REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 10 NÚM. 1 (2021) • PÁGS. 201-230 • DOI 10.5354/0719-2584.2021.58776
RECIBIDO: 30/9/2020 • APROBADO: 7/6/2021 • PUBLICADO: 30/6/2021

DOCTRINA

La responsabilidad de la Administración del Estado por incidentes de ciberseguridad

Liability of the State Administration for cybersecurity breaches

Natalia Jara Fuentealba y Antonia Jorquera Cruz
Philippi Prietocarrizosa Ferrero DU & Uría, Chile

RESUMEN El presente trabajo analiza la responsabilidad civil del Estado derivada de los daños causados a las personas por la ocurrencia de incidentes de ciberseguridad y que constituyan un incumplimiento al deber de seguridad en el tratamiento de datos personales, conforme el derecho chileno. Bajo el concepto de *falta de servicio*, se analizan los estándares de ciberseguridad que debe observar el Estado como responsable del tratamiento de datos personales, además del estándar de diligencia exigible al Estado en caso de incidentes que afecten a los sistemas informáticos utilizados para la provisión de dichos servicios públicos y que, como resultado, producen perjuicios para los titulares de datos personales.

PALABRAS CLAVE Responsabilidad del Estado, falta de servicio, ciberseguridad, protección de datos personales.

ABSTRACT This article analyses the civil liability of the State derived from damages caused to individuals by cybersecurity incidents, when they constitute a breach of the obligation of security in data processing in Chile. Under the concept of *lack of service*, this article analyzes the standards of cyber security that the State must observe as a responsible of personal data processing, the standard of diligence required in case of incidents that affect the computer systems used for the provision of public services and, as a result, causes damages to personal data holders.

KEYWORDS State liability, lack of service, cyber-security, data protection.

Introducción

En Chile, los órganos de la Administración del Estado en general, y aquellos encargados de la provisión de ciertos servicios públicos en particular, recaban, almacenan y utilizan distintos tipos de datos —en los términos de la Ley 19.628 sobre Protección de la Vida Privada—[1] de miles y millones de personas. Con la dictación de la Ley 21.189 sobre la Transformación Digital del Estado, la creciente digitalización de los procesos administrativos y de gestión de los servicios públicos es un hecho inevitable que incrementa las exigencias en relación con el tratamiento de datos personales (Boletín 11.882-06, Mensaje presidencial). Especialmente por los principios de «excepcionalidad del papel»[2] y de interoperabilidad[3] de sistemas y cooperación entre órganos, ya que esto implica, entre otras consecuencias, que el tratamiento que llevan a cabo los órganos administrativos de los datos personales de los usuarios de dichos servicios requerirá del uso intensivo y creciente de soportes electrónicos y plataformas digitales (Boletín 11.882-06), lo cual puede exponer las bases de datos que gestionan a riesgos cibernéticos que, de concretarse, pueden producir perjuicios a los titulares de los datos tratados en ellas.[4]

Frente a la existencia de riesgos cibernéticos,[5] cobra relevancia el estándar de cuidado que es exigible a los órganos administrativos tratantes de datos personales, pues de ello dependerá la configuración de un supuesto de falta de servicio ante un daño producido a los usuarios del servicio por la fuga, alteración, pérdida o mal uso de sus datos personales, obtenidos de las bases de datos de los servicios públicos, sea

1. El artículo 2, letra o) de la Ley 19.628 define el *tratamiento de datos* como «cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma».

2. El artículo 1 de la Ley 21.189 modifica el principio de escrituración de la Ley 19.880, que Establece Bases de los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado, indica: «El procedimiento y los actos administrativos a los cuales da origen se expresarán por escrito a través de medios electrónicos, a menos que se configure alguna excepción establecida en la ley».

3. Además, el artículo 1 de la Ley 21.189 introduce en la Ley 19.880 los principios generales relativos a los medios electrónicos, entre los cuales se define el principio de interoperabilidad como aquel en que «los medios electrónicos deben ser capaces de interactuar y operar entre sí al interior de la Administración del Estado, a través de estándares abiertos que permitan una segura y expedita interconexión entre ellos».

4. En el informe «Perspectivas económicas de América Latina» de la OCDE se relevó la importancia de identificar los sectores vulnerables a incidentes de seguridad digital, ya que, en la medida que aumenta la predisposición hacia economías y servicios públicos digitales, los incidentes de seguridad serán cada vez más frecuentes, y podrán ocasionar perjuicios sociales y económicos (OCDE, 2020: 23).

5. Un riesgo cibernético puede definirse como la probabilidad de que exista una amenaza accidental o intencionada como consecuencia de una vulnerabilidad particular o de un sistema de información (Jimeno Muñoz, 2019: 31). Es decir, consiste en un género que contiene distintos supuestos, como fuga de datos, destrucción de la información o ciberataques.

por acciones u omisiones, culposas o dolosas, de agentes internos o externos de la Administración.

En otras palabras, a fin de atribuir responsabilidad civil a los órganos administrativos responsables del tratamiento de datos personales frente a un evento en que se vulnere la seguridad de los sistemas informáticos de la Administración y, con ello, se generen perjuicios a los titulares de dichos datos, es necesario contar con lineamientos respecto del estándar de ciberseguridad exigible al Estado, especialmente considerando el tratamiento de datos sensibles que llevan a cabo algunos servicios públicos. Para ello, las secciones siguientes abordan ciertos conceptos básicos relativos al tratamiento de datos, los riesgos cibernéticos, ciberincidentes y ciberataques asociados a la utilización de sistemas informáticos interconectados y la ciberseguridad en general, para luego profundizar en el análisis del estándar de cuidado que debería observar el Estado en esta materia.

Tratamiento de datos personales y derecho a la privacidad

Desde junio de 2018, en nuestro ordenamiento jurídico la protección de datos personales y la autodeterminación informativa —que consiste en el derecho a «controlar la obtención, tenencia, tratamiento y transmisión de datos relativos a su persona, decidiendo en cuanto a los mismos las condiciones en que dichas operaciones puede llevarse a cabo» (Reusser Monsálvez, 2018: 53)— son derechos asegurados por la Constitución Política de la República.[6]

No obstante, la protección de datos de carácter personal, entendida como aquella protección de los individuos contra el uso o tratamiento indebido o no autorizado de su información personal por parte de terceros (Salas Retamal, 2018: 99), tiene fundamento legal expreso desde el año 1999, cuando fue publicada la Ley 19.628 sobre Protección de la Vida Privada.

Esta ley contiene una definición amplia de datos personales, caracterizados como aquellos relativos a cualquier información concerniente a personas naturales identificadas o identificables (artículo, 2 letra f).[7] Asimismo, define el tratamiento de datos personales como:

6. El derecho a la autodeterminación informativa se identifica como una respuesta jurídica a la necesidad «controlar o dar legitimidad al proceso de captura, procesamiento y transmisión de datos personales, que permitiera, por una parte, el flujo de información imprescindible para el funcionamiento de una sociedad moderna e informatizada; y, por otra, garantizara la no afectación de los derechos fundamentales de las personas» (Álvarez Valenzuela, 2020: 2).

7. Como se advierte, solo se consideran como datos personales aquellos relativos a personas naturales, por lo que la protección de la Ley no se extiende a personas jurídicas. Con todo, en este punto, cabe mencionar que existe jurisprudencia en sentido contrario, en la cual se reconoce el derecho de protección de datos personales a las personas jurídicas.

> Cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma (artículo 2 letra o).

De este modo, tanto el concepto de dato personal como el de tratamiento de datos son lo suficientemente amplios como para abarcar las múltiples actividades que los servicios públicos realizan con respecto a la información de sus usuarios, las cuales, gracias a los procesos actuales de modernización y digitalización de la Administración del Estado, son ejecutados en mayor medida por sistemas informáticos interconectados al ciberespacio.[8] Por lo tanto, para la Ley los órganos de la Administración del Estado serán responsables de bancos o bases de datos (artículo 2, letra n), porque serán quienes tomen las decisiones relacionadas con el tratamiento de los datos personales de los ciudadanos o usuarios de los servicios públicos.

