op. cit., pp. 9.
[144] Ibid., pp. 10-14.
[145] El RGPD contempla la modalidad de realizar las comunicaciones en fases o etapas, dependiendo del contexto y la gravedad de la brecha de seguridad. ART. 29WP, 2017a, op. cit., pp. 15.
[146] Ibid., pp. 26.

los principios que gobiernan las actividades del tratamiento. Por su parte, se recomienda que se agregue a los registros los razonamientos en virtud de los cuales se decidió no notificar una determinada brecha de seguridad, incluyendo a su vez la justificación de porqué no se consideró que éstas son riesgosas en relación con los derechos y libertades de los titulares de datos personales.[147]

Además, en la práctica es ventajoso tanto para el responsable como el encargado del tratamiento el documentar exhaustivamente en el registro el procedimiento que se utiliza internamente para hacer frente a las brechas de seguridad, que puede comprender los pasos una vez la vulneración ha sido descubierta, incluyendo cómo contener, gestionar y recuperar el incidente, realizar la gestión de riesgos y notificar la brecha de seguridad. En el mismo sentido, también puede ser útil demostrar que los empleados tomaron conocimiento del procedimiento y son capaces de reaccionar a las brechas de seguridad.[148]

Por todo lo anterior, a estas alturas no hay mejor ejemplo que demuestre que el Principio de Responsabilidad Proactiva es el eje vertebrador de este deber. Se deja patente que se trata de una obligación de rendición de cuentas, pero al mismo tiempo este principio no solo dictamina que debe rendirse cuentas a la autoridad, sino que también a los titulares de los datos afectados en determinados casos. Al igual que como se comentó *ut supra*, el sentido de esta disposición se origina del deber del responsable de crear medios de prueba que le permitan acreditar el debido cumplimiento al Principio de Responsabilidad Proactiva.[149]

### 2.1.3. DELEGADO DE PROTECCIÓN DE DATOS PERSONALES

Al igual que en los artículos 37, 38 y 39 del RGPD[150], el Proyecto de Ley contempla en su artículo 50[151] la designación de un Encargado de Prevención o Delegado de Protección de Datos (en adelante el "Delegado").

En este artículo se desarrollan los métodos de designación y las características que debe reunir el Delegado. Además, se específica las funciones mínimas que debe realizar, entre las que se destaca el informar y asesorar al responsable en materia de protección de datos personales, participar de la política de protección de datos del responsable, supervisar el

[147] ART. 29 WP, 2017a, op. cit., pp. 27.
[148] Loc. Cit.
[149] ICO, 2019, op. cit., pp. 258.
[150] UE, 2016, RGPD, pp. 55-56.
[151] CCLJRS, 2020a, op. cit., pp. 201.

cumplimiento de la ley, absolver las consultas y solicitudes de los titulares de datos y ser el punto de contacto con el Consejo para la Transparencia y Protección de Datos Personales.[152]

En general el solo hecho de que el Proyecto de Ley contemple esta medida supone un gran avance en materia de prevención de riesgos. No obstante lo anterior, cabe destacar que la designación del Delegado supone una implementación interna y organizativa del Principio de Responsabilidad Proactiva[153]. Así, gracias a su inclusión, se permite y facilita que el responsable pueda demostrar y garantizar el debido cumplimiento a sus obligaciones y dar efectividad a los principios básicos del Proyecto.

Otra cuestión de importancia es que la designación del Delegado en el Proyecto es considerada un "Modelo de Prevención de Infracciones"[154], lo que permite, sistematizando la normativa, que además este mecanismo pueda ser certificado por la autoridad de control[155], tal como ocurre en el RGPD.

Sin embargo, existen algunas diferencias respecto al estándar internacional. En primer lugar, la adopción de esta medida es voluntaria por parte del responsable. Lo anterior no tendría sentido si no existiesen en el Proyecto incentivos adecuados para su implementación, lo que ocurre, por ejemplo, con una atenuante por prevenir infracciones que permite al responsable atenuar su responsabilidad si, con anterioridad a la comisión de la infracción, implementó un Modelo de Prevención de Infracciones certificado por la autoridad de control[156]. Por otro lado, y con un carácter disuasivo y que incentiva la proactividad, se considera la creación de un registro público por parte de la autoridad de control, en el que se consignarán aquellas entidades que posean una certificación y aquellas cuya certificación haya sido revocada.[157]

No obstante lo anterior, pareciera ser demasiado optimista el Legislador al permitir que esta medida sea voluntaria, ya que podría restarle fuerza al modelo tal como comentó en la Comisión el H. Senador De Urresti[158]. Sería mucho más factible y seguro que el Proyecto contemplase situaciones o condiciones explícitas bajo las cuales esta medida deba ser implementada obligatoriamente, como ocurre actualmente en el RGPD:

[152] Ibid., pp. 207-208.
[153] ICO, 2019, op. cit. pp. 208.
[154] CCLJRS, 2020a, op. cit., pp. 201-202. Artículo 49 del Proyecto de Ley.
[155] Ibid., pp. 212-213. Artículo 52 del Proyecto de Ley.
[156] Ibid., pp. 157-158. Artículo 36 (5) del Proyecto de Ley.
[157] Ibid., pp. 213.
[158] CCLJRS, 2018, op. cit., pp. 554.

"*El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:*

*a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;*

*b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o*

*c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10."* [159]

En subsidio, al menos se debería facultar a la autoridad de control el determinar cuáles y cuando esas condiciones o situaciones pueden constituir un riesgo para los derechos y libertades de los titulares de datos, recomendando así la implementación de esta medida. Entonces, el problema consiste en haber propuesto la designación del Delegado como un Modelo de Prevención de Infracciones, los que internacionalmente han sido de implementación voluntaria.[160]

Por otro lado, el hecho de que esta medida sea un Modelo de Prevención de Infracciones evita que, en virtud del Principio de Responsabilidad Proactiva, existan incentivos a documentar y fundamentar las razones y análisis en virtud de los cuales se decidió no designar a un Delegado de Protección de Datos Personales, en orden de rendir cuentas ante la autoridad de control de ser necesario y actualizar dicha decisión en el caso de que el responsable o encargado del tratamiento se encuentren en la situación de realizar nuevas actividades o prestar diferentes servicios que puedan reunir las condiciones que conviertan a esta designación en obligatoria, como ocurre en la Unión Europea.[161]

Por su parte, parece poco razonable que el Proyecto no contemple la obligatoriedad de esta medida cuando el responsable o encargado del tratamiento es una autoridad u organismo públicos, entendidos los riesgos que conllevan las actividades de procesamiento de datos personales que realizan estas instituciones por su naturaleza y volumen. Además, es

[159] UE, 2016, op. cit., pp. 55.
[160] CCLJRS, 2018, op. cit., pp. 555.
[161] ARTICLE 29 DATA PROTECTION WORKING PARTY (ART. 29WP), *Guidelines on Data Protection Officers ('DPOs')*. Bruselas, Bélgica, 2016, pp. 5. Disponible en: https://bit.ly/3oFdvoF

importante destacar que no solamente este tipo de organizaciones llevan adelante políticas o actividades públicas, sino que también pueden hacerlo otras entidades o personas jurídicas privadas en áreas como las de transporte público, suministro eléctrico, servicio de agua potable, telecomunicaciones, etc.[162]

En el caso anterior, estas otras instituciones u organizaciones privadas se encuentran en una situación similar a la que se encuentras autoridades u organismos públicos al momento de procesar datos personales. En ese sentido, la obligatoriedad de esta medida en el Proyecto se podría convertir a su vez, como ocurre en la Unión Europea, en un incentivo para que estas otras instituciones consideren adoptar esta medida aunque no estén obligadas a ello, tomando también en cuenta las ventajas que una situación de este tipo conlleva, como el hecho de que el Delegado puede además ejercer sus facultades sobre todas las actividades del tratamiento de datos personales que realiza la institución, estén estas o no relacionadas a actividades públicas o el ejercicio de una determinada potestad pública llevadas a cabo por entidades privadas.[163]

Más allá de lo comentado anteriormente, se hace necesario mencionar que cuando se discutió la situación de los Modelos de Prevención de Infracciones y la designación de un Delegado de Protección de Datos en la Comisión, sí surgió la cuestión respecto a la obligatoriedad de estas medidas respecto a las instituciones u organismos públicos[164]. Debido a ello, se decidió incorporar el artículo 48 al Proyecto de Ley, que establece que:

> "*Los responsables de datos, sean personas naturales o jurídicas, públicas o privadas, deberán adoptar acciones destinadas a prevenir la comisión de las infracciones establecidas en los artículos 34 bis, 34 ter y 34 quater*"[165]

Sin embargo, como puede notarse al leer sistemáticamente estas disposiciones intrínsecamente relacionadas, queda de manifiesto que esta suerte de obligatoriedad a la que deben responder las instituciones públicas, ya que deben adoptar acciones destinadas a prevenir infracciones, no las obliga a designar a un Delegado de Protección de Datos directa o explícitamente, aun cuando de la lectura del artículo 50 inciso 8[166] del Proyecto de Ley se

[162] ART. 29WP, 2016, op. cit., pp. 6.
[163] Loc. Cit.
[164] CCLJRS, 2018, op. cit., pp. 557.
[165] CCLJRS, 2020a, op. cit., pp. 197-198.
[166] Ibid., pp. 205-206. Textualmente, el Proyecto de Ley estatuye lo siguiente en su artículo 50 inciso 8: *"El encargado de prevención o delegado de protección de datos estará obligado a mantener estricto secreto o confidencialidad de los datos personales que conociere en ejercicio de su cargo. Los funcionarios públicos que desempeñen estas funciones e infrinjan este deber de secreto o confidencialidad, serán sancionados de conformidad a lo que se prescribe en los artículos 246 a 247 bis del Código Penal (…)"*

puede asumir que este contempla antedicha situación, al remarcar la responsabilidad respecto a los deberes de secreto y confidencialidad frente a la cual deben responder los funcionarios públicos que asuman como Delegados en sus respectivos organismos.

Así, la técnica legislativa del Proyecto de Ley no permite evidenciar o dejar claramente patente si todos o algunos organismos públicos u instituciones privadas relacionadas deberán adoptar esta importante medida. Por lo pronto, tampoco se dejó en claro dentro de la discusión en la Comisión, que es importante a los efectos de interpretar como corresponde la normativa, si va a ser necesario otorgarle nuevas o diferentes facultades al Consejo para la Transparencia y Protección de Datos Personales para que este recomiende o incluso determine qué instituciones públicas o privadas necesitarán designar un Delegado de Protección de Datos Personales, aun cuando, contradictoriamente, el Proyecto de Ley no lo haga.

Por otro lado, y al igual como ocurre en la Unión Europea y se referenció *ut supra*, sería recomendable que se estableciera la obligatoriedad de esta medida en el caso de que las actividades principales del responsable o encargado del tratamiento, por su naturaleza, fines o alcances, requieran una observación habitual a gran escala.

En ese sentido, este caso es de más difícil implementación práctica y podría sobrecargar las labores de la autoridad de control, pero aun con todo lo anterior, se trata de una situación que puede ser solventada si, por ejemplo, se establece su implementación gradual.

La importancia de lo comentado anteriormente se ve fundamentada por las implicancias que conlleva esta situación obligatoria de designación en el RGPD, que dicen relación con situaciones cotidianas en cualquier sociedad digitalizada. Así, cuando se mención a las actividades principales del responsable, se hace referencia a aquellas que son claves para cumplir los objetivos fijados por éste. No obstante aquello, también se puede aplicar esta condición por ejemplo a un Hospital, que aun cuando su actividad principal consiste en prestar servicios de salud, no puede hacerlo de forma efectiva y segura sin procesar datos relacionados a la salud, tal como las fichas médicas de los pacientes. Otro ejemplo dice relación con las empresas que prestan servicios de seguridad en espacios públicos o privados, como lo serían centros comerciales o plazas y parques, que deben procesar datos personales intrínsecamente relacionados a su actividad principal.[167]

[167] ART. 29WP, 2016, op. cit., pp. 7.

