REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 9 NÚM. 1 (2020) • PÁGS. 227-279 • DOI 10.5354/0719-2584.2020.56660
RECIBIDO: 2/3/2020 • APROBADO: 15/5/2020 • PUBLICADO: 30/6/2020

INFORMES

Obligaciones de seguridad en el tratamiento de datos personales en Chile: Escenario actual y desafíos regulatorios pendientes

Security obligations on the personal data processing in Chile: Current regulatory landscape and pending regulatory challenges

Carlo Benussi Díaz
Abogado, Chile

RESUMEN El siguiente trabajo tiene por objeto examinar y esquematizar el panorama regulatorio actual y futuro de obligaciones legales de seguridad vinculadas al tratamiento de datos personales efectuado en Chile. Para esto, hacemos una revisión de lo que sobre estas obligaciones dispone la Ley 19.628 sobre Protección de la Vida Privada; la Ley 20.584 que «Regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud» y su reglamento; la Ley 20.120 «Sobre la investigación científica en el ser humano, su genoma, y prohíbe la clonación humana» y su reglamento; y el proyecto de ley que modifica la Ley 19.628 sobre Protección de la Vida Privada, Boletín 11.144-07. En este examen se incluyen algunas consideraciones jurídicas particulares relativas a las obligaciones introducidas por este proyecto de ley.

PALABRAS CLAVE Datos personales, protección de datos, obligaciones de seguridad, brecha de seguridad, proyecto de ley.

ABSTRACT The purpose of the following article is to examine and map the current and future regulatory landscape of legal security obligations concerning the processing of personal data in Chile. For this purpose, we review the security obligations included in the Law 19,628 on the Protection of the Private Life; the Law 20,584, that "Regulates the rights and duties of the individuals regarding actions related with their health care", and its regulation; the Law 20,120, "On scientific research in the human being, its genome, and prohibits human cloning", and its regulation; and the bill of law that amends the Law 19,628 on the Protection of the Private Life, Bill 11,144-07. Specific legal considerations are explored concerning the obligations that are introduced in this bill of law.

KEYWORDS Personal data, data protection, security obligations, data breach, bill of law.

Introducción

El progresivo aumento en el uso que han tenido en la última década las nuevas tecnologías ha generado diversas industrias[1] estructuradas en base al tratamiento masivo de datos personales.[2] Esta masificación en el tratamiento de datos, junto con la complejidad y vulnerabilidad de los sistemas informáticos en que operan,[3] ha llevado a un aumento relevante en los riesgos para la seguridad de esos datos y, junto con ello, para los derechos de las personas, a la vida privada o la inviolabilidad de sus comunicaciones (Álvarez Valenzuela, 2019: 2; Smedinghoff, 2007: 2; Wacks, 2015b: 102).[4]

Este escenario de riesgos se ha venido confirmando año a año en la medida que —periódicamente— se han ido revelando vulneraciones a medidas de seguridad en sistemas informáticos, las que han implicado la filtración de miles de datos personales, que generan perjuicios a los titulares de datos y a los responsables que sufrieron la vulneración, y merman la confianza de los consumidores en el comercio electrónico (Hartzog, 2018: 3; Lehuedé, 2019: 8-9; OECD, 2013: 26; Schneier, 2015: 137-138).[5]

Bajo este panorama, la necesidad por aplicar —a nivel institucional e individual— mecanismos de seguridad en el tratamiento de datos personales se ha vuelto una

1. Por ejemplo, industrias relacionadas con las comunicaciones por internet, como el correo electrónico, las redes sociales y la mensajería instantánea. Véase Álvarez Valenzuela (2019: 242), quien señala que la sociedad de la información, asociada a la masiva disponibilidad de datos, ha significado un cambio social, cultural y económico mayor al de la Revolución Industrial.

2. «NIST Privacy Framework: A tool for improving privacy through enterprise risk management», National Institute of Standards and Technology, 16 de enero de 2020, pp. 1-2, disponible en https://bit.ly/30FgJQj. En Chile hay muchos ejemplos de industrias cuyo negocio se basa en el tratamiento masivo de datos personales, así como otras cuyo negocio tradicional está siendo transformado digitalmente al incorporar el tratamiento de datos personales como forma de generar valor y adaptarse al mercado. Véase Rodrigo Martínez «La transformación digital que irrumpe en las empresas chilenas», *La Tercera*, 4 de agosto de 2019, disponible en https://bit.ly/2AjDLRU; o Nicolás Sepúlveda, «Alguien te mira: Así funciona el gigante de las campañas políticas que controla Sosafe», *Ciper Chile*, 11 de septiembre de 2019, disponible en https://bit.ly/30sk6Km.

3. En esta línea, se ha señalado que el ecosistema digital actual es complejo, con diferentes niveles de interconexión, y con varios actores cumpliendo un rol diferente en distintas etapas de los ciclos de vida de los productos, por lo que se sugiere que la seguridad digital de los productos y servicios sea considerada desde el inicio y en todo su ciclo de vida (OCDE, 2019: 12).

4. La protección de datos personales es relevante porque su afectación puede generar un sinnúmero de consecuencias indeseables para sus titulares, desde problemas asociados a comunicaciones privadas, discriminación, suplantación de identidad, honor, vigilancia, libertades políticas, igualdad ante la ley y otras situaciones complejas (véase NIST, «NIST Privacy Network»; UNCTAD, 2019).

5. Schneier (2015: 149) profundiza este punto señalado que no todas las vulneraciones son iguales y tienen los mismos efectos, y, en consecuencia, los mismos daños en las personas. De esta manera, es distinto que una vulneración haga que la policía conozca las conexiones de un individuo con el uso de drogas, que esa misma información la conozca un familiar cercano.

prioridad para garantizar los derechos de las personas y su confianza en la economía digital (Wacks, 2015a: 131-138).[6] En pleno siglo XXI, la Cuarta Revolución Industrial[7] necesita de la confianza de los usuarios y, en ese contexto, la óptima seguridad en el manejo de datos personales es un requisito mínimo (Hartzog, 2018: 9, 97-98; Maqueo Ramírez, Moreno González y Recio Gayo, 2017: 94; OCDE, 2019: 5-6; Smedinghoff, 2007: 3-4; UNCTAD, 2019: 28).

El establecimiento de medidas de seguridad implica recursos, modificaciones organizacionales, controles y conocimiento técnico; por lo mismo, la generación de políticas públicas, estándares y normas obligatorias juega un rol fundamental (Schneier, 2015: 225-229).[8] En este último aspecto, se han ido generando obligaciones en el tratamiento de datos personales que exigen a los responsables la aplicación de medidas desde una mirada de gestión de riesgos (GT29, 2018: 5-6; Lehuedé, 2019: 10; Smedinghoff, 2007: 33-37).[9]

No obstante la claridad existente, la aplicación de medidas adecuadas de seguridad no parece ser una práctica consolidada en Chile, al menos, cuando ésta se

6. El desarrollo tecnológico y la masificación con que la industria y los Estados utilizan datos personales no solo ha significado la exposición a un riesgo mayor en cuanto a la amenaza que problemas de seguridad pueden conllevar a los derechos de las personas, sino que ha dejado en evidencia que el derecho muchas veces se encuentra en una posición inadecuada para abordar los desafíos jurídicos que tal desarrollo propone (Wacks, 2015a: 131-132).

7. La Cuarta Revolución Industrial —también llamada economía 4.0 o industria 4.0— corresponde a un cambio en el modelo social, político, cultural y económico actual vinculado fundamentalmente al uso de tecnologías y el procesamiento masivo de datos, y que se asocia a la mezcla de elementos físicos, biológicos y digitales (como, en inteligencia artificial, drones, vehículos autónomos, nanotecnología, computación en la nube, etcétera). De acuerdo con lo que señala el World Economic Forum, estamos en el inicio de la Cuarta Revolución Industrial, la cual constituirá un cambio en la forma en que vivimos, trabajamos y nos relacionamos. Véase Nicholas Davis, «What is the fourth industrial revolution?», World Economic Forum, 16 de enero 2016, disponible en https://bit.ly/3dR20W3; Klaus Schawab, «The Fourth Industrial Revolution: What it means, how to respond», World Economic Forum, 14 de enero 2016, disponible en https://bit.ly/2XNmZn6; y Alejandro Micco y Francisca Pérez, «Cuarta Revolución Industrial: Más que amenaza un desafío», Facultad de Economía y Negocios Universidad de Chile, 20 de agosto 2019, disponible en https://bit.ly/37dp2UG.

8. La OCDE establece que, para mejorar la seguridad digital, es necesario que los reguladores consideren un amplio espectro de medidas, que puede incluir tanto regulación como autorregulación por parte de las industrias. En sus recomendaciones, considera generar instancias de dialogo *multi-stakeholders* y evitar soluciones similares para todos los escenarios, pues muchos de éstos pueden presentar riesgos diferentes (OCDE, 2019: 10-11).

9. No solo en la Unión Europea se ha avanzado en la generación de obligaciones legales de seguridad para el tratamiento de datos personales, sino que también en otras latitudes, como Estados Unidos. A nivel latinoamericano, la existencia de este tipo de obligaciones de seguridad se puede encontrar, por ejemplo, en Colombia, México y Uruguay (Lehuedé, 2019: 50).

revisa en comparación al resto del mundo.[10] De este modo, resulta relevante revisar el escenario regulatorio vigente en nuestro país respecto de las obligaciones de seguridad en el tratamiento de datos personales, así como examinar de forma crítica las disposiciones establecidas en el proyecto de ley que modifica la Ley 19.628 sobre Protección de la Vida Privada,[11] sobre todo si tenemos presente que contempla normas específicas de seguridad, y que su discusión a nivel doctrinario ha sido discreta hasta ahora.

Este trabajo contiene una primera sección introductoria relativa a la protección de datos personales en general y las obligaciones de seguridad en su tratamiento, en el que se revisa brevemente la base de este derecho desde un punto de vista de garantías fundamentales, y la relación que existe entre los conceptos señalados. Enseguida, se examinan algunos tópicos asociados con la ciberseguridad en el tratamiento de datos personales.

En la segunda parte, se revisa la normativa vigente en materia de obligaciones asociadas con la seguridad en el tratamiento de datos personales en Chile, en el que examinamos en detalle lo que a este respecto dispone la Ley 19.628[12] y cierta regulación específica del área de la salud, en especial en lo que concierne a ficha clínica y datos del genoma humano.[13]

La tercera parte del trabajo contiene una descripción y análisis de las obligaciones sobre seguridad en el tratamiento de datos personales que se contienen en el proyec-

10. El National Cyber Security Index de la e-Governance Academy Foundation califica a Chile, en su versión de febrero 2020, con nota 1 (sobre 7) en los indicadores número 5, sobre protección de servicios digitales; número 6, sobre protección de servicios esenciales; y número 8, sobre protección de datos personales (disponible en https://bit.ly/2YePSHQ). Véase además Mariana Marusic, «Gasto de firmas chilenas en ciberseguridad subió 6% en 2018, pero aún está debajo del mundo», *La Tercera*, 4 de agosto de 2019, disponible en https://bit.ly/2YhpoqB. Por último, también es ilustrativo el disminuido desempeño que tuvo Chile en la versión 2019 del ranking de UNCTAD que, entre otras cosas, evalúa el acceso a servidores seguros de internet (disponible en https://bit.ly/2YgmMb2).

11. Su tramitación legislativa está en el sitio web de la Cámara de Diputados, disponible en https://bit.ly/2ZetMaE.

12. Bajo la Ley 19.628, los datos personales corresponden a «los relativos a cualquier información concerniente a personas naturales, identificadas o identificables».

13. Se ha elegido esta regulación en particular fundamentalmente por dos razones. En primer lugar, esta regulación atañe al ámbito de los datos personales sensibles que, como veremos, constituyen un tipo de dato personal que por sus características requiere de mayor resguardo, el que también alcanza a las medidas y obligaciones de seguridad asociadas en su tratamiento. En segundo lugar, hemos elegido esta norma porque constituye, dentro del actual ordenamiento jurídico nacional, una de las más prolíficas en cuanto a reglamentar obligaciones de seguridad que deben adoptar los responsables de datos.

to de ley que modifica la actual Ley 19.628, Boletines 11.144[14] y 11.092,[15] refundidos, y correspondientes a la moción de los senadores Harboe, Araya, De Urresti, Espina y Larraín, y el mensaje de la expresidenta de la República Michelle Bachelet.

El trabajo termina con una sección de conclusiones de la investigación, que tienen como objetivo contribuir al debate jurídico vinculado con las obligaciones de seguridad en el tratamiento de datos personales en Chile y, en menor medida, en la región.[16]

El derecho a la protección de datos personales como garantía fundamental y la seguridad en su tratamiento

La relación entre el derecho a la protección de datos personales y la obligación de seguridad en el tratamiento de éstos implica considerar el enfoque que, a nivel de garantías fundamentales, existe de estos conceptos.[17] Sin el ánimo de ser exhaustivos, a continuación se revisa en forma somera esa consagración.

El derecho a la vida privada[18] —de donde se ha originado históricamente el derecho a la protección de datos personales— se reconoce en múltiples instrumentos internacionales de derechos humanos, como la Declaración Universal de los Dere-

14. Denominado «Proyecto de ley, iniciado en mensaje de la S.E. la Presidenta de la República, que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales», ingresado al Congreso Nacional el 15 de marzo de 2017.

15. Denominado «Proyecto de ley, iniciado en moción de los honorables senadores señores Harboe, Araya, De Urresti, Espina y Larraín, sobre protección de datos personales», ingresado al Congreso Nacional el 17 de enero de 2017.

16. El desarrollo doctrinario y jurisprudencial en Chile respecto de la intersección existente entre derecho y tecnologías, y sus variables, como ciberseguridad, datos personales, ciberespacio, privacidad, y otros, es limitado, y así lo hemos advertido al preparar este trabajo. En esta línea, véase Álvarez Valenzuela (2017).

17. La asociación entre seguridad y datos personales también es comúnmente referida a la tensión generada entre la protección a los derechos a la privacidad o vida privada de los individuos, y el concepto de seguridad nacional a través de, por ejemplo, mecanismos de vigilancia masiva de individuos. La seguridad nacional, en esos casos, constituye muchas veces un elemento moderador o limitante de la protección otorgada por los derechos vinculados a la privacidad en aras del bien común. En la misma línea, Álvarez Valenzuela (2019: 255) señala que la seguridad pública cumple una función normativa de límite externo al derecho a la vida privada y al derecho a la inviolabilidad de las comunicaciones privadas. Sobre esto, véase también Ramírez (2016).

18. Para efectos prácticos de este trabajo, tomaremos el vocablo *privacidad* en términos equivalentes a *vida privada*, sin perjuicio de que ambos constituyen derechos doctrinaria y jurisprudencialmente diferentes. Cabe señalar que, a nivel de tribunales internacionales, se ha entendido al derecho a la vida privada como un derecho que excede en amplitud al derecho a la privacidad (Maqueo Ramírez, Moreno González y Recio Gayo, 2017: 79). Para una revisión del derecho a vida privada en la doctrina, véase Novoa (1979), Barros Bourie (1998), Corral Talciani (2000) o Tapia (2008).

chos Humanos de las Naciones Unidas (Maqueo Ramírez, Moreno González y Recio Gayo, 2017: 80-82; Schneier, 2015: 273). Este instrumento señala: «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación.[19] Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».[20]

Por su parte, existen múltiples dimensiones en el concepto de seguridad, incluyendo seguridad nacional, seguridad ciudadana, seguridad pública, y la que se vincula para este trabajo con datos personales, la seguridad humana (Álvarez Valenzuela, 2019: 254; Álvarez Valenzuela y Vera Hott, 2017: 42).[21] El derecho a la seguridad del ser humano también tiene fundamento en la Declaración, al establecer que «todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona».

A nivel regional, la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica) sigue la misma línea, al establecer en su artículo 7 el derecho a la seguridad personal, y en su artículo 11 la protección a la vida privada.[22] Lo mismo ocurre en Europa, donde el Convenio Europeo de Derechos Humanos[23] establece garantías asociadas a la vida privada y la seguridad de los individuos (artículos 8 y 5, respectivamente). Sin embargo, a diferencia de los demás instrumentos, en Europa la protección de datos personales se garantiza de manera autónoma y expresa en la Carta de los Derechos Fundamentales de la Unión Europea,[24] lo cual es reforzado en

19. A esta protección se le suma la consagración de los principios de universalidad e indivisibilidad de los derechos humanos (preámbulo y artículos 1 y 2 de la Declaración), lo que ha sido ratificado por la declaración del 29 de junio de 2012 de la Asamblea General de Naciones Unidas sobre la promoción, protección y disfrute de los derechos humanos en internet, y la de 21 de enero de 2014 sobre el derecho a la privacidad en la era digital (Álvarez Valenzuela y Vera Hott, 2017: 50). La Declaración fue proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948 en su Resolución 217 A (III).

20. En el mismo sentido el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de diciembre de 1966, y el artículo 16 de la Convención sobre los Derechos del Niño de 1989. Véase también Shahrul Mizan Ismail, «Data protection as a crucial human right», *New Straits Times*, 29 de mayo de 2018, disponible en https://bit.ly/2BUlooJ.

21. La seguridad humana se define como la libertad de las personas del miedo, de la necesidad o de la miseria, y la libertad para vivir con dignidad (Álvarez Valenzuela y Vera Hott, 2017: 42).

22. La Convención Americana sobre Derechos Humanos fue aprobada en Chile por el Decreto 873 de 1991 del Ministerio de Relaciones Exteriores. Texto disponible en https://bit.ly/2Yiiu35.

23. «Convención Europea de los Derechos Humanos (versión simplificada)», Consejo de Europa, disponible en https://bit.ly/3haL4fe. Algunos elementos sobre la concepción europea del derecho a la privacidad se pueden encontrar en «Data protection», Supervisor Europeo de Protección de Datos, disponible en https://bit.ly/3onBocZ.

24. A partir del Tratado de Lisboa del año 2009, la Carta de los Derechos Fundamentales de la Unión Europea tiene rango de tratado constitucional, por lo que es obligatoria para los Estados miembros de la Unión. Por otra parte, el Tratado de Funcionamiento de la Unión Europea también se refiere a datos personales, al establecer que «toda persona tiene derecho a la protección de los datos de carácter perso-

el Reglamento General de Protección de Datos Personales (RGPD) de la Unión Europea (Maqueo Ramírez, Moreno González y Recio Gayo, 2017: 81).[25]

Con estos derechos a nivel de garantías fundamentales es posible sentar, a nuestro juicio, las bases de una cierta relación entre los conceptos de protección de datos personales y obligaciones asociadas a la seguridad en su tratamiento, la cual ha sido reconocida alrededor del mundo, y que tiene como eje que los datos personales deben ser tratados sobre la base de principios, y de manera adecuada y segura, so pena de constituir una fuente de riesgos para los derechos de los individuos, como el derecho a la vida privada, la igualdad y la no discriminación (Bachelet, 2019; Maqueo Ramírez, Moreno González y Recio Gayo, 2017: 92-93).[26]

Este vínculo se puede apreciar concretamente en el considerando 85 del RGPD, en el que se advierte que la seguridad en el tratamiento de datos personales constituye un prerrequisito para el ejercicio y goce de diversos derechos. Este considerando establece:

> Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión.

En Chile, los derechos establecidos en la Declaración y los demás tratados sobre derechos humanos suscritos y ratificados por Chile son reconocidos en la Constitu-

---

nal que le conciernan» (Contreras Vásquez y Trigo Kramcsák, 2019: 77).