Por otro lado, cabe tener presente que la Ley sobre Protección de la Vida Privada establece las reglas mínimas aplicables al tratamiento efectuado por los organismos públicos, eximiéndolos de la obligación de recabar el consentimiento del titular de los datos para efectuar su tratamiento cuando dicho tratamiento se encuentre dentro de la «esfera de su competencia» y cumpla con los demás requisitos de la Ley (artículo 20). En otras palabras, y a diferencia de las entidades de carácter privado que tratan datos personales, el Estado maneja legítimamente datos respecto de los cuales los titulares no solo no han consentido en su recolección o forma de tratamiento, sino que, incluso, pueden no tener conocimiento de su existencia.[9]

Para efectos del presente trabajo, solo se desarrollarán los problemas jurídicos que pueden originarse por una infracción a la obligación de seguridad en el tratamiento de datos personales que realiza un organismo público, establecida en el artículo 11 de la Ley, sin referirnos a eventuales problemas de ilicitud del tratamiento de datos, o el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Nuestro interés es evaluar las posibles consecuencias jurídicas que se derivan de dicha infrac-

8. El Departamento de Comercio de los Estados Unidos define *ciberespacio* como «la red interdependiente de infraestructuras tecnologías de información, que incluye internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias críticas». NIST, «Glossary», s. v. «cyberspace», disponible en bit.ly/3ja1l7K.

9. En virtud del principio de licitud en el tratamiento de datos personales, si los privados acceden a bases de datos personales sin consentimiento del titular, este tratamiento será ilícito porque no cuenta con una fuente de licitud. Sin perjuicio de ello, en la práctica existe un mercado de datos personales en el sector privado, lo cual deriva en que existan diversos supuestos en donde se efectúe un tratamiento de datos personales en desconocimiento del titular. Sin perjuicio de lo anterior, se destaca que el consentimiento no es necesario en el caso de la recolección de datos personales de fuentes de acceso público, conforme a lo dispuesto en el artículo 4, inciso quinto de la Ley.

ción, en particular la generación de responsabilidad del Estado por los perjuicios que esta infracción pueda ocasionar a los titulares de datos personales. Por lo anterior, no abordaremos otros efectos jurídicos del incumplimiento de la referida obligación de seguridad, ni aspectos como la existencia de una entidad fiscalizadora que pueda investigar y sancionar este incumplimiento.[10]

Riesgos cibernéticos y ciberseguridad

El riesgo cibernético puede definirse como aquel asociado al uso de tecnologías de información, en términos que cualquier sistema tecnológico que se encuentre conectado a otro puede verse afectado por estos riesgos emergentes, pudiendo afectar tanto intereses públicos como privados. Lo anterior es precisamente lo que hace necesario el análisis respecto a la concurrencia al daño y la distribución de responsabilidad entre los agentes participantes del ciberespacio (Jimeno Muñoz, 2017: 11).

De acuerdo con la conceptualización de Jimeno Muñoz, los riesgos cibernéticos o *ciberriesgos*: «Son los riesgos operativos ocasionados por acciones u omisiones realizadas por personas que forman o no parte de la institución afectada (*insiders* o *outsiders*) de forma voluntaria o involuntaria, conforme las siguientes características:

- *Acciones involuntarias* ejercitadas inintencionadamente como consecuencia de fallos, errores u omisiones generalmente ocasionados por quien padece el daño o forma parte de la institución afectada.
- *Acciones intencionadas* que se ejercitan de forma voluntaria y ocasionan un fraude, sabotaje, robo o vandalismo.
- *Omisiones* que pueden ser causa de la falta del conocimiento, los sistemas o las habilidades adecuadas para actuar» (Jimeno Muñoz, 2017: 25; énfasis en el original).

10. En Chile existen entidades encargadas de supervisar la ciberseguridad en el tratamiento de datos personales. Por ejemplo, en el ámbito bancario, las instituciones bancarias y compañías de seguros deben reportar incidentes a la Comisión para el Mercado Financiero; en el caso del sector eléctrico, las «entidades responsables» (empresas coordinadas y el Coordinador Eléctrico Nacional) deberán reportar al coordinador y a la Superintendencia de Electricidad y Combustibles la ocurrencia de un incidente de ciberseguridad («Estándar de ciberseguridad para el sector eléctrico», Coordinador Eléctrico Nacional, julio de 2020, disponible en bit.ly/3d9Sm2l). En el caso de los concesionarios y permisionarios de servicios de telecomunicaciones, estos deben reportar oportunamente a la Subsecretaría de Telecomunicaciones (Resolución Exenta 1.318, del 10 de agosto de 2020, de la Subsecretaría de Telecomunicaciones, que Aprueba Norma Técnica Sobre Fundamentos Generales de Ciberseguridad para el Diseño, Instalación y Operación de Redes y Sistemas Utilizados para la Prestación de Servicios de Telecomunicaciones).

Dada la amplitud de las acciones u omisiones que pueden generar amenazas a la seguridad de los sistemas de información y, eventualmente, concretarse en una fuga de datos, por ejemplo, el riesgo de ocurrencia de estas es constante y requiere de un proceso de gestión continua.[11] Por otra parte, si también se considera la gran cantidad de datos personales tratados por los organismos del Estado y la importancia estratégica que algunos de estos representan para la Administración, porque muchos fueron tratados para el adecuado funcionamiento de servicios esenciales y otras prestaciones de relevancia para la ciudadanía, resulta razonable esperar que aumente la posibilidad de que estos riesgos se concreten en acciones u omisiones que vulneran la seguridad de los sistemas de información utilizados por los organismos públicos, tanto para su funcionamiento interno como para la provisión de los servicios públicos que estos organismos están llamados a prestar. En efecto, precisamente por el valor e importancia estratégica de esta información, es posible especular que el riesgo de ocurrencia de ciberataques es más alto, en tanto dicha información puede ser de gran interés para terceros que deseen acceder a los datos personales tratados por los diferentes organismos públicos.[12]

La interconectividad de los sistemas y la globalización de las comunicaciones, con el consecuente aumento del riesgo de ataques cibernéticos, ha implicado el desarrollo y permanente actualización de protocolos y medidas de ciberseguridad en todas las organizaciones (Jimeno Muñoz, 2017: 18). Estas materias son una preocupación creciente, y los recursos y esfuerzos destinados a fortalecer la seguridad de los sistemas informáticos, tanto de entidades privadas como de organismos públicos, van en aumento.[13] La relevancia del debido resguardo de los sistemas de información de los Es-

11. En efecto, en materia de ciberseguridad, los riesgos son gestionados conociendo las amenazas y vulnerabilidades de los sistemas informáticos, mediante procesos de gestión de riesgos (López Torres, 2020: 65).

12. Como ejemplo de la importancia de los datos personales a los que se puede acceder con un ciberataque a los organismos públicos, podemos mencionar el ataque efectuado en octubre de 2020 a los sistemas informáticos de la Clave Única de la División de Desarrollo Digital. Gracias a este hecho, aumentó la preocupación por poner urgencia a los proyectos de ley sobre delitos informáticos (Boletín 12.192-25), sobre protección de datos personales que crea la nueva Agencia de Protección de Datos Personales (Boletín 11.144-07 y Boletín 11.092-07) e ingresar la nueva ley del Sistema Nacional de Ciberseguridad (Boletín 12.192-07). Discusión parlamentaria en «Hackeo a Clave Única: Demandan esclarecimiento de las circunstancias del ataque y sanciones a los responsables», Senado de Chile, 14 de octubre de 2020, disponible en bit.ly/3dc4j7X.

13. En el contexto internacional, se pueden mencionar ejemplos que demuestran el creciente interés por regular y generar estrategias de ciberseguridad. En la Unión Europa, está la comunicación de la Comisión Europea titulada «Reforzar el sistema de ciber resiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora», de 2016; la Recomendación (UE) 2019/534 sobre la «Ciberseguridad de las redes 5G», de 2019; y el nuevo Reglamento de ENISA del Parlamento Europeo y el Consejo de la Unión Europea del mismo año. En la Unión Europa, también se presentó un informe

tados resulta evidente desde el punto de vista de la seguridad nacional, por ejemplo, dada la importancia de los sistemas de información en materia de infraestructura crítica y seguridad interior y exterior del Estado (Sánchez Rojas, 2010: 140).