Otra cuestión que no fue materia de discusión en la Comisión, y que debiese de ser modificada en un futuro en el Proyecto, tiene relación con el hecho de que solamente es el responsable del tratamiento[168] el facultado para designar un Delegado de Protección de Datos Personales, a diferencia de lo que ocurre en la Unión Europea, en el que tanto el responsable como el encargado del tratamiento pueden o deben hacerlo.

Así, no existen razones que justifiquen la exclusión de los encargados del tratamiento para que estos puedan designar un Delegado. Los riesgos o situaciones a las que se pueden ver enfrentados los encargados del tratamiento son similares a las de los responsables, que pueden transformarse en infracciones a la normativa usando la terminología del Proyecto. Por otro lado, esto genera problemas contractuales de gran importancia, ya que el encargado se ve impedido de utilizar una medida que puede mejorar su estándar en materia de protección de datos personales, cuestión que puede ser necesaria a la hora de prestar sus servicios o contratar con responsables que la requieran y, también, para acreditar el debido cumplimiento a la normativa.

En la práctica, no existe incompatibilidad de esta medida cuando se trata de implementarla tanto por el responsable o encargado del tratamiento. Tanto es así, que en la Unión Europea se pueden dar una serie de casos de implementación, como el hecho de que deban obligatoriamente designar un Delegado tanto el responsable como el encargado del tratamiento, o que por razones de buenas prácticas y el contexto del tratamiento, el encargado decida llevar a cabo la medida sin estar obligado a ello.[169]

Finalmente, se hace necesario analizar y destacar las facultades y funciones que el Proyecto de Ley contempla para el Delegado de Protección de Datos Personales:

> *a) "Informar y asesorar al responsable de datos, a los terceros encargados o mandatarios y a los dependientes del responsable, respecto de las disposiciones legales y reglamentarias relativas al derecho a la protección de los datos personales y a la regulación de su tratamiento.*
>
> *b) Promover y participar en la política que dicte el responsable de datos respecto de la protección y el tratamiento de los datos personales.*

[168] CCLJRS, 2020a, op. cit., pp. 201-202. Así lo establece el artículo 49 del Proyecto: "*Los responsables de datos podrán voluntariamente adoptar un modelo de prevención de infracciones (…)*"
[169] ART. 29WP, 2016, op. cit., pp. 9.

*c) Supervisar el cumplimiento de la presente ley y de la política que dicte el responsable, dentro del ámbito de su competencia.*

*d) Preocuparse de la formación permanente de las personas que participan en las operaciones de tratamiento de datos.*

*e) Desarrollar un plan anual de trabajo y rendir cuenta de sus resultados.*

*f) Absolver las consultas y solicitudes de los titulares de datos.*

*g) Cooperar y actuar como punto de contacto del Consejo para la Transparencia y la Protección de Datos Personales".*[170]

El literal a) del artículo 50 inciso final del Proyecto contiene una de las funciones más importantes que le son encomendadas al Delegado, y dejan entrever las características que son necesarias para que cualquier persona pueda ser nombrado como tal. En ese sentido, la persona que sea investida como Delegado debe reunir *"los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones"*[171]

Por ello, se entiende que el Delegado debe tener, como mínimo, conocimientos profesionales referidos a la legislación interna y reglamentaria en materia de protección de datos personales. Por su parte, también es útil que en la práctica cuente con conocimientos del sector empresarial en el que se desarrolla el tratamiento de datos, en conjunto con un buen entendimiento de las operaciones del tratamiento que se llevan a cabo, los sistemas informáticos, ciberseguridad y las necesidades del responsable del tratamiento.[172]

En el literal c) se hace referencia a las funciones en materia de cumplimiento de la normativa que tendrá que ejercer el Delegado, que en la práctica se verán reflejadas en una gran cantidad de medidas, pero particularmente en:

*i) "Recolectar información para poder identificar las actividades del tratamiento.*
*ii) Analizar y verificar el nivel cumplimiento que presentan las actividades del tratamiento.*
*iii) Informar, asesorar y emitir recomendaciones al responsable del tratamiento."*[173]

[170] CCLJRS, 2020a, op. cit., pp. 207-208. Artículo 50 inciso final.
[171] Ibid., pp. 205. Artículo 50 inciso 6 del Proyecto de Ley.
[172] ART. 29WP, 2016, op. cit., pp. 11.
[173] Ibid., pp. 17.

No obstante lo anterior, es necesario recalcar que la inclusión de la antedicha función no hace personalmente responsable al Delegado por el hecho de que existan incumplimientos a la normativa. En virtud del Principio de Responsabilidad Proactiva, que justifica esta disposición, el cumplimiento en materia de protección de datos personales consiste en una responsabilidad corporativa del responsable del tratamiento, no del Delegado.[174]

Por su parte, el supervisar el cumplimiento de la normativa se da, por sobre todo, dentro de las baterías de medidas que tiene relación con el Principio de Responsabilidad Proactiva, como lo serían las reseñadas notificaciones de las brechas de seguridad y la adopción de medidas de seguridad y los Principios de Protección de Datos desde el Diseño y por Defecto.

En ese sentido, y respecto a la obligación de notificar las brechas de seguridad, el Delegado puede cumplir funciones relativas a su registro. Para ello, podrá otorgar su opinión al responsable del tratamiento respecto a la estructura, montaje y administración de la documentación de las brechas de seguridad. Así, cumple un rol fundamental a la hora de asistir la prevención de, o la preparación para, una brecha de seguridad, proveyendo de asesoramiento y supervisando el cumplimiento de la normativa mientras ocurre una vulneración o se realiza la subsecuente investigación por parte de la autoridad de control, lo que a su vez requiere que el Delegado sea adecuada y prontamente informado sobre la existencia de una brecha de seguridad con el objetivo de que se involucre durante su desarrollo y proceso de notificación.[175]

Además, se daría dentro de los Modelos de Cumplimiento Diferenciado, que serán comentados más adelante al igual los deberes de transparencia activa y cumplimiento en materia de transferencias internacionales de datos. Para finalizar, el Delegado tiene importantes funciones en la implementación de Evaluaciones de Impacto y el llevar un registro de las actividades del tratamiento, medidas que aun no son consideradas por el Proyecto y que, por lo mismo, serán analizadas en mayor profundidad como propuestas en los subcapítulos siguientes debido a la inclusión del Delegado dentro de las medidas que puede adoptar el responsable del tratamiento.

Por otro lado, el literal f) hace hincapié en la función recíproca que conlleva la posibilidad de que los titulares de datos se pongan en contacto con el Delegado en lo que respecta a todas

[174] ART. 29WP, 2016, op. cit., pp. 17.
[175] ART. 29WP, 2017a, op. cit., pp. 28.

las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos amparados por la normativa.[176]

En ese sentido, y aunque el Proyecto no contempla explícitamente en su artículo 14 ter[177] que se deba mantener a disposición del público los datos de contacto del Delegado como si lo hace respecto a los del responsable, en virtud del deber de información y transparencia, se hace necesario para cumplir esta función que se publiquen los datos de contacto e identificación del Delegado.[178]

Además, sería recomendable incluir en el Proyecto que antedichos datos de contacto deban ser comunicados a la autoridad de control respectiva. Lo anterior tiene como objetivo asegurar que los titulares de datos y el Consejo para la Transparencia y Protección de Datos Personales puedan fácil y directamente contactarse con el Delegado.[179]

En la práctica, los datos de contacto del Delegado debiesen de incluir su domicilio postal, un número de teléfono y/o un correo electrónico dedicado. Además, se considera una buena práctica incluir el nombre del Delegado para efectos de garantizar un adecuado punto de contacto con la autoridad de control, además de compartir sus datos de contacto con los empleados del responsable del tratamiento publicándolos, por ejemplo, en la intranet de la empresa o institución.[180]

Finalmente, el literal g) dicen relación con el rol de facilitador del que está investido el Delegado.[181] Así, este actúa para facilitarle el acceso a la autoridad de control a la información y documentación relevante en virtud de las funciones que posee el Consejo para la Transparencia y Protección de Datos Personales, que están ubicadas en el artículo 33 de la Ley N°20.285, y entre las que encontraremos debido al Proyecto de Ley, por ejemplo, el "*fiscalizar y sancionar el adecuado cumplimiento de la ley N°19.628, sobre protección de los datos personales*".[182]

[176] CCLJRS, 2020a, op. cit., pp. 205.
[177] Ibid., pp. 54.
[178] ART. 29WP, 2016, op. cit., pp. 12.
[179] Loc. cit.
[180] Ibid., pp. 13.
[181] Ibid., pp. 18.
[182] CCLJRS, 2020a, op. cit., pp. 227-230. Artículo 33 literal m) de la Ley N°20.285.

## 2.2. INNOVACIONES: MODELOS DE CUMPLIMIENTO DIFERENCIADO

El Proyecto de Ley contempla, en su artículo 14 septies, la diferenciación de estándares de cumplimiento respecto a los deberes de información y transparencia y el de adoptar medidas de seguridad[183].

Esta diferenciación según el Proyecto se hará en razón del tamaño de la entidad o empresa de acuerdo con las categorías establecidas en el artículo segundo de la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño, y además teniendo presente las actividades que desarrollan, el volumen, naturaleza y las finalidades de los datos personales que tratan.

Dicha diferenciación la realizará el Consejo para la Transparencia y Protección de Datos Personales a través de una instrucción general[184]. Sin embargo, antedicha cuestión no estuvo exenta de discusión en la Comisión, en el entendido de que en un primer momento el establecimiento de los modelos diferenciados de cumplimiento iba a realizarse a través de un reglamento expedido por el Ministerio de Hacienda y suscrito por el Ministro de Economía, Fomento y Turismo, previo informe de la Agencia de Protección de Datos Personales.[185]

Lo anterior tiene relevancia ya que aquella discusión da luces del carácter normativo que van a tener estos modelos de cumplimiento diferenciado. Así, según el texto actual será el Consejo para la Transparencia y Protección de Datos Personales el encargado de fijar aquellos estándares mínimos adecuados al sector productivo o industrial respectivos, a través de la facultad de dictar instrucciones generales de carácter obligatorio tal como lo hace hoy por hoy la Comisión para el Mercado Financiero.[186]

En ese sentido, cabe destacar que el Consejo para la Transparencia ya cuenta con facultades de esta índole en virtud del artículo 33 letra d) de la ley N°20.285, pero en materias relacionadas a Transparencia y Acceso a la Información Pública[187], por lo que además deben ser extendidas para ajustarse a los requerimientos de esta nueva medida.

---

[183] CCLJRS, 2020a, op. cit., pp. 61-62.
[184] Loc. cit.
[185] CCLJRS, 2020a, op. cit., pp. 62.
[186] COMISIÓN CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO DEL SENADO (CCLJRS). *Segundo Informe recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*. 2020b, pp. 176.
[187] CHILE. Ley N°20.285*, Sobre Acceso a la Información Pública*. Diario Oficial de la República de Chile, Santiago, Chile, 20 de Agosto de 2008, pp. 13. Disponible en: https://bit.ly/3orDfVw

Por su parte, se decidió realizar este cambio para evitar que la potestad reglamentaria[188], en el caso de que los modelos de cumplimiento diferenciado fueran establecidos por un Ministerio, tuviera cualquier tipo de interferencia en la autonomía de la autoridad de control de protección de datos personales. Así, se garantiza la autonomía del Consejo para la Transparencia y Protección de Datos Personales, al mismo tiempo que se le otorgan facultades normativas armónicas con la Constitución y las Leyes.[189]

En síntesis, y tal como consignó el H. Senador Harboe[190], no es posible que se aplique el mismo criterio de cumplimiento a todo tipo de empresas, pero hay que tener en consideración que los "*riesgos para los titulares de datos no dependen del tamaño de los responsables del tratamiento*"[191] y, en ese sentido, tal como comentó Eduardo Bertoni, Director Nacional de Protección de Datos de Argentina, es necesario encontrar el equilibrio entre una aproximación a la protección de datos preventiva con el libre intercambio y tratamiento de estos para que no se convierta en una barrera para la inversión, la innovación y el avance de la tecnología.[192]

Sin embargo, tal como comenta el señor Jesús Rubí[193], representante adjunto de la Agencia Española de Protección de Datos, el modelo de cumplimiento diferenciado pareciera ser insuficiente. Podría aprovecharse de mejor manera extendiendo, por ejemplo, sus alcances a otros deberes u obligaciones.