25. Reglamento (UE) 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. Entre otros objetivos, desde hace varios años la Unión Europea ha estado impulsando medidas enfocadas en la protección de la seguridad de los datos personales que son tratados. La Directiva 95/46/CE fue uno de los primeros impulsos relevantes y, según han señalado los autores, causó controversia en cuanto a las medidas establecidas, sobre todo en lo referente a la transmisión de datos personales a países sin leyes de protección adecuadas. Este impulso regulatorio fue considerado por Estados Unidos como un entorpecimiento al crecimiento y desarrollo del comercio electrónico, cuyo principal recurso es el flujo de información y datos personales (Hamelink, 2015: 193).

26. El objetivo de esta apreciación es sentar las bases y dejar un planteamiento general de que, a nuestro juicio, existe una relación esencial entre garantías fundamentales asociadas a la protección de la vida privada y la garantía de seguridad individual de las personas, lo cual ha generado cierto impacto e influencia en la posterior generación de obligaciones legales de seguridad en el tratamiento de datos personales a nivel de legislaciones locales. Sin perjuicio de esto, el ejercicio de examen detallado de este planteamiento excede ampliamente el objetivo y límites de este trabajo y, por lo tanto, ha sido dejado para una investigación posterior.

ción y constituyen una limitación al ejercicio de la soberanía.[27] En lo que se refiere a la vida privada y datos personales propiamente tal, la Constitución garantiza los derechos a la vida privada, a la protección de datos personales, a la inviolabilidad del hogar, a la inviolabilidad de las comunicaciones privadas, y a la inviolabilidad de los documentos privados, los cuales, en conjunto con las normas establecidas en los tratados suscritos y ratificados por Chile, forman el sistema constitucional de protección a la privacidad (Álvarez Valenzuela, 2019: 252).[28] En cuanto a seguridad, la Constitución asegura «el derecho a la libertad personal y a la seguridad individual».

El derecho a la protección de datos personales fue reconocido recientemente en la Constitución,[29] al pasar el numeral 4 del artículo 19 de la Constitución a asegurar 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». Añadiendo sobre este último que «el tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley».[30]

A partir de esto, y sin perjuicio de que consideramos que la elaboración de un estándar de seguridad de datos personales podría eventualmente ser construido a partir del sistema constitucional de protección a la privacidad que señala Álvarez Valenzuela,[31] y el derecho a la seguridad individual, el establecimiento particular de

27. El artículo 5 de la Constitución establece: «La soberanía reside esencialmente en la Nación. Su ejercicio se realiza por el pueblo a través del plebiscito y de elecciones periódicas y, también, por las autoridades que esta Constitución establece. Ningún sector del pueblo ni individuo alguno puede atribuirse su ejercicio. El ejercicio de la soberanía reconoce como limitación el respeto a los derechos esenciales que emanan de la naturaleza humana. Es deber de los órganos del Estado respetar y promover tales derechos, garantizados por esta Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes».

28. A juicio de Álvarez Valenzuela (2019: 252), este sistema constitucional de protección a la privacidad es multipropósito, pues sirve de mandato constitucional para el legislador al momento de desarrollar normas a nivel legal sobre estos derechos; un mandato para el juez al interpretar y aplicar los derechos; y mandato para las autoridades en el desempeño de sus funciones.

29. A través de la Ley 21.096, que Consagra el Derecho a la Protección de los Datos Personales, del 16 de junio del año 2018, artículo único.

30. Raúl Arrieta Cortés, «El nuevo entorno regulatorio de la protección de datos personales en Chile», IAPP Privacy Tracker, 4 de septiembre de 2019, disponible en https://bit.ly/2AWmGNX. No obstante, con anterioridad a ella los autores y la jurisprudencia estaban contestes en que el derecho a la protección de datos personales derivaba de la garantía consagrada en el artículos 19 número 4 de la Constitución, relativa a la protección a la vida privada de la persona (Anguita, 2007: 289; Cerda, 2012: 13). Misma interpretación ha sido construida en instancias judiciales de tribunales internacionales de derechos humanos, al interpretar la amplitud del derecho a la vida privada (Maqueo Ramírez, Moreno González y Recio Gayo, 2017: 87-88). Para una revisión en Chile de este tema, véase también Quezada (2012).

31. La revisión de este estándar de seguridad de rango constitucional para el tratamiento de datos personales excede el ámbito de este trabajo, a pesar de que un examen de este tipo sería útil a la hora de generar mecanismos para interpretar las futuras normas legales y reglamentarias vinculadas con este tema.

obligaciones de seguridad asociadas al tratamiento de datos personales es remitido por la Constitución a disposiciones de rango legal, según explicaremos más adelante.

Ciberseguridad en el tratamiento de datos personales

La relación de seguridad en el tratamiento de datos personales no se circunscribe solo al ámbito análogo, sino que también al tratamiento que ocurre en el contexto digital o del ciberespacio.[32]

La relación entre ciberespacio y seguridad suele entenderse bajo el concepto de *ciberseguridad*.[33] Un enfoque de derechos humanos en el ciberespacio permea el concepto de ciberseguridad, lo cual redunda en la forma en que se debe hacer tratamiento de datos personales en el contexto de ciberespacio (Álvarez Valenzuela y Vera Hott, 2017: 61).

Los autores ya se han referido a los derechos en el ciberespacio, y han puesto el foco en que, dadas las particularidades de este escenario, éstos se ven puestos en tensión, entre otras cosas, con el aumento de la globalización, la masificación de internet y la vigilancia ejecutada a través de éste (Hamelink, 2015: 191; Schneier, 2015: 165, 168; Wacks, 2015b: 13-14, 18-24).[34]

Bajo esta perspectiva, se ha construido una conexión entre este «espacio» y los derechos de privacidad, la protección de datos personales,[35] libertad de expresión, in-

32. Esta relación entre ciberseguridad y privacidad o datos personales se puede visualizar, entre otras cosas, en que para ambos campos existen riesgos y efectos perniciosos que derivan de un mismo hecho: una brecha de seguridad que afecta datos personales (*data breach*). NIST, «NIST Privacy Network», 6.

33. En la práctica, este no es un concepto cuyo significado sea unívoco entre los autores. En el ordenamiento jurídico nacional, existe una definición de ciberseguridad en el Decreto Supremo 533 de 2015 del Ministerio del Interior y Seguridad Pública, que Crea el Comité Interministerial sobre Ciberseguridad. Bajo el Decreto 579 de 2020, que modificó el Decreto 533, el término *ciberseguridad* se entiende como «aquella condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, como también el conjunto de políticas y técnicas destinadas a lograr dicha condición». Esta definición es similar a la que propone la Política Nacional de Ciberseguridad. Por su parte, se ha señalado que la ciberseguridad es un fenómeno complejo y multifactorial que involucra tanto la seguridad de las redes estatales, privadas, infraestructura crítica, prevención de delitos, educación, buenas prácticas, alianzas y relaciones internacionales, entre otros elementos (Álvarez Valenzuela y Vera Hott, 2017: 54).

34. En este sentido, la inexistencia de seguridad en el tratamiento de datos personales a través del ciberespacio es potencialmente una afección al derecho humano a la privacidad. Hamelink (2015: 153) ha observado que un enfoque en derechos humanos relativos a la privacidad y a la seguridad genera tensión vinculada con la masificación de tecnologías digitales y del ciberespacio, donde se crean nuevas formas de vulnerabilidad social que podemos visualizar con lo que actualmente ocurre con los datos personales.

35. El vínculo entre seguridad en ambientes digitales y protección de datos personales da cuenta de la necesaria relación del derecho humano a la privacidad y el ciberespacio (Álvarez Valenzuela, 2018: 29-30).

formación, seguridad y libertad personal, y no discriminación,[36] lo cual es coherente con la dependencia existente en sistemas digitales para operar cada aspecto de la vida moderna y que ha hecho que la seguridad en el tratamiento de datos en el ciberespacio sea un tópico de gran relevancia actual (Álvarez Valenzuela y Vera Hott, 2017: 50-51; Bachelet, 2019; Granados Paredes, 2006: 3; Kuner y otros, 2017: 73).

Esta relación ha resultado en que uno de los principios fundamentales del tratamiento de datos personales sea precisamente el de seguridad, el que ha sido reconocido en la mayoría de los sistemas y regímenes regulatorios de datos personales alrededor del mundo,[37] incluyendo los principios para el tratamiento de datos personales de la OCDE (OCDE Privacy Framework),[38] la Directiva 95/46/CE[39] y el RGPD, ambos de la Unión Europea, y en las guías de privacidad del Foro de Cooperación

36. En esta línea, la Política Nacional de Ciberseguridad establece como uno de los objetivos al año 2022 «el respeto y promoción de derechos fundamentales», especificando que «todas las medidas propuestas por la Política se deben diseñar y ejecutar con un enfoque de derechos fundamentales, atendiendo su carácter universal e indivisible y sobre la base de que el ciberespacio es un ambiente donde las personas cuentan con los mismos derechos que en el mundo físico». La Política Nacional tomó como antecedente la resolución A/HRC/20/L.13 del Consejo de Derechos Humanos de las Naciones Unidas sobre Promoción, Protección y Disfrute de los Derechos Humanos en Internet, que declaró sobre este tema que «los derechos de las personas también deben estar protegidos en internet». Para más antecedentes sobre los derechos humanos en el ciberespacio desde una óptica nacional, véase José Pablo Lapostol, «DDHH en la primera línea de internet», Derechos Digitales, 13 de junio de 2018, disponible en https://bit.ly/3f9juNH.

37. Se reconocen hoy en día como los sistemas o regímenes regulatorios relevantes sobre datos personales alrededor del mundo el RGPD; las leyes sobre datos personales de Estados Unidos a nivel federal, como la Ley de Modernización de Servicios Financieros (GLBA), la Ley Federal de Seguridad de la Información (FISMA) y la Ley de Transferencia y Responsabilidad de Seguro Médico (HIPAA); el OCDE Privacy Framework; y el APEC Privacy Framework (Lehuedé, 2019: 11-17).

38. El principio de seguridad que establece el OCDE Privacy Framework de 1980, señala que los datos personales deben ser protegidos por mecanismos de seguridad razonables contra riesgos como pérdida o acceso no autorizado, destrucción, uso, modificación o revelación de los datos (OCDE, 2013: 15; Wacks, 2015b: 104). Por su parte, en su revisión del año 2013 se introdujeron nuevos elementos, entre ellos un acápite específico sobre notificaciones de brechas de seguridad de datos (OCDE, 2013: 26).

39. La Directiva 95/46/CE se denomina «Directiva 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» y fue emitida el año 1995 por el Parlamento Europeo y el Consejo de la Unión Europea, que entró en vigor en octubre del año 1998. La Directiva regulaba en su artículo 17 la seguridad en el tratamiento de datos al indicar que «los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse».

Económica de Asia Pacífico (APEC Privacy Framework)[40] (Kuner y otros, 2017: 73-74; Lehuedé, 2019: 12-19; Smedinghoff, 2007: 13-14; Wacks, 2015b: 110-111).

Finalmente, esta relación no solo ha quedado en el ámbito de los principios, sino que también ha derivado en verdaderas obligaciones de nivel legal para los responsables y mandatarios o encargados[41] de datos personales que, en varias legislaciones,[42] deben implementar medidas de seguridad acordes con el estado del arte y el nivel de riesgos asociados al tratamiento; y a reportar, tanto a autoridades como a titulares de datos, vulneraciones sufridas a las medidas de seguridad. Esta clase de obligaciones se puede observar, por ejemplo, en el RGPD y en normativa estadounidense federal y estatal (Hartzog, 2018: 155-156; Laube y Böhme, 2016: 30; Smedinghoff, 2007: 5, 9-10).[43]

Tratamiento de datos personales en Chile y obligaciones de seguridad asociadas

Sin perjuicio del sistema constitucional de protección de la privacidad y, en particular, la garantía constitucional de protección a los datos personales que establece recientemente la Constitución, el tratamiento de datos personales y las obligaciones de seguridad asociadas a ellos se regulan en Chile a nivel legal, principalmente bajo la Ley 19.628 y la Ley 20.575, que Establece el Principio de Finalidad en el Tratamiento de Datos Personales.[44]

40. El APEC Privacy Framework constituye un conjunto de principios aplicables al tratamiento de datos personales que buscan promover el flujo de información entre los distintos países que componen la APEC. Para un análisis comparativo las normas establecidas en este instrumento, véase Álex Wall, «GDPR matchup: The APEC Privacy Framework and cross-border privacy rules», IAPP Privacy Tracker, disponible en 31 de mayo de 2017, disponible en https://bit.ly/3fq7tDz.

41. Para efectos prácticos de este trabajo y evitar confusiones, utilizaremos de forma indistinta los vocablos *mandatario*, *encargado*, *delegado* o *procesador* para todos aquellos casos en que nos refiramos a una situación en que una entidad o sujeto hace el tratamiento de datos personales en nombre y lugar de un responsable. Sin perjuicio de esto —y siguiendo la nomenclatura usualmente utilizada en Chile—, hemos privilegiado el uso del vocablo *mandatario* a lo largo del trabajo.

42. El reconocimiento de esto a nivel internacional ha sido recogido por instituciones vinculadas con la ciberseguridad, como el National Cyber Security Index de la e-Governance Academy Foundation que, entre los parámetros utilizados, considera precisamente la normativa nacional sobre protección de datos personales. El índice tiene por objetivo medir el nivel de preparación de los países para prevenir amenazas a la ciberseguridad y la gestión de incidentes cibernéticos.

43. Por ejemplo, en la reciente Ley de Privacidad de los Consumidores de California (CCPA) del estado de California en Estados Unidos, que entró en vigor el 1 de enero del 2020.

44. También conocida como Ley Dicom, busca regular el tratamiento de datos de carácter económico, financiero, bancario o comercial por parte de distribuidores de esa clase de información o burós de crédito, al establecer en su artículo 1 que solo podrán hacerlo respetando el principio de finalidad que será «exclusivamente para la evaluación de riesgo comercial y para el proceso de crédito».

En ámbito sectorial, también encontramos normas relativas a datos personales y obligaciones de su seguridad, las que están dirigidas principalmente a la reserva de los datos objeto del tratamiento. Aquí encontramos la Ley 20.584, que «Regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud» y su Decreto 41 del Ministerio de Salud del año 2012, que aprueba el reglamento de fichas clínicas; la Ley 20.120, «Sobre la investigación científica en el ser humano, su genoma, y prohíbe la clonación humana en materia de datos de salud»; la Ley 19.799, «Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma», relacionada con la confidencialidad de la información de los titulares de firmas electrónicas; el artículo 154 bis del Código del Trabajo en relación con la información del trabajador; disposiciones de la Ley 18.290, que «Fija el texto refundido, coordinado y sistematizado de la ley del tránsito», asociadas a la a reserva de información del conductor; y la Ley 19.223, que Tipifica Figuras Penales Relativas a la Informática (Lehuedé, 2019: 39-40; Pavlovic Jeldres, 2016).

A nivel de derecho público y normativa para los organismos del Estado, podemos destacar la Ley 21.180 sobre Transformación Digital del Estado, y el Decreto Supremo 83 del Ministerio Secretaría General de la Presidencia del año 2005, que «Aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos».[45]

En cuanto a regulación financiera en específico encontramos, fundamentalmente, los Capítulos 20-7[46] y 20-8[47] de la Recopilación Actualizada de Normas (RAN)[48] de la Superintendencia de Bancos e Instituciones Financieras (actual Comisión para el

45. Aquí podemos agregar el Decreto Supremo 1 del Ministerio de Justicia del año 2015, que aprueba norma técnica sobre sistemas y sitios web de los órganos de la administración del Estado; y el Decreto Supremo 779 del Ministerio de Justicia del año 2000, que aprueba el reglamento del registro de bancos de datos personales a cargo de organismos públicos, y que contiene normas sobre el tratamiento de datos realizado por aquellas entidades.

46. Capítulo 20-7 sobre externalización de servicios y que fue modificado en diciembre del año 2019, que flexibiliza la exigencia sobre la mantención de un sitio de procesamiento de datos en Chile para los servicios que se externalizan en el extranjero y que afectan actividades críticas o estratégicas.

47. Capítulo 20-8 sobre información de incidentes operacionales. Para una revisión de las modificaciones que sufrió este capítulo en el año 2018, véase Paulina Silva y Carlo Benussi «Modificaciones a la regulación sobre ciberseguridad en la industria financiera», *Hipervínculos*, 24 de septiembre de 2018, disponible en https://bit.ly/30sCdQ9.

48. En noviembre de 2019, la Comisión para el Mercado Financiero (CMF) publicó en consulta una propuesta para la dictación de un nuevo Capítulo 20-10 sobre gestión de seguridad de la información y ciberseguridad. El periodo de consulta se mantuvo abierto hasta el 27 de diciembre de 2019 y a la fecha de este artículo el nuevo capítulo todavía no entraba en vigor. Para más detalle de este proceso de consulta, véase «CMF publica en consulta la normativa para la Gestión de la Seguridad de la Información y Ciberseguridad», Comisión para el Mercado Financiero, 25 de noviembre de 2019, disponible en https://bit.ly/2Yo6lcK.

Mercado Financiero); el artículo 1 del DFL 707 del Ministerio de Justicia, que fija el texto refundido, coordinado y sistematizado de la ley sobre cuentas corrientes bancarias y cheques; y el artículo 154 del DFL 3 del Ministerio de Hacienda de 1997, que fija el texto refundido de la ley general de bancos y que regula el secreto bancario.[49]

Sin perjuicio de este conjunto de normas, las disposiciones sobre obligaciones de seguridad para los sistemas que tratan datos personales se presentan hasta ahora en Chile de forma limitada, inorgánica y poco sistemática, lo que dificulta su protección ante los riesgos del desarrollo tecnológico. Antecedentes que evidencian de mayor o menor manera estos problemas son la ausencia de obligaciones precisas y transversales relativas a la adopción de medidas de seguridad y al reporte de brechas; y las nuevas normas sobre seguridad que se incluyen en el proyecto que modifica la Ley 19.628 (Lehuedé, 2019: 39-41; Vergara Rojas, 2017: 136).[50]

Bajo este panorama, resulta necesario observar con mayor detalle el estado de las obligaciones sobre seguridad en el tratamiento de datos personales que existe en Chile. Para esto, abordamos a continuación la regulación que establece la Ley 19.628, la Ley 20.584 y su Decreto 41, y la Ley 20.120 en materia de datos de salud.[51]

La obligación de seguridad de datos personales en la Ley 19.628

La Ley 19.628 ha recibido múltiples críticas durante su vigencia, como la ausencia de un órgano administrativo que vele por su cumplimiento; la inexistencia de un procedimiento de reclamo eficiente; la ausencia de un catálogo apropiado de infrac-

49. Para un visión global de la regulación chilena sobre ciberseguridad financiera hasta fines del año 2018, véase José Pablo Lapostol y Paulina Silva «Aterrizaje forzoso: Una visión general de la regulación chilena sobre ciberseguridad financiera», *Hipervínculos*, 16 de noviembre de 2018, disponible en https://bit.ly/3f8DsYU.

50. Además, hay que considerar que nuestro país todavía no cuenta con una norma sobre ciberseguridad que regule el reporte de incidentes de forma transversal. Cabe destacar que tanto el avance de un proyecto de ley de ciberseguridad como el avance de una nueva ley de datos personales, constituyen objetivos establecidos en la Política Nacional de Ciberseguridad (PNCS) para el periodo que comprendía los años 2017 a 2018, los cuales, al año 2020, todavía están pendientes. Para una revisión del avance que tiene el desarrollo de la agenda digital del Gobierno de Chile, véase el sitio web http://www.agendadigital.gob.cl.