En efecto, en 2017, el Gobierno de Chile publicó la Política Nacional de Ciberseguridad, que tiene por objeto «desarrollar una estrategia de seguridad digital que proteja a los usuarios privados y públicos» (p. 5), apuntando a lograr un ciberespacio libre, abierto, seguro y resiliente para el año 2022.[14] Asimismo, en 2018, el presidente de la República dictó el Instructivo Presidencial 8, del 23 de octubre de 2018, a través del cual se impartieron instrucciones urgentes en materia de ciberseguridad para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado. Sin embargo, pese a dicha iniciativa, en materia de servicios públicos, y en particular respecto de la posible afectación a los usuarios titulares de datos personales, la importancia de la seguridad de los sistemas de información no ha sido un gran foco de preocupación, ni tampoco tratado de forma equitativa por todos los organismos públicos. Por el contrario, hasta la fecha, solo unas pocas instituciones —entidades fiscalizadoras en mercados regulados, como la Subsecretaría de Telecomunicaciones, la Comisión para el Mercado Financiero y la Superintendencia de Pensiones, entre otras— han dictado normas propias, relacionadas con aspectos técnicos y organizativos para abordar los riesgos en el ciberespacio y sus efectos en los datos personales de los usuarios.[15]

Sin perjuicio de lo anterior, la regulación de la ciberseguridad en el sector público chileno es escasa, aunque en la actualidad se observan esfuerzos para mejorar la regulación mediante la tramitación del proyecto de ley sobre delitos informáticos,[16]

---

sobre «Progresos realizados en la aplicación y el seguimiento de los resultados de la Cumbre Mundial sobre la Sociedad de la Información a nivel regional e internacional», en 2017.

14. En la Política Nacional de Ciberseguridad se identificaron, a nivel nacional, necesidades vinculadas con: i) resguardar la seguridad de las personas en el ciberespacio, esto es, asegurar el normal desarrollo de sus actividades personales, sociales y comunitarias, y del ejercicio de sus derechos fundamentales en el ciberespacio; ii) proteger la seguridad del país; iii) promover la colaboración y coordinación entre instituciones, organizaciones y empresas, tanto del sector público como privado; iv) gestionar los riesgos en el ciberespacio de los sistemas informáticos de distintas instituciones, organizaciones o empresas.

15. A modo de ejemplo, se pueden mencionar el «Estándar de ciberseguridad para el sector eléctrico» del Coordinador Eléctrico Nacional, del 20 de julio de 2020. Este documento tiene como objetivo proteger las instalaciones eléctricas y los activos informáticos en contra de los riesgos o ciberataques que puedan poner en riesgo la seguridad y continuidad del servicio del Servicio Eléctrico Nacional. Esta norma se encuentra disponible en bit.ly/3d9Sm2l. Por otra parte, está la «Norma técnica sobre fundamentos generales de ciberseguridad para el diseño, instalación y operación de redes y sistemas utilizados para la prestación de servicios de telecomunicaciones», de la Subsecretaría de Telecomunicaciones, del 10 de agosto de 2020, disponible en bit.ly/3xOfVG6.

16. Boletín 12.192-25, que Establece normas sobre delitos informáticos, deroga la Ley 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest, del 25 de octubre de 2018.

la dictación de normas técnicas sectoriales y el fortalecimiento del Comité Interministerial sobre Ciberseguridad.[17] Por otro lado, pese a la escasa normativa existente en esta materia, cabe destacar que los organismos públicos, al igual que actores del sector privado, suelen mantener estándares técnicos de confidencialidad de información en sistemas informáticos adecuados debido a la adopción de las normas ISO homologadas por el Instituto Nacional de Normalización (INN).[18] En este aspecto, destacan las normas técnicas relacionadas con los sistemas de gestión de seguridad de la información, gestión del riesgo de seguridad de la información; la guía de implementación del sistema de gestión de la información; y las normas de seguridad de almacenamiento, entre otras. Por lo anterior, no se debe subvalorar el aporte que las buenas prácticas de la industria han efectuado a la construcción de estándares de seguridad informática de alcance general.

Concepto de seguridad informática o ciberseguridad

La *ciberseguridad* puede conceptualizarse en términos generales como el conjunto de acciones desplegadas para la protección de la información presente en el ciberespacio (Jimeno Muñoz, 2017: 28), o en un determinado sistema informático interconectado a este, además de la infraestructura que soporta dicha información. Es decir, es la seguridad que busca proteger y garantizar la interacción entre seres humanos, entre computadores, y entre seres humanos y computadores, a partir de la protección de la información y la forma o medios de comunicarla (López Torres, 2020: 51).

En cuanto a definiciones normativas del concepto ciberseguridad, el Decreto Supremo 533, de 2015, del Ministerio del Interior y Seguridad Pública, conceptualiza la ciberseguridad 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» (artículo 1 bis). Sin embargo, este concepto ha evolucionado en cuerpos normativos más recientes. A modo de ejemplo, la norma técnica sobre los fundamentos generales de ciberseguridad en

17. Este comité fue creado por el Decreto Supremo 533 de 2015, del Ministerio del Interior y Seguridad Pública. No obstante, con el Decreto Supremo 579 de 2019, del mismo Ministerio, el comité se fortaleció creando una comisión asesora técnica, a fin de proponer el seguimiento y avance de la Política Nacional de Ciberseguridad.

18. Conforme al Reglamento del Servicio de Normalización, R307-01, el proceso normalización consiste en un conjunto de actividades efectuadas por el INN para formular, elaborar, publicar e implementar normas internacionales destinadas a establecer disposiciones para un uso común y repetido, dirigidos a la obtención de un grado óptimo de orden en un contexto determinado (por ejemplo, ciberseguridad y datos personales). «Reglamento del Servicio de Normalización», Instituto Nacional de Normalización, 24 de junio de 2019, disponible en bit.ly/3zT9rY5.

servicios de telecomunicaciones de la Subtel define la ciberseguridad como el «conjunto de acciones posibles para la prevención, mitigación, investigación y manejo de las amenazas e incidentes sobre los activos de información, datos y servicios, así como para la reducción de los efectos de estos y del daño causado antes, durante y después de su ocurrencia».[19]

A modo de referencia de la conceptualización de la seguridad cibernética a nivel internacional, el US NIST Cybersecurity Framework reconoce como elementos principales de la ciberseguridad la identificación, la protección, la detección, la respuesta y la recuperación de los sistemas. Es decir, está compuesta por un conjunto de actividades interdependientes para obtener un resultado óptimo, el cual demostrará, en caso de verificación de un incidente, que el responsable de la seguridad ha empleado un adecuado nivel de diligencia.

La identificación de los sistemas corresponde al proceso de conocimiento sobre el sistema informático, con la finalidad de advertir riesgos y asignar en forma adecuada los recursos, priorizando aquellos aspectos del sistema que se identifiquen como más vulnerables (Jimeno Muñoz, 2017: 31). En esta categoría de actividades se enmarcan las labores de *compliance* (protocolos de prevención detección y respuesta frente a riesgos derivados de incumplimiento de la regulación aplicable) respecto de aquellas entidades para las cuales existe regulación sobre seguridad cibernética.

Por su parte, la protección se refiere a la implementación de medidas concretas de seguridad de los sistemas, que habitualmente implican el desarrollo de controles de acceso a estos, monitoreo de sistemas de correo electrónico y limitación de navegación en internet a páginas seguras, implementación de softwares, e información y capacitación a las personas al interior de la organización respecto de la importancia de los protocolos de seguridad y la relevancia de las acciones involuntarias en la generación de brechas de seguridad.

La detección implica en esencia el monitoreo e identificación de posibles brechas de seguridad, así como la alerta y detección temprana de amenazas a la ciberseguridad de los sistemas. A partir de la detección, proceden las acciones de respuesta ante las ciberamenazas detectadas, en cuya implementación es especialmente relevante el tiempo de respuesta o reacción al ciberataque (Jimeno Muñoz, 2017: 32). En este sentido, tanto el elemento de detección como el de respuesta concentran la mayor importancia en términos de los efectos de la vulneración de la seguridad de un sistema, pues la magnitud del daño que el ciberataque pueda representar para dicho sistema —incluyendo la cantidad de información que pueda fugarse producto de este— depende en gran medida del tiempo que transcurra entre la detección de la brecha y la toma de medidas para anular, repeler o neutralizar el ataque (Jimeno Muñoz, 2017: 32).