Una manera de evitar que suceda, en general, lo comentado en el párrafo anterior, es que el Proyecto de Ley sea lo suficientemente explícito y claro respecto a las medidas y los deberes que puede o debe cumplir un determinado responsable, o que se especifiquen las condiciones en las que determinadas conductas por parte de este requieren un especial cuidado. Así, la autoridad de control va a poder, tal como ocurre en el estándar internacional, guiar, modelar o sistematizar el sistema de cumplimiento en la medida de que avanza la implementación de la normativa, sin salirse de sus márgenes. La propuesta general es que, en el fondo, la futura legislación pueda ser autosuficiente y auto explicativa, y que simplemente sus detalles deban ser desarrollados con mayor profundidad.

---

[188] En este caso estamos en presencia de la Potestad Reglamentaria de Ejecución o la de reglamentos *secundum legem*, es decir, *"los dictados en desarrollo y para la aplicación de una ley*". CORDERO VEGA, Luis. *Lecciones de Derecho Administrativo*. Legal Publishing Chile, 2da edición corregida, Chile, 2015, pp. 147.
[189] CCLJRS, 2020b, op. cit., pp. 177.
[190] CCLJRS., 2018, op. cit., pp. 334.
[191] EC, 2020a, op. cit., pp. 23. Traducción nuestra.
[192] CCLJRS., 2018, op. cit., pp. 173 y 175.
[193] Ibid., pp. 178.

## 2.3. OTRAS MEDIDAS Y OBLIGACIONES DEL SISTEMA DE CUMPLIMIENTO

El Proyecto de Ley contempla variadas medidas y obligaciones que poseen un marcado carácter proactivo y preventivo:

Una de las primeras y más importantes se encuentra en el artículo 11[194] del Proyecto que establece, en el marco de la solicitud o requerimiento del titular de datos para ejercer sus derechos, el deber del responsable de responder por escrito al titular y almacenar los respaldos que le permitan demostrar la remisión de su respuesta, junto con el contenido y la fecha de ésta.

Lógicamente, y tal como se ha dejado patente en este ensayo, el objetivo de esta obligación consiste en permitirle al responsable el construir, con anterioridad, los medios de prueba que le permitan acreditar el cumplimiento al Principio de Responsabilidad Proactiva. Al mismo tiempo se alivianan las labores de la autoridad de control en esta materia y se evita que se pasen a llevar los derechos y libertades de los titulares, cambiando el *onus probandi* y garantizando que recibirán la respuesta que necesitan en la forma y plazos preestablecidos.

### 2.3.1. ACREDITAR LA OBTENCIÓN DEL CONSENTIMIENTO DEL TITULAR

Por su parte, el artículo 12[195] del Proyecto consigna la obligación del responsable de probar que el tratamiento de datos realizados contó con el consentimiento del titular, lo que tendrá que hacer tomando las medidas técnicas apropiadas que permitan al titular consentir en el uso de sus datos personales, con el objetivo de dejar documentado el referido mecanismo y acto del titular.

El Proyecto de Ley define al consentimiento de la siguiente forma en su artículo 2, letra o):

> *"Consentimiento: toda manifestación de voluntad libre, específica, inequívoca e informada, mediante la cual el titular de datos, su representante legal o mandatario, según corresponda, autoriza el tratamiento de los datos personales que le conciernen."*[196]

La definición anteriormente citada se condice con la preceptuada en el RGPD en su artículo 4 numeral 11, que además estuvo basada en la establecida por la Directiva 95/46/EC,

[194] CCLJRS, 2020a, op. cit., pp. 37-40. Dicha obligación contempla el siguiente texto: "*El responsable deberá responder por escrito al titular a su domicilio o la dirección de correo electrónico fijada por éste. El responsable debe almacenar los respaldos que le permitan demostrar la remisión de la respuesta a la dirección física o electrónica que corresponda, su fecha y el contenido íntegro de ella."*
[195] CCLJRS. 2020a, op. cit., pp. 46 y, en el mismo sentido, CCLJRS, 2018, op. cit., pp. 302.
[196] CCLJRS, 2020b, op. cit., pp. 50-51.

convirtiéndose en la más importante base de licitud para las actividades de tratamiento llevadas a cabo por el responsable o encargado del tratamiento en el modelo europeo.[197]

Por su parte, el artículo 12 inciso 2 del Proyecto profundiza la obligación de la siguiente manera:

> *"El consentimiento del titular debe ser libre, informado y específico en cuanto a su finalidad o finalidades. El consentimiento debe manifestarse de manera inequívoca, mediante una declaración verbal, escrita o expresada a través de un medio electrónico equivalente, o mediante un acto afirmativo que dé cuenta con claridad de la voluntad del titular".*[198]

De forma similar a lo estatuido en el Proyecto y lo discutido en la Comisión del Senado, la obligación del responsable del tratamiento de demostrar y probar que el titular de los datos personales prestó su consentimiento está amparado también en el artículo 7 numeral 1 del RGPD.[199]

Por ello, aunque el texto de esta obligación no indica cómo puede ser demostrado o probado lo anterior, en primera instancia esta obligación persiste mientras dure la actividad del tratamiento para la cual fueron recogidos los datos personales de los titulares y, es por esto, que el responsable debe ser capaz de llevar un registro en dónde como mínimo se detalle cómo el consentimiento fue obtenido, cuándo fue obtenido y la información que le proveyó al titular de datos en aquel momento. Además, se recomienda que este consentimiento sea actualizado con el tiempo, tomando en consideración que este durará dependiendo de factores tales como el contexto y la voluntad del titular de los datos.[200]

Aparte de las ventajas en materia de cumplimiento que esta obligación genera, la Comisaria de Justicia, Consumidores y Equidad de Género de la Unión Europea, señora Vera Jourová, señaló que las pequeñas y medianas empresas europeas reconocen la utilidad práctica de la aplicación del RGPD, ya que les facilita el organizar los datos que tratan y desechar aquellos que no le son provechosos. En ese sentido, solo pueden conservar los datos de aquellas personas que otorgaron su consentimiento de manera informada, por lo que se disminuye el

---

[197] EUROPEAN DATA PROTECTIÓN BOARD (EDPB). *Guidelines 05/2020 on consent under Regulation 2016/679,* 2020b, pp.6. Disponible en: https://bit.ly/36ESjZR
[198] CCLJRS, 2020b, op. cit., pp. 44-45.
[199] EDPB, 2020b, op. cit., pp. 22.
[200] Ibid., pp. 23.

volumen de la conservación de estos datos y, por tanto, se reducen los riesgos de que ocurra un ciberataque.[201]

### 2.3.2. ACREDITAR LA LICITUD DEL TRATAMIENTO

De una manera similar, el artículo 13[202] del Proyecto establece el deber del responsable de acreditar la licitud del tratamiento de datos que realiza. Esto ocurre porque el responsable está en mejores condiciones de probar que el tratamiento que realiza es lícito de acuerdo con el Proyecto. Lo anterior trae aparejadas dos ventajas: a) El titular de los datos no tendrá que probar que el tratamiento de sus datos fue realizado de manera ilícita y b) La autoridad de control va a ver disminuida su carga de trabajo.

En ese sentido, tal como señaló el Honorable Senador Felipe Harboe, es necesario que existan este tipo de obligaciones para robustecer la lógica que se encuentra detrás de todo el proyecto, esto es, para cada tipo de tratamiento deben determinarse sus fines y los datos personales recolectados.[203]

### 2.3.3. DEBER DE SECRETO Y CONFIDENCIALIDAD

Por otro lado, el artículo 14 bis[204] del Proyecto, que trata el deber de secreto y confidencialidad, establece que el responsable debe tomar las medidas necesarias para que sus dependientes, o las personas naturales o jurídicas que ejecuten operaciones de tratamiento de datos bajo su responsabilidad, cumplan el deber de secreto o confidencialidad.[205]

Lo anterior por cierto puede realizarse a través de la designación de un Delegado de Protección de Datos, que entre sus funciones contempla la organización, asesoramiento y capacitación continua de los dependientes del responsable, o con la implementación de un Programa de Cumplimiento.

### 2.3.4. DEBER DE INFORMACIÓN Y TRANSPARENCIA: TRANSPARENCIA ACTIVA

Además, en el artículo 14 ter[206] del Proyecto, que trata el deber de información y transparencia, se consigna la obligación de transparencia activa por medio de la cual el responsable tendrá

[201] CCLJRS, 2020b, op. cit., pp. 42.
[202] Ibid., pp. 49.
[203] Ibid., pp. 145.
[204] CCLJRS, 2020a, op. cit., pp. 51-52. Este deber ha quedado de la siguiente manera en el Proyecto: "*El responsable de datos está obligado a mantener secreto o confidencialidad acerca de los datos personales que conciernan a un titular, salvo cuando el titular los hubiere hecho manifiestamente públicos. Este deber subsiste aún después de concluida la relación con el titular (…)"*
[205] Ibid., pp. 53.
[206] Ibid., pp. 53-55.

que mantener a disposición del público y la autoridad de control, por medio de su página web o cualquier otro sitio de información equivalente, a lo menos:

> "*a) La política de tratamiento de datos personales que haya adoptado, la fecha y versión de la misma.*
>
> *b) La individualización del responsable de datos y su representante legal y la identificación del encargado de prevención, si existiere.*
>
> *c) El domicilio postal, la dirección de correo electrónico, el formulario de contacto o la identificación del medio tecnológico equivalente mediante el cual se le notifican las solicitudes que realicen los titulares.*
>
> *d) Las categorías, clases o tipos de datos que trata; la descripción genérica del universo de personas que comprenden sus bases de datos; los destinatarios a los que se prevé comunicar o ceder los datos, las finalidades de los tratamientos que realiza y los tratamientos que se basan en la satisfacción de intereses legítimos.*
>
> *e) La política y las medidas de seguridad adoptadas para proteger las bases de datos personales que administra.*
>
> *f) El derecho que le asiste al titular para solicitar ante el responsable, acceso, rectificación, cancelación, oposición y portabilidad de sus datos personales, de conformidad a la ley, y*
>
> *g) El derecho que le asiste al titular de recurrir ante el Consejo para la Transparencia y la Protección de Datos Personales, en caso que el responsable rechace o no responda oportunamente las solicitudes que le formule*."[207]

De esta manera, la ejecución de la función fiscalizadora de la autoridad de control respectiva se verá en gran medida alivianada. Por otro lado, el principio de transparencia les permite a los titulares de datos estar informados y robustecer la confianza digital en las actividades de tratamiento que utilizan sus propios datos personales, permitiéndoles entender por qué son necesarios.[208]

Así, el deber de transparencia tiene directa relación con el Principio de Responsabilidad Proactiva, ya que siempre debe el responsable del tratamiento ser capaz de demostrar que los datos personales están siendo tratados de forma transparente en relación con los titulares

[207] CCLJRS, 2020a, op. cit., pp. 53-55.
[208] ARTICLE 29 DATA PROTECTION WORKING PARTY (ART. 29WP). *Guidelines on transparency under Regulation 2016/679*. 2017b, Bruselas, Bélgica, pp. 4. Disponible en: https://bit.ly/39JdprU

de estos datos y, unido a lo anterior, el Principio de Responsabilidad Proactiva requiere que las actividades del tratamiento sean transparentes en orden de que los responsables sean capaces de demostrar el debido cumplimiento a los deberes y principios establecidos.[209]

En ese sentido, los responsables del tratamiento deben determinar si existen riesgos capaces de materializarse en personas naturales cuando se lleva a cabo un tratamiento de datos, lo que a su vez debe ser informado y destacado a los titulares de datos personales al momento de su recolección. Consecuentemente, esto podría ser de ayuda al responsable ya que tendría a la vista una imagen global de las actividades del tratamiento que pueden acarrear un mayor riesgo e impacto en los derechos fundamentales y libertades de los titulares de datos personales.[210]

Por otro lado, es necesario destacar que esta obligación no solamente debe ser cumplida al momento de recolectar los datos personales de los titulares de estos datos, sino que también durante todo el ciclo de vida del procesamiento de estos datos, incluyendo por ello información referente a cualquier tipo de cambios subsecuentes en las actividades de tratamiento llevadas a cabo y cómo estos pueden afectar las expectativas y la voluntad de los titulares de datos personales involucrados.[211]

### 2.3.5. DEBERES Y OBLIGACIONES EN MATERIA DE TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

Por su parte, internacionalmente el uso de cláusulas contractuales tipo (en inglés "*Standard Contractual Clauses*", en adelante "CCTs" por sus siglas en español) es el mecanismo más utilizado a la hora de realizar transferencias de datos[212]. Las CCTs no solo se utilizan en las transferencias internacionales de datos, sino que además internamente, por ejemplo, regulando la relación entre el responsable y el encargado del tratamiento. Así, el Proyecto de Ley en su artículo 15 bis[213] establece que la autoridad de control pondrá a disposición en su página web modelos tipos de contratos de esta especie.