51. El ámbito de revisión de este trabajo se ha circunscrito a la normativa sectorial de salud, que se ha determinado relevante en relación con obligaciones de seguridad de datos personales. En efecto, excede del ámbito de este trabajo la revisión general de la normativa nacional existente sobre datos de salud, como la dispuesta en la Ley 19.970 que Crea el Sistema Nacional de Registros de ADN y su reglamento; el Decreto 634 del año 2008 del Ministerio de Justicia; el Oficio 602 de 2008 de la Fiscalía Nacional del Ministerio Publico, que establece criterios generales de actuación para la implementación del Sistema Nacional de Registros de ADN, de conformidad con la Ley 19.970; o aquella contenida en el DFL 1 del Ministerio de Salud, que fija el texto refundido, coordinado y sistematizado del Decreto Ley 2.763, de 1979 y de las Leyes 18.933 y 18.469; entre otros instrumentos.

ciones y sanciones; la falta de regulación para la transferencia internacional de datos personales; la pobre redacción de las excepciones al consentimiento; la falta de bases de legalidad para ciertos tratamiento de datos específicos; y, como ya enunciamos, la falta de obligaciones precisas y transversales relativas a medidas de seguridad (Anguita, 2007: 332-333; Jijena Leiva, 2002: 77-88; Lehuedé, 2019: 39-41; Muñoz Cordal, 2016: 35; Vergara Rojas, 2017: 136).[52]

En lo que a seguridad se refiere, la Ley 19.628 solo contempla en su artículo 11 una obligación general de seguridad de datos personales que le impone al responsable del banco de datos:[53] i) cuidar de ellos con la debida diligencia; y ii) hacerse responsable de los daños.[54] En efecto, señala expresamente esta norma que «el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños».[55]

De esta forma, se puede apreciar que la Ley 19.628 basa la obligación de seguridad en virtud del concepto de «debida diligencia» que, según lo ha entendido la doctrina, se construye a partir del estándar medio de conducta correspondiente al «buen padre de familia», lo que tiene como efecto que el responsable responda de la culpa leve en la aplicación de las medidas de seguridad sobre datos personales (Jijena Leiva, 2002: 86).[56]

---

52. Los autores han reparado también en que esta norma no contempla un registro público de bases de datos privadas; garantiza limitadamente el derecho de oposición del titular de datos personales; permite en exceso el tratamiento de datos por parte del Estado; y no contempla tipos penales específicos (Jijena Leiva, 2002: 76-77; Vergara Rojas, 2017: 136). Para una revisión de críticas adicionales al texto de esta ley, véase Raimundo, «Consulta experta sobre la Ley de Protección de la vida Privada de las Personales», Biblioteca del Congreso Nacional de Chile, asesoría técnica parlamentaria, octubre de 2018, disponible en https://bit.ly/3f8FuZ2.

53. De acuerdo con el artículo 2 de la Ley 19.628, el responsable del registro o banco de datos es «la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal».

54. El proyecto que dio origen a la Ley 19.628 (Boletín 896-07) establecía, en relación con la seguridad de datos, que el usuario deberá tomar las precauciones necesarias para preservar la seguridad de las informaciones contenidas en sus memorias informatizadas e impedir su deformación, daño o transmisión a terceros no autorizados (Anguita, 2007: 246).

55. La Ley 19.628 contempla también un deber de confidencialidad establecido en su artículo 7, que señala: «Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo».

56. El artículo 44 del Código Civil distingue tres especies de culpa o descuido: culpa grave, leve y levísima.

El Consejo para la Transparencia[57] ha interpretado esta norma entendiendo que este estándar medio se cumpliría estableciendo medidas de seguridad, técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información.[58]

Sin perjuicio de este criterio orientador, la verificación concreta de la suficiencia de las medidas implementadas por un responsable en el tratamiento de datos personales es una cuestión que requiere ser determinada caso a caso por los tribunales ordinarios de justicia en un procedimiento civil, quienes ven si en el caso particular el responsable actuó bajo el estándar medio de conducta del buen padre de familia (Cerda, 2012: 26).[59]

En efecto, ante el incumplimiento de esta obligación de cuidado del artículo 11, la única forma de reparación disponible para el titular de datos es la demanda de indemnización de perjuicios que consagra la norma de responsabilidad contenida en el artículo 23 de la Ley 19.628,[60] y en virtud del cual se puede buscar la reparación del daño moral y patrimonial sufrido mediante un procedimiento de juicio sumario que debe llevarse bajo las reglas generales de responsabilidad extracontractual del Código Civil (Corral Talciani, 2014: 55; Muñoz Cordal, 2016: 48, nota al pie).

Si bien la jurisprudencia nacional se ha referido en limitadas ocasiones al conte-

57. El Consejo para la Trasparencia es una corporación autónoma de derecho público cuya misión es velar por el cumplimiento de la Ley 20.285, sobre Acceso a la Información Pública. En materia de protección de datos personales, tiene como misión «velar por el adecuado cumplimiento de la Ley 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado».

58. Véase Acuerdo S/N; Sesión 278 del Consejo para la Transparencia del año 2011 «Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado».

59. En esta línea, el considerando decimosegundo de la sentencia en causa RIT T-60-2018 del Juzgado de Letras del Trabajo de Calama señaló: «Sin embargo, y pese a verificar la infracción a lo establecido en el artículo 11 de la referida Ley (Ley 19.628), no es posible hacer efectiva la responsabilidad del demandado en sede laboral, atendido a que es conocimiento de dichas infracciones la judicatura civil, quien es el llamado a determinar el estándar de cuidado o medidas concretas para velar por la seguridad de los datos y prevenir los daños provocados por dicha infracción».

60. Este artículo señala: «La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal. La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta Ley establece. La prueba se apreciará en conciencia por el juez. El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos».

nido de esta obligación de debida diligencia, hemos identificado dos casos relevantes en cuanto a su aplicación.

El primero de ellos ante el Decimosexto Juzgado Civil de Santiago el año 2015 (rol C-29221-2015), en el que se condenó a un reconocido banco de la plaza al pago de una indemnización por concepto de daño moral a tres clientes. Los hechos que derivaron en esta acción fueron el abandono en la vía pública de documentación que contenía datos personales,[61] lo que, a criterio del tribunal implicó una infracción a los artículos 6[62] y 11 de la Ley 19.628, y cuyo daño correspondía reparar conforme al artículo 23 de esa misma Ley.[63] Lo relevante de este caso es que se trata —muy probablemente— del primero en que un tribunal reconoció la existencia de daño moral de un titular de datos personales por infracción a los mencionados artículos, uno de los cuales corresponde precisamente a la obligación de seguridad que tiene que seguir un responsable en el tratamiento de datos.[64]

Un caso más reciente se encuentra en sede laboral por una acción por vulneración

61. En los documentos que fueron abandonados se encontraron copias de cédulas de identidad, estados de situación financiera, evaluaciones crediticias, liquidaciones de sueldo, cheques personales y de terceros, información sobre dineros en cuentas personales, entre otros. Carlo Benussi, «Indemnización de daño moral por tratamiento indebido de datos personales: Un caso reciente», *Hipervínculos,* 5 de mayo de 2017, disponible en https://bit.ly/3cRFMBS.

62. Este artículo establece una serie de obligaciones para el responsable, al señalar: «Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos. Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación. El responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad de requerimiento del titular».

63. En la determinación de la indemnización destaca el considerando decimosegundo de la sentencia, que señala: «Las partes demandantes vieron vulnerada su confianza depositada en [el demandado], quien no cuidó con la debida diligencia los datos personales y sensibles que de ellos obtuvo. Por eso, se inició una serie de actos que terminó con los datos de estas personas absolutamente expuestos y vulnerables ante terceros, y es dable concluir que por ello, según sus alegaciones y pruebas aportadas, esta situación les causó gran trastorno moral, preocupación e incluso angustia, durante el periodo de tiempo que duraron estas circunstancias e incluso después, por la sensación de inseguridad producida, por lo que se accederá a la demanda».

64. Benussi, «Indemnización…». Mismo criterio fue adoptado por el Quinto Juzgado Civil de Santiago (rol C-29221-2015) en un caso derivado de los mismos hechos en cuanto a establecer que existía una infracción a la obligación general de resguardar la seguridad de los datos personales por el abandono en la vía pública de documentos que contenían datos personales. En este caso, si bien se estableció la infracción, se rechazó la indemnización de perjuicios. La sentencia fue confirmada por la Corte de Apelaciones de Santiago con un voto minoritario del fiscal Norambuena (rol 11788-2017). Véase «Corte de Santiago confirma condena a Banco por infringir protección de datos de clientes», *Diario Constitucional,* 11 de junio de 2018, disponible en https://bit.ly/3fcioAQ.

de derechos fundamentales deducida ante el Juzgado de Letras del Trabajo de Calama el año 2018 (RIT T-60-2018), en el cual se declaró que Codelco vulneró el derecho a la intimidad del demandante.[65] Los hechos en que se basó la acción fueron la filtración de datos personales de un trabajador mediante la publicación en internet de una imagen de pantalla extraída del sistema SAP de la minera.[66] De acuerdo con el tribunal, la infracción al estándar del artículo 11 de la Ley 19.628 se generó a partir de las falencias de seguridad existentes en el sistema SAP[67] y en la deficiente investigación que llevó a cabo para determinar a los responsables de la filtración.[68]

Ahora bien, se han formulado una serie de críticas a la regulación que la Ley 19.628 dispone sobre obligaciones de seguridad en el tratamiento de datos personales estructurado sobre la base del estándar de debida diligencia, entre las que encontramos las señaladas a continuación (Anguita, 2007: 314, 342; Jijena Leiva, 2002: 76-77, nota al pie).

Primero, la ausencia de una obligación que requiera establecer medidas concretas y precisas de seguridad por parte del responsable, que atiendan a criterios mínimos como el estado de arte, los costos de implementar medidas, la naturaleza de los datos personales, el tipo de tratamiento o a los posibles riesgos que éste conlleva. El estándar actual supone una evaluación caso a caso por los tribunales, en la que los jueces no tienen parámetros específicos de control. En una sociedad en que los tratamientos de datos son cada día más complejos, es necesario entregar herramientas sobre las cuales los responsables, jueces y la eventual autoridad administrativa, puedan aterrizar el estándar requerido, de modo de aplicar y calificar correctamente la obligación de seguridad.[69]

65. El demandado de esta acción fue Codelco Chile División Chuquicamata.

66. La imagen filtrada fue subida a un blog denominado *Codelco corrupción* y contenía la cantidad de días de vacaciones pendientes del demandante.

67. Entre estas falencias, la sentencia señaló la carencia de trazabilidad de los perfiles que visualizan o consultan datos y antecedentes en la aplicación, así como la inadecuada asignación de perfiles que permitían el acceso de trabajadores a información privada (considerando decimosexto de la sentencia).

68. La sentencia ordenó al demandado adoptar las siguientes medidas para corregir su conducta: i) reestudiar los perfiles de acceso a información crítica y restringir accesos a consultas en las aplicaciones SAP, permitiendo establecer trazabilidad de quienes acceden a una aplicación determinada; y ii) que el área de seguridad informática haga una campaña de difusión que refuerce los controles de acceso y advierta a los usuarios del mal uso de la información y sus implicancias legales.

69. Estos parámetros disminuirían los riesgos derivados de que estas materias no sean resueltas por jueces especializados, pues es razonable pensar que construir el estándar de debida diligencia para un contexto de tratamiento de datos personales complejo es mucho más difícil que operar a partir de parámetros mínimos prefijados por la norma, como los riesgos asociados y el estado del arte. El fallo del 25 de octubre de 2019 de la Tercera Sala de la Corte Suprema (rol 12.793-2019), que ordena la entrega de información sobre todos los nombres de dominio .CL registrados en NIC Chile da cuenta que, en aspectos asociados a tecnologías, ciberseguridad y datos personales, el escenario de mayor justicia será aquel en

Segundo, la ausencia de obligaciones asociadas al reporte de vulneraciones que afecten medidas de seguridad a una autoridad o a los titulares de datos afectados, de forma que puedan tomar aquellos resguardos que permitan atenuar los efectos adversos derivados de la vulneración.

Tercero, la ausencia de la posibilidad de que los titulares exijan a los responsables la aplicación de medidas de seguridad específicas para garantizar la seguridad de los datos tratados.

Cuarto, la ausencia de obligaciones de seguridad particulares para el mandatario o encargado que trata los datos personales en lugar y nombre del responsable del banco de datos.[70]

Quinto, la ausencia de un principio de seguridad que inspire el tratamiento de los datos personales por los responsables del banco de datos y los mandatarios.

De esta forma, advertimos que la Ley 19.628 contiene múltiples vacíos a nivel de obligaciones de seguridad, lo que, sumado al sistema de cumplimiento o *enforcement* que implica recurrir a los tribunales para sancionar un incumplimiento al estándar de debida diligencia ha generado que, en la práctica, el establecimiento de medidas de seguridad adecuadas y robustas para el tratamiento de datos personales en Chile se configure como un acto cuasivoluntario cuya inobservancia no tiene consecuencias adversas, o las probabilidades de que ellas se materialicen son muy reducidas.

La precariedad de la Ley 19.628, tanto en obligaciones de seguridad como en otros aspectos sustantivos, es un tema que ya ha sido latamente discutido por la doctrina y se ha visto reflejado, entre otras cosas, en la gran cantidad de proyectos de ley presentes hoy en el Congreso Nacional que buscan reformarla y en las inquietudes manifestadas por la OCDE para que Chile mejore sus estándares en materia de protección de datos personales (Anguita, 2007: 342-348; Vergara Rojas, 2017: 135-136).[71]

Con todo, la obligación de seguridad revisada podría cambiar próximamente en virtud del contenido del proyecto que busca modificar la regulación actual de la Ley

---

que se le otorgue al juez mayores y mejores elementos para ponderar el cumplimiento normativo, pues, en ciertos casos, éste no va a estar especializado en la materia. Para más información de este fallo véase César Vega, «ONG rechaza fallo que obliga a entregar datos de dominios .CL y asegura que personas pueden negarse», *Biobío* Chile, 29 de noviembre de 2019, disponible en https://bit.ly/2YnzMx. Para el comunicado de NIC Chile sobre el tema, véase «Corte Suprema acoge recurso de queja y ordena a Universidad de Chile entrega de listado de todos los nombres de dominio .CL», NIC Chile, 27 de noviembre de 2019, disponible en https://bit.ly/3h7Wb8G.

70. Esto se ha traducido en que las obligaciones de seguridad aplicables actualmente para los mandatarios son solo aquéllas que le pueda imponer contractualmente el responsable de la base de datos de acuerdo con el artículo 8 de la Ley 19.628, y que dispone que en esos casos el mandato para el tratamiento deberá ser otorgado «dejando especial constancia de las condiciones de utilización de los datos».

71. Véase también Arrieta Cortés, «Nuevo entorno…». Respecto a este punto, véase lo señalado por la Fundación Datos Protegidos, disponible en https://bit.ly/2MLIgHx.

19.628 abordando en gran parte los vacíos señalados, y mejorando de manera sustancial el actual estándar de seguridad de los datos personales tratados en Chile.

Obligaciones de seguridad de datos personales en la regulación del área de la salud

Al analizar el panorama vigente en Chile respecto de las obligaciones de seguridad en el tratamiento de datos personales, resulta también ilustrativo revisar lo que ocurre respecto de la información personal de salud,[72] la cual, dado su carácter de dato sensible,[73] ha sido conferida —en ciertos casos— de una protección mayor en lo que a seguridad se refiere.

El tratamiento de datos de salud en Chile no está regulado por un cuerpo normativo único y específico, sino que está integrado por denso grupo de diversas normas cuyo eje no es solo el sector salud, ni tampoco la regulación de los datos de salud propiamente tal.

Bajo este escenario, además de la Ley 19.628 ya comentada, identificamos —sin ánimo de ser exhaustivos— las siguientes normas relativas a datos de salud: la Constitución; el Código Sanitario; la Ley 20.584 y el Decreto 41; la Ley 18.933, que «Crea la Superintendencia de Instituciones de Salud Previsional en relación al plan de salud»; la Ley 20.120 «Sobre la investigación científica en el ser humano, su genoma, y prohíbe la clonación humana»; la Ley 19.970 que Crea el Sistema Nacional de Registros de ADN y su reglamento; el Decreto 634 del año 2008 del Ministerio de Justicia; el Ofi-

72. El dato de salud no está definido en la Ley 19.628 ni tampoco en el proyecto. El RGPD, por su parte, entiende a los «datos relativos a la salud» como «datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud».

73. De acuerdo con la Ley 19.628, son datos sensibles «aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual». Señala la doctrina que todos los datos de salud deben entenderse como datos sensibles aun cuando no se refiere exclusivamente a estados de salud físicos o psíquicos, debido a que la definición de dato sensible no es taxativa y, por lo tanto, así podría ser calificada por un juez en cuanto el tratamiento de ella pueda afectar garantías fundamentales y conllevar decisiones arbitrarias. Esto aplicaría, por ejemplo, a información sobre el ADN, «que no revela estados de salud sino predisposiciones de una persona a ciertas afecciones» (Donoso Abarca, 2011: 85). Por su parte, cabe destacar que el artículo 10 de la Ley 19.628 establece las bases de legalidad aplicables para el tratamiento de datos personales sensibles, señalando que «no pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares». De esta forma, vemos que la regla general para esta clase de datos es la prohibición de tratamiento sin perjuicio de la aplicación de alguna de las causales habilitantes que contempla la norma.

cio 602 de 2008 de la Fiscalía Nacional del Ministerio Publico, que establece criterios generales de actuación para la implementación del Sistema Nacional de Registros de ADN, de conformidad con la Ley 19.970; y el DFL 1 del Ministerio de Salud, que fija el texto refundido, coordinado y sistematizado del Decreto Ley 2.763, de 1979 y de las Leyes 18.933 y 18.469 (Donoso Abarca, 2011: 82-83, 86; Eterovic Barreda, 2019: 48; Pavlovic Jeldres, 2016).

Sin perjuicio de este grupo de normas, para efectos de obligaciones de seguridad en el tratamiento de datos de salud es posible advertir que, dentro del ámbito de normas sectoriales en salud, las obligaciones más relevantes están contenidas en la Ley 20.584 y el Decreto 41, y en la Ley 20.120, a las cuales hemos circunscrito esta sección.

Ley 20.584 y el Decreto 41

Esta normativa se refiere a la llamada «ficha clínica»[74] e impone medidas de seguridad especiales para ella y los datos que contiene. En línea con las definiciones dispuestas por la Ley 19.628, la Ley 20.584 establece que cualquier información que surja de la ficha clínica será considerada dato sensible,[75] por lo que se entiende que las medidas de protección asociadas han sido generadas con el fin de impedir que los titulares de datos (pacientes en este caso) sufran diferenciaciones arbitrarias y discriminatorias de parte de terceros que accedan a ellos (Eterovic Barreda, 2019: 58; Muñoz Cordal, 2016: 34-35).

La Ley 20.584 permite que la ficha clínica pueda ser almacenada tanto en soporte físico como electrónico, estableciendo como condición que los registros sean com-

74. De acuerdo con la Ley 20.584, constituye la ficha clínica «el instrumento obligatorio en el que se registra el conjunto de antecedentes relativos a las diferentes áreas relacionadas con la salud de las personas, que tiene como finalidad la integración de la información necesaria en el proceso asistencial de cada paciente». Entre los datos que contiene la ficha clínica, se encuentra el nombre del paciente, número y tipo de documento de identificación, sexo, fecha de nacimiento, domicilio, correo electrónico, ocupación, registro de atenciones recibidas de salud, procedimientos de diagnósticos y terapéuticos, etcétera. Por otro lado, Eterovic Barreda define a la ficha clínica como el «documento escrito, sin importar su soporte, desarrollado obligatoriamente por el facultativo, que emana de la relación comunicacional médico-paciente, donde constan interpretaciones subjetivas del médico y el conjunto de análisis objetivo de exámenes, con el objeto de establecer, a lo largo de un proceso asistencial, los distintos estados de evolución del paciente, su ingreso, tratamiento, pronóstico y estado hasta el alta, garantizando el ejercicio de la autonomía del paciente a través de la toma de decisiones informadas, y el correcto ejercicio de la profesión» (Eterovic Barreda, 2019: 28).