19. Artículo 2 de la Resolución Exenta 1.318/2020, del 14 de agosto de 2020, de la Subsecretaría de Telecomunicaciones del Ministerio de Transportes y Telecomunicaciones.

El último elemento de la ciberseguridad corresponde a la recuperación, que abarca todas las acciones tendientes a restablecer las funciones y servicios que hayan sido afectados por un ciberataque; el desarrollo e implementación de medidas concretas de defensa a partir de la experiencia de la brecha de seguridad detectada, y la ejecución de un plan de recuperación que puede involucrar —según la entidad víctima, el tipo de ataque y la naturaleza de la información que puede haber sido comprometida— tanto la ejecución de acciones en el plano estrictamente informático, como también la toma de medidas en cuanto a comunicación del incidente, medidas de resguardo reputacional y de reparación a usuarios o clientes de la entidad, cuando se hayan visto afectados (Jimeno Muñoz, 2017: 33).

En cuanto a los efectos de un ciberataque, cabe tener presente que estos pueden ser muy diversos, según la naturaleza y finalidad del ataque. Por una parte, el impacto operativo de los ciberataques, es decir, los efectos que produce en el sistema, corresponden más comúnmente a los siguientes: i) uso no autorizado de recursos —que requieren ciertos privilegios— para impedir el acceso de los usuarios; ii) obtención de privilegios de acceso como usuario por un sujeto no autorizado; iii) obtención de privilegios de acceso como administrador del sistema por parte de un usuario; iv) uso de las vulnerabilidades de un sistema para facilitar un ataque contra otro sistema; v) instalación de programas de código malicioso (virus, *spyware*, troyano, gusanos, etcétera) y obtención de control sobre el sistema; vi) denegación del acceso a los usuarios a recursos o sistema en particular (Jimeno Muñoz, 2017: 40).

Por otra parte, el impacto de un ciberataque en la información del sistema puede implicar los siguientes efectos: i) modificación de archivos y datos; ii) prohibición de acceso a los usuarios —usualmente por modificación de contraseñas o datos de acceso—; iv) destrucción o inutilización de archivos; v) revelación de datos no autorizada, o vi) revelación de información oculta en el sistema que permite identificar sus vulnerabilidades (Jimeno Muñoz, 2017: 42).

En consideración a lo anterior, es pertinente establecer la relación entre los ciberataques y los estándares de seguridad de la información definidos, entre otras fuentes, en las normas ISO (en especial las normas ISO 27.001 y 27.002), pues es posible indicar que el elemento clave para mantener la confidencialidad, integridad y disponibilidad de la información contenida en un sistema informático —incluyendo datos personales— es la adecuada «evaluación de riesgos».[20] Para esto, se requiere sobre

20. Las normas ISO son un conjunto de normas técnicas y de seguridad que permiten orientar la gestión de una empresa en distintos ámbitos. Sin perjuicio de que su adopción es voluntaria, en el mercado son ampliamente aceptadas y han adquirido reconocimiento internacional. En materia de riesgos y seguridad informática, las normas técnicas recomiendan hacer una evaluación de los activos de información para evaluar los riesgos de la organización. De esta manera, se reconocen las vulnerabilidades y amenazas del sistema informático. Para más información, véase NCh ISO/IEC 27.701:2020, que

todo que la organización responsable del tratamiento de la información identifique en forma adecuada y suficiente los siguientes elementos: i) los activos de información de la organización, esto es, toda información de valor, incluyendo información sensible, datos personales e incluso los soporte físicos e intelectuales de la organización; ii) las vulnerabilidades de dichos activos; iii) las amenazas a dichos activos y potenciales riesgos; iv) los requisitos legales y contractuales que obligan a la organización para con sus usuarios, clientes o proveedores; v) la probabilidad de ocurrencia de cada uno de los riesgos identificados. A partir de esta identificación, la organización puede elaborar un plan de gestión de riesgos de la información.[21]

No obstante, como es posible observar, las vías por las que un ciberataque puede afectar la confidencialidad o integridad de los datos personales de los usuarios de un determinado sistema informático son múltiples. Dada la interconectividad del ciberespacio, los ataques o amenazas cibernéticas pueden afectar a las personas o usuarios en forma individual, pero también constituir una amenaza al interés público.

Cuando el ciberataque tiene por objeto la obtención de datos e información personal de ciertos usuarios de un sistema, esta afectación resulta en un daño al usuario por sí misma, por cuanto el derecho fundamental a la vida privada y el derecho fundamental a la protección de los datos personales consagrado en el número 4 del artículo 19 de la Constitución[22] se ve directamente vulnerado por el acceso no autorizado de terceros a datos personales y, en consecuencia, al derecho a la autodeterminación informativa. No obstante, la magnitud del perjuicio producido a las personas por la afectación de dicha privacidad puede ser aún más relevante en términos de intensidad y alcance del daño. Lo anterior es evidente, por ejemplo, en un caso de fuga de datos de carácter financiero de los clientes de un banco u operador o emisor no bancario de tarjetas de pago. A partir de la información financiera obtenida mediante un ciberataque a los sistemas de un banco o de dichas entidades no bancarias, los atacantes pueden realizar acciones ante la entidad bancaria como si fueran los clientes, lo que afecta directamente su patrimonio y produce, por lo tanto, un perjuicio

establece las técnicas de seguridad, extensiones ISO/IEC 27.001 e ISO/IEC 27.002 para la gestión de la información de privacidad.

21. En la norma ISO 27.001 sobre los sistemas de gestión de seguridad de la información, las actividades descritas se consideran como aspectos claves para su diseño e implementación en una organización. «¿Qué son las normas ISO y cuál es su dificultad?», ISO Tools, 19 de marzo de 2015, disponible en bit.ly/2UAXEh6.

22. Artículo 19 de la Constitución Política de la República: «La Constitución asegura a todas las personas: […] 4. El respeto y protección a la vida privada y a la honra de la persona y su familia, *y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley*» (el énfasis es nuestro). La mención a la protección de los datos personales fue agregada a este artículo por la Ley 20.050 que Consagra el Derecho a Protección de Datos Personales, publicada en el *Diario Oficial* el 16 de junio de 2018.

económico evidente a dichos clientes.

Una situación similar puede darse respecto de servicios públicos como los servicios de atención primaria de salud, el Servicio de Registro Civil e Identificación, los consultorios y hospitales públicos, el Fondo Nacional de Salud, el Instituto de Previsión Social, etcétera, en tanto la información que estos manejan respecto de sus usuarios puede ser perfectamente asociada a un individuo específico y, en gran medida, corresponde a datos sensibles.

Atendido lo anterior, a continuación, se desarrollará un panorama general de las obligaciones de seguridad de los datos personales en nuestro derecho, cómo ha interpretado la jurisprudencia dicha obligación de seguridad y cómo aplicaría dicha obligación a los organismos públicos. De esta manera, se pretende primero relacionar los conceptos de ciberseguridad, ciberataques y los datos personales, para luego desarrollar cómo este tipo de vulneraciones a la seguridad de los sistemas informáticos generarán responsabilidad para los organismos públicos que hacen tratamiento de datos personales.

Ciberseguridad y datos personales

La Ley sobre Protección de la Vida Privada establece las obligaciones de seguridad asociadas al tratamiento de datos personales sin distinguir si dicho tratamiento es realizado por una institución pública o privada. En efecto, a nivel legal es posible fundamentar la existencia una obligación de seguridad en el ciberespacio de los datos personales tratados, pese a que no está explícitamente regulado así en nuestra legislación.[23] Lo anterior es posible en virtud de lo dispuesto en el artículo 11 de la Ley, conforme al cual el responsable del tratamiento de datos personales está obligado a: i) mantener un deber de cuidado con debida diligencia y a ii) responder civilmente por los daños ocasionados (Benussi Díaz, 2020: 240). De esta manera, la Ley no establece un listado específico de infracciones ni de sanciones respecto del responsable del tratamiento de datos personales que, gracias a un acción u omisión culposa o dolosa, infrinja o vulnere la seguridad de los datos personales sobre los cuales realiza un tratamiento. Por lo mismo, es posible interpretar que cualquier vulneración a la seguridad de los datos, atribuible a la «culpa leve» del responsable del tratamiento (Jijena Leiva, 2002: 86), puede originar responsabilidad civil si dicho acto u omisión

23. Sin perjuicio de ello, cabe tener presente que el proyecto de ley que busca implementar el Convenio de Budapest sobre cibercrimen está considerando eximir de responsabilidad penal a los hackers o investigadores que encuentren vulneraciones en el sistema informático y notifiquen de inmediato a la entidad responsable para que tome las medidas correspondientes (Álvarez Valenzuela y Hevia Angulo, 2020: 1). Esta notificación no se establece para el titular de los datos personales eventualmente afectados por el aspecto vulnerable del sistema. Sin embargo, representa un avance desde el punto de vista de la obligación de seguridad que compete a la autoridad responsable del tratamiento de datos personales.

genera daños a los titulares y usuarios del sistema.