No obstante lo anterior, y al igual que lo que sucede con los códigos de conducta, las CCTs pueden resultar mecanismos autorregulatorios muy eficaces, ya que pueden adaptar las

[209] ART. 29WP, 2017b, op. cit., pp. 5.
[210] Loc. Cit.
[211] Ibid., pp. 16.
[212] EC, 2020a, op. cit., pp. 36.
[213] CCLJRS, 2020a, op. cit., pp. 68.

características de un determinada actividad o sector (como la banca) al sistema de garantías de la normativa[214].

Sería prudente, entonces, hacer menciones y ejemplificaciones especificas a estos mecanismos autorregulatorios a lo largo de la normativa para incentivar y promover su uso entre los interesados. De esta manera se podría aprovechar mejor el Mecanismo de Certificación que propone el Proyecto permitiendo que, por ejemplo, se puedan presentar a certificación CCTs o Códigos de Conducta para demostrar, reforzar y garantizar el cumplimiento a los principios y deberes de los responsables.

Finalmente, en materia de transferencia internacional de datos personales, el Proyecto consigna en su artículo 28[215], inciso final, que será deber del responsable acreditar que efectuó la transferencia en conformidad a lo establecido en la normativa.

Esta obligación requiere que tanto el exportador como importador de datos personales (sean estos responsables o encargados del tratamiento) vayan más allá de un cumplimiento pasivo en relación con el derecho fundamental de protección de datos personales. Así, deben poner en marcha medidas legales, organizacionales y técnicas para darle efectividad al Principio de Responsabilidad Proactiva y garantizar su cumplimiento.[216]

Este Principio es en si mismo aplicado a las transferencias internacionales de datos personales ya que este tipo de actividades son consideradas a su vez un procesamiento o tratamiento de datos personales. Por ello, es de responsabilidad de los exportadores e importadores el garantizar un nivel de cumplimiento acorde a la normativa establecida, pudiendo incluso suspender o terminar el o los contratos si varias o unas de las partes ya no son capaces de garantizar el estándar de protección requerido en materia de datos personales.[217]

En este caso, la pregunta del cómo es que se puede garantizar el cumplimiento de la normativa en materia de transferencias internacionales de datos y esta obligación, se le puede dar respuesta siguiendo un procedimiento de cumplimiento que hila la normativa y las herramientas o medidas contenidas tanto en el Proyecto de Ley como en el RGPD.

---

[214] CCLJRS, 2018, op. cit., pp 178.
[215] CCLJRS, 2020a, op. cit., pp. 121.
[216] EUROPEAN DATA PROTECTION BOARD (EDPB). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.* 2020c, pp. 7. Disponible en: https://bit.ly/2JMRtRQ
[217] Loc. Cit.

Así, un primer paso consiste en tener claridad y documentar adecuadamente todas las transferencias internacionales de datos realizadas o por realizar. Lo anterior puede resultar extremadamente difícil, tomando en consideración que existen empresas, instituciones u organismos que realizan estas actividades de manera compleja, involucrando a una gran cantidad de actores que procesan o sub-procesan grandes volúmenes de datos.[218]

Por ello, es recomendable o puede ser útil hacerse valer de un registro de las actividades del tratamiento, que está contemplado de forma obligatoria en el RGPD en su artículo 30[219], y que será analizado más adelante en este ensayo como parte de las propuestas e inclusiones que se le pueden hacer al Proyecto de Ley. En el mismo sentido, es importante que se verifique que los datos que se vayan a transferir sean los adecuados, pertinentes y relevantes en relación con los propósitos para los que van a ser transferidos y procesados, en concordancia con el principio de "minimización de datos", además del hecho de que se tienen que considerar como transferencias internacionales de datos aquellos casos en los que se dé acceso remoto a bases de datos o a servicios de almacenamiento en la nube situados en otro país a terceros extranjeros.[220]

Posteriormente, para dar cumplimiento a esta obligación es recomendable que se detalle o determinen aquellas medidas apropiadas de carácter contractual que al exportador de datos le permitan garantizar un estándar en protección de datos personales equivalente en ambos países involucrados, como lo podrían ser la utilización de cláusulas contractuales tipo (CCTs), códigos de conducta, mecanismos de certificación y cláusulas contractuales ad hoc.[221]

Sin embargo, para garantizar la efectividad de estas medidas, un siguiente paso consistiría en determinar, en colaboración con el importador de los datos personales, la existencia de cualquier regulación legal o práctica habitual por parte del país extranjero que pudiese restarle eficacia a estas medidas en el contexto específico de la transferencia a realizar. En ese sentido, el tercero extranjero debe colaborar, cuando sea apropiado, en la entrega de información respecto a la legislación aplicable en el país extranjero relativa a la transferencia internacional de datos que se realizará.[222]

[218] Ibid., pp. 8.
[219] EDPB, 2020c, op. cit, pp. 8.
[220] Ibid., pp. 9.
[221] Ibid., pp. 11.
[222] Ibid., pp. 12.

El contexto al que se hace alusión en este caso debe ser determinado tomando en consideración las siguientes circunstancias:

a) *"el propósito que justifica la transferencia de los datos personales;*

*b) tipos de entidades involucradas (públicas o privadas/ responsables o encargados del tratamiento);*

*c) el sector dentro del cual ocurriría (telecomunicaciones, financiero, público, etc.);*

*d) categorías de datos personales a transferir;*

*e) si los datos personales van a ser almacenados por el tercero extranjero o se trata de un acceso remoto a bases de datos;*

*f) formato en el que se realizará la transferencia internacional de datos personales (pseudoanonimización, encriptación, etc.);*

*g) Posibilidad de que el importador transfiera a su vez a otro tercero extranjero los datos personales a transferir*."[223]

Consiguientemente, es necesario que todo este examen sea detalladamente documentado, basado especialmente en la legislación extranjera y en otros recursos de carácter objetivo, tales como informes y ejercicios públicos realizados por la autoridad de control en materia de protección de datos personales extranjera, con el objetivo de obtener los medios de prueba suficientes para rendir cuentas y justificar la decisión al momento de realizar la transferencia internacional de datos personales,[224] teniendo siempre presente que pueden tomarse otras medidas suplementarias para reducir riesgos y reevaluar periódicamente el procedimiento monitoreando la transferencia de datos en colaboración con el importador extranjero.[225]

Además, dentro de esta materia, destacamos los numerales b), c) y f) del artículo 27[226] del Proyecto de Ley, que determina los casos en que las transferencias internacionales de datos son lícitas en virtud del Proyecto.

Así, en el literal b) y c) se establece que serán lícitas las transferencias cuando éstas se encuentren amparadas en cláusulas contractuales u otros instrumentos jurídicos que determinen las obligaciones, responsabilidades, garantías y medidas de control mutuas que

[223] EDPB, 2020c. op. cit., pp. 12. Traducción nuestra.
[224] Ibid., pp.14.
[225] Ibid., pp. 15-19.
[226] CCLJRS, 2020a, op. cit., pp. 115-117.

deberán seguir tanto el importador como exportador de los datos personales.[227] Del mismo, las transferencias serán lícitas cuando el importador y exportador de datos adopten un modelo de cumplimiento, o medidas autorregulatorias o certificaciones vinculantes reguladas por la legislación aplicable a cada uno de ellos.[228]

Por su parte, el literal f) del artículo 27 del proyecto merece un análisis más pormenorizado. Así, éste estatuye, en parte, que será lícita la transferencia internacional de datos:

> *"Cuando la transferencia se efectúe entre sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador en los términos previstos en la Ley de Mercado de Valores, siempre que todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales."*[229]

La antedicha concepción formó parte de la propuesta hecha en el Mensaje[230] del ejecutivo para contemplar aquellas situaciones en las que, entre las sociedades de un mismo grupo empresarial, término definido en el artículo 96 de la Ley de Mercado de Valores, empresas relacionadas o sujetas a un mismo controlador, se realizasen transferencias internacionales de datos.

Sin embargo, aquella redacción suscitó una nueva discusión en la Comisión relativa al caso en que una empresa chilena perteneciente a un holding internacional, que obtuvo datos personales de titulares gracias a su consentimiento, transfiera aquellos datos personales a la empresa controladora en el extranjero. Así, la autoridad de control chilena no tendría forma de fiscalizar o sancionar aquella transferencia, debido a que se trata de un caso de aplicación extraterritorial de la ley.[231]

Por ello, y para garantizar la responsabilidad del responsable en esta materia y evitar que se diluyan las facultades de la autoridad de control[232], finalmente se decidió en la Comisión agregar el siguiente texto al literal f) del artículo 27:

> *"El responsable que efectúe la transferencia de datos asumirá la responsabilidad por cualquier infracción a los estándares y* ***políticas corporativas vinculantes*** *en que incurra algunos de los miembros del grupo empresarial. El responsable sólo podrá exonerarse de*

[227] Ibid., pp. 115.
[228] Ibid., pp. 116.
[229] CCLJRS, 2020a, op. cit., pp. 116-117.
[230] CCLJRS, 2018, pp. 413.
[231] Ibid., pp. 413-415.
[232] Ibid., pp. 416.

*esta responsabilidad cuando acredite que la infracción no fue imputable al miembro del grupo empresarial correspondiente."*[233]

Más allá del acierto legislativo, al contemplar y solucionar una hipótesis casuística de gran importancia en la práctica, el texto agregado al literal f) permite interpretar y comprender de mejor manera a qué hace referencia el legislador cuando habla de la condición que deben cumplir las empresas de un mismo grupo empresarial para considerar que realizan las transferencias de datos personales de forma lícita, esto es, operar bajo los mismos estándares y políticas en materia de protección de datos personales.

Y es que, en este tipo de situaciones, una medida internacionalmente reconocida para demostrar el debido cumplimiento a la normativa en materia de protección de datos personales consiste en la utilización de políticas corporativas vinculantes o "*Binding Corporate Rules"* (BCRs).[234]

Las BCRs pueden ser descritas como marcos o códigos de privacidad implementados por empresas[235], y están extensamente reguladas en el artículo 47[236] del RGPD. Sin embargo, en el Proyecto de Ley ésta es la única ocasión en la que se hace referencia a ellas, aun cuando permiten que el más alto nivel de protección de datos personales sea vinculante en un mismo grupo de empresas a nivel global.[237]

Así, las BCRs pueden contener, entre otras medidas, una política de privacidad, la designación de un Delegado de Protección de Datos Personales, la forma en que se facilita a los interesados la información sobre las BCRs, la justificación de su carácter jurídicamente vinculante interna y externamente, procedimientos de reclamación, mecanismos de cooperación con la autoridad de control, etc.[238]

En razón de todo lo anterior, podemos además sustentar el desaprovechamiento de los mecanismos de certificación que contempla el Proyecto de Ley. Cómo se ha mencionado en otras ocasiones a lo largo de este ensayo, el Proyecto establece en su artículo 52[239] la existencia de una certificación, llevada a cabo por el Consejo para la Transparencia y Protección de Datos Personales, de los Modelos de Prevención de Infracciones y los

[233] CCLJRS, 2020a, op. cit, pp. 117. El destacado es nuestro.
[234] POTHOS, Mary, 2018, op. cit. pp. 222.
[235] Ibid., pp. 222.
[236] UE, 2016, op. cit., pp. 62-64.
[237] POTHOS, Mary, 2018, op. cit., pp. 222.
[238] USTARAN, Eduardo. *International Data Transfers*. En: INTERNATIONAL ASSOCIATION OF PRIVACY PROFFESIONALS (IAPP*), European Data Protection: Law and Practice*. Ed: Eduardo Ustaran, 2018, pp. 237-238.
[239] CCLJRS, 2020a, op. cit., pp. 212.