75. Esto se encuentra establecido en el inciso final del artículo 12 de la Ley 20.584 que señala que «toda la información que surja, tanto de la ficha clínica como de los estudios y demás documentos donde se registren procedimientos y tratamientos a los que fueron sometidas las personas, será considerada como dato sensible, de conformidad con lo dispuesto en la letra g) del artículo 2 de la Ley 19.628».

pletos y se asegure el oportuno acceso, conservación y confidencialidad de los datos,[76] así como la autenticidad de su contenido y de los cambios efectuados en ella.[77] En relación con el tipo de soporte, los autores han entendido que se configuran desafíos de seguridad propios y específicos que requieren especiales medidas de protección, lo que, como veremos, constituye la aproximación que tomó el reglamento de esta ley (Sotomayor Saavedra y otros, 2014: 123).

Por su parte, esta normativa contiene una obligación de custodia y reserva, al establecer —a nivel de acceso— una regla transversal en cuanto a que terceros no relacionados directamente con la atención de salud no pueden tener acceso a la información de la ficha clínica, e indica específicamente quiénes y cuándo pueden acceder a ella, lo que Muñoz ha entendido como niveles de acceso *originarios* y *secundarios*.[78] Además, se establece un deber especial de reserva para aquellos que puedan tener acceso a la ficha clínica (Eterovic Barreda, 2019: 58; Muñoz Cordal, 2016: 54).

Sin perjuicio de lo anterior, cabe destacar que esta normativa no se queda solo con requisitos amplios asociados a la seguridad que se debe aplicar en el manejo de la ficha clínica o la información que contiene, sino que establece medidas concretas a este respecto que difieren del estándar general de seguridad que contempla la Ley 19.628.

En efecto, el artículo 8 del Decreto 41 ordena que las fichas clínicas deben «almacenarse en un archivo o repositorio que garantice que los registros son completos y asegure el acceso oportuno, la conservación y confidencialidad de los datos, así como la autenticidad de su contenido y de los cambios efectuados en ella». Establece luego que, respecto de las fichas en soporte electrónico, se deben contemplar medidas de respaldo, copias de seguridad, barreras de protección frente accesos no autorizados,

76. La confidencialidad de la información y datos de salud en específico tiene regulación diseminada en varios cuerpos normativos del área de la salud, entre los que se encuentran el Código Sanitario en sus artículos 101, 130, y 134; el Reglamento de Hospitales y Clínicas en relación con información bioestadística o clínica; y el Manual SOME relativo a las fichas (Donoso Abarca, 2011: 93; Muñoz Cordal, 2016: 50-51).

77. Esta aproximación es coherente con la tríada clásica de seguridad de la información en cuanto requiere la integridad, disponibilidad y confidencialidad de los datos contenidos en la ficha clínica.

78. Esta norma señala: «Los terceros que no estén directamente relacionados con la atención de salud de la persona no tendrán acceso a la información contenida en la respectiva ficha clínica. Ello incluye al personal de salud y administrativo del mismo prestador, no vinculado a la atención de la persona». Esta misma norma establece expresamente a quiénes se les puede otorgar acceso a la ficha clínica: «a) Al titular de la ficha clínica, a su representante legal o, en caso de fallecimiento del titular, a sus herederos; b) a un tercero debidamente autorizado por el titular, mediante poder simple otorgado ante notario; c) a los tribunales de justicia, siempre que la información contenida en la ficha clínica se relacione con las causas que estuvieren conociendo; d) a los fiscales del Ministerio Público y a los abogados, previa autorización del juez competente, cuando la información se vincule directamente con las investigaciones o defensas que tengan a su cargo; e) al Instituto de Salud Pública, en el ejercicio de sus facultades».

medidas de sustitución de información y medidas de continuidad de servicio.[79] Por su parte, en cuanto a las fichas en soporte papel, el mismo artículo ordena que se deberá contemplar tener archivos únicos y centralizados, mantención de carátulas, control de perdidas, medidas de orden secuencial, trazabilidad de solicitudes de acceso y registros de entradas y salidas (Eterovic Barreda, 2019: 76-78).[80]

Estas medidas destinadas a la seguridad de los datos incorporados en la ficha clínica se complementan con el título 3 del mismo reglamento, que se refiere a la administración, acceso y eliminación de la ficha clínica.[81] Señala la doctrina que la regulación de las fichas clínicas en papel sería mucho más «administrativa» que la establecida para las fichas dispuestas en formato electrónico, en las que la regla parece ser programática y «de principios» (Eterovic Barreda, 2019: 78).

En cuanto a la entidad encargada de dar cumplimiento a estas reglas de resguardo, ésta será aquel prestador institucional o individual[82] quien, al mismo tiempo, tendrá la calidad de responsable del banco de datos bajo la Ley 19.628. Ante un incumplimiento, los remedios legales que se podrán aplicar son las reglas del artículo 23 de la Ley 19.628 sobre tratamiento indebido, o aquellas a establecidas en el artículo 37 de la Ley 20.584, que faculta recurrir ante la Superintendencia de Salud o iniciar un procedimiento de mediación bajo la Ley 19.966,[83] lo cual sin duda genera mayores garantías que el régimen aplicable para los datos personales fuera del ámbito de la ficha clínica. Por su parte, a nivel constitucional, se podría aplicar la

79. El artículo 8 establece que, respecto de la ficha en soporte electrónico: «a) La información debe respaldarse en cada proceso de incorporación de los documentos; b) habrá una copia de seguridad en el lugar de operación de los sistemas de información y otra en un centro de almacenamiento de datos electrónicos que tenga un estricto control de acceso, registro de entrada y salida de respaldos; c) medidas de seguridad y barreras de protección frente a accesos no autorizados; d) sustitución de la información por la versión más reciente que se disponga, en el menor tiempo posible, en casos de alteración no programada; e) programas que permitan la restauración del servicio en el menor tiempo posible en los casos que deje de operar».

80. El artículo requiere sobre la ficha en soporte papel: «a) archivo único y centralizado con fichas ordenadas con características que permitan su ubicación expedita; b) mantención, conservación y reposición de carátulas en casos de deterioros; c) control de extravíos y omisiones de documentos; d) archivo ordenado con orden secuencial por números de fichas o letras; e) sistema de constancia de solicitudes de acceso a las fichas; f) registro de entrada y salida de las fichas con indicación del destinatario responsable y fechas de pedido y de devolución».

81. Este título 3 profundiza en los requisitos de manejo centralizado de las fichas y su seguridad. Destaca el establecimiento en su artículo 12 del procedimiento requerido para la eliminación de las fichas clínicas, el cual debe asegurar la confidencialidad de la información y la efectiva destrucción de la ficha.

82. De acuerdo con el artículo 3 de la Ley 20.584, el prestador de salud es «toda persona, natural o jurídica, pública o privada, cuya actividad sea el otorgamiento de atenciones de salud. Los prestadores son de dos categorías: institucionales e individuales».

83. Ley 19.966 que Establece un Régimen de Garantías en Salud del año 2004, cuyo procedimiento de mediación se encuentra regulado en sus artículos 43 y siguientes.

acción constitucional de protección regulada en la Constitución (Muñoz Cordal, 2016: 48-49).[84]

Como vemos, la relación existente entre la Ley 19.628 y las normas sobre datos de salud y la ficha clínica es estrecha y debe ser perfeccionada para permitir la adecuada seguridad de los datos incluidos en esta última.[85] De este modo, compartimos lo que señala Muñoz Cordal en cuanto a que, dada la interacción entre ambos estatutos, es necesario que la Ley 19.628 sea perfeccionada bajo estándares internacionales, pues «se corre el riesgo de que los déficits de dicha normativa impacten negativamente en el modo de comprender y aplicar las reglas sobre ficha clínica» (Muñoz Cordal, 2016: 56).[86]

Ley 20.120

Nos queda referirnos a la Ley 20.120, «Sobre la investigación científica en el ser humano, su genoma, y prohíbe la clonación humana». El artículo 13 de esta ley señala que la recopilación, almacenamiento, tratamiento y difusión del genoma de las personas se ajustará a las disposiciones de la Ley 19.628, y que los datos del genoma humano que permitan la identificación de una persona deberán ser encriptados para su almacenamiento y transmisión. Agrega que la encriptación podrá omitirse temporalmente por razones de utilidad pública.

El reglamento de esta Ley,[87] en su artículo 23, profundiza esta disposición incorporando que «la información genética de un ser humano será reservada, sin perjuicio

84. Ésta corresponde a la acción que la Constitución concede a las personas que, como consecuencia de actos u omisiones arbitrarias o ilegales, sufren privación, perturbación o amenaza en el legítimo ejercicio de los derechos y garantías señaladas en su artículo 20. Entre los derechos protegidos se encuentra precisamente la garantía de protección de datos personales que establece el numeral 4 del artículo 19 de la Constitución. El objetivo de esta acción es que se adopten las providencias necesarias para restablecer el imperio del derecho y asegurar la debida protección del afectado.

85. Donoso Abarca (2011: 90-92) señala que la aplicación del principio de seguridad en los datos de salud va asociada a los requerimientos de seguridad en el ámbito sanitario, los cuales son de nivel elevado. A su juicio, en lo que se refiere a datos personales, los sistemas de apoyo a la gestión del sector de la salud en Chile deben implementar medidas de seguridad del más alto nivel, sobre todo en la transferencia electrónica de datos. Como medidas específicas, se refiere a sistemas de acceso personalizado a datos personales, y medidas de aseguramiento de continuidad del servicio.

86. El proyecto contiene una nueva regulación en materia de datos de salud, sin perjuicio de que, en lo que se refiere a obligaciones de seguridad, les serán aplicables las nuevas normas generales de seguridad que revisamos más adelante en este trabajo. Para un análisis de la regulación de datos de salud en el proyecto, véase Michelle Bordachar, «Los datos de salud en el proyecto de ley de protección de datos personales», *El Mercurio Legal*, 4 de octubre de 2019, disponible en https://bit.ly/2BLbNib.

87. La Ley 20.120 tiene un reglamento que profundiza sus disposiciones y que corresponde al Decreto 114 del año 2013 del Ministerio de Salud.

de las facultades de los tribunales de justicia en los casos y en las formas establecidas en la ley».

La relevancia de establecer medidas de seguridad en el tratamiento de esta clase de datos obedece a sus características intrínsecas y potencial identificador. Se ha indicado que las muestras genéticas, aun cuando no estén asociadas a un sujeto, pueden ser cotejadas para identificar con facilidad a un individuo, lo que, bajo la Ley 19.628, las sitúan como datos de personales de carácter sensible por excelencia (Muñoz Cordal, 2016: 55).[88]

Por último, podemos apreciar que se incluye en forma expresa la medida de encriptación[89] de los datos del genoma humano como mecanismo para su adecuado almacenamiento y transmisión, lo cual difiere de la Ley 19.628 y de la Ley 20.584, que no hacen referencia expresa a su implementación. Esto es muy relevante y constituye un avance, pues el uso de encriptación garantiza las propiedades de confidencialidad e integridad de los datos elevando el estándar de protección asociado (Álvarez Valenzuela, 2019: 249).[90]

Las obligaciones de seguridad en el proyecto para el tratamiento de datos personales

Tras haber observado el panorama de obligaciones de seguridad vigentes para el tratamiento de datos personales bajo la Ley 19.628, y lo que la normativa sectorial de salud dispone para éstos cuando se trata de datos contenidos en la ficha clínica y el genoma humano, corresponde que revisemos lo que señala el texto del proyecto.

El proyecto se encuentra actualmente en tramitación legislativa en el Congreso Nacional, por lo que es relevante señalar que para este trabajo hemos utilizado la versión que contiene las disposiciones aprobadas por la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado hasta la sesión del 8 de enero de 2020. A la fecha de este trabajo, el proyecto se encontraba próximo a concluir su primer

88. El autor sostiene que, dado el hecho de que la información genética es sensible, es relevante la postura que se establezca frente a su protección, sobre todo cuando es muy probable que existan terceros que pudieran querer utilizar esta clase de información en beneficio propio (Muñoz 2016, 55).

89. De acuerdo con Granados Paredes (2006: 6), la encriptación puede definirse como la ciencia encargada de diseñar funciones o dispositivos capaces de transformar mensajes legibles a mensajes cifrados de tal manera que esta transformación (cifrar) y su transformación inversa (descifrar) solo pueda ser factible con el conocimiento de una o más llaves. Por su parte, Álvarez Valenzuela (2019: 243) explica el cifrado de comunicaciones señalando que corresponde a la «utilización de un algoritmo matemático que envuelve un mensaje de manera que solo el receptor legitimo pueda abrirlo y hacerse de su contenido, mediante la utilización de una llave o clave única que desenvuelve el mensaje».

90. La Política Nacional de Ciberseguridad reconoce el valor de las tecnologías de cifrado estableciendo que las medidas que se implementen basadas en ella deben promover la adopción de cifrado punto a punto para los usuarios en línea con los estándares internacionales (página 13).

trámite constitucional en la Comisión de Hacienda del Senado, para luego pasar a la Cámara de Diputados a su segundo trámite constitucional.

El proyecto contempla una modificación de la mayoría de las normas que existen en la Ley 19.628,[91] en conjunto con la incorporación de un gran número de nuevas disposiciones (Vergara Rojas, 2017: 137).[92] Dado que uno de los objetivos del proyecto es adecuar la normativa a estándares internacionales sobre protección en el tratamiento de datos personales, éste ha tomado muchos elementos del RGPD,[93] y las obligaciones sobre seguridad en el tratamiento de datos no han sido la excepción.[94]

Dentro del articulado del proyecto, las disposiciones sobre seguridad del tratamiento de datos personales las podemos agrupar bajo los siguientes ejes:

- Principio de seguridad.
- Obligación de adoptar medidas de seguridad.
- Obligación de reportar y registrar vulneraciones a las medidas de seguridad.

91. El proyecto busca una modificación transversal de la Ley 19.628 y del tratamiento de datos personales en Chile. Entre algunos de los nuevos elementos que considera encontramos: i) contempla nuevas bases de legalidad que establecen los casos que habilitan el tratamiento de datos personales incluyendo, por ejemplo, cuando los datos son necesarios para la celebración o ejecución de un contrato entre el titular y el responsable, el interés legítimo del responsable, o sean datos relativos a obligaciones de carácter comercial; ii) establece al Consejo para la Transparencia como la autoridad autónoma, cuyo objetivo será velar por el cumplimiento de la ley y con capacidad de imponer multas; iii) se regulan de manera explícita los principios del tratamiento de datos, incluidos los principios de finalidad, proporcionalidad y seguridad, entre otros; iv) se regula la transferencia internacional de datos personales; y v) se regula el tratamiento automatizado de grandes volúmenes de datos, entre otras materias (Arrieta Cortés, «Nuevo entorno…»; Vergara Rojas, 2017: 138-144). Para un análisis de las materias que contempla el proyecto, véase Guillermo Carey y Paulina Silva, «Se aprueba en general el proyecto de ley que modifica la Ley de protección de datos», *Hipervínculos*, 16 de abril de 2018, disponible en https://bit.ly/2Uu4QIS. Por otro lado, en relación con interés legítimo establecido en la regulación como base de licitud habilitante para el tratamiento de datos, véase Contreras Vásquez y Trigo Kramcsák (2019).

92. Bajo el proyecto, también hay algunas disposiciones de la Ley 19.628 que, hasta ahora, se mantienen sin modificación, como aquellas relativas a los datos personales sobre obligaciones de carácter económico, financiero, bancario o comercial.

93. El RGPD fue publicado en 2016 y entró en vigor en mayo de 2018, sustituyendo a la Directiva 95/46/CE. Un elemento relevante de este cambio es que son instrumentos normativos distintos. En el contexto de la regulación europea, un reglamento no trata de armonizar ordenamientos jurídicos estatales, sino que se busca imponer una norma única y aplicable de forma directa. En efecto, desde que entró en vigor el RGPD, la Unión Europea tiene una norma común en materia de datos personales. Por su parte, esta actualización de Directiva al RGPD ha sido señalada como un mecanismo para afrontar los desafíos que la proliferación del ciberespacio ha generado en los derechos de privacidad y seguridad de las personas (Aparicio Vaquero, 2016: 28; Wolters, 2017: 165;).

94. Arrieta Cortés, «Nuevo entorno…». El RGPD establece en sus artículos 32, 33 y 34 las obligaciones de seguridad referidas al responsable de datos y al mandatario.

- Obligaciones de seguridad para el mandatario en el tratamiento de datos personales.[95]
- Elementos adicionales vinculados con las obligaciones de seguridad.

Cabe señalar que estas disposiciones son comunes para las distintas categorías de datos personales que contempla el proyecto, incluyendo los datos personales relativos a la salud y al perfil biológico humano.[96] A su vez, el proyecto no establece obligaciones de seguridad específicas o especiales para el tratamiento de datos personales relativos a la salud; no obstante que, de su condición de sensibles se desprende que el resguardo que deberá tener el responsable en la aplicación de las obligaciones comunes deberá ser mayor.

A continuación, pasamos a revisar las disposiciones sobre seguridad de datos personales que establece el proyecto.

Un nuevo principio de seguridad

El proyecto regula una serie de principios[97] para el tratamiento de datos personales, entre los que se encuentra el nuevo principio de seguridad que se establece su artículo 3 letra f) de la siguiente manera:

> 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.

Si bien el artículo 3 señala que el tratamiento de datos se rige por los principios enumerados en sus literales, el artículo 14 del proyecto establece la obligación de cada

95. El Proyecto señala en su artículo 2 que el tercero mandatario o encargado corresponde a «la persona natural o jurídica que trate datos personales por cuenta del responsable de datos». Para que un responsable pueda hacer tratamiento de datos a través de un mandatario se requerirá, bajo el artículo 15 bis del proyecto, la celebración de un contrato entre ambas partes que establezca i) el objeto y la duración del encargo, ii) la finalidad del tratamiento, iii) el tipo de datos personales tratados, iv) las categorías de titulares a quienes conciernen los datos, y v) los derechos y obligaciones de las partes.

96. A consecuencia de esto es que no se ha considerado necesario, para este trabajo, la generación de un acápite separado sobre obligaciones de seguridad para el tratamiento de datos relativos a la salud bajo el proyecto.

97. Los principios del tratamiento de datos se han entendido —a lo largo de las legislaciones— como elementos estructurales sobre los que establecen normas específicas y detalladas para efectuar el tratamiento de datos (Cerda, 2012: 20). Entre los principios del tratamiento de datos que contempla el proyecto se encuentran el principio de licitud del tratamiento, de finalidad, de proporcionalidad, de calidad, de responsabilidad, de seguridad, de transparencia e información, y de confidencialidad.

responsable[98] de cumplir con ellos como verdaderas obligaciones:[99] «El responsable de datos, sin perjuicio de las demás disposiciones previstas en esta ley, tiene las siguientes obligaciones: […] e) Cumplir con los demás principios y obligaciones que rigen el tratamiento de los datos personales previstos en esta ley».