Sin perjuicio lo anterior, respecto del sector público, el Consejo para la Transparencia[24] ha interpretado que el estándar medio de diligencia establecido en el artículo 11 de la Ley se refiere a establecer «medidas de seguridad, técnicas y organizativas que garanticen la confidencialidad, integridad y disposición de la información».[25] En otros términos, si el tratamiento de datos se efectúa —como en la mayoría de los casos— en el ciberespacio, la institución u organismo público responsable del tratamiento debe adoptar todas las medidas para identificar, proteger, detectar, dar respuesta oportuna y recuperar los sistemas, así como también la información contenida en ellos, de acuerdo con los planes, protocolos y acciones mencionados en la sección anterior.

A mayor abundamiento, es importante notar que el Consejo para la Transparencia incluso ha recomendado complementar la obligación de seguridad en el tratamiento de datos personales de los órganos públicos con las medidas de seguridad establecidas en el Decreto Supremo 83, de 2004, del Ministerio Secretaría General de la Presidencia, que aprobó la norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos. De este modo, aconseja que los órganos públicos establezcan directrices generales

24. El Consejo para la Transparencia es una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio, creada por la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado. En la actualidad, la protección de datos personales, cuando su tratamiento sea realizado por organismos de la administración del Estado, es parte de su misión institucional. Sin embargo, el proyecto de ley que intenta modificar la Ley sobre Protección de la Vida Privada busca designar al Consejo como autoridad autónoma, con el objetivo de velar por el cumplimiento de la ley y con capacidad de imponer multas (Boletín 11.144-07 y Boletín 11.092-07, refundidos, artículo 30).

25. Mediante la Resolución Exenta 304, del 30 de noviembre de 2020, el Consejo para la Transparencia aprobó el texto actualizado y refundido de las «Recomendaciones del Consejo para la Transparencia sobre la protección de datos personales por parte de los órganos de la Administración del Estado».

También la Contraloría General de la República se ha pronunciado respecto del alcance de los deberes de la Administración en cuanto a protección de datos personales; sin embargo, estos dictámenes se han centrado sobre todo en la resolución del «conflicto» entre transparencia y protección de datos personales (véase, por ejemplo, el Dictamen 30.041, del 25 de agosto de 2020) y recientemente, a propósito de la contingencia sanitaria, en el alcance de la protección de datos sensibles de los funcionarios de la Administración (véase, por ejemplo, el Dictamen 37.912, del 23 de septiembre de 2020), sin abordar explícitamente la dimensión de las obligaciones de ciberseguridad del tratamiento de datos personales por parte de órganos públicos. En el Dictamen 11.171, del 5 de agosto de 2020, la Contraloría General tuvo la oportunidad de pronunciarse respecto de la obligación de seguridad que le competen a la Secretaría Regional Ministerial de Vivienda y Urbanismo de la región de Los Lagos en el uso de una plataforma virtual para una consulta pública; sin embargo, pese a que se refirió al alcance del uso de los datos personales recabados por esta repartición, no abordó en forma alguna el aspecto tecnológico asociado a una adecuada protección de dichos datos personales.

orientadoras para resguardar específicamente la seguridad de los datos personales en las que se defina un encargado y responsable de la seguridad de cada banco de datos dentro del servicio.[26]

Por otra parte, desde una mirada práctica, las medidas de seguridad, técnicas y organizativas a las que se refiere el Consejo para la Transparencia se pueden implementar mediante la adopción y certificación de las referidas normas ISO.[27] En este sentido, y dado que el objetivo de dichas normas técnicas es proteger la confidencialidad en los sistemas informáticos, esto incluye necesariamente a los bancos de datos utilizados por el respectivo organismo público para la ejecución de sus funciones, por lo cual estos estándares técnicos permiten evaluar el nivel de diligencia que ha demostrado el órgano en la adopción de las referidas medidas técnicas y organizativas.[28] Asimismo, para determinar si dichas medidas técnicas y organizativas son adecuadas para cumplir con el estándar de cuidado,[29] será necesario evaluarlas y compararlas con el estado de la técnica disponible al momento en que ocurre el incidente de se-

26. Nótese que el Consejo para la Transparencia establece que debe existir un responsable por cada banco o base de datos dentro del servicio, lo cual resulta muy exigente, considerando que la gran mayoría de los órganos del sector ni siquiera ha desarrollado o aprobado una norma técnica de ciberseguridad.

27. Por ejemplo, la norma Nch-ISO 27.001:2013, que define las «Directrices para la gestión de seguridad de la información»; Nch-ISO 27.002:2013, que establece el «Código de prácticas para los controles de seguridad de la información»; y Nch-ISO 22.301:2013, que indica los «Aspectos de la continuidad del negocio».

28. A modo de ejemplo de medidas técnicas y organizativas de seguridad de los sistemas, se pueden mencionar: i) la designación de un encargado de seguridad en la información; ii) el establecimiento de un comité de seguridad; iii) la segregación de funciones para reducir el riesgo de negligencia, mal uso o compromiso de la información de la institución; iv) la designación de un encargado del contacto con autoridades y grupos de interés —sobre todo en el caso de las instituciones obligadas a reportar a otra entidad la ocurrencia de un incidente—; v) la formalización de las responsabilidades de seguridad de la información en los contratos laborales y en los contratos con proveedores de servicios tecnológicos; vi) la identificación de activos de información de la institución y asignación de responsables, incluyendo, en este caso, la identificación de los bancos de datos personales y su naturaleza, entre otros elementos relacionados; vii) la gestión de los medios almacenamiento de la información y datos; viii) la definición de políticas para el control de acceso; ix) la definición de procedimientos de acceso y responsables del usuario con acceso al sistema de información o banco de datos; x) la definición sobre uso de controles de criptografía, anonimización u otros mecanismos para proteger los datos personales; xi) la implementación de controles contra código malicioso; xii) la seguridad de las comunicaciones; xiii) la gestión de incidentes; xiv) la seguridad en la continuidad de las operaciones; y xv) la política de privacidad y protección de datos personales, entre otras.

29. El estándar de cuidado se ha conceptualizado en materia civil como el patrón de conducta con el que se conduce «una persona diligente, caracterizada por emplear un cuidado ordinario o mediano». En definitiva, el estándar de cuidado o nivel de cuidado, exigible según lo dispuesto en el artículo 44 del Código Civil, puede ser apreciado sobre la base de dos paradigmas complementarios: i) el estándar de una persona modelo o ii) el que resulta racionalmente exigible para determinadas circunstancias (Barros Bourie, 2006: 81).

guridad —es decir, existe una obligación de actualizar y mejorar las medidas si la tecnología permite perfeccionar los estándares de seguridad—, porque las obligaciones de seguridad en el ciberespacio requieren que las medidas de prevención, detección y reacción sean constantemente revisadas y mejoradas.

Cabe destacar que, motivados por los casos *Globos*[30] y *Drones*,[31] el Consejo para la Transparencia profundizó las recomendaciones relacionadas con la obligación de seguridad en el tratamiento de datos, para el caso de los dispositivos de videovigilancia utilizados con fines de seguridad comunal y control del orden público. Luego de reconocer que las imágenes de las personas deben ser consideradas como datos personales, el Consejo para la Transparencia indica que la obligación de seguridad que tienen los municipios respecto del tratamiento de imágenes consiste en «asegurar el debido resguardo en la confidencialidad de la información». Para esto, recomienda: i) prohibir la comunicación y transferencia total o parcial, de las imágenes grabadas o captadas por los sistemas de vigilancia, exceptuándose las imágenes que han capturado un ilícito, las cuales serán entregadas a las autoridades competentes; ii) definir perfiles de acceso de las personas y funcionarios que podrán acceder y tratar las imágenes; y iii) encriptar las imágenes comunicadas, transferidas o cedidas.