Programas de Cumplimiento, que incluye entonces la certificación respecto a la designación de un Delegado por parte del responsable, y que además contempla la creación de un "Registro Nacional de Cumplimiento y Sanciones"[240] en el que se detallará aquellas entidades que cuentan con la debida certificación y aquellas cuya certificación ha sido revocada.[241]

Así, sería razonable que el mecanismo de certificación no solo refiera a este tipo de herramientas, sino que sea extendido a medidas autorregulatorias como los códigos de conducta o BCRs, cuestión que ocurre en la Unión Europea a través del denominado "Mecanismo de Coherencia" contenido en el artículo 63[242] del RGPD, y mediante el cual la autoridad de control competente puede aprobar o rechazar la adopción de, por ejemplo, BCRs[243], medida que, como se acabó de explicar, se encuentra contemplada actualmente en el Proyecto de Ley.

Este punto es crucial para solventar esta serie de vacíos regulatorios en el Proyecto, ya que la autoridad de control chilena va a gastar muchísimos más recursos y tiempo en supervisar, fiscalizar y sancionar a los responsables que utilicen estos mecanismos autorregulatorios debido a que antes no tuvo la facultad de certificarlos correspondientemente. En el mismo sentido, se coloca en un riesgo innecesario a los titulares de datos personales, producto de que no existen garantías de que estos mecanismos autorregulatorios incertificables sean suficientes para garantizar sus derechos, intereses y libertades.

No obstante lo analizado hasta ahora, y sin perjuicio de estar diseminadas a lo largo del proyecto, las medidas comentadas en este acápite tienen por objeto general la elaboración de instrumentos, por parte del responsable del tratamiento, que permitan probar eventualmente el cumplimiento de sus obligaciones y de paso, los principios rectores. Entonces, estas medidas no pueden sino ser interpretadas como la cristalización del Principio de Responsabilidad Proactiva, cuya inclusión, por cierto, ayudaría a sistematizar y explicar de mejor manera los lineamientos y objetivos centrales de la normativa.

---

[240] CCLJRS, 2020a, pp. 13. *"Es un registro nacional de carácter público administrado por el Consejo para la Transparencia y la Protección de Datos Personales que consigna los modelos certificados de prevención; los responsables de datos que los hayan adoptado; las sanciones que se hayan impuesto a los responsables de datos que hayan infringido la ley, y aquellos a quienes se les haya revocado la certificación, de conformidad a dispuesto en el artículo 54."*

[241] Ibid., pp. 213.

[242] UE, 2016, op. cit., pp. 73.

[243] UE, 2016, op. cit, pp. 62. Artículo 47 del RGPD: "*La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63 (…)*"

## 2.4. PROPUESTAS

### 2.4.1. EVALUACIONES DE IMPACTO

Durante la tramitación del Proyecto de Ley se discutió en particular la inclusión de las Evaluaciones de Impacto al cuerpo normativo[244]. Lamentablemente, debido a que se tenía como punto de partida al Mensaje del Ejecutivo, el grupo de asesores recomendó desechar una serie de artículos, entre ellos el artículo 33[245] de la Moción Parlamentaria, que reglaba las antedichas Evaluaciones y las situaciones en las que tenían un carácter obligatorio,[246] que a su vez coinciden con las estipuladas en el RGPD.

Estas medidas están presentes en el artículo 35 del RGPD y, al igual que en la Moción, buscan evitar que un determinado tipo de tratamiento que implica un alto riesgo a los derechos y libertades de los titulares pueda verse materializado. Gracias a ello, de manera anticipada y preventiva, el responsable podrá o deberá evaluar la necesidad del tratamiento y su proporcionalidad, gestionando los potenciales riesgos involucrados para reducirlos, a través de distintas medidas, a rangos aceptables.[247] Por su parte, además pueden ser útiles para determinar el nivel de impacto que puede acarrear el desarrollo de un producto tecnológico, como algún tipo de "*hardware*" o "*software",* que podrían ser utilizados por distintos responsables o encargados del tratamiento para llevar a cabo distintas actividades de tratamiento.[248]

En ese sentido, las Evaluaciones de Impacto, consideradas tanto en la Moción como en el RGPD en su artículo 35.7, deben contener como mínimo:

---

[244] CCLJRS, 2018, op. cit., pp. 331.
[245] Boletín 11.092-07. Enero del 2017, op. cit., pp. 24.
[246] CCLJRS, 2018, op. cit., pp. 331. "*Esta evaluación será obligatoria en caso de:*
*a) evaluación sistemática y exhaustiva de aspectos personales de personas naturales que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales o que les afecten significativamente de modo similar;*
*b) tratamiento a gran escala de las categorías especiales datos o de los datos personales relativos a condenas e infracciones.*
*c) observación sistemática a gran escala de una zona de acceso público."*
Según el GT29, esta lista no es exhaustiva ni taxativa, sino que más bien desea guiar la comprensión y ejemplificación de qué actividades pueden conllevar un alto riesgo a los derechos y libertades de los titulares de datos. ARTICLE 29 DATA PROTECTION WORKING PARTY (ART. 29WP). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. Bruselas, Bélgica, 2017c, pp. 9. Disponible en: https://bit.ly/2KqGIEI
[247] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD*). Evaluaciones de impacto de protección de datos*. 9 de Marzo 2020c. Disponible en https://bit.ly/3f5lOpg.
[248]ART. 29WP. 2017c, op. cit., pp. 8.

a) *"Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento.*
b) *Una evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.*
c) *Una evaluación de los riesgos para los derechos y libertades de los interesados (…)*
d) *Las medidas provistas para afrontar los riesgos, incluidas garantías, medidas de seguridad, y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y otras personas afectadas"*[249]

Por tanto, las Evaluaciones de Impacto se componen de una serie de fases que apuntan a un objetivo en común: proporcionar una visión detallada y objetiva de la *"gestión de los riesgos relativos a la protección de datos que se realiza durante el ciclo de vida de los datos asociados a las actividades de tratamiento para poder garantizar los derechos y libertades de las personas físicas*".[250] En ese sentido, encontramos las siguientes fases de ejecución: Contexto del Tratamiento, Gestión de Riesgos y Conclusión.[251]

Consiguientemente, encontramos en la primera etapa del proceso, constituida por el "Contexto del Tratamiento", la descripción del ciclo de vida y flujo de los datos personales, con el objetivo de obtener una visión en detalle que facilite la identificación de las amenazas y los riesgos a los que se ven expuestos los datos de carácter personal.[252]

Una vez realizada aquella labor, la segunda parte de esta etapa consiste en determinar la necesariedad y proporcionalidad del tratamiento. En ese sentido, se requiere, a razón del Principio de Responsabilidad Proactiva, dar el debido cumplimiento al principio de "minimización de datos", que establece que los datos personales serán los adecuados y pertinentes en relación con los fines del tratamiento, lo que a su vez lleva a determinar cuáles son aquellos datos estrictamente necesarios para realizar las actividades del tratamiento.

Por su parte, para determinar la proporcionalidad del tratamiento es de importancia realizar una evaluación para establecer si la finalidad de las operaciones del tratamiento puede ser

[249] UE, 2016, op. cit., pp. 54.
[250] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *Guía Práctica para las Evaluaciones de Impacto en la Protección de los Datos Sujetas al RGPD* [en línea]. Madrid, España, 2019c, pp. 10. Disponible en: https://bit.ly/2LxWdLU
[251] Ibid., pp. 12.
[252] Loc. Cit.

alcanzada a través de medios diferentes, utilizando otros datos personales, limitando la cantidad de personas afectadas, haciendo uso de distintas tecnologías o aplicando otros tipos de tratamiento.[253]

Luego, en íntima relación a las Evaluaciones de Impacto, encontramos la Gestión de Riesgos entendida como aquellas particulares actividades y tareas que permiten controlar la incertidumbre relativa a determinadas amenazas, que incluye una serie de etapas entre las que encontramos la identificación y evaluación de los riesgos, como también la toma de medidas para tratarlos y conseguir su reducción o mitigación.[254]

Por ello, las amenazas son entendidas como cualquier factor de riesgo con potencial para materializar un daño o perjuicios a los interesados sobre cuyos datos personales se va a realizar un determinado tratamiento. Así, un riesgo puede ser concebido como aquella combinación entre la posibilidad de que se materialice una amenaza y sus consecuencias negativas, por lo que en la etapa de identificar los riesgos siempre es posible considerar aquella amenaza que les origina.[255]

En relación con lo anterior, se puede mencionar entonces que un determinado riesgo puede producir un impacto, lo que a su vez se establece en la etapa de evaluación de riesgos. Así, un impacto se determina tomando en consideración los posibles daños que se pueden producir si una amenaza se materializa.[256]

Por último, las Evaluaciones de Impacto conllevan la obligación de realizar la debida supervisión de la implementación de las medidas establecidas para tratar y controlar los riesgos inherentes a las actividades del tratamiento. En ese sentido, se hace necesario hacer una revisión de estas y evaluar su implementación hasta conseguir que los riesgos residuales[257] permitan garantizar los derechos y libertades de las personas físicas.[258]

Así, se requiere al final del proceso generar un plan de acción que establezca todas aquellas medidas que van a ser implementadas, y por tanto, supervisadas, indicando a su vez aquellos

---

[253] Ibid., pp. 20.
[254] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales Sujetos al RGPD* [en línea]. Madrid, España, 2019d, pp. 3. Disponible en: https://bit.ly/2KjOUqD
[255] Ibid., pp. 3-4.
[256] Loc. Cit.,
[257] AEPD, 2019c, op. cit., pp. 32. "*El riesgo residual es el riesgo de cada actividad una vez se hayan aplicado las medidas de control para mitigar y/o reducir su nivel de exposición. A diferencia del riesgo inherente, el riesgo residual contempla las medidas de control definidas sobre la actividad de tratamiento para valorar la probabilidad y/o el impacto asociado al riesgo.*"
[258] Ibid., pp. 36

responsables de su implementación y los plazos para llevarlo a cabo.[259] A su vez, estas medidas deben ser documentadas exhaustivamente en orden dar el debido cumplimiento al Principio de Responsabilidad Proactiva.[260]

Debido a lo anterior, si antes no existían razones para incorporar las Evaluaciones de Impacto al Proyecto, porque se consideraban obligatoriamente para ciertas situaciones, ahora existen mínimo tres. En primer lugar, tal como se analizó *ut supra*, actualmente el Proyecto contempla el deber de Protección de Datos desde el Diseño (PDdDI) que está fuertemente ligado a las Evaluaciones de Impacto porque estas permiten conferirle efectividad. Así, se integra al desarrollo y diseño de proyectos de alto riesgo y a las actividades de los responsables una aproximación y concientización preventiva, proactiva y basada en los riesgos de determinados tipos de tratamiento de datos.