Si bien como técnica legislativa esto puede parecer poco prolijo, al menos es coherente con el nivel de detalle que contempla el principio de seguridad, ya que establece elementos que se deben considerar para alcanzar el nivel adecuado de seguridad, como el tipo de tratamiento y la naturaleza de los datos, así como los objetivos específicos al que ese estándar debe propender: evitar el tratamiento no autorizado o ilícito, la pérdida, filtración, daño accidental o destrucción de los datos.[100]

Es relevante señalar que este nuevo principio tiene directa relación con el cumplimiento de otros principios y obligaciones del responsable bajo el proyecto, hasta constituirse en una suerte de prerrequisito. En este sentido, se pueden advertir múltiples situaciones en que medidas de seguridad inadecuadas pueden implicar, por ejemplo, una transferencia internacional indebida a un país no permitido; el mantenimiento de bases de datos inexactas o con información incorrecta del titular; o el incumplimiento del principio de confidencialidad que supone guardar secreto sobre los datos personales (OCDE, 2013: 26-27; Room, 2018: 169).[101]

Por último, otra relación relevante es la existente entre el principio de seguridad y el de proporcionalidad (artículo 3 letra c del proyecto), que establece que los datos que se traten «se deben limitar a los que resulten necesarios en relación con los fines del tratamiento». Con la proliferación del ciberespacio, cada día son más los datos personales que se recolectan, lo que lleva a un incremento en los riesgos. De esta

98. El proyecto modifica el concepto de responsable del registro o banco de datos que contiene la Ley 19.628 por el de responsable de datos o responsable. El responsable de datos o responsable es, bajo el artículo 2 del proyecto, «toda persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento de datos personales, con independencia de si los datos son tratados directamente por ella o a través de un tercero mandatario o encargado».

99. Esto va en línea con el régimen sancionatorio que dispone el proyecto que, en su artículo 33, establece que «el responsable de datos, sea una persona natural o jurídica, de derecho público o privado, que en sus operaciones de tratamiento de datos personales infrinja los principios, derechos y obligaciones establecidos en esta ley, será sancionado de conformidad con las normas del presente título».

100. El RGPD contiene también un principio de seguridad muy parecido al que establece el proyecto en su artículo 5(1) letra f), que establece que los datos deben ser «tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ("integridad y confidencialidad")».

101. El proyecto establece el principio de confidencialidad en un sentido parecido a la Ley 19.628: «El responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad acerca de los mismos. El responsable establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste aun después de concluida la relación con el titular».

manera, vemos que el principio de proporcionalidad colabora con la seguridad de los datos personales limitando precisamente el volumen de datos tratados por el responsable y, al mismo tiempo, disminuyendo el nivel de riesgos de seguridad asociado (Hamelink, 2015: 194).[102]

El establecimiento de la obligación de adoptar medidas de seguridad

El artículo 14 quinquies del proyecto contempla la obligación de adoptar medidas de seguridad de la siguiente forma:

> El responsable de datos debe adoptar las medidas necesarias para resguardar el cumplimiento del principio de seguridad establecido en esta ley, considerando el estado actual de la técnica y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados. Las medidas aplicadas por el responsable deben asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos. Asimismo, deberán evitar la alteración, destrucción, pérdida, tratamiento o acceso no autorizado.
>
> Si las bases de datos que opera el responsable tienen distintos niveles de riesgo, deberá adoptar las medidas de seguridad que correspondan al nivel más alto.
>
> Ante la ocurrencia de un incidente de seguridad, y en caso de controversia judicial o administrativa, corresponderá al responsable acreditar la existencia y el funcionamiento de las medidas de seguridad adoptadas en base a los niveles de riesgo y a la tecnología disponible.

En términos generales, este artículo contiene la obligación para el responsable de mantener seguros los datos personales que trata de acuerdo con ciertos parámetros. La totalidad de esta obligación representa una novedad para la regulación vigente en la Ley 19.628, y constituye un avance que requerirá a los responsables revisar las medidas implementadas y evaluar dónde y cómo tienen que mejorar.

Al analizar la disposición, podemos dividir su contenido según los tres aspectos que debe considerar el responsable en su cumplimiento. Además, agregamos un cuarto aspecto asociado con los estándares de cumplimiento, los cuales —a nuestro juicio— también son relevantes para efectos de esta obligación.

En primer lugar, los parámetros específicos que deberá tener en cuenta el respon-

102. Una aproximación racional de un responsable de datos será no solo recolectar estrictamente los datos personales que sean necesarios para el cumplimiento de la finalidad en atención al nuevo principio de proporcionalidad, sino que también determinará cuidadosamente cuál es la fundamentación de cada una de las finalidades que está aplicando y si son coherentes con su negocio. Hamelink (2015: 194-195) complementa esta idea señalando que la verdadera pregunta no debería ser si los conjuntos de datos pueden protegerse de manera adecuada, sino «si deberían existir en primer lugar» (véase también Hartzog, 2018: 256-257).

sable a la hora de implementar las medidas de seguridad son:[103] i) el estado actual de la técnica y los costos de aplicación; ii) la naturaleza, alcance, contexto y fines del tratamiento de datos; iii) la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos; y iv) la naturaleza de los datos tratados. Este último, tomado del principio de seguridad que vimos anteriormente.

De esta forma, el eje central en la aplicación de medidas estará, al igual que en el RGPD,[104] en la gestión de riesgos asociados al tratamiento de datos, lo cual implicará del responsable tomar en cuenta los riesgos existentes a lo largo de todo el espectro técnico y organizacional, incluyendo, por ejemplo, el derivado de la actividad de un subcontratista con acceso a bases de datos en calidad de encargado del tratamiento, o el derivado de ataques informáticos sofisticados (Room, 2018: 171-172).[105]

En segundo lugar, los objetivos que deben tener las medidas de seguridad implementadas por el responsable de datos: i) Asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos;[106] ii) evitar

103. Sería adecuado evaluar la incorporación de los conceptos de proporcionalidad y razonabilidad de las medidas a aplicar, algo que ya está comprendido en la Directiva NIS de la Unión Europea (2016/1148), que busca que los requisitos de seguridad que se impongan sean proporcionados en relación con los riesgos (Wolters, 2017: 177). Si bien esto no alteraría el núcleo de la norma, reforzaría —a nuestro juicio— lo propuesto por los estándares diferenciados de cumplimiento.

104. A nivel de RGPD, la aplicación de medidas de seguridad se encuentra regulada en su artículo 32. Éste establece la obligación general para el responsable y el mandatario de aplicar «medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo» (Wolters, 2017: 167). Estas medidas deberán tener en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y fines del tratamiento, y los riesgos de probabilidad y gravedad para los derechos y libertades de las personas. A continuación, establece una enumeración de medidas que deberán ser consideradas, que incluye: i) la seudonimización y el cifrado de datos personales; ii) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; iii) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; y iv) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

105. Con este análisis de riesgos, el responsable deberá determinar los controles que sean apropiados para su correcta mitigación. Se ha señalado que las vulneraciones de seguridad que afectan datos personales, si bien pueden ser resultado de múltiples y diversas acciones, por lo general tienen como causa subyacente al responsable de datos. Esto, aun cuando la causa directa e inmediata de la vulneración ha sido generada por un agente distinto, como empleados que no aplican los procedimientos establecidos; delincuentes informáticos que obtienen acceso a bases de datos que contienen datos personales; o la falta de capacitación adecuada de los trabajadores (OCDE, 2013: 26). Por su parte, hay que destacar que los riesgos a la seguridad en el ciberespacio son ocasionados por diversos factores, incluyendo elementos organizacionales, administrativos, técnicos y hasta sociológicos o políticos. En efecto, los riesgos obedecen a múltiples elementos y no necesariamente a una vulnerabilidad determinada en un programa computacional; todo lo cual deberá tomarse en cuenta cuando el responsable opere en este ámbito para el tratamiento de datos personales (Hamelink, 2015: 162-163).

106. En el ámbito de seguridad de la información, se ha señalado que la confidencialidad se refiere

la alteración, destrucción, pérdida, tratamiento o acceso no autorizado a los datos personales;[107] y iii) resguardar el cumplimiento del principio de seguridad que, en la práctica, agrega proteger los datos contra el tratamiento ilícito, la filtración de datos[108] y el daño accidental.

A nuestro juicio, pareciera que los objetivos de los números ii) y iii) están ya comprendidos dentro del objetivo i), relativo al aseguramiento de la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos, y que va en línea de la definición clásica de seguridad de la información que comprende los elementos confidencialidad, integridad y disponibilidad. Por lo general, se ha entendido que el compromiso de alguno de estos elementos supone, al menos, una vulneración en la seguridad de los datos (Álvarez Valenzuela y Vera Hott, 2017: 42-43; Laube y Böhme, 2016: 29; Room, 2018: 174).

En tercer lugar, la demostración de cumplimiento de las medidas implementadas ante la ocurrencia de un incidente de seguridad, lo cual requerirá al responsable acreditar «la existencia y el funcionamiento de las medidas de seguridad adoptadas en base a los niveles de riesgo y a la tecnología disponible».

El proyecto establece un modelo de responsabilidad demostrada, en virtud del

---

a la mantención de la privacidad de los datos, y que solo puedan acceder a ellos quienes estén autorizados. La integridad, por su parte, corresponde a que los datos no hayan sido alterados, modificados o eliminados sin la autorización del titular. La disponibilidad comprende la posibilidad de acceder a los datos o de usar un sistema para los fines que fue diseñado y que éste se mantenga operando y disponible. Por último, la resiliencia permite a los sistemas resistir, sobreponerse y recuperarse frente a amenazas o vulneraciones contra su seguridad (Álvarez Valenzuela y Vera Hott, 2017: 43; Smedinghoff, 2007: 8-9; Wolters, 2017: 166).

107. Por la amplitud de este objetivo, es posible incluir diversas hipótesis y clasificaciones asociadas al acceso no autorizado, por ejemplo, el acceso no autorizado con o sin daño en los sistemas de información que almacenan datos personales, el acceso autorizado por cuyo usuario excede el ámbito de la autorización en el tratamiento de datos, o el acceso no autorizado con o sin la superación de barreras técnicas de seguridad. Para estos efectos, resulta interesante la discusión que se ha dado respecto del proyecto de ley sobre delitos informáticos, que deroga la Ley 19.223 y modifica otros cuerpos legales con el objetivo de adecuarlos al Convenio de Budapest, Boletín 12.192-25. Este proyecto contiene un artículo que busca sancionar penalmente el acceso ilícito a un sistema informático. Para una revisión crítica del proyecto, sugerimos revisar el *position paper* sobre el tema publicado por la Alianza Chilena de Ciberseguridad, disponible en https://bit.ly/2zoIWQ7.

108. A nuestro juicio, en este punto se debe aplicar un criterio amplio, que considere tanto aquellas filtraciones que ocurran por la falta de medidas de seguridad apropiadas de la organización, como aquéllas que sean causa de una acción maliciosa externa capaz de traspasar las medidas de seguridad. En uno u otro caso, la autoridad deberá revisar si la organización que tenía a su cargo el resguardo de los datos personales dio antes integro cumplimiento a todos los requerimientos que establece este artículo 14 quinquies, en particular si, dentro de las medidas que tenía implementadas, tomó en consideración los parámetros requeridos, como, por ejemplo, el estado de la técnica y los costos, así como la naturaleza, alcance, contexto y fines del tratamiento, entre otros.

cual el responsable debe ser capaz de dar cuenta de las medidas de seguridad adoptadas y su funcionamiento.[109] Esto es coherente con el principio de responsabilidad del RGPD,[110] y requerirá a los responsables entender y tener documentada la información correspondiente a sus medidas de seguridad y al análisis de riesgos que hicieron a la hora implementarlas (Contreras Vásquez y Trigo Kramcsák, 2019: 88; Room, 2018: 172).[111]

Además de esto, se puede argumentar que esta disposición invierte la carga de la prueba en cuanto es el responsable, y no el titular o la autoridad, quien, ante un incidente, deberá probar que tenía implementadas medidas de seguridad acorde a la evaluación de los riesgos asociados y que, aun en ese caso, aconteció la vulneración que afectó los datos personales tratados.[112]

En cuarto lugar, el estándar de cumplimiento de estas medidas de seguridad que deberá tener en cuenta el responsable y que está dispuesto en el artículo 14 septies del proyecto. Este artículo establece que las condiciones mínimas que se impongan al responsable para el cumplimiento de la obligación de seguridad serán determinadas considerando: i) la calidad del responsable de datos (persona natural o jurídica); ii) el tamaño de la entidad o empresa y la actividad que desarrolla; iii) el tipo, volumen y naturaleza de los datos personales tratados; y iv) las finalidades del tratamiento. Estos estándares de cumplimiento serán especificados por el Consejo para la Transparencia y la Protección de Datos Personales[113] en una instrucción general.

---

109. El proyecto advierte un modelo de responsabilidad demostrada basado en i) el principio de responsabilidad que hace responsable del cumplimiento de los principios y obligaciones a quienes realicen tratamiento de datos personales (artículo 3 letra e), en conjunto con ii) este artículo 14 quinquies sobre medidas de seguridad, y iii) el artículo 13, que obliga al responsable a acreditar la licitud del tratamiento de datos personales. Arrieta Cortés, «Nuevo entorno…».

110. Bajo el RGPD, tanto el responsable como el mandatario del tratamiento deben ser capaces de demostrar que están aplicando las medidas de seguridad apropiadas respecto de los datos personales que tratan. Esta obligación se origina del principio de establecido en el artículo 5 número 2 sobre responsabilidad proactiva en relación con el artículo 24 sobre responsabilidad del responsable del tratamiento. La misma obligación para los mandatarios, en consideración con el responsable, está en el artículo 28 número 3 letra h) (Room, 2018: 172).

111. Arrieta Cortés, «Nuevo entorno…».

112. Esto se vincula con el nuevo deber de información y transparencia que establece el proyecto en su artículo 14 ter, en cuanto requiere que los responsables de datos mantengan permanentemente información sobre, entre otras cosas, la política y las medidas de seguridad adoptadas para proteger las bases de datos personales que administran.

113. El Consejo para la Transparencia y la Protección de Datos Personales (antes solo Consejo para la Transparencia) constituye, bajo el título 6 del Proyecto, la autoridad de control de carácter administrativo encargada de velar por el cumplimiento de la normativa de protección de datos. Su establecimiento fue aprobado durante la discusión legislativa en la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado en sesión del 5 de agosto de 2019. Votaron a favor de su nombramiento los senadores Andrés Allamand, Víctor Pérez Varela y Francisco Huenchumilla, mientras que en contra estuvieron

Estimamos que esta disposición no busca disminuir la relevancia de la seguridad de los datos personales, sino tratar de generar criterios de razonabilidad para cuando el Consejo o el juez califiquen el cumplimiento del deber de seguridad.[114] Una mirada similar ha adoptado la OCDE, que ha indicado que las pequeñas y medianas empresas tienen particularidades propias que deben ser atendidas al establecer una regulación referente a la seguridad de datos (OCDE, 2016: 27-28).[115]

Tras haber analizado estos cuatro puntos esenciales, podemos ver que la aplicación concreta de medidas de seguridad dependerá finalmente de las condiciones asociadas a cada tratamiento de datos y los riesgos que existan en cada caso. De esta forma, las medidas de seguridad que necesite un responsable no necesariamente van a ser las mismas que utilice otro responsable solo por tener, en apariencia, actividades de procesamiento similares.[116]

---

los senadores Felipe Harboe y Alfonso de Urresti. El establecimiento del Consejo para la Transparencia como autoridad de control de datos personales no ha estado exento de debate. De hecho, a lo largo de las discusiones de reforma de la Ley 19.628 han existido partidarios de establecer estas funciones en variadas instituciones, como la Contraloría General de la República, el Servicio Nacional del Consumidor, o en una nueva institución exclusiva e independiente para datos personales (Vergara Rojas, 2017: 141). Para un análisis de este tema con argumentos a favor del nombramiento del Consejo para la Transparencia véase Álvarez Valenzuela (2016). Por su parte, en cuanto a razones que se han esgrimido en contra de que el Consejo para la Trasparencia haga esta labor, véase «Organizaciones se pronuncian sobre la autoridad de protección de datos en Chile», Datos Protegidos, 31 de mayo de 2019, disponible en https://bit.ly/3hgiSrj; y Jessica Matus, «Por qué Chile necesita una autoridad exclusiva para la protección de los datos personales» *CNN Chile*, 15 de julio de 2019, disponible en https://bit.ly/3fbYLJ9.

114. Si bien esto puede parecer reiterativo analizado bajo el paraguas de la gestión de riesgos y los parámetros ya señalados por la norma, creemos que esta aproximación puede ciertamente tener un efecto positivo, sobre todo cuando el cambio de paradigma en seguridad de datos personales que propone el proyecto es sustantivo no solo para los responsables, sino también para la autoridad y los jueces que estarán encargados de fiscalizar el cumplimiento de la ley.

115. La misma OCDE ha señalado que estas empresas son críticas para el crecimiento económico, la competencia, la innovación y la creación de empleos. Agrega también que una buena política que se haga cargo de la seguridad de datos personales debería educar a las pequeñas y medianas empresas en el uso y los riesgos de las tecnologías digitales y establecer estándares de cumplimiento responsables y proporcionados (OCDE, 2016: 33).

116. La doctrina ha señalado medidas de seguridad que se pueden aplicar a relativo bajo costo por parte de un responsable: i) la elaboración de un instructivo de seguridad con normas para el personal que maneje datos personales; ii) la identificación y descripción de las funciones y obligaciones que tienen los empleados autorizados a manipular datos personales; iii) capacitar al personal sobre la importancia de la adecuada protección de los datos; iv) en caso de comunicaciones de datos a terceros, contar con registros que permitan identificar los datos personales involucrados en dicha comunicación (Donoso Abarca y Velásquez Silva, 2013: 180-181). Por su parte, cabe destacar que, desde la masificación de las nuevas tecnologías, las medidas para la seguridad se han modificado en consecuencia. Antes de esta proliferación, el uso de medidas físicas era la forma de generar seguridad, ya sea a través de cajas fuertes, medidas administrativas, generación de políticas, guardias, procedimientos de clasificación de docu-

Es importante mencionar que esta aproximación basada en la gestión de riesgos y el hecho de que el principio de seguridad requiera de medidas «apropiadas», implica que el legislador no está obligando a los responsables a alcanzar una seguridad absoluta e infranqueable, sino que, más bien, a implementar medidas basadas en la mayor o menor probabilidad e impacto de los riesgos de seguridad que se identifiquen. A mayor probabilidad o impacto, el responsable requerirá mayor nivel de sofisticación en las medidas de seguridad, por ejemplo, en el caso de hacer tratamiento de datos de carácter sensible (Room, 2018: 173; Smedinghoff, 2007: 29-32; Wolters, 2017: 172).

Este análisis de riesgos, no obstante, deberá también vincularse estrechamente con los demás parámetros de medición establecidos por la norma, que incluyen tanto los que señala el artículo 14 quinquies (por ejemplo, el estado actual de la técnica), como los del artículo 14 septies sobre el estándar de cumplimiento. En este último caso, especial consideración se deberá tener con el tamaño de la entidad y la actividad que desarrolla, así como la finalidad del tratamiento.[117]

Por último, cabe destacar que en esta área existe desde hace varios años un desarrollo técnico relevante asociado a las ramas de la seguridad de información o la ciberseguridad,[118] por lo que estimamos que el cumplimiento de esta obligación no debería —en principio— ser tan complejo para los responsables y mandatarios. Sin embargo, esto obligará a la protección de datos a salir del texto normativo para apoyarse en el conocimiento de seguridad de la información y sus estándares (Hartzog, 2018: 165-167; Room, 2018: 171).[119]

---

mentos, medidas perimetrales, medidas de escritorio limpio, u otras. Como señala Granados Paredes (2006: 3), el uso de la computadora y de internet ha hecho indispensable el uso de herramientas para la protección de la información digital. Sin embargo, es relevante señalar que con el advenimiento digital muchas organizaciones dejan en segundo plano lo que se refiere a seguridad física y analógica, a pesar de que en realidad tiene igual o mayor relevancia que la seguridad de los componentes tecnológicos (Room, 2018: 187). En este sentido, véase Hutter (2016).