En otras palabras, existen recomendaciones específicas en materia de tratamiento de imágenes por parte de municipalidades que llevan a cabo videovigilancia, las cuales pueden —y debiesen— extenderse a cualquier forma de tratamiento de datos por parte órganos públicos, no circunscribirse únicamente al ámbito municipal. A este respecto, consideramos que solo la adopción de dichas recomendaciones en forma conjunta con las medidas seguridad de la información por lo general consideradas adecuadas en las ciencias informáticas —según la cantidad, tipo de información, tamaño del sistema, y en particular su atractivo para los ciberatacantes— permitiría afirmar que dichas entidades resguardan en forma adecuada la confidencialidad, integridad y disponibilidad de toda la información que tratan, incluidos, en especial, los datos personales de sus usuarios.

Como se podrá advertir, pese a la existencia de estas dos recomendaciones del Consejo para la Transparencia, la regulación de los estándares de seguridad de la información es imprecisa e insuficiente desde el punto vista del titular de los datos

30. En este caso, las municipalidades de Las Condes y Lo Barnechea adquirieron tres globos aerostáticos equipados con cámaras de alta definición, con visión de 360 grados y capacidad para capturar imágenes de objetivos a más de 3 km de distancia. En este caso, los vecinos presentaron un recurso de protección por la eventual afectación del derecho a la vida privada, consagrado en el artículo 19, numeral 4 de la Constitución.

31. En este caso, la Municipalidad de Las Condes adquirió tres drones con cámaras de alta resolución, y con mayor capacidad de movilidad que los globos aerostáticos. Los vecinos también presentaron un recurso de protección por la eventual afectación del derecho a la vida privada consagrado en el artículo 19, numeral 4 de la Constitución.

personales que pueden verse afectados por una brecha de ciberseguridad, porque solo apuntan a sancionar a organismos que no han cumplido con el estándar de cuidado exigido por la normativa vigente. De hecho, no existe norma ni recomendación alguna que obligue al responsable del tratamiento a informar al titular de los datos personales, la ocurrencia de un ciberataque o la concreción de algún otro riesgo respecto de los datos personales tratados por el sistema informático vulnerado, por lo cual pareciera ser que una de las principales víctimas del hecho, los titulares, no han sido consideradas en las disposiciones aplicables (Benussi Díaz, 2020: 243).

En efecto, a raíz de estas deficiencias, han surgido en la doctrina distintas críticas a la normativa vigente, entre las cuales se destacan:

- No existe una obligación de actualizar o implementar medidas especiales, en virtud de la naturaleza del dato personal tratado (por ejemplo, no existe consideración especial si los datos tratados son sensibles).
- No existe una obligación de informar o reportar al titular la ocurrencia, naturaleza o medidas de mitigación en caso de una brecha de seguridad.
- Los titulares de datos personales no pueden exigir al responsable un estándar o medidas de seguridad específicas, lo cual es aún más grave si se considera que el tratamiento de datos personales por parte de organismos públicos no requiere del consentimiento ni el conocimiento del titular.
- No existe vinculación de responsabilidad o principio de seguridad, en caso de que el tratamiento se lleve a cabo por medio de un mandatario (Benussi Díaz, 2020: 244).[32]

De esta forma, con independencia de si el responsable del tratamiento de datos personales es una entidad pública o una privada, la responsabilidad civil originada por una infracción a la obligación de seguridad de los datos es difícil de atribuir bajo la Ley sobre Protección de la Vida Privada, porque el verdadero alcance de esta obligación será determinado caso a caso por un tribunal, y la ley no contempla mecanismos de protección «a todo evento» para el titular del dato personal (Benussi Díaz, 2020: 243-244).

Por consiguiente, una eventual acción de indemnización de perjuicios originada por un ciberataque que afecta datos personales, en la práctica, dependerá exclusivamente de que el responsable del tratamiento de datos le informe al titular sobre

32. Los órganos o servicios públicos, en conformidad con lo dispuesto en el artículo 8 de la Ley 19.628, podrán encargar el tratamiento de los datos a un tercero, el que tendrá la calidad de mandatario. El mandatario deberá respetar las condiciones de utilización de los datos personales encargados en el contrato de mandato. Sin embargo, para efectos de la responsabilidad en el tratamiento, el responsable del tratamiento frente a los titulares será el mandante.

la ocurrencia de dicho ataque, en tanto no existe obligación legal o contractual de efectuar esta comunicación y esta puede ser la única manera de que el titular tome conocimiento del incidente. En este sentido, el hecho de notificar al titular puede significar al órgano el ejercicio de una acción de responsabilidad en su contra que, de no haber existido dicha comunicación, probablemente no se habría ejercido.

Como se observa, pese a que la obligación de seguridad de los datos personales está presente genéricamente en nuestra legislación, en la práctica es difícil que sus titulares puedan ejercer en forma efectiva su derecho a ser indemnizados por los perjuicios que puedan derivarse de un ciberataque con resultado fuga de datos, toda vez que: i) el marco normativo no obliga al responsable del tratamiento a informarle sobre la ocurrencia de un incidente de ciberseguridad, ii) la acción de responsabilidad civil dependerá del análisis caso a caso del juez, del estándar de cuidado observado en el cumplimiento de la obligación y, sobre todo, iii) se impone al actor la carga de probar la ocurrencia y el monto de los perjuicios sufridos, aun cuando el alcance de los efectos de la brecha de seguridad no sean inmediatos o completamente conocidos por el afectado.

Por lo anterior, en los juicios en que se persiga esta responsabilidad civil siempre será un tema relevante determinar si la mera filtración o revelación de los datos personales como consecuencia de un ciberataque es suficiente para que el titular alegue la existencia de un perjuicio. A este respecto, cabe distinguir el tipo de dato personal objeto del ciberataque, ya que no es lo mismo para el titular del dato la filtración de un dato personal no sensible, que la filtración de sus datos sensibles de salud, datos biométricos, genéticos o la revelación de un dato de geolocalización. Sin embargo, en nuestro sistema jurídico esto deberá someterse al conocimiento del juez civil y se deberán analizar aspectos como la naturaleza de los datos personales afectados (esto es, si son datos sensibles, genéticos, biométricos o de geolocalización), y si es posible encontrar o extraer los datos de fuentes de acceso público, independiente de la ocurrencia de la filtración o vulneración de su seguridad. Con todo, esta materia aún es incipiente en nuestra jurisprudencia, por lo que deberemos esperar para observar cómo evoluciona el criterio judicial para la determinación y avaluación de los perjuicios en estos casos, en especial considerando que la Ley sobre Protección de la Vida Privada contempla entre los daños indemnizables tanto los perjuicios morales como los patrimoniales.

En la sección siguiente se abordarán situaciones hipotéticas en las que, a nuestro juicio, pueden darse afectaciones relevantes a la confidencialidad o integridad de los datos personales de los ciudadanos y usuarios de servicios públicos, con consecuencias dañosas importantes y masivas ante la consumación de ataques cibernéticos a los sistemas de los órganos administrativos a cargo de la provisión de ciertos servicios públicos.

Falta de servicio en el tratamiento de datos personales

Consideración previa sobre el concepto de servicio público

Antes de entrar en el análisis de los elementos de la responsabilidad del Estado y su aplicación en los ciberataques, cabe hacer presente que, a efectos de este trabajo, utilizamos la expresión *servicio público* en el sentido general que le otorga la doctrina administrativista, englobando en dicha expresión todas las actividades desplegadas por el Estado para la satisfacción de necesidades entendidas como esenciales para el funcionamiento de la sociedad (Cordero Vega, 2015: 470), al margen de la discusión —más bien política— sobre qué actividades o sectores corresponden primordialmente al Estado o a los privados y sobre la subsidiariedad del Estado respecto del desarrollo de actividades económicas. En este sentido, nos referimos a servicio público en sentido amplio, abarcando todas aquellas actividades que el Estado provee a los ciudadanos satisfaciendo, o aspirando a satisfacer, necesidades esenciales para el funcionamiento de la sociedad y el cumplimiento de ciertos mandatos constitucionales y legales. Las instituciones que hemos abordado como ejemplos en lo sucesivo han sido seleccionadas por la relevancia y sensibilidad de los datos tratados, así como de la intensidad del tratamiento de datos necesariamente efectuado para la provisión adecuada del respectivo servicio.