Entonces se trata, en el fondo, de una relación simbiótica, es decir, si se desea que la PDdDI no sea solo una declaración de buenas intenciones, sería prudente que el texto normativo explicite o contenga al menos una medida que permita dotarle de efectividad. Un caso ejemplificador y teórico en el que se pudo haber realizado recientemente una Evaluación de Impacto para evitar la materialización de altos riesgos, en atención al tipo de datos tratados, es el del diseño y desarrollo de la aplicación "CoronApp" del Ministerio de Salud, que tenía por objetivo realizar un seguimiento y control de las personas afectadas y/o contagiadas por el virus COVID-19, pero que fue duramente criticada en su minuto puesto que no cumplía con estándares en materia de protección de datos personales adecuados a los fines del tratamiento ya que, por ejemplo, permitía la conservación de las bases de datos hasta por 15 años, de forma totalmente desproporcionada. [261]

En segundo lugar, el Proyecto de Ley contempla hoy por hoy la designación de un Delegado de Protección de Datos al que se le podrían conferir, tal como en el RGPD, funciones relativas al desarrollo de Evaluaciones de Impacto. Así, el Delegado podría asesorar al responsable de datos en esta materia y monitorear el desarrollo de la evaluación respectiva.[262] Sin embargo, es necesario recalcar que esta función, no considerada en la Moción ni en el Proyecto, debe remarcar el hecho de que es el responsable del tratamiento el encargado de llevar a cabo la Evaluación de Impacto[263], no obstante puede recurrir al Delegado para que este último le

[259] Ibid., pp. 33.
[260] ART. 29WP, 2017c, op. cit., pp. 12.
[261] BORDACHAR, Michelle y CONTRERAS, Pablo. *Problemas de protección de los datos personales de la aplicación "CoronApp*". CIPER Chile. [en línea]. 2020, Disponible en https://bit.ly/2ZOJsQr.
[262] ICO, 2019, op. cit., pp 210.
[263] AEPD, 2019c, op. cit., pp. 7.

provea del asesoramiento requerido, en el caso de que este haya sido nombrado, tomando en cuenta el hecho de que su nombramiento es facultativo, pero promovido por la propuesta hecha en el Proyecto de Ley.

Particularmente, se recomienda que el responsable del tratamiento acuda al Delegado en las siguientes circunstancias o para resolver los siguientes problemas:

a) *"Determinar si se debe o no llevar a cabo una Evaluación de Impacto.*
b) *Determinar qué metodología seguir para llevar a cabo una Evaluación de Impacto.*
c) *Determinar si llevar a cabo la Evaluación de Impacto internamente o subcontratarla.*
d) *Determinar qué garantías (incluyendo medidas técnicas y organizativas) aplicar para mitigar los riesgos a los derechos e intereses de los titulares de datos.*
e) *Determinar si la Evaluación de Impacto se llevo a cabo correctamente y si sus conclusiones están en concordancia y cumplen con la normativa".*[264]

En ese sentido, el Delegado además debe actuar selectivamente, basado en los riesgos de las actividades del tratamiento llevadas a cabo por el responsable del tratamiento, enfocándose especialmente en aquellas que suponen un mayor riesgo a los derechos e intereses de los titulares de datos. Por esa razón, el asesoramiento que ofrece el Delegado en esta materia se vuelve pragmático y permite evaluar otras cuestiones, como lo sería el determinar qué áreas podrían ser auditadas en materia de protección de datos personales interna o externamente, qué actividades de formación interna podrían ser proporcionadas al personal o los directivos y aconsejar a qué operaciones del tratamiento se les debe dedicar mayor atención y recursos.[265]

Además, si el responsable del tratamiento no está de acuerdo con el asesoramiento brindado por el Delegado, la documentación de la Evaluación de Impacto debiese de justificar específicamente las razones por las cuales el antedicho asesoramiento no se tomó en consideración[266], cuestión que en futuro podría ser requerida por la autoridad de control.

En tercer lugar, la consagración expresa de este mecanismo de cumplimiento preventivo le permitiría al Consejo para la Transparencia y Protección de Datos Personales, en el marco de los modelos diferenciados de cumplimiento, profundizar en la materia, teniendo como referencia al propio texto de la ley, especialmente en la parte técnica y procedimental de la

[264] ART. 29 WP, 2016, op. cit., pp. 17. Traducción nuestra.
[265] Ibid., pp. 18.
[266] Ibid., pp. 17.

Evaluación. Por otro lado, sería recomendable, a la luz de esta oportunidad, conferirle expresa y legalmente a la autoridad de control, dentro del texto que contenga en nuestro futuro ordenamiento a las Evaluaciones de Impacto, la facultad de publicar y confeccionar una lista de las operaciones de tratamiento que requieran o no de una medida de este tipo, tal como se encuentra establecido en los apartados 4 y 5 del artículo 37 del RGPD.[267]

De esta manera, al mismo tiempo que se delimitan de mejor manera las facultades de la autoridad de control en el ámbito de los modelos diferenciados de cumplimiento y medidas como las Evaluaciones de Impacto, se consigue restringir su discrecionalidad administrativa para llevarla al lado de una discrecionalidad más bien técnica.[268]

Finalmente, en relación con el control que podría ejercer el Consejo para la Transparencia y Protección de Datos Personales, es importante destacar el eminentemente carácter objetivo de las Evaluaciones de Impacto, ya que dispone de un proceso sistemático estandarizado que garantizan la homogeneidad, repetitividad y comparabilidad en su ejecución[269], lo que a su vez permitiría que se inserte de forma natural en el sistema de cumplimiento del Proyecto, en base al Principio de Responsabilidad Proactiva, que busca generar los medios de prueba que permitan acreditar el debido cumplimiento, ante la autoridad de control, de los principios y obligaciones en materia de protección de datos personales[270]. Además, en el caso que corresponda y el responsable del tratamiento no sea capaz de establecer las medidas suficientes y necesarias para reducir los riesgos a rangos aceptables, es bastante útil otorgarle la facultad de acudir y consultar a la autoridad de control antes de poner en marcha la actividad de tratamiento prevista.[271]

[267] UE, 2016, op. cit., pp. 54.
[268] GUZMÁN SUARÉZ, Lionel. *El Control de la Discrecionalidad Administrativa en Chile*. Repositorio Académico de la Universidad de Chile. 2001. Pp. 51-52. El autor define a la discrecionalidad técnica de la siguiente manera: "*se conoce con esta denominación a aquellos casos en que la ley confiere un ámbito de decisión a la Administración para obtener un resultado conforme a evaluaciones de naturaleza exclusivamente técnica, que en muchos casos está a su vez delimitada o guiada por conceptos jurídicos indeterminados (mérito y capacidad, justo precio, oferta más ventajosa, etc..), pero cuya concreción es con frecuencia incierta y opinable.* (…)" Disponible en: https://bit.ly/39ws9Kn
[269] AEPD, 2019c, op. cit., pp. 10.
[270] ART. 29WP. 2017C, op. cit., pp. 4.
[271] Ibid., pp. 19.

### 2.4.2. REGISTRO DE LAS ACTIVIDADES DEL TRATAMIENTO

Por otro lado, algo similar ocurrió con la obligación de llevar un registro de las actividades del tratamiento. Así, el grupo de asesores parlamentarios recomendó desechar el artículo 26[272] de la Moción Parlamentaria y aprobar el texto del Mensaje.

Este artículo contenía la obligación de llevar una bitácora de las actividades de tratamiento efectuadas, y que debían contener, por ejemplo y como mínimo, las categorías de tratamiento y las transferencias internacionales de datos realizadas en el caso que corresponda.[273] Sin embargo, esta obligación contenida en el artículo 30 del RGPD, puede y debe ser utilizada para crear la documentación necesaria para acreditar el debido cumplimiento al Principio de Responsabilidad Proactiva.[274]

A diferencia de lo establecido en el RGPD, el artículo desechado no contenía la obligación del responsable o encargado del tratamiento, o de su representante respectivo, de poner a disposición de la autoridad de control el registro correspondiente. Lo anterior tiene gran importancia para una posible futura discusión legislativa, en el sentido de que al mismo tiempo obliga a los responsables a mantener actualizado el antedicho registro en un formato claro y legible, que requiere a su vez revisión continua frente a potenciales cambios en las actividades del tratamiento.[275]

Por otro lado, en la práctica, un tratamiento puede identificarse como el conjunto de operaciones predispuestas con el objetivo de alcanzar una determinada finalidad legitimadas en una misma base jurídica. Así, incluirán operaciones tales como la recogida, registro, estructuración, organización, utilización o consulta de datos. Por tanto, una actividad del tratamiento debe ser registrada antes de su puesta en marcha, facilitándose esta labor al utilizar la información previa documentada durante la fase de definición del tratamiento.[276]

---

[272] CCLJRS, 2018, op. cit., pp. 316-317.

[273] Ibid., pp. 316. Las cuestiones a registrar propuestas en la moción parlamentaria son las siguientes: "*a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable;*
*b) los fines del tratamiento;*
*c) una descripción de las categorías de titulares y de las categorías de datos personales;*
*d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;*
*e) en su caso, las transferencias internacionales de datos personales y la documentación de garantías adecuadas;*
*f) Los plazos previstos para la cancelación o eliminación de las diferentes categorías de datos;*
*g) Una descripción general de las medidas técnicas y organizativas de seguridad*."

[274] ICO, 2019, op. cit., pp. 183-184.

[275] AEPD, 2019d, op. cit., pp. 18.

[276] Ibid., pp. 17

No obstante lo anterior, según el Informe de la Comisión Europea (CE) que evalúa la aplicación del RGPD durante estos dos años, de fecha 24 de junio del 2020, las pequeñas y medianas empresas (Pymes) tienden a tener problemas al momento de tratar de implementar el Principio de Responsabilidad Proactiva. En ese sentido, muchas veces incurren en gastos extras, como abogados y consultores, para poder obtener suficiente orientación o consejos prácticos respecto a sus obligaciones (como las de registro o transparencia). Así, las Pymes consideran que el registro de las actividades de tratamiento corresponde a una carga administrativa engorrosa, por lo que las autoridades están buscando alternativas que les permitan simplificar esa carga, como el uso de plantillas de registro simplificado, de forma que puedan cumplir con sus obligaciones.[277]

Tomando en consideración lo comentado en aquel informe, existen todavía razones para consagrar esta obligación en el Proyecto:

En primer lugar, y tal como expuso el Señor Jesús Rubí en la Comisión, uno de los objetivos de la instauración de este deber, en línea con el Principio de Responsabilidad Proactiva, es que la autoridad de control no se sobrecargue de tareas fiscalizadoras que acarreen un desembolso enorme de recursos. Así, la solución viene dada por un modelo de cumplimiento proactivo en el que los responsables son los encargados de mantener sus registros a disposición de la autoridad de control, y para aquello además se incorpora, como garantía, la figura del Delegado de Protección de Datos.[278]

Adicionalmente, es importante destacar el hecho de que, al momento de realizar la debida Gestión de Riesgos, es importante al principio del proceso identificar el tipo de tratamiento que se va a realizar y, por consiguiente, identificar las distintas finalidades del tratamiento de datos personales, lo que a su vez facilita el antedicho proceso.[279] Por ello, correspondería a cada organización, de acuerdo con el Principio de Responsabilidad Proactiva, decidir el nivel de agregación o segregación para elaborar el registro de actividades del tratamiento y hasta qué punto se condice aquello con las finalidades, bases jurídicas y grupos de individuos potencialmente afectados.[280]

Consiguientemente, aquel esfuerzo permite entrelazar y consolidar en una medida con marcada objetividad como lo es el registro de actividades del tratamiento, el comienzo de

[277] EC, 2020a, op. cit., pp. 24.
[278] CCLJRS, 2018, op. cit., pp. 178.
[279] AEPD, 2019d, op. cit., pp. 17.
[280] Ibid., pp 9.

cualquier tratamiento de datos personales que podría afectar los derechos de los interesados y los principios u obligaciones legales establecidos por el Legislador.

Así, esta medida es una herramienta esencial al momento de evaluar cualquier tipo de procesamiento de datos que se vaya a planear o ya se esté llevando a cabo, con el objetivo de facilitar la gestión de riesgos *de facto* que lleva adelante el responsable o encargado del tratamiento en relación con los derechos de los titulares de datos, permitiéndoles identificar de mejor manera aquellas medidas más apropiadas para salvaguardar los datos personales involucrados, que son a su vez complementos claves del Principio de Responsabilidad Proactiva.[281]

En ese sentido, esta medida se vuelve un esencial complemento a las herramientas anteriormente reseñadas en este ensayo, como lo serían las Evaluaciones de Impacto, los Principios de Protección de Datos desde el Diseño y por Defecto, el establecimiento de medidas de seguridad y, en su caso, las correspondientes notificaciones a la autoridad de control de las brechas de seguridad.

Sin embargo, la ausencia formal en el Proyecto de Ley del Principio de Responsabilidad Proactiva resta harmonía a la construcción e interpretación normativa que se realiza, especialmente si consideramos que se hace esencial "*identificar adecuadamente las actividades del tratamiento y documentar los análisis realizados, así como, dejar trazabilidad de los mismos y de las conclusiones que los soportan para poder garantizar la responsabilidad proactiva*".[282] En suma, la ausencia formal tanto del Principio de Responsabilidad Proactiva como de la medida de llevar un registro de las actividades del tratamiento dificulta y resta efectividad al Proyecto de Ley, permitiendo inconsistencias internas en el sistema de cumplimiento.