117. Como dijimos, esta norma aporta un criterio de razonabilidad en cuanto a la exigencia que se le puede requerir a determinada entidad en sus medidas de seguridad. Además de esto, el responsable deberá tener en cuenta, a la hora de aplicar medidas, los elementos que se establece en el proyecto para la determinación del monto de las multas. En efecto, el artículo 37 del proyecto señala que, para establecer el monto específico de la multa, el Consejo deberá considerar, entre otros: i) la capacidad económica de la persona jurídica de derecho privado; ii) los beneficios obtenidos por el responsable a consecuencia de la infracción; y iii) si el tratamiento incluye datos personales sensibles o datos personales de niños, niñas y adolescentes.

118. Solo cabe considerar que el estándar BS 7799 sobre seguridad de la información y que fue el origen del estándar internacional ISO/IEC 17799, fue publicado por primera vez en el año 1995 por la British Standards Institution (BSI Group).

119. Ejemplo de esto es el desarrollo de mejores prácticas o estándares de seguridad reconocidos internacionalmente, como la versión 1.0 del NIST Privacy Framework elaborado por el National Institute of Standards and Technology; la norma ISO/IEC 27701:2019 Security techniques. Extensión de ISO/

El establecimiento de la obligación de reportar y registrar vulneraciones a las medidas de seguridad

Estas obligaciones se contemplan en el artículo 14 sexies del proyecto de la siguiente manera:

> El responsable y el encargado de datos deberán reportar a el Consejo para la Transparencia y la Protección de Datos Personales, por los medios más expeditos posibles y sin dilaciones indebidas, las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no autorizado a dichos datos, cuando exista un riesgo razonable para los derechos y libertades de los titulares.
>
> El responsable y el encargado de datos deberán registrar estas comunicaciones, describiendo la naturaleza de las vulneraciones sufridas, sus efectos, las categorías de datos y el número aproximado de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.
>
> Cuando dichas vulneraciones se refieran a datos personales sensibles, datos relativos a niños y niñas menores de catorce años, o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, el responsable y el encargado de datos deberán también efectuar esta comunicación a los titulares de estos datos. Esta comunicación deberá realizarse en un lenguaje claro y sencillo, singularizando los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas. La notificación se deberá realizar a cada titular afectado y si ello no fuere posible, se realizará mediante la difusión o publicación de un aviso en un medio de comunicación social masivo y de alcance nacional.

Este artículo establece que, en caso de un incidente o vulneración[120] que conlle-

IEC 27001 and ISO/IEC 27002 for privacy information management: Requirements and guidelines; el Payment Card Industry Data Security Standard, o el IoT Trust Framework de la Online Trust Alliance, que identifica ciertos requisitos que los fabricantes, proveedores de servicio, distribuidores y legisladores deben evaluar para mejorar la seguridad y privacidad de dispositivos de internet de las cosas (IOT) (Room, 2018: 183; Smedinghoff, 2007: 41-42; UNCTAD, 2019: 135).

120. El término en inglés corresponde a *data breach*, que en español por lo general se traduce como «brecha de seguridad» o «filtración de datos». Para efectos de este trabajo, nos importan aquellos incidentes que se refieren a los tipos de eventos notificables que indica la norma. No obstante, cabe señalar que *brecha de seguridad* es un término que obedece a la rama de la seguridad de la información y que ya ha sido definido por diversos instrumentos. Por ejemplo, el artículo 4 de la Directiva NIS de la Unión Europea (2016/1148) define *incidente* como «todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información». En el caso de NIST, se define *data breach* como «un incidente que involucra información sensible, protegida, o confidencial que es copiada, transmitida, vista, robada, o usada por un individuo no autorizado para hacerlo. La información expuesta puede incluir números de tarjeta de crédito, información personal de salud, datos de clientes, secretos comerciales, o materias de seguridad nacional, por ejemplo» (la traducción es nuestra). El glosario de términos de NIST se puede encontrar en https://bit.ly/3dT94BH.

ve un riesgo razonable para los derechos y libertades de los titulares, el responsable y el encargado del tratamiento deberán reportar al Consejo para la Transparencia y la Protección de Datos Personales dicha circunstancia por los medios más expeditos posibles y sin dilaciones indebidas.[121] Se califica de incidente, para efectos del proyecto, a i) las vulneraciones a medidas de seguridad que ocasionen destrucción, filtración, pérdida o alteración de los datos que trate; o ii) la comunicación o acceso no autorizado a esos mismos datos.

En caso de que las vulneraciones impliquen datos personales sensibles,[122] datos relativos a menores de catorce años, o datos comerciales, el responsable y el mandatario, además de notificar al Consejo, deberán hacerlo a los titulares de esos datos cumpliendo con ciertos requisitos mínimos señalados en la norma.[123] Ahora bien, es

121. A nivel comparado, las notificaciones de vulneraciones de seguridad tienen como destinatario tanto a los titulares de los datos como a ciertas autoridades administrativas. La elección respecto de uno u otro destinatario se puede ver reflejada en las diferencias que existen entre las obligaciones que establece la Unión Europea y Estados Unidos. En el RGPD se prefiere a la autoridad de control como la entidad encargada de recibir las notificaciones, mientras que las notificaciones se dejan al titular para los casos en que la vulneración implica un riesgo mayor (artículo 34). De forma distinta, en Estados Unidos la regla general sería la notificación al titular que, en ciertos casos, se complementa con una notificación a alguna autoridad; Carlo Benussi, «¿En qué consiste la nueva obligación de reportar vulneraciones a medidas de seguridad en el tratamiento de datos personales?», *Hipervínculos*, 28 de junio de 2018, disponible en https://bit.ly/3cVcbaI. En la misma línea, véase José Pablo Lapostol, «Brechas de datos, a propósito de la filtración de datos de tarjetas de crédito», *Diario Constitucional*, 30 de julio de 2018, disponible en https://bit.ly/37wZZfz. Bajo esta perspectiva, el proyecto sigue el modelo del RGPD con ciertos matices, en los que se establece como regla general la notificación al Consejo para la Transparencia para la mayoría de las vulneraciones, y sólo cuando éstas involucren cierta clase de datos la notificación además debe efectuarse a los titulares afectados. Para las diferencias entre los modelos estadounidense y europeo véase, «General Data Protection Regulation (GDPR)», PWC, disponible en https://pwc.to/2MPExJo.

122. Bajo el proyecto, los datos personales sensibles son «solo aquellos datos personales que revelen el origen étnico o racial, la afiliación política, sindical o gremial, hábitos personales, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural». En este caso, advertimos que el proyecto considera un estándar de protección mayor para los datos sensibles, incluidos los datos personales relativos a la salud y al perfil biológico humano.

123. Se ha señalado que pueden existir circunstancias que hagan recomendable no notificar a los titulares de datos cuando existan, por ejemplo, riesgos asociados para ellos o que de la notificación se pueda impedir una investigación llevada por la autoridad (OCDE, 2013: 26-27). De la literalidad del texto del proyecto vemos que, en principio, no sería posible considerar estos factores para demorar una notificación a los titulares, sin perjuicio de que creemos que el Consejo, en uso de sus facultades amplias, podría anteponerse requiriendo que, en una vulneración de medidas de seguridad específica, la notificación se dilate intencionalmente con el fin de prevenir un riesgo mayor. Por otro lado, se ha señalado también que la aproximación que establece el proyecto puede limitar la protección a los titulares en aquellos casos en que la vulneración de medidas no involucra los tipos de datos señalados específicamente por la

adecuado preguntarse por qué el legislador requiere la notificación al titular menor de catorce años cuando al mismo tiempo lo priva de poder consentir en el tratamiento de sus datos personales.[124] En este caso, tal vez sería más consistente con el proyecto requerir que la notificación sea dirigida a quien otorgó el consentimiento en lugar del menor, sus padres o representantes legales según corresponda.

En cuanto al contenido de la notificación, la norma solo lo establece para aquella que se hace al titular de los datos, pero no para los casos en que la notificación se debe hacer al Consejo. De aprobarse el texto como está, la posición conservadora a nuestro juicio sería notificar incluyendo los antecedentes señalados tanto para el registro de vulneraciones como para la notificación a los titulares.

Sin perjuicio de lo anterior, creemos relevante que se aclare este punto, dado que el contenido de la notificación es un elemento esencial que debe estar definido con anterioridad a la ocurrencia de un incidente, al menos en sus puntos esenciales. Sobre el contenido propiamente tal, una práctica recomendable sería revisar ejemplos comparados y nacionales con el fin de alcanzar un balance óptimo entre la calidad de la información que se pide al hacer la notificación y la carga del obligado, evaluando la utilización de modelos o formularios que permitan la sistematización de la información de forma más eficiente.[125] En el evento que este tema no quede suficien-

---

norma, pero que de su vulneración se genere de igual modo un grave riesgo de afectación. Para prevenir esto, el proyecto podría explorar la aplicación de un sistema más cercano al del RGPD, en cuanto lo detonante de la notificación en ese cuerpo normativo a los titulares radica en el «alto riesgo» para sus derechos y libertades, sin estar circunscrito a una clase específica de datos personales (Hartzog, 2018: 4), Benussi, «En qué consiste…».

124. El proyecto establece en su artículo 16 quater que, para tratar datos personales relativos a niños menores de catorce años, se requiere el consentimiento otorgado por sus padres o representantes legales o por quien tiene a su cargo el cuidado personal, salvo que expresamente lo autorice la ley. A esto se suma el requisito que el tratamiento sólo puede hacerse atendiendo al interés superior del niño y al respeto de su autonomía progresiva.

125. En el ámbito bancario, el capítulo 20-8 de la Recopilación Actualizada de Normas de la Superintendencia de Bancos e Instituciones Financieras establece con detalle el contenido de la notificación que se debe hacer a la CMF tanto al momento de inicio del incidente como al cierre. Entre sus elementos se encuentran: número único identificador del incidente (asignado por la CMF), nombre de la entidad informante, descripción del incidente, fecha y hora de inicio del incidente, causas posibles o identificadas, productos o servicios afectados, tipo y nombre de proveedor o tercero involucrado (si corresponde), tipo y número estimado de clientes afectados, dependencias o activos afectados (si corresponde), medidas adoptadas y en curso. Otro ejemplo lo podemos encontrar en el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) del Ministerio del Interior y Seguridad Pública, disponible en https://www.csirt.gob.cl/. A nivel comparado, podemos observar que en el caso estadounidense el contenido habitual que requieren las notificaciones involucra información de contacto del responsable y la fecha o fechas de la vulneración. En el caso del estado de California, la notificación requiere adjuntar un modelo de notificación para los titulares de datos, la fecha en que la vulneración fue descubierta, la fecha de notificación a los titulares, señalar si la vulneración se ha comunicado a la prensa, señalar si la vulneración se

temente desarrollado durante lo que resta del proceso legislativo, sería adecuado que el Consejo lo abordara haciendo uso de sus facultades.[126]

Junto con la notificación, el responsable de datos y el mandatario deberán llevar un registro de las comunicaciones en el que indiquen las siguientes cinco menciones: i) la naturaleza de las vulneraciones; ii) los efectos de las vulneraciones; iii) las categorías de datos afectados; iv) el número aproximado de titulares afectados; y v) las medidas adoptadas para gestionar las vulneraciones y precaver incidentes futuros.

Cabe señalar que esta obligación difiere del RGPD en cuanto el registro se refiere a las «comunicaciones» y no a «cualquier clase de vulneración», sin perjuicio de que creemos que, bajo cualquier estándar de seguridad adecuado, un responsable o encargado deberá registrar todas las vulneraciones que sufra aun cuando no requiera notificarlas, de forma de acreditar cumplimiento de sus demás obligaciones de seguridad en línea con el principio de responsabilidad demostrada (Room, 2018: 179).

De esta revisión, se advierte que el enfoque adoptado por el proyecto toma ciertos elementos del RGPD para construir la obligación de reporte, y agrega otros nuevos.[127]

---

ha comunicado o no a las policías, entre otros elementos (Benussi, «En qué consiste…»). En relación con el estado de California, véase «Submit Data Security Breach», State of California Department of Justice, disponible en https://bit.ly/37ks4Xj.

126. Benussi, «En qué consiste…». Dentro de la potestad reglamentaria que se le confiere al Consejo en el artículo 31 del proyecto, se establece expresamente la facultad de impartir instrucciones de carácter general a las personas naturales o jurídicas que hagan tratamiento de datos personales. A su vez, considera la posibilidad de proponer, al presidente de la República y al Congreso Nacional, las normas legales y reglamentarias para asegurar a las personas la debida protección de sus datos personales y perfeccionar la regulación sobre el tratamiento y uso de esta información.

127. El RGPD establece la obligación general para todos los responsables y mandatarios de notificar brechas de seguridad que afecten datos personales en su artículo 33 (autoridad de control) y 34 (titulares de datos) indicando el primero que, «en caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento». En cuanto al contenido de la notificación, se establece que ésta deberá «a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados; b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; c) describir las posibles consecuencias de la violación de la seguridad de los datos personales; d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. Si no fuera posible facilitar

Como elementos comunes vemos el hecho de que la vulneración deba ser calificada previamente: solo las que constituyan un «riesgo de perjuicio» para los titulares debe ser notificada; y que la notificación deba hacerse «sin dilaciones indebidas». Algunos elementos novedosos o distintos del RGPD son: la causal de notificación a los titulares de datos solo cuando la afectación se presente respecto de datos sensibles, datos relativos a menores de catorce años, o datos comerciales; la ausencia de normas que configuren «puertos seguros»; el hecho de que la calificación de riesgos que debe hacer el responsable y el mandatario para determinar la notificación a la autoridad y a los titulares es similar (riesgo razonable); y el establecimiento de la obligación de notificación a los titulares por parte del mandatario, entre otros aspectos.[128]

Con todo, vemos a esta nueva obligación de notificación y registro como un avance importante para la seguridad de los datos personales tratados en Chile, la que constituiría la primera obligación transversal de notificación asociada a brechas de seguridad que afecten datos personales,[129] y lo que iría en estrecha concordancia con

---

la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida». Por último, se establece una obligación de registro: «El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo». Por su parte, el artículo 34 del RGPD establece: «Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d). La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes: a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado; b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1; c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3».

128. Benussi, «En qué consiste…». Otro elemento distintivo es la ausencia en el proyecto de un plazo sugerido de notificación de la vulneración como el de 72 horas que contempla el RGPD.

129. En el ordenamiento jurídico nacional existen actualmente algunas obligaciones sectoriales relativas a la notificación de incidentes de seguridad, y que pueden tener vinculación con datos personales en caso de que éstos los lleguen a afectar. Estas obligaciones las encontramos a nivel financiero en el Capítulo 20-8 de la RAN de la Superintendencia de Bancos e Instituciones Financieras (actual CMF),

el camino tomado por varias jurisdicciones alrededor del mundo, incluyendo en Estados Unidos,[130] Europa[131] y América Latina[132] (OCDE, 2013: 26-27; Laube y Böhme,

---

que contiene la obligación de notificar incidentes operacionales que afecten o pongan en riesgo la continuidad del negocio, los fondos o recursos de la entidad o de sus clientes, la calidad de los servicios o la imagen de la institución en un plazo de 30 minutos a la autoridad; así como de notificar a los usuarios o clientes cuando se traten de incidentes «que afecten la calidad o continuidad de los servicios a los clientes o se trate de un hecho de público conocimiento». En el ámbito público, también existe una obligación de reportar incidentes en el instructivo presidencial que imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado, del 23 de octubre de 2018, y que establece el reporte obligatorio —para los órganos de la Administración del Estado— de incidentes de ciberseguridad al Centro de Coordinación de Entidades de Gobierno tan pronto tomen conocimiento de ellos. Para un detalle del contenido en este instructivo presidencial, véase Paulina Silva, «Instructivo presidencial sobre ciberseguridad», *Hipervínculos*, 29 de octubre de 2018, disponible en https://bit.ly/3fgLXBb, y Datos Protegidos, «Instructivo presidencial sobre ciberseguridad: Medidas urgentes para hacerse cargo de los problemas de hoy», 30 de octubre de 2018, disponible en https://bit.ly/3hjjjB8. Por último, cabe destacar que en el ámbito de las telecomunicaciones existen medidas de notificación a la Subsecretaria de Telecomunicaciones asociadas a la infraestructura crítica de telecomunicaciones, y cuya regulación se encuentra en la Ley 18.168 General de Telecomunicaciones, la Ley 20.478 «Sobre recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones», que agregó el título 8, «De las infraestructuras críticas de telecomunicaciones» a la Ley 18.168, y el Decreto 60 del año 2012 para la interoperación y difusión de la mensajería de alerta, declaración y resguardo de infraestructura crítica de telecomunicaciones e información sobre fallas significativas en los sistemas de telecomunicaciones.

130. Estados Unidos fue pionero en esta clase de obligaciones con la California S.B. 1386 del año 2003. A la fecha, ya se han publicado leyes de este tipo en los 50 estados y el Distrito de Columbia. Estas leyes sobre reporte de brechas de seguridad difieren en varios aspectos, como el plazo de notificación, la forma de la notificación y su contenido. Sin embargo, también coinciden en otros, como que la notificación sea por regla general a los sujetos afectados y, sólo bajo ciertos parámetros, a las autoridades. Por su parte, también existen leyes a nivel federal que contienen obligaciones sobre reporte de vulneraciones, encontrándose entre las más relevantes la Ley de Transferencia y Responsabilidad de Seguro Médico (HIPAA) y la Ley Gramm-Leach-Bliley (GLBA) (Laube y Böhme, 2016: 30; Smedinghoff, 2007: 16-17; Sullivan y Leigh Maniff, 2016; 67, 71). Para información sobre estas leyes, véase el sitio web del National Conference of States Legislatures, disponible en https://bit.ly/3f88CzE. Para más información sobre HIPAA, véase el sitio del U.S Department of Health & Human Services, disponible en https://bit.ly/3himU2s.

131. En la Unión Europea, parte relevante de las obligaciones de notificación de vulneraciones fueron establecidas inicialmente para el área de telecomunicaciones bajo la Directiva 2009/136/EC, que modificó la Directiva 2002/58/EC sobre privacidad y comunicaciones electrónicas o también conocida como ePrivacy Directive, específicamente respecto de proveedores de servicios de comunicaciones electrónicas (Laube y Böhme, 2016: 30-31).

132. A nivel latinoamericano, es posible encontrar obligaciones de reporte de brechas de seguridad en Colombia, México y Uruguay (Lehuedé, 2019: 50). Por su parte, en el caso de Argentina, existe la Resolución 47/2018 sobre «Medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados», que se refiere a brechas de seguridad y el mecanismo de notificación a la Agencia de Acceso a la Información Pública. Sin embargo, esta resolución no es de carácter obligatorio para los responsables. Véase la resolución en InfoLEG, Ministerio de Justicia y De-

2016: 30-31; Smedinghoff, 2007: 43-46).