Dada la naturaleza de los servicios que estas instituciones ofrecen, los datos que recolectan, almacenan, transmiten y en general tratan, revisten el carácter de datos personales sensibles de acuerdo con la Ley sobre Protección de la Vida Privada. En efecto, tanto el Servicio de Registro Civil e Identificación como el Fondo Nacional de Salud (Fonasa) tratan datos biométricos de los usuarios; Fonasa, los hospitales y la red de atención primaria de salud tratan toda clase de datos referidos a las características físicas de los usuarios, a hechos y circunstancias de su intimidad, su origen racial y su estado de salud físico y síquico, incluyendo, en algunos casos, referidos a su vida sexual; el Ministerio de Educación tiene a su cargo bases de datos de información general de los estudiantes (que incluye las calificaciones de enseñanza básica y media, entre otros datos referidos a los estudiantes, docentes, padres y apoderados de los establecimientos de educación básica y media), de información recabada en el marco del Sistema de Admisión Escolar, y de estudiantes extranjeros para los procesos de validación de estudios, entre otras, que podrían ser considerados datos sensibles.

Atendido lo anterior, en la determinación de responsabilidad por infracciones a la obligación de seguridad es relevante conocer la naturaleza de los datos personales afectados por el incidente de ciberseguridad. En efecto, pese a que todos los datos personales merecen protección conforme a la normativa vigente, el estándar de diligencia exigido para los datos sensibles debiese ser más elevado, porque se trata de información que reviste un mayor grado de importancia para las personas desde el

punto de vista de su intimidad, y porque un mal uso de estos puede generar discriminaciones arbitrarias con base en sus características inherentes como raza, sexo, estado de salud, opinión política, etcétera (Garrido Iglesias y Becker Castellaro, 2017: 72).[33] En efecto, la información sensible ha sido dotada de una protección más intensa por parte del legislador respecto de otros tipos de información personal,[34] al considerarse que su valor es más alto. En virtud de lo anterior, incluso se puede presumir que el daño en caso de una incidencia de seguridad puede ser mayor respecto de los datos sensibles.[35]

La falta de servicio en la responsabilidad de la Administración del Estado

En materia de responsabilidad de la Administración del Estado,[36] el debate sobre el carácter objetivo o subjetivo de la responsabilidad del Estado resulta especialmente relevante para una aproximación a los estándares de ciberseguridad que debiesen

33. Los datos sensibles son aquéllos que en esencia están no excluyentemente vinculados a la privacidad y, por tanto, poseen una mayor potencialidad discriminatoria (Garrido Iglesias y Becker Castellaro, 2017: 72). En el mismo sentido se ha pronunciado el Consejo por la Transparencia en las recomendaciones para elevar los estándares de protección de datos personales y sensibles en organismos públicos: «En ausencia de autorización legal, los organismos de la Administración del Estado no podrán tratar datos personales sensibles, a menos que obtengan consentimiento expreso del titular o que sea necesario para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares de dichos datos» (cita de Gloria de la Fuente, presidenta del Consejo para la Transparencia, en «CPLT publica recomendaciones para elevar estándares de protección de datos personales y sensibles en organismos públicos», Consejo para la Transparencia, 9 de diciembre de 2020, disponible en bit.ly/3vV4M4P).

34. En el proyecto de ley que busca modificar la Ley sobre Protección de la Vida Privada incluso se está considerando establecer una obligación de reportar y registrar las vulneraciones a las medidas de seguridad. En la actualidad, el artículo 14 sexies indica: «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».

35. Del proyecto de ley que busca modificar la Ley sobre Protección de la Vida Privada se desprende que el resguardo que deberá tener el responsable de los bancos de datos personales sensibles será mayor por el valor de la información tratada (Benussi Díaz, 2020: 252).

36. Cuando nos referimos a la responsabilidad de la Administración del Estado, solemos comenzar el análisis con su evolución histórica en el derecho continental —y particularmente en el derecho francés—, desde la irresponsabilidad absoluta del soberano a la distinción entre acto de autoridad y acto de gobierno, para llegar a la discusión respecto de su carácter objetivo o subjetivo, entre otros elementos relevantes. En cuanto a su evolución, nos remitimos a la gran cantidad de doctrina que ha abordado esta materia, pues excede los límites de este trabajo.

observar los organismos públicos que manejan bases de datos, y aún más si aquellos datos son de carácter sensible.

Como es sabido, el sistema de responsabilidad del Estado por falta de servicio proviene del derecho francés, fundamentalmente de la jurisprudencia del Consejo de Estado, que al momento de delimitar la responsabilidad personal de los funcionarios respecto de la responsabilidad del órgano administrativo distinguió entre la falta personal (culpa del funcionario) y la falta del órgano, es decir, la falta de servicio. La «falta» se produce con independencia de la legalidad de la actuación administrativa (Cordero Vega, 2015: 656), abarcando todas aquellas circunstancias en que se configura un incumplimiento del estándar de funcionamiento normal del servicio, sea porque no funciona o porque lo hace tardía o defectuosamente, lo que produce un perjuicio al ciudadano por esta causa. Así, la falta del órgano se configura cuando el daño causado por el funcionamiento anormal del servicio no puede atribuirse a la falta o culpa de un funcionario en específico[37] y es entendida en este sistema como una especie de culpa impersonal, anónima o difusa dentro del órgano administrativo (Cordero Vega, 2015: 653).

Si bien se reconoce ampliamente la importancia e influencia del derecho francés en el derecho administrativo chileno, el desarrollo de la responsabilidad del Estado en la doctrina, y en especial en la jurisprudencia chilena, ha sido también fuertemente influenciado por el derecho español (Cordero Vega, 2015: 674). A partir de estas influencias y del desarrollo jurisprudencial de la responsabilidad de la Administración del Estado en Chile, se ha venido desarrollando el debate en la doctrina respecto de su carácter objetivo o subjetivo.

Como punto de partida, la doctrina reconoce, sin diferencias, como requisitos de procedencia de dicha responsabilidad la actuación u omisión de un órgano de la Administración del Estado y la existencia de una relación causal entre esta actuación u omisión y el resultado lesivo, el que consiste en una afectación negativa o menoscabo a los derechos de la víctima (Enteiche Rosales, 2011: 111). Dichos requisitos derivan de los artículos 38 inciso segundo de la Constitución[38] y del artículo 42 de la Ley Orgáni-

37. Además de las complicaciones probatorias de atribuir la acción dañosa a una persona en particular dentro de la organización del Estado, el Consejo de Estado también utilizó argumentos de justicia para distinguir la falta de servicio de la falta personal, por ejemplo, cuando de la naturaleza y magnitud del daño causado resultaba evidente que la capacidad de reparación pecuniaria del funcionario en cuestión era insuficiente para reparar el mal causado por su actuación culposa o dolosa. En este sentido, a propósito del caso *Laumonnier Carriol* (del 5 de mayo de 1877), Cordero Vega (2015: 654) señala: «La *falta personal* es la que conviene dejar de cargo de su autor, la *falta de servicio* es aquella que sería inconveniente o injusto de hacer soportar personalmente al funcionario».

38. Inciso segundo del artículo 38: «Cualquier persona que sea lesionada en sus derechos por la Administración del Estado, de sus organismos o de las municipalidades, podrá reclamar ante los tribunales

ca Constitucional de Bases Generales de la Administración del Estado,[39] disposiciones sobre las cuales la doctrina y la jurisprudencia han construido la responsabilidad civil del Estado.