En segundo lugar, el Proyecto de Ley contempla estándares diferenciados de cumplimiento, por lo que sería de provecho utilizarlos para simplificar o reducir la información que las Pymes deben incluir en sus respectivos registros. Esto conllevaría la necesidad de consagrar extensa y explícitamente esta obligación dentro del Título II Párrafo Primero del Proyecto, de forma que de la simple lectura del texto el sistema de deberes y obligaciones sea coherente y fácil de entender.

---

[281] ARTICLE 29 WORKING PARTY (ART. 29WP). *WORKING PARTY 29 POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*. Bruselas, Bélgica, 2018, pp. 2. Disponible en: https://bit.ly/3geblJI

[282] AEPD, 2019d, op. cit., pp. 10.

Además, se le permitiría al Consejo para la Transparencia y Protección de Datos Personales el utilizar este mecanismo para adecuar a las empresas, en virtud del tamaño, necesidades y el tipo de tratamiento de datos que realizan, el nivel de exigencia en materia de cumplimiento de la futura normativa mientras esta se implementa a lo largo de los años, permitiéndole evaluar y resolver los problemas que puedan presentarse en el intertanto. Algo en este sentido se puede entrever en la propuesta parlamentaria y en el artículo 30 numeral 5 del RGPD, pero haciendo énfasis en la cantidad de trabajadores empleados por el responsable o encargado del tratamiento, con excepciones vinculadas justamente al nivel de riesgo de las actividades de tratamiento involucradas en consideración a los derechos de los titulares de datos.[283]

Por su parte, y como se ha reseñado *ut supra*, el Proyecto actualmente contempla la figura del Delegado de Protección de Datos Personales, al que a su vez se le pueden conferir facultades para llevar y mantener el registro de las actividades del tratamiento a cuenta del responsable. Antedicha facultad, que en la Unión Europea es una práctica recomendada, le permite al Delegado cumplir de mejor manera su función de supervisar el cumplimiento de la normativa, convirtiéndose esta relación en una efectiva medida de cumplimiento.[284]

Para finalizar, la peor opción, sin lugar a duda, sería que no se incluyera esta obligación bajo el pretexto de que se podría afectar el crecimiento y desenvolvimiento de las Pymes en la economía, al atribuirle cargas desproporcionadas. En ese escenario, se estaría beneficiando injustamente a las empresas de mayor tamaño que, por lo general, presentan mayores niveles de riesgos en su tratamiento por la cantidad y fines de los datos que procesan. Así, un contrargumento a esta postura se puede resumir en la siguiente cita:

> *"Like all regulation, data protection rules have inherent compliance costs for companies. However, these costs are outweighed by the opportunities and advantages of strengthened trust in digital innovation and the societal benefits resulting from respecting a fundamental right".*[285]

---

[283] CCLJRS, 2018, op. cit., pp. 316. *"Las obligaciones anteriores no se aplicarán a ninguna empresa ni organización que emplee a menos de 200 personas salvo que el tratamiento que realice pueda producir un riesgo para los derechos y libertades de los titulares, tales como el tratamiento masivo de datos, los datos tratados en el desarrollo de aplicaciones móviles o el tratamiento de datos especialmente protegidos.".*
Por su parte, el artículo 30 numeral 5 del RGPD estatuye lo siguiente: "*Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10."* UE, 2016, pp. 51.

[284] ART. 2WP, 2016, op. cit., pp.19.

[285] EC, 2020a, op. cit., pp. 22.

### 2.4.3. CONSAGRACIÓN EXPRESA DEL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

En este ensayo se ha perseguido el objetivo de justificar la consagración explícita del Principio de Responsabilidad Proactiva en el Proyecto de Ley que reforma la Ley 19.628 Sobre Protección de la Vida Privada. En ese sentido, en el capítulo 1ero del mismo, se revisó la historia del Principio a la luz de su desarrollo en manos de la OCDE y la Unión Europea.

De esta manera se concluyó que su significación va más allá de un simple principio de responsabilidad legal, ya que además requiere que el responsable sea capaz de demostrar, rindiendo cuentas de sus acciones, el cumplimiento a las obligaciones y principios básicos en materia de protección de datos personales.

No obstante aquello, supone igualmente que el responsable adopte una aproximación basada en los riesgos del tratamiento que realiza o controla, de forma que pueda tomar las medidas técnicas y organizativas apropiadas, tanto interna como externamente, para acreditar y garantizar el debido cumplimiento de sus obligaciones. En ese sentido, lo que se busca es fomentar la concientización y la integración de la protección de los datos personales a las actividades y decisiones que toman los responsables, incluso con anterioridad a su desarrollo, con el fin de evitar que se puedan afectar los derechos y libertades de los titulares de datos.

Así, el más alto estándar internacional, representado por el RGPD, establece un sistema de cumplimiento que contiene una batería de medidas concretas, voluntarias, autoregulatorias y/u obligatorias, que orbitan sobre el eje del Principio de Responsabilidad Proactiva, con el fin de llevar de la teoría a la práctica, esto es, dotar de efectividad, a los principios básicos en materia de protección de datos personales.

Entonces, se ha podido constatar que el antedicho sistema ha sido el punto de referencia para que Chile, a través del Proyecto de Ley, pueda adecuar sus políticas y marco normativo en esta materia. De esta manera, se analizó críticamente el sistema de cumplimiento propuesto por el Proyecto de Ley, para confirmar que está basado, casi en su totalidad, en el del RGPD.

Del análisis realizado se puede colegir que el sistema propuesto posee un carácter eminentemente proactivo y preventivo. Sin embargo, puede ser perfeccionado todavía, más aún si se considera que le falta el corazón que dotó de coherencia, efectividad y reconocimiento mundial al modelo de la Unión Europea.

Además, se dejó patente que la consagración de este principio no impone nuevas obligaciones o requisitos a los responsables. El resultado del propio análisis arroja que la mayoría de las medidas u obligaciones del sistema ya se encuentran consideradas en el Proyecto, tanto explícita como implícitamente. Inclusive, el Proyecto ya consigna que existe responsabilidad legal respecto al cumplimiento de los principios y obligaciones. Desde esta perspectiva, la inclusión del Principio de Responsabilidad Proactiva no supone una gran novedad, empero, la gran diferencia que trae su consagración es que permite, al mismo tiempo, asegurar y reforzar *de facto* la efectividad de los principios y obligaciones prestablecidos.[286]

En relación con lo anterior, y como última propuesta de este ensayo, se recomienda la consagración expresa del Principio de Responsabilidad Proactiva en el Proyecto de Ley. Así, el artículo 3 letra e) del texto debiese de ser reemplazado, como mínimo, por la propuesta hecha en la Moción Parlamentaria de los Honorables Senadores Harboe, Araya, De Urresti, Espina y Larraín, con la siguiente enmienda:

> "*Principio de Responsabilidad Proactiva*: *El responsable del tratamiento será responsable del cumplimiento de los principios y obligaciones de la presente ley, debiendo ser capaz de demostrarlo".*

[286] ART. 29WP, 2010, op. cit., pp. 10.

## CONCLUSIONES

En razón de este ensayo, se puede concluir que en Chile se está debatiendo la inclusión, a su marco legal, de un sistema de cumplimiento eminentemente proactivo y preventivo en materia de protección de datos personales. Antedicho sistema no es nuevo, ya que ha sido desarrollado por más de 30 años en el ámbito internacional, tanto por la OCDE como por la Unión Europea a través de su "Reglamento General de Protección de Datos" (RGPD).

El centro de este modelo de sistema de cumplimiento está basado en la implementación del Principio de Responsabilidad Proactiva (*Accountability Principle*), que considera la adopción de una batería de medidas por parte del responsable que buscan dotar de efectividad a los demás principios rectores en materia de protección y tratamiento de datos personales, y garantizar los derechos y libertades de los titulares de datos personales.

Sin embargo, el presente trabajo concluye que este principio no encuentra consagración legal y expresa en el estado de avance actual del proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletines 11.144-07 y 11.092-07, refundidos), por lo que contiene una serie de fallas orgánicas y de técnica legislativa en materia de cumplimiento de la normativa.

En ese sentido, se colige que aun cuando no se tiene consagración explícita de este principio, el sistema de cumplimiento propuesto por el proyecto está basado casi íntegramente en el innovador sistema que establece el RGPD de la Unión Europea. De esta manera, se puede afirmar que las medidas contenidas en el Reglamento de la UE se encuentran, en parte, reproducidas en el Proyecto, y por tanto se pueden encontrar los deberes de protección de datos desde el diseño y por defecto, la obligación de adoptar medidas de seguridad y notificar las brechas de seguridad, la posibilidad de designar un Delegado de Protección de Datos, obligaciones referidas a las bases de licitud del tratamiento de datos personales, el deber de transparencia activa, mecanismos de certificación y obligaciones o medidas en materia de transferencias internacionales de datos personales.

Por ello, cada una de estas medidas fueron analizadas y comentadas a lo largo de este ensayo, pudiéndose concluir que, aun cuando constituyen inclusiones similares a las hechas por el RGPD, contienen diferencias sustanciales en materia de cumplimiento, como lo serían algunas veces la inexistencia de condiciones de aplicación obligatoria, mecanismos de certificación adecuados o plazos explícitamente establecidos.

Estas cuestiones permitieron, a su vez, alcanzar uno de los objetivos de este trabajo, esto es, realizar las propuestas necesarias en materia de cumplimiento a las medidas contempladas actualmente por el Proyecto en virtud del Principio de Responsabilidad Proactiva.

Sin embargo, se logró constatar, además, la existencia en la discusión parlamentaria de dos medidas que fueron excluidas del Proyecto de Ley. Estas medidas son las Evaluaciones de Impacto sobre protección de datos personales y el deber de llevar un registro de las actividades del tratamiento de datos personales.

Debido a lo anterior, se puede colegir que sus inclusiones son cruciales, en virtud del Principio de Responsabilidad Proactiva, para dotar de efectividad a la batería de herramientas que actualmente contiene el Proyecto de Ley, por lo que se hizo hincapié en cómo se relacionaban en la práctica con las medidas ya preestablecidas y los perjuicios prácticos y económicos que podría traer en materia de cumplimiento su falta de implementación.

Así, este ensayo adicionalmente se convierte en una primera aproximación a una guía práctica de cumplimiento, en español, relativa a los principios, deberes y obligaciones que contendrá la futura legislación chilena en materia de protección de datos personales, proponiendo realizar, por ahora, una lectura del sistema de cumplimiento bajo el prisma de la implementación interpretativa del Principio de Responsabilidad Proactiva.

Por tanto, se concluye que la consagración explícita de este principio permitiría a los responsables y encargados del tratamiento de datos personales entender y sistematizar mejor sus obligaciones, deberes y el sistema general de cumplimiento propuesto, reforzando de esta manera la efectividad del sistema, ya que se cristalizaría en la adopción de medidas concretas por parte de los responsables que garantizarían tanto a los principios rectores en materia de protección de datos personales como a los derechos y libertades de los titulares de estos datos.

**BIBLIOGRAFÍA**


31TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS (31TH ICDPPC), *The Madrid Resolution.* Madrid, España, 2009. Disponible en: https://bit.ly/3n86OLf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *Guía de Privacidad desde el Diseño*. [en línea] [Archivo PDF] 2019a. Disponible en: https://bit.ly/341tmpH

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), *La K-anonimidad como medida de privacidad*, 2019b. Disponible en: https://bit.ly/3gAFRNY

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *Guía Práctica para las Evaluaciones de Impacto en la Protección de los Datos Sujetas al RGPD* [en línea]. Madrid, España, 2019c. Disponible en: https://bit.ly/2LxWdLU

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales Sujetos al RGPD* [en línea]. Madrid, España, 2019d. Disponible en: https://bit.ly/2KjOUqD

ALHADEFF, J., VAN ALSENOY, B. and DUMORTIER, J. *The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions*. En: POSTIGO, H., NEYLAND, D., KROENER, I., Ilten, C., HEMPEL, L. and GUAGNIN, D. *Managing Privacy Through Accountability*. Basingstoke: Palgrave Macmillan. 2012, pp. 49-82.