Se ha señalado que la lógica subyacente a su establecimiento es que a través de ellas se otorga información que permite a los titulares de datos y empresas protegerse de las vulneraciones, y así mitigar sus efectos perjudiciales;[133] y se incentiva la inversión en seguridad de la información y medidas de ciberseguridad, en vista que esta clase de notificaciones pueden dañar la reputación y el valor de la empresa afectada y enfrentarla a acciones de indemnización o multas (Laube y Böhme, 2016: 29; OCDE, 2013: 26-27; Room, 2018: 176-177; Smedinghoff, 2007: 43; Sullivan y Leigh Maniff, 2016: 65).[134]

Ahora bien, de la revisión de esta nueva obligación nos surgen las siguientes consideraciones adicionales que estimamos relevantes para alcanzar el propósito de la norma y del proyecto en general:

Se requiere evaluar medidas para coordinar las gestiones de notificación y mitigación con otras autoridades. Las vulneraciones a medidas de seguridad muchas veces no solo se vinculan con la protección de datos personales, sino que también con otras áreas como ciberseguridad, protección al consumidor, regulación bancaria, y delitos informáticos, por nombrar algunas.[135] Esto puede generar que una institución, por un mismo incidente, deba efectuar distintas notificaciones a varias autoridades y bajo distintos supuestos, lo cual puede generar ineficiencias y retardos en el sistema de protección (Hartzog, 2018: 276-277; OCDE, 2013: 26-27).[136]

Se requiere aplicar medidas que guíen y orienten a los responsables y mandatarios en la correcta notificación de vulneraciones en, al menos, dos aspectos: i) la identificación de riesgos, dado que la notificación de vulneraciones sin que se evalúe correctamente que de ellas puede derivar «un riesgo razonable para los derechos y libertades

---

rechos Humanos, Presidencia de la Nación, disponible en https://bit.ly/2MTqdPu.

133. En este contexto, las vulneraciones de seguridad no sólo generarían un costo a las instituciones directamente afectadas, sino que, en virtud de la interdependencia de los sistemas de información, éstas pueden también afectar a otras entidades, por lo que constituirían una externalidad negativa que justificaría las obligaciones de reporte (Laube y Böhme, 2016: 29; Schneier, 2015: 225).

134. Estas razones son consistentes con las expresadas en los considerandos 85.º a 87.º del RGPD, que establecen que el objetivo de las obligaciones de reporte es que se tomen a tiempo medidas que permitan evitar que las vulneraciones ocasionen daños a los titulares. Por su parte, se ha indicado que el cumplimiento de estas obligaciones otorga información a las autoridades y otros organismos para determinar la investigación del incidente o la aplicación de otras medidas (OCDE, 2013: 26-27).

135. Como se señaló, en Chile ya existen normas asociadas a la notificación de vulneraciones que se encuentran vigentes, como las del Capítulo 20-8 de la RAN o las del instructivo presidencial que imparte instrucciones urgentes en materia de ciberseguridad.

136. En relación con esto, hay que considerar que las autoridades han señalado que enviarán pronto un proyecto de ley al Congreso que establezca una regulación marco sobre ciberseguridad. Véase Rosario Zanetta, «Gobierno y la Ley Marco de Ciberseguridad: "Es probable que salga durante el próximo año"», *Pauta*, 14 de octubre de 2019, disponible en https://bit.ly/3htYXFE.

de los titulares» —como pide la norma—, puede llegar a generar un número excesivo de comunicaciones cuya revisión la autoridad no tenga la capacidad de efectuar o que, por su volumen, no sean tomadas en cuenta por los titulares de datos; y ii) en la determinación de la imposibilidad de notificación al afectado que autoriza la comunicación por un medio de comunicación masivo, dado que su interpretación puede dar lugar a múltiples categorías de imposibilidad restringiendo, en consecuencia, la protección de los titulares de datos (Hartzog, 2018: 175-179; OCDE, 2013: 26-27).[137]

Se requiere considerar ciertas hipótesis de «puerto seguro» que otorguen razonabilidad y eficiencia a la norma exceptuando la obligación de notificación.[138] A nivel comparado existen circunstancias en las cuales la regulación entiende que la notificación de una vulneración no es un mecanismo necesariamente idóneo para resguardar los derechos de los titulares, como cuando hay otras normas que contemplan medidas de notificación similares, o cuando se han tomado precauciones que disminuyen o eliminan los riesgos.[139] Incorporar esta clase de elementos dentro de la obligación

137. Se puede argumentar la existencia de, por ejemplo, imposibilidades asociadas a términos económicos, capacidad técnica, tamaño de la empresa, etcétera, que, dada la amplitud del requisito, pueden dar lugar a la notificación mediante un medio de comunicación masivo sin que corresponda. Además de esto, se ha sugerido adecuado establecer la posibilidad de notificar por medios electrónicos en la medida que fuera posible contactar a los titulares de datos por tal mecanismo, lo que permitirá reducir los costos de la gestión, alcanzando a un gran número de titulares en un plazo reducido de tiempo. Benussi, «En qué consiste…».

138. Se denomina habitualmente *puerto seguro* a aquellas disposiciones que establecen que, cierta conducta, no se va a considerar una infracción o un incumplimiento a una obligación. En el diccionario Merriam-Webster, se señala que el término en inglés *safe harbor*, se refiere a cierta norma que otorga protección respecto de una sanción o responsabilidad (*Mirriam Webster Dictionary*, s. v. «safe harbor», disponible en https://bit.ly/30KNBqX; la traducción es nuestra). En Chile, el término se ha utilizado generalmente para referirse al régimen de limitación de responsabilidad de los prestadores de servicios de internet, lo cual está regulado en los artículos 85 L y siguientes de la Ley 17.336 sobre Propiedad Intelectual. De acuerdo con lo que señala Alberto Cerda (2014), el sistema de puerto seguro que establece esta ley corresponde a un conjunto de reglas que limitan la responsabilidad de los prestadores de servicio de internet en la medida que éstos cumplan con determinadas obligaciones.

139. En Estados Unidos, algunos estados no requieren que las entidades notifiquen las brechas de seguridad si los datos afectados se encontraban encriptados, y las llaves no fueron comprometidas, o si la entidad obligada ha dado cumplimiento a otras leyes asociadas como HIPAA o GLBA. Por su parte, en ese mismo país la mayoría de las leyes sobre notificación de filtraciones de datos personales permiten a las empresas dilatar la notificación al titular si ello podría perjudicar una investigación criminal en curso como, por ejemplo, en el estado de California. Para un reporte sobre las obligaciones de notificación en Estados Unidos véase «Data breach notification in the United States and territories», IAPP Privacy Tracker, disponible en https://bit.ly/2YpG6mq. En el caso de la Unión Europea, el RGPD contempla hipótesis de puerto seguro en su artículo 34, en el que se establece que la notificación al titular de datos no será requerida si: i) el responsable ha adoptado medidas de protección apropiadas y éstas se han aplicado a los datos afectados como, por ejemplo, el cifrado; o ii) si el responsable ha tomado medidas que garanticen que ya no existe la probabilidad de que se concrete el alto riesgo para los derechos y libertades del

de notificación otorgaría razonabilidad y eficiencia a la norma, limitando la cantidad de notificaciones, reduciendo los gastos para los responsables[140] y resguardando de mejor manera los derechos de las personas, en cuanto se asignarían de manera más eficiente los esfuerzos de implementación de mecanismos de seguridad y los planes para la notificación de vulneraciones (Hartzog, 2018: 182-183; Room, 2018: 179).

La incorporación de obligaciones de seguridad para el mandatario en el tratamiento de datos personales

El inciso cuarto del artículo 15 bis del proyecto sobre tratamiento de datos a través de un tercero encargado establece:

> El tercero mandatario o encargado deberá cumplir con lo dispuesto en los artículos 14 bis, 14 quater, 14 quinquies y artículo 14 sexies. La diferenciación de estándares de seguridad establecida en el inciso primero del artículo 14 septies también será aplicable al tercero mandatario o encargado. Tratándose de una vulneración a las medidas de seguridad, el tercero o mandatario deberá reportar este hecho al Consejo para la Transparencia y la Protección de Datos Personales y al responsable.

De esta forma, la norma señala que cuando un tratamiento de datos personales se efectúe a través de un mandatario, éste deberá cumplir con las mismas obligaciones del responsable de datos vinculadas a la adopción de medidas de seguridad (artículo 14 quinquies) y al reporte y registro de vulneraciones a esas medidas (14 sexies); así como una obligación específica de notificación al responsable de datos.[141]

La norma viene a suplir el importante vacío que existe bajo la Ley 19.628 en cuanto a la seguridad que deben aplicar los mandatarios en el tratamiento de datos, y constituye un avance sustancial en lo que se refiere a la protección de los titulares de datos personales en Chile. No obstante, la norma nos parece todavía perfectible en lo que a las obligaciones de notificación se refiere en los siguientes aspectos:

En primer lugar, la norma requiere que el mandatario notifique directamente a los titulares de datos frente a una vulneración de medidas de seguridad. Esto, se establece, por una parte, en la remisión íntegra que el inciso cuarto del artículo 15 bis hace al artículo 14 sexies que contempla la notificación de datos al titular; por otra, lo que

titular (Room, 2018: 179). Benussi, «En qué consiste…».

140. Sobre todo, si tenemos presente que las obligaciones que establece el proyecto son aplicables de forma transversal tanto para personas jurídicas como personas naturales en conformidad con lo que dispone su artículo 1.

141. El proyecto no establece expresamente un plazo para la notificación desde el encargado al responsable de datos. Sin embargo, una posición conservadora sería aplicar la regla general establecida en el artículo 14 sexies para las notificaciones al Consejo y que requieren que éstas sean llevadas a cabo por los medios más expeditos posibles y sin dilaciones indebidas.

dispone ese mismo artículo 14 sexies en cuanto señala que, al tratarse de una vulneración que se refiera a datos personales sensibles, relativos a niños y niñas menores de catorce años o datos de carácter comercial, «el responsable y el encargado deberán también efectuar esta comunicación a los titulares de estos datos».

De esta forma, podemos observar que el proyecto contempla una obligación de notificación mayor para el mandatario que para el responsable de datos al tener que, en ciertos casos, estar obligado a hacer tres notificaciones diferentes para la misma vulneración: al Consejo para la Trasparencia y la Protección de Datos Personales, al responsable de datos, y a los titulares en los casos que establece el inciso tercero del artículo 14 sexies.[142] Esto parece, en principio, contrario a la naturaleza del responsable y el encargado, y al hecho de que ambos tienen un papel diferente dentro del esquema de tratamiento de datos personales.

En segundo lugar, la norma contempla un régimen de notificaciones paralelas de parte del mandatario y el responsable de datos tanto al Consejo, como al titular de datos personales, lo cual también es contrario a la naturaleza de las entidades y puede generar ineficiencias en el sistema de protección de derechos.[143]

El texto propuesto da lugar a notificaciones simultáneas por los mismos eventos tanto al Consejo como a los titulares de los datos, lo cual podría generar confusión y dificultades en la coordinación de respuestas frente a incidentes, además de implicar un gasto injustificado de recursos al desconocer que el responsable es quien, por sus características y facultades, en la generalidad de los casos está en una mejor posición para acceder a los datos y calificar la existencia e impacto de una vulneración.[144] La asignación de responsabilidad a quien esté en mejor posición de minimizar el riesgo es una idea que ya ha sido señalada por los autores al referirse a vulneraciones de seguridad (Schneier, 2015: 225-229).

Por todo lo anterior, nos parece que se debería explorar una modificación de los

142. En los casos correspondientes a vulneraciones que se refiera a datos personales sensibles, niños menores de catorce años, o datos comerciales.

143. Benussi, «En qué consiste…».

144. Se ha señalado que, si bien es deseable que exista mayor transparencia a la hora de acontecer vulneraciones de medidas de seguridad, una obligación de reporte idéntica para responsable y el encargado generará dificultades en su aplicación. El reporte de una vulneración requiere una calificación técnica (destrucción, filtración o alteración de datos) y una calificación jurídica (riesgo razonable de perjuicios al titular). La existencia de dos obligados a realizar estas calificaciones como propone el Proyecto sobre un mismo evento puede generar inconvenientes y descoordinaciones en el Consejo y en los titulares de datos, quienes pueden verse enfrentados, por ejemplo, a notificaciones contradictorias o incoherentes entre sí respecto de un mismo hecho (Benussi, 2018). No obstante esto, hay que tener en cuenta que también existen casos en que el mandatario puede ser quien esté en una mejor posición para calificar una vulneración, como por ejemplo, en el caso de prestadores de servicios de tecnología de gran tamaño que exceden el ámbito de conocimiento técnico y jurídico del responsable.

artículos 14 sexies y 15 bis del proyecto para aproximarlos al RGPD,[145] requiriendo únicamente la obligación de notificación desde el mandatario al responsable, y que éste último sea el único encargado de notificar al Consejo y a los titulares de los datos en caso de ser aplicable. Alternativamente, se podría evaluar una participación más activa de los mandatarios, pero con la precaución de evitar notificaciones simultáneas y estableciendo con claridad a cuál de las entidades (responsable o mandatario) corresponde la obligación de notificación y a qué destinatario en específico.

Elementos adicionales vinculados con las obligaciones de seguridad

Sin perjuicio que las obligaciones descritas en las secciones anteriores son —a nuestro juicio— las principales en cuanto a obligaciones de seguridad en el tratamiento de datos personales, en el texto del proyecto existen otras disposiciones cuya vinculación con las normas sobre seguridad revisadas también es relevante. Estas disposiciones incluyen aquellas relativas a i) encriptación, anonimización y seudonimización; ii) el deber de protección desde el diseño y por defecto; y iii) la incorporación de infracciones específicas.

Encriptación, anonimización y seudonimización

Hoy muchos sistemas utilizan encriptación para proteger los datos que circulan a través de internet, mecanismo de seguridad que contemplado en nuestra legislación de manera limitada (Álvarez Valenzuela, 2019: 245-246, 251, nota al pie).[146] Por su parte, se establece expresamente en el RGPD en su artículo 32 al referirse a las medidas de seguridad que deberá implementar el responsable y el mandatario en el tratamiento de datos personales.[147]

145. Bajo los artículos 33 y 34 del RGPD, la obligación de notificar una violación de seguridad a la autoridad y al titular compete únicamente al responsable y no al mandatario. El mandatario tiene, por su parte, la obligación de notificar lo antes posible al responsable la ocurrencia de una vulneración de seguridad. Además, adoptar la lógica que establece el RGPD refuerza la idea de que el responsable de los datos es quien realmente tiene, valga la redundancia, la responsabilidad por la seguridad de los datos que trata. En su actuar, y bajo lo que dispone el artículo 15 bis del proyecto, está la decisión última de tratar o no los datos que ha recolectado a través de un encargado, y, en consecuencia, de responder frente al Consejo y los titulares en caso de que su mandatario sufra una vulneración de seguridad.

146. Particularmente en la Ley 20.120, así como de manera indirecta en la Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma. Además, se refiere a ella el título 3 del Capítulo 20-7 de la RAN, que exige a aquellos bancos que externalicen servicios de procesamiento de datos que cualquier información una vez procesada, sea almacenada y transportada en forma encriptada.

147. En cuanto a si datos personales encriptados constituyen datos personales sugerimos revisar el interesante trabajo de Josh Gresham, «Is encrypted data personal data under the GDPR », IAPP Privacy

A diferencia de estos casos, el proyecto no se refiere a la encriptación en específico, pues se limita a señalar aquellas consideraciones que se deberán tomar en cuenta para el establecimiento de medidas de seguridad. Sin embargo, el hecho de no señalarse en forma expresa no es óbice para su aplicación como medida de seguridad en cuanto dentro de estas «consideraciones» se debe atender al estado de la técnica y nadie podría discutir hoy que el cifrado no forma parte éste (Room, 2018: 173).[148]

Por otro lado, el proyecto define *anonimización* o *disociación* como:

> Procedimiento irreversible en virtud del cual un dato personal no pueden vincularse o asociarse a una persona determinada, ni permitir su identificación, por haberse destruido o eliminado el nexo con la información que vincula, asocia o identifica a esa persona. Un dato que ha sido anonimizado deja de ser un dato personal.

Bajo la definición, el proyecto revoca al tratamiento de datos anonimizados de su carácter de tratamiento de datos personales, dejándolo fuera de la aplicación de la norma (Vergara Rojas, 2017: 138). Este procedimiento es contemplado en distintas partes del texto legal, incluyendo: i) la aplicación del principio de proporcionalidad cuando los datos personales deben ser cancelados o anonimizados al haber transcurrido el tiempo necesario para cumplir con los fines del tratamiento; y ii) cuando los responsables deben cancelar o anonimizar los datos personales de un titular cuyos datos fueron obtenidos para la ejecución de medidas precontractuales.[149]

Por último, la *seudonimización* se define en el proyecto como:

> Tratamiento de datos personales que se efectúa de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas

Perspectives, 6 de marzo de 2019, disponible en https://bit.ly/3dZmE6q. Una aproximación ilustrativa en este tema es la que establece el artículo 34 del RGPD, en el que no se requiere la notificación de la violación de seguridad de datos personales al titular cuando los datos hayan sido protegidos precisamente mediante una técnica de cifrado.

148. El uso de sistemas de encriptación para garantizar la protección de los datos personales y sistemas seguros de identificación digital ha sido ya avalado por la Comisión Europea y la Alta Representante de la Unión para Asuntos Exteriores y Políticas de Seguridad en Comunicación Conjunta al Parlamento Europea y al Consejo Resiliencia, Disuasión y Defensa: fortalecer la ciberseguridad de la Unión Europea (Álvarez Valenzuela, 2019: 248). Sin perjuicio de esto, los responsables siempre deben ser conscientes de los avances de seguridad, pues puede ser que mañana la encriptación no sea el mecanismo más seguro o recomendable. Los mismos autores señalan que la criptografía tiene factores que la pueden debilitar, incluyendo un sistema informático mal diseñado y el —siempre determinante— factor humano (Granados Paredes, 2006: 15).

149. El Proyecto contempla también el uso del procedimiento de anonimización en relación con el tratamiento de datos personales sensibles basado en el interés legítimo, y la publicación de resultados de estudios e investigaciones científicas que utilicen datos personales.

> destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable.

Si bien el texto define este concepto, no se incluye una regulación específica al respecto. Según la Information Commissioner's Office (ICO) —la autoridad de protección de datos personales del Reino Unido—, en términos prácticos este mecanismo se puede aplicar mediante el reemplazo de identificadores referentes a personas naturales, por ejemplo, por números de referencia o seudónimos. Mientras que un responsable tiene la forma de cruzar los datos para identificar a las personas, introduce medidas técnicas y organizativas para mantener la información relevante adicional y que permite el cruce, separada, de forma que quienes operan con la información seudonimizada no pueden identificarlas.[150]

Se ha entendido a la seudonimización como un procedimiento que permite colaborar en el cumplimiento a las obligaciones de seguridad y de privacidad desde el diseño y por defecto que impone la ley (Aparicio Vaquero, 2016: 31). Por último, cabe destacar que un dato seudonimizado sigue siendo personal para el responsable y, por lo tanto, sujeto a las obligaciones que establece el proyecto para su tratamiento.[151]

Deber de protección desde el diseño y por defecto

Este deber constituye una novedad relevante en el proyecto cuyo origen se encuentra en el RGPD.[152] Está regulado en el artículo 14 quater de la siguiente manera:

---

150. Esto está expuesto en el sitio web de ICO. Véase «What is personal data?», ICO, https://bit.ly/2XUMnXY.

151. La encriptación puede ser uno de los mecanismos técnicos utilizados para alcanzar la seudonimización de datos personales. Además, puede utilizarse para la protección de la información adicional que debe sujetarse a medidas técnicas y organizativas que garanticen que los datos personales no se atribuyan a una persona natural identificada o identificable. Por su parte, puede haber otros mecanismos para la seudonimización y que no están relacionados con el cifrado de datos, como la utilización de funciones de *hash* o la *tokenización*. Para una revisión de este tema, sugerimos ver GT29 (2014) e «Introducción al *hash* como técnica de seudonimización de datos personales», Agencia Española de Protección de Datos, octubre de 2019, disponible en https://bit.ly/2C5fZtr.