ÁLVAREZ VALENZUELA, Daniel. *La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa.* Revista Chilena de Derecho y Tecnología. 9(1), 2020.

ARTICLE 29 DATA PROTECTION WORKING PARTY (ART. 29WP). *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.* Bruselas, Bélgica, 2009. Disponible en https://bit.ly/2O6XE1Y

ARTICLE 29 DATA PROTECTION WORKING PARTY (ART. 29WP). *Opinion 3/2010 on the principle of accountability*. Bruselas, Bélgica, 2010. Disponible en https://bit.ly/3gx4s4Q

ARTICLE 29 DATA PROTECTION WORKING PARTY (ART. 29WP), *Guidelines on Data Protection Officers ('DPOs')*. Bruselas, Bélgica, 2016. Disponible en: https://bit.ly/3oFdvoF

ARTICLE 29 DATA PROTECTION WORKING PARTY (ART. 29WP), *Guidelines on Personal data breach notification under Regulation 2016/679*. 2017a, Bruselas, Bélgica. Disponible en: https://bit.ly/3mmHaI2

ARTICLE 29 DATA PROTECTION WORKING PARTY (ART. 29WP). *Guidelines on transparency under Regulation 2016/679*, 2017b, Bruselas, Bélgica. Disponible en: https://bit.ly/39JdprU

ARTICLE 29 DATA PROTECTION WORKING PARTY (ART. 29WP). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. Bruselas, Bélgica, 2017c. Disponible en: https://bit.ly/2KqGIEI

ARTICLE 29 DATA PROTECTION WORKING PARTY (ART. 29WP). *WORKING PARTY 29 POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*. Bruselas, Bélgica, 2018. Disponible en: https://bit.ly/3geblJI

BANCO INTERAMERICANO DE DESARROLLO Y ORGANIZACIÓN DE ESTADOS AMERICANOS (BID y OEA). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*, 2020. http://dx.doi.org/10.18235/0002513

BERNAL, Paul. *Internet Privacy Rights*. Cambridge: Cambridge University Press. 2014.

Boletín de indicaciones formuladas durante la discusión en general del proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletín de Indicaciones). 2018. Disponible en https://bit.ly/2Oi7yxT

BORDACHAR, Michelle y CONTRERAS, Pablo. *Problemas de protección de los datos personales de la aplicación "CoronApp"*. CIPER Chile. [en línea]. 2020, Disponible en https://bit.ly/2ZOJsQr

COMISIÓN CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO DE LA CÁMARA DE DIPUTADOS (CCLJRD). *Segundo Informe recaído en el proyecto de reforma constitucional que consagra el derecho a la protección de los datos personales (Boletín 9.384-07).* Abril de 2018. Disponible en: https://bit.ly/3oI2DWZ

COMISIÓN CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO DEL SENADO (CCLJRS). *Primer Informe sobre el Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletines 11.144-07 y 11.092-07, refundidos)*. Marzo del 2018. Disponible en https://bit.ly/2CeD5hm

COMISIÓN CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO DEL SENADO (CCLJRS). *Comparado Primer Trámite Constitucional: 2do Informe sobre el Proyecto de Ley que modifica la ley 19.628, con el fin de regular la protección y el tratamiento de los datos personales (Boletines 11.144-07 y 11.092-07, refundidos)*. 2020a. Disponible en https://bit.ly/2CbKpKy

COMISIÓN CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO DEL SENADO (CCLJRS). *Segundo Informe recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*. 2020b.

CORDERO VEGA, Luis. *Lecciones de Derecho Administrativo*. Legal Publishing Chile, 2da edición corregida, Chile, 2015.

DE HERT, Paul. *Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights La.* En: POSTIGO, H., NEYLAND, D., KROENER, I., Ilten, C., HEMPEL, L. and GUAGNIN, D. *Managing Privacy Through Accountability*. Basingstoke: Palgrave Macmillan. 2012, pp. 193-232.

DEPARTAMENTO DE ASUNTOS ECONÓMICOS Y SOCIALES DE LA ORGANIZACIÓN DE NACIONES UNIDAS [ONU:DAES]. *United Nations E-Government Survey 2020*. [s.l.]: United Nations, 2020. Disponible en: https://bit.ly/3a9TzpQ

EUROPEAN COMMISSION (EC). *Commission Staff Working document accompanying the document: Communication from The Commission to the European Parliament and The Council: Data protection rules as a pillar of citizens empowerment and EUs approach to digital*

*transition - two years of application of the General Data Protection Regulation*. 2020a. Disponible en https://bit.ly/2CdjTjV

EUROPEAN DATA PROTECTION BOARD (EDPB). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. [en línea] Versión 2.0, 2020a, pp. 5. Disponible en https://bit.ly/3qGu2KF

EUROPEAN DATA PROTECTIÓN BOARD (EDPB). *Guidelines 05/2020 on consent under Regulation 2016/679,* 2020b. Disponible en: https://bit.ly/36ESjZR

EUROPEAN DATA PROTECTION BOARD (EDPB). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.* 2020c. Disponible en: https://bit.ly/2JMRtRQ

FRIGERIO, Catalina. *Mecanismos De Regulación De Datos Personales: Una Mirada Desde El Análisis Económico Del Derecho*. Revista Chilena de Derecho y Tecnología 7(2): 2018. doi:10.5354/0719-2584.2018.50578.

GUZMÁN SUARÉZ, Lionel. *El Control de la Discrecionalidad Administrativa en Chile*. Repositorio Académico de la Universidad de Chile. 2001. Disponible en: https://bit.ly/39ws9Kn

INFORMATION COMMISSIONER'S OFFICE (ICO). *Guide to the General Data Protection Regulation (GDPR)*. [en línea] 2019. Disponible en https://bit.ly/3fbFN5H

LEÓN, Ricardo y MEZA, Sebastián. *Brecha en el uso de internet: Desigualdad digital en el 2020.* Fundación País Digital: Centro de Estudios Digitales. 2020. Disponible en: https://bit.ly/3nlLceM

LISONI, Diego. *Modernización y Transformación Digital del Estado: Desafíos, Oportunidades y Propuestas a la luz de la Crisis Sanitaria y el Estallido Social en Chile.* CAF- Banco de Desarrollo de América Latina, 2020. Disponible en: https://bit.ly/3afGE5A

MCMULLAN, Katie. *Legislative Framework*. En: INTERNATIONAL ASSOCIATION OF PRIVACY PROFFESIONALS (IAPP), *European Data Protection: Law and Practice*. Ed: Eduardo Ustaran, 2018, pp. 52-75.

MOLINA, Paulina. *Plebiscito histórico en Chile: apruebo o rechazo, las opciones que tenían los chilenos en el referendo de cambio de Constitución.* BBC Mundo: News. [en línea] Octubre de 2020. Disponible en: https://bbc.in/346edmL

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. 1980. Disponible en: https://bit.ly/320wD8e

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD). *The OECD Privacy Framework*. París: OECD Publishing. 2013. p. 69. Disponible en https://bit.ly/2Z4AS0N

POTHOS, Mary. *Accountability Requirements*. En: INTERNATIONAL ASSOCIATION OF PRIVACY PROFFESIONALS (IAPP), *European Data Protection: Law and Practice*. Ed: Eduardo Ustaran, 2018, pp. 204-224.

RUDGARD, Sian. *Origins and Historical Context of Data Protection Law*. En: INTERNATIONAL ASSOCIATION OF PRIVACY PROFFESIONALS (IAPP), *European Data Protection: Law and Practice.* Ed: Eduardo Ustaran, 2018, pp. 15-35.

ŠTARCHOŇ, Peter y PIKULÍK, Tomáš. *GDPR principles in Data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones.* Procedia Computer Science. Vol. 151, 2019. DOI 10.1016/j.procs.2019.04.043

THE CIVIL SOCIETY, *The Madrid Privacy Declaration*. Madrid, España, 2009. Disponible en: https://bit.ly/3n9LOUC

USTARAN, Eduardo. *International Data Transfers*. En: INTERNATIONAL ASSOCIATION OF PRIVACY PROFFESIONALS (IAPP*), European Data Protection: Law and Practice*. Ed: Eduardo Ustaran, 2018, pp. 225-241.

WORLD ECONOMIC FORUM (WEF). *The Global Risks Report 2020.* Suiza, 15 de Enero de 2020. Disponible en: https://bit.ly/348zrAL

**PÁGINAS WEB**

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *FACILITA RGPD: Herramienta de ayuda para empresas que realicen un tratamiento de datos personales de escaso riesgo para el cumplimiento del Reglamento General de Protección de Datos*. [en línea] s/f, Disponible en https://bit.ly/3gGDEiD

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *Medidas de Cumplimiento*. [en línea] 27 de Febrero de 2020a, Disponible en: https://bit.ly/2Z7IkrU

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). *Medidas de protección de datos desde el diseño y por defecto.* [en línea] 27 de Febrero de 2020b, Disponible en https://bit.ly/38zpQ6Y

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD*). Evaluaciones de impacto de protección de datos*. 9 de Marzo de 2020c. Disponible en https://bit.ly/3f5lOpg

BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE*. Proyectos de Modificación Ley N°19.628*. BCN/Ley Chile [en línea] Disponible en: https://bit.ly/3a7f5eQ

EUROPEAN COMMISSION (EC). *Informe de la Comisión: las normas de protección de datos de la UE empoderan a los ciudadanos y están adaptadas a la era digital*. European Union's Official Website. 2020b. Comunicado de prensa disponible en: https://bit.ly/2ZM6kAe

GLOBAL PRIVACY ASSEMBLY. *History of the Assembly*. [en línea]. Disponible en: https://bit.ly/2W8AqfI

**LEGISLACIÓN Y NORMATIVA**

CHILE, Ley N°19.628, *Sobre Protección de la Vida Privada*. Diario Oficial de la República de Chile, Santiago de Chile, 28 de Agosto de 1999.

CHILE. Constitución Política de la República de Chile, Diario Oficial de la República de Chile, Santiago, Chile. Disponible en: https://bit.ly/3oKneK6

CHILE. Ley N°20.285*, Sobre Acceso a la Información Pública*. Diario Oficial de la República de Chile, Santiago, Chile, 20 de Agosto de 2008. Disponible en: https://bit.ly/3orDfVw

CHILE. Ley N°21.096, *Consagra el Derecho a la Protección de los Datos Personales*. Diario Oficial de la República de Chile, Santiago, Chile, 16 de Junio de 2018. Disponible en: https://bit.ly/3a7Z6NN

CHILE. MINISTERIO DE RELACIONES EXTERIORES. *Decreto Supremo N°28 que promulga el Acuerdo por el que se establece una Asociación entre la República de Chile, por una parte, y la Comunidad Europea y sus estados miembros, por la otra, sus anexos, declaraciones conjuntas y la corrección introducida al articulo 40 del Anexo III, en su versión en español*. 2003. Disponible en https://bit.ly/2VWl12t

CHILE. Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N°11.144-07. Marzo del 2017. Disponible en https://bit.ly/3fb3knt

CHILE. Proyecto de ley sobre Protección de Datos Personales. Boletín N°11.092-07. Enero del 2017. Disponible en https://bit.ly/3iAuTbX

CHILE. Proyecto de reforma constitucional que consagra el derecho a la protección de los datos personales. Boletín N°9.384-07. Junio de 2014. Disponible en: https://bit.ly/2IGXWxo

ESTADOS DE CANADÁ, *Personal Information Protection and Electronic Documents Act (PIPEDA).* 13 de Abril del 2000. Disponible en: https://bit.ly/2WbRG3M

UNIÓN EUROPEA (UE). *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva 95/46/CE)*. Diario Oficial de la Unión Europea, 24 de Octubre de 1995, Disponible en español en https://bit.ly/31RjZZr.

UNIÓN EUROPEA (UE). *Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE*. Diario Oficial de la Unión Europea, 27 de Abril de 2016. Disponible en español en: https://bit.ly/2BFSyqV