152. La protección de datos desde el diseño y por defecto se encuentra regulada en el artículo 25 del RGPD. Si bien tiene elementos muy similares a la norma propuesta en el proyecto, este artículo tiene algunas diferencias. Por ejemplo, precisa de mayor manera el momento de aplicar la protección desde el diseño, estableciendo que el responsable las aplicara «tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento». En cuanto al objeto del deber de protección desde el diseño, la norma del RGPD también señala como ejemplo concreto de la medida, la seudonimización, cuestión que no se encuentra en la norma del proyecto. En cuanto al deber de protección por defecto, el RGPD contiene una obligación específica que establece que «tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas». Esta mención no se incluyó en el proyecto. Por otro

> El responsable debe aplicar 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 establecidos en esta ley. Las medidas deben ser adoptadas considerando el estado de la técnica, los costos de implementación y la naturaleza, ámbito, contexto y fines del tratamiento de datos, así como los riesgos.
>
> El responsable de datos deberá aplicar 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. Esta obligación se aplicará al número de datos recogidos, a la extensión del tratamiento, al plazo de conservación de los datos y a su accesibilidad.

Según se puede apreciar, el primer inciso del artículo se refiere al deber de protección desde el diseño, en virtud del cual el responsable debe aplicar medidas de protección de datos personales antes y durante el tratamiento. Se busca que el responsable tome un papel preventivo y proactivo, incorporando la protección de los datos a lo largo de todo el ciclo de vida del tratamiento, por ejemplo, desde la creación de un nuevo producto o servicio. En este caso, el legislador no establece medidas específicas de protección, sino que requiere que el responsable aplique un cierto procedimiento que asegure que, nuevos tratamientos, se hagan desde el comienzo bajo una perspectiva de protección de datos (Hartzog, 2018: 179-180).[153]

El inciso segundo se refiere al deber de protección por defecto, en el cual el responsable deberá aplicar medidas para que el tratamiento de datos se limite a aquéllos que sean necesarios para la finalidad perseguida. De acuerdo con Hartzog (2018: 181-182), esta obligación —a nivel del RGPD— establece tanto un control obligatorio en el proceso de diseño, como la obligación de que las opciones que otorguen mayor protección de datos personales deben ser ofrecidas y activadas por defecto.

Infracciones específicas vinculadas a la seguridad de datos personales

Para el proyecto, serán infracciones graves (multa de 101 a 5.000 UTM)[154] vulnerar las obligaciones de seguridad establecidas en el artículo 14 quinquies, y omitir las comunicaciones o registros en los casos de vulneraciones a medidas de seguridad establecidas en el artículo 14 sexies. Se considerará infracción gravísima (multa de

lado, cabe destacar que el 20 de noviembre de 2019 el European Data Protection Board abrió una consulta pública en relación con una guía acerca de privacidad desde el diseño y por defecto (Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, disponible en https://bit.ly/2UzlTJC).

153. ICO tiene una guía sobre protección de datos desde el diseño y por defecto, disponible en https://bit.ly/2XV5ktz.

154. Unidad tributaria mensual, que corresponde a un monto de dinero expresado en pesos chilenos determinado por ley, y que se actualiza por el índice de precios al consumidor (IPC).

5.001 a 10.000 UTM) omitir de forma deliberada las comunicaciones de vulneraciones a medidas de seguridad que puedan afectar la confidencialidad, disponibilidad o integridad de los datos.[155]

Este nuevo catálogo de multas constituye una importante novedad tanto por la amplitud de los casos en los que aplican, como por los montos asociados. Cabe señalar que el régimen vigente de la Ley 19.628 solo contiene multas en los casos en que se reclame judicialmente a través de una acción *habeas data,*[156] y cuyo monto máximo asciende a 50 UTM en el caso de que los datos se hayan referido a los relativos a obligaciones de carácter económico, financiero, bancario o comercial (Corral Talciani, 2014: 50-54).

Para materializar estas infracciones en sanciones efectivas, el proyecto contempla dos tipos de procedimientos, uno administrativo y uno posterior de tipo judicial. Se espera que la creación de este procedimiento administrativo supla las deficiencias del sistema vigente bajo la Ley 19.628 que, como vimos, solo permite la reclamación en tribunales y es de escasa aplicación. Por lo demás, en el cumplimiento de las obligaciones de seguridad, los responsables y mandatarios deberán recurrir al conocimiento técnico existente en seguridad de la información, lo cual otorgará más certeza a los jueces y a la futura autoridad respecto de la configuración de un incumplimiento (Room, 2018: 171; Vergara Rojas, 2017: 142-143).

Finalmente, el proyecto contempla una serie de facultades de auditoría a favor del Consejo para fiscalizar el cumplimiento de las normas sobre tratamiento de datos por parte de los responsables y mandatarios,[157] mecanismo que los autores han indicado

155. Además, cabe destacar que el proyecto considera infracción leve (multa de 1 a 100 UTM) el hecho de cometer cualquier otra infracción a los derechos y obligaciones establecidas en la ley, que no sea calificada como una infracción grave o gravísima.

156. La acción *habeas data* está regulada en el artículo 16 de la Ley 19.628 y busca amparar el ejercicio de los derechos de información, modificación, bloqueo y cancelación de datos personales del titular, cuando i) el responsable no se ha pronunciado de la solicitud del requirente dentro de los dos días hábiles siguientes; o ii) si el responsable ha denegado la solicitud por causa distinta a la seguridad de la nación o el interés nacional (Corral Talciani, 2014: 50-52).

157. El proyecto establece facultades específicas del Consejo tendientes a auditar y fiscalizar su cumplimiento. Éstas se encuentran fundamentalmente en su artículo 31, en el que se establece que el Consejo tendrá como función y atribución: «a) Fiscalizar y velar por el cumplimiento de los principios, derechos y obligaciones establecidos en esta ley. Para efectos de fiscalización se podrá solicitar la entrega de cualquier documento, libro o antecedente que sea necesario; […] d) investigar y determinar las infracciones en que incurran los responsables de datos y ejercer, en conformidad a la ley, la potestad sancionatoria. Para tales efectos, podrá citar a declarar, entre otros, al titular, a los representantes legales, administradores, asesores y dependientes del responsable de datos, así como a toda persona que haya tenido participación o conocimiento respecto de algún hecho que sea relevante para resolver un procedimiento sancionatorio; […] o) obtener el acceso a los locales del responsable y del tercero mandatario o encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con las normas procesales que regulen la materia».

como relevante para la efectividad de las normas sobre notificación de brechas de seguridad (Laube y Böhme, 2016: 37-38; Sullivan y Leigh Maniff, 2016: 68).[158]

Conclusiones

La relevancia que ha adquirido el tratamiento masivo de datos personales, en conjunto con el incremento de los incidentes de seguridad vinculados a ellos, ha generado que la necesidad de avanzar en mejor regulación en materia de obligaciones de seguridad de datos personales sea un tema relevante para la protección de los derechos fundamentales en nuestro país.

Bajo este panorama, a lo largo este trabajo revisamos someramente la protección de datos personales y las obligaciones de seguridad desde una mirada de garantías fundamentales, la que se puede construir a partir de distintos instrumentos internacionales y lo dispuesto en nuestra Constitución. A continuación, pasamos a explorar una revisión general de este tema desde el ámbito de la ciberseguridad.

Posteriormente, examinamos las obligaciones de seguridad que establece el ordenamiento jurídico chileno para el tratamiento de datos personales, en particular en la Ley 19.628 y en la normativa sectorial de salud sobre ficha clínica y datos del genoma humano. En esta sección, vimos algunas de las deficiencias que se le han atribuido a estos cuerpos normativos, y las razones de por qué no estarían resultando eficaces en la actualidad.

Luego, pasamos a revisar la nueva regulación sobre obligaciones de seguridad que introduce el proyecto que busca modificar la Ley 19.628, entre las que encontramos la incorporación de un nuevo principio de seguridad, la obligación de adoptar medidas de seguridad bajo ciertos criterios, el establecimiento de obligaciones específicas para los mandatarios, y el establecimiento de una obligación de reporte y registro de vulneraciones a medidas de seguridad. Esta última es de gran importancia al constituir la primera obligación de este tipo en la legislación nacional y que, bajo el contexto tecnológico y de amenazas de ciberseguridad, hacen que su promulgación sea apremiante.

Pudimos advertir también que la regulación sobre obligaciones de seguridad dispuesta en el proyecto es de carácter común y general para todas las categorías de datos personales que se traten. Esto, sin perjuicio de establecer la notificación de vulneraciones a los titulares en el caso de que éstas se refieran, entre otros, a datos personales sensibles, como los relativos a la salud.

Además de estas obligaciones, identificamos —como elementos relevantes des-

158. En particular, Laube y Böhme (2016: 37-38) señalan que el establecimiento de auditorías de seguridad y sanciones puede servir de incentivo a los responsables de datos para notificar las brechas de seguridad que sufran a las autoridades, independiente de los costos asociados a la revelación.

de un punto de vista de seguridad de datos personales— aquellas disposiciones del proyecto relativas a encriptación, anonimización y seudonimización; el deber de protección desde el diseño y por defecto; y la incorporación de infracciones específicas.

En cuanto a estas nuevas obligaciones, advertimos que los autores del proyecto han tomado varios elementos del Reglamento General de Protección de Datos y han agregado otros nuevos. En términos generales, vemos que ellas están bien encaminadas y constituyen un avance importante respecto de las obligaciones hoy existentes. No obstante, identificamos ciertos puntos cuya mejora o mayor precisión permitirá establecer obligaciones más claras y eficientes tanto para los obligados como para la futura autoridad de control, lo que incluye la necesidad de generar coherencia entre las funciones que los responsables y mandatarios tendrán frente a la notificación de una misma brecha de seguridad.

Referencias

Álvarez Valenzuela, Daniel (2016). «Acceso a la información pública y protección de datos personales: ¿Puede el consejo para la transparencia ser la autoridad de control en materia de protección de datos?». *Revista de Derecho (Coquimbo)*, 23 (1): 51-79. DOI: 10.4067/S0718-97532016000100003.

—. (2017). «Los desafíos de la ciberseguridad en Chile». *Revista Chilena de Derecho y Tecnología*, 6 (2): 1-2. DOI: 10.5354/0719-2584.2017.48027.

—. (2018). «Privacidad en línea en la jurisprudencia constitucional chilena». *Revista de Derecho Público*, 89: 11-32. DOI: 10.5354/0719-5249.2018.52027.

—. (2019). «Algunos aspectos jurídicos del cifrado de comunicaciones». *Derecho PUCP*, 83: 241-262. DOI: 10.18800/derechopucp.201902.008.

Álvarez Valenzuela, Daniel y Francisco Vera Hott (2017). «Ciberseguridad y derechos humanos en América Latina». En Agustina del Campo (compiladora), *Hacia una internet libre de censura II: Perspectivas en América Latina* (pp. 37-63). Córdoba: Universidad de Palermo. Disponible en https://bit.ly/2MTlvRR.

Anguita, Pedro (2007). *La protección de los datos personales y el derecho a la vida privada: Régimen jurídico, jurisprudencia y derecho comparado*. Santiago: Legal Publishing.

Aparicio Vaquero, Juan Pablo (2016). «La protección de datos que viene: el nuevo Reglamento General europeo». *Ars Iuris Salmanticensis. Tribuna de Actualidad*, 4: 27-34. Disponible en https://bit.ly/2B8BR6t.

Bachelet, Michelle (2019). «Human rights in the digital age: Can they make a difference». Discurso para UN High Commissioner for Human Rights. Japan Society, Nueva York. Disponible en https://bit.ly/2B9WOoQ.

Barros Bourie, Enrique (1998). «Honra, privacidad e información: Un crucial conflicto de bienes jurídicos». *Revista de Derecho, Universidad Católica del Norte*, 5: 45-58. Disponible en https://bit.ly/2XZQow3.

Cerda, Alberto (2012). «Legislación sobre protección de las personas frente al tratamiento de datos personales». Material de estudio del Centro de Estudios en Derecho Informático, Facultad de Derecho, Universidad de Chile. DOI: 10.13140/RG.2.2.33767.47522.

—. (2014). «Limitación de responsabilidad de los prestadores de servicios de internet por infracción a los derechos de autor en línea». *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso,* (42), 121-148. DOI: 10.4067/S0718-68512014000100004.

Contreras Vásquez, Pablo y Pablo Trigo Kramcsák (2019). «Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile». *Revista Chilena de Derecho y Tecnología*, 8 (1): 69-106. DOI: 10.5354/0719-2584.2019.52915.

Corral Talciani, Hernán (2000). «Configuración jurídica del derecho a la privacidad: Concepto y delimitación». *Revista Chilena de Derecho*, 27 (2): 331-355. Disponible en https://bit.ly/3flbqJJ.

—. (2014). «De los derechos de las personas sobre los responsables de bancos de datos: el *habeas data* chileno». En Jorge Wahl Silva (editor), *Tratamiento de datos personales y protección de la vida privada* (pp. 39-57). Santiago: Universidad de los Andes.

Donoso Abarca, Lorena (2011). «El problema del tratamiento abusivo de los datos personales en salud». En *Reflexiones sobre el uso y abuso de los datos personales en Chile* (pp. 79-99). Santiago: Ediciones Universidad Diego Portales.

Donoso Abarca, Lorena y Juan Velásquez Silva (2013). *Tratamiento de datos personales en internet: Los desafíos jurídicos en la era digital.* Santiago: Legal Publishing.

Eterovic Barreda, Pablo (2019). *Acceso a la ficha clínica en el derecho chileno.* Santiago: Ediciones Jurídicas de Santiago.

Granados Paredes, Gibrán. (2006). «Introducción a la criptografía». *Revista Digital Universitaria*, 7 (7): 2-17. Disponible en https://bit.ly/3hpFvK3.

GT29, Grupo de Trabajo del Artículo 29 (2014). «Opinion 05/2014 on Anonymisation Techniques». 0829/EN WP216. Disponible en https://bit.ly/2MXldKo.

—. (2018). «Guidelines on personal data breach notification under Regulation 2016/679». 18/EN WP250rev.01. Disponible en https://bit.ly/2B7iJps.

Hamelink, Cess J. (2015). *La ética del ciberespacio*. Ciudad de México: Siglo XXI.

Hartzog, Woodrow (2018). *Privacy's blueprint: The battle to control the design of new technologies*. Cambridge: Harvard University Press.

Hutter, David (2016). «Physical security and why it is important». Information Security Reading Room. SANS Institute. Disponible en https://bit.ly/37qB3Gt.

Jijena Leiva, Renato (2002). *Comercio electrónico, firma digital y derecho: Análisis de la Ley 19.799*. Santiago: Jurídica de Chile.

Kuner, Christopher, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey y Christopher Millard (2017). «The rise of cybersecurity and its impact on data protection». *International Data Privacy Law*, 7 (2): 73-75. DOI: 10.1093/idpl/ipx009.

Laube, Stefan y Rainer Böhme (2016). «The economics of mandatory security breach reporting to authorities». *Journal of Cybersecurity*, 2 (1): 29-41. DOI: 10.1093/cybsec/tyw002.

Lehuedé, Héctor (2019). *Corporate governance and data protection in Latin America and the Caribbean*. Production Development 223 (LC/TS.2019/38). Santiago: Economic Commission for Latin America and the Caribbean (ECLAC). Disponible en https://bit.ly/2AnCoBP.

Maqueo Ramírez, María Solange, Jimena Moreno González y Miguel Recio Gayo (2017). «Protección de datos personales, privacidad y vida privada: La inquietante búsqueda de un equilibrio global necesario». *Revista de Derecho (Valdivia)*, 30 (1): 77-96. DOI: 10.4067/S0718-09502017000100004.

Muñoz Cordal, Gabriel (2016). «Normativa sobre la ficha clínica y la protección de datos de salud en Chile». *Revista de Derecho Público*, 85: 33-60. DOI: 10.5354/0719-5249.2016.44959.

Novoa, Eduardo (1979). *Derecho a la vida privada y libertad de información*. Ciudad de México: Siglo XXI.

OCDE, Organización para la Cooperación y el Desarrollo Económicos (2013). *The OECD Privacy Framework*. París: OECD Publishing. Disponible en https://bit.ly/2XWa6XY.

—. (2016). *Managing digital security and privacy risk. 2016 Ministerial meeting on the digital economy*. OECD Digital Economy Papers 254. París: OECD Publishing. DOI: 10.1787/20716826.

—. (2019). *Roles and responsibilities of actors for digital security*. OECD Digital Economy Papers 286. París: OECD Publishing. DOI: 10.1787/20716826.

Pavlovic Jeldres, Sebastián (2016). «Acceso a la información personal de salud y su protección». Superintendencia de Salud, Comisión de Salud, Honorable Cámara de Diputados. Disponible en https://bit.ly/30LZcpq.

Quezada, Flavio (2012). «La protección de datos personales en la jurisprudencia del Tribunal Constitucional de Chile». *Revista Chilena de Derecho y Tecnología*, 1 (1): 125-147. DOI: 10.5354/0719-2584.2012.24027.

Ramírez, Tomás (2016). «Nuevas tecnologías al servicio de la seguridad pública y afectación de la privacidad: Criterios de ponderación». *Revista Chilena de Derecho y Tecnología*, 5 (1): 57-86. DOI: 10.5354/0719-2584.2016.41688.

Room, Stewart (2018). «Security of personal data». En *European data protection: Law and practice* (pp. 169-194.). Portsmouth: International Association of Privacy Professionals.

Schneier, Bruce (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. Nueva York: W.W. Norton & Company.

Smedinghoff, Thomas J. (2007). «It's all about trust: The expanding scope of security obligations in global privacy and e-transactions law». *Michigan State University College of Law Journal of International Law*, 16 (1): 1-47. Disponible en https://ssrn.com/abstract=1100712.

Sotomayor Saavedra, María, Luis López Dávila, Claude Verges y Patricia Sorokin. (2014). «Ficha clínica, protección de datos y derecho a la intimidad». *Revista Redbioética*, 2 (10): 119-129. Disponible en https://bit.ly/3d4vtKM.

Sullivan, Richard J. y Jesse Leigh Maniff (2016). «Data breach notification laws». *Economic Review, Federal Reserve Bank of Kansas City,* 101 (1): 65-85. Disponible en https://bit.ly/3e4zEaN.

Tapia, Mauricio (2008). «Fronteras de la vida privada en el derecho chileno». *Revista Chilena de Derecho Privado*, 11: 117-144.

UNCTAD, United Nations Conference on Trade and Development (2019). *Digital Economy report 2019*. Ginebra: Naciones Unidas. Disponible en https://bit.ly/2XLESCI.

Vergara Rojas, Manuel (2017) «Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales». *Revista Chilena de Derecho y Tecnología*, 6 (2): 135-152. DOI: 10.5354/0719-2584.2017.45822.

Wolters, P. T. J. (2017). «The security of personal data under the RGPD: a harmonized duty or a shared responsibility?». *International Data Privacy Law*, 7 (3): 165–178. DOI: 10.1093/idpl/ipx008.

Wacks, Raymond (2015a). *Law: A very short introduction*. Oxford: Oxford University Press.

—. (2015b). *Privacy: A very short introduction*. Oxford: Oxford University Press.

Sobre el autor

Carlo Benussi Díaz es abogado. Licenciado en Ciencias Jurídicas y Sociales de la Facultad de Derecho de la Universidad de Chile. Diplomado de Postítulo en Ciberseguridad y Ciberdefensa, Universidad de Chile. Miembro colaborador de la Alianza Chilena de Ciberseguridad. Abogado del estudio jurídico Carey y Cía. Su correo electrónico es c.benussi@gmail.com. https://orcid.org/0000-0001-8745-4491.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La Revista de Chilena de Derecho y Tecnología es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

editor general
Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

sitio web
rchdt.uchile.cl

correo electrónico
rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).