La concurrencia o no del requisito de la culpa en la imputación de responsabilidad al Estado determina en los autores y los jueces la inclinación por definir el sistema chileno como uno de responsabilidad objetiva o como uno de responsabilidad subjetiva. En términos simplificados, el debate se ha centrado en si es suficiente para imputar responsabilidad a los órganos administrativos que se acredite la existencia del daño y la relación de causalidad entre este y la actuación del órgano en cuestión (responsabilidad objetiva) o si, además, se requiere que el daño causado por la acción u omisión dañosa sea atribuible a dolo o culpa del agente (responsabilidad subjetiva).[40]

La consideración de la responsabilidad del Estado como responsabilidad objetiva encontró su justificación en el artículo 38, inciso segundo de la Constitución, a partir del cual la doctrina construyó la noción de que la expresión *lesión* utilizada por dicha norma era evidencia de que la Constitución ponía el foco en la afectación a la víctima del perjuicio antijurídico, con independencia de la conducta de la Administración: «Bastando que exista una víctima que no esté jurídicamente obligada a soportar el daño; es decir, todo el problema de la responsabilidad o irresponsabilidad de la Administración se resuelve mediante la determinación de si la víctima se encuentra en la obligación jurídica de soportar la lesión» (Cordero Vega, 2010: 136). Así, a partir de la igualdad ante las cargas públicas y el principio de indemnidad patrimonial, puede

---

que determine la ley, sin perjuicio de la responsabilidad que pudiere afectar al funcionario que hubiere causado el daño».

39. Artículo 42: «Los órganos de la Administración serán responsables del daño que causen por falta de servicio. No obstante, el Estado tendrá derecho a repetir en contra del funcionario que hubiere incurrido en falta personal».

40. La culpa del servicio o culpa del órgano ha sido la aproximación más común a la caracterización de la responsabilidad patrimonial de la Administración como una de carácter subjetivo, y principalmente responde a la aplicación de los conceptos doctrinarios civiles de la responsabilidad, adaptados a la realidad de la organización estatal. Sin embargo, tanto la doctrina administrativista como civilista han venido revisando esta concepción y precisando sus elementos. En este sentido, es relevante la precisión efectuada por Enrique Barros respecto de la caracterización de la responsabilidad por culpa como subjetiva: «A efectos de desterrar algunos de los equívocos que han provocado infértiles confusiones conceptuales en el derecho chileno, conviene reiterar que *la culpa civil es objetiva*, en el sentido de que responde a un estándar de cuidado que prescinde del juicio moral de reproche al sujeto que incurre en responsabilidad. Por eso, es equívoca la oposición entre *responsabilidad objetiva*, que prescindiría de todo juicio de valor respecto del sujeto responsable, y *responsabilidad subjetiva*, que tendría por antecedente la culpa, porque también en esta última la valoración de la conducta se realiza de conformidad con un estándar de conducta y en consideración objetiva de las circunstancias» (Barros Bourie, 2006: 485; énfasis en el original).

determinarse si es la víctima o el Estado el obligado a soportar las consecuencias dañosas de la actividad de la Administración (Cordero Vega, 2010: 151). Esta noción, además, permite la atribución de responsabilidad por conductas lícitas, pues la ilicitud no estaría considerada como un requisito de esta, al considerarse de mayor importancia la antijuridicidad del daño, frente a la antijuridicidad de la acción u omisión causante, que predomina en el sistema de responsabilidad subjetiva o por falta de servicio. En esta construcción doctrinaria es posible reconocer la preeminencia de la influencia del derecho español con respecto al derecho francés.

Por otra parte, la responsabilidad por falta de servicio se fundamenta en el artículo 42 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado, que la menciona expresamente, aunque sin conceptualizarla ni definir criterios para su aplicación, lo que ha llevado a cuestionar que en efecto consagre un sistema de responsabilidad subjetiva.

Dado que una explicación más detallada de este debate excede el propósito de este trabajo, baste con señalar que en la jurisprudencia de la Corte Suprema se terminó por imponer la falta de servicio como criterio de imputación subjetiva de la responsabilidad de la Administración del Estado, con ciertas excepciones en materia de derechos humanos. El principal promotor de esta postura fue Pedro Pierry, quien sostenía la falta de servicio como una especie de culpa del servicio, asimilando la noción de culpa civil al no funcionamiento del servicio o su funcionamiento tardío o irregular, aplicándose, en consecuencia, las normas del Código Civil en forma supletoria (Cordero Vega, 2017: 15).[41] No obstante, algunos autores han cuestionado la asimilación entre la culpa civil y la falta de servicio, en particular debido a la importancia del principio de juridicidad de la Administración en la definición del estándar de funcionamiento del servicio, con el que por necesidad se contrasta su funcionamiento real, pues los criterios para apreciar la culpa en derecho civil no son necesariamente reproducibles para un órgano administrativo, como la «actuación del hombre prudente».

En este sentido, al construir el juez el estándar que debió haber observado el servicio en su funcionamiento,[42] atiende sobre todo al marco normativo de la actividad

41. La falta de servicio ha sido entendida por algunos autores como un factor de atribución equivalente a la culpa en la responsabilidad civil extracontractual. En opinión de Cristián Román Cordero (2012: 26): «Algunos autores no solo la califican de subjetiva, porque reconoce —por regla general— como presupuesto dicho factor de atribución, sino, también, porque le otorgan a la falta de servicio un carácter análogo a como históricamente se entendía a la culpa en la responsabilidad civil extracontractual, vale decir, como un *factor de imputación* evocador de la idea de *pecado jurídico*. Pues bien, sostenida por la defensa fiscal y acogida muchas veces por nuestros tribunales, dicha doctrina, en los hechos, ha convertido a la falta de servicio en un obstáculo insalvable, un *presupuesto diabólico*, para que dicha responsabilidad se comprometa o, si se quiere, para que el administrado lesionado sea reparado».

42. Como se evidencia, la falta de servicio es un concepto jurídico indeterminado, por lo que su apli-

y del órgano en cuestión, pues el servicio no funciona, funciona en forma deficiente o funciona en forma tardía con respecto a un estándar que está definido por la norma que le otorga competencia y define sus funciones y atribuciones, que son factores objetivos. Al mismo tiempo, la responsabilidad del Estado es subjetiva cuando el criterio de imputación predominante para la decisión del juez es la afectación o menoscabo de derechos de la víctima, pues, incluso en casos en que no existe un incumplimiento normativo propiamente tal por parte de la Administración, se considera configurada la responsabilidad del órgano administrativo por ser el causante de un daño, en tanto el estándar de cuidado —o de servicio— está dado por las circunstancias particulares del caso y los principios que pueden derivarse de las funciones y atribuciones que la Constitución y las leyes han establecido para la entidad causante del daño.[43]

Estándar de funcionamiento del servicio en materia de ciberseguridad y tratamiento de datos personales

Como se observa, la discusión entre responsabilidad objetiva o subjetiva del Estado tiende a desdibujarse en la noción de falta de servicio, pues esta última puede configurarse tanto por la infracción a determinadas normas como por la inobservancia de estándares de actuación que pueden no estar explicitados en la norma, construyéndose caso a caso por el juez. Sin embargo, hasta ahora existen escasas e insuficientes normas positivas que establecen ciertos estándares que deben observar los servicios públicos en esta materia, como el Decreto Supremo 1.299, de 2004, del Ministerio del Interior;[44] el Decreto Supremo 83, de 2004, del Ministerio Secretaría General de

---

cación al caso concreto corresponderá al juez de la causa. Así, para definir la ocurrencia de un supuesto de falta de servicio, «deberá ser el juez quien señale si un determinado hecho dañoso es o no constitutivo de ella» (Bermúdez Soto, 2002: 257).

43. En el mismo sentido, Román Cordero (2012: 27) señala: «Si bien, por regla general, la responsabilidad patrimonial de la Administración se sujeta a la ocurrencia de la falta de servicio, no por ello dicho sistema debe ser entendido como *subjetivo* y menos aún en los términos antes referidos, sino que al contrario, como *objetivado* u *objetivo*, ya que tal factor de atribución (conceptualizado como deficiente organización o funcionamiento de la Administración) y, a su vez, dicha responsabilidad se presume de la infracción por parte de la Administración de sus deberes (de cuidado o de actuación) o, bien, del daño experimentado por el administrado (o sea, sobre la base de la causalidad material)».

44. Si bien puede argumentarse que el artículo sexto de dicha norma establece a grandes rasgos un estándar de ciberseguridad, la pertenencia de un determinado servicio público a la red interconectada a la que se refiere dicha disposición es voluntaria, por lo que no hemos considerado este cuerpo normativo como un estándar por lo general obligatorio para todos los órganos de la Administración del Estado. Además, el estándar que establece no se refiere expresamente a materias de ciberseguridad, sino en forma más general a estándares técnicos. El referido artículo sexto señala lo siguiente: «Las redes interconectadas deberán operar basadas en protocolos y estándares abiertos para redes de paquetes, debiendo ser compatibles con las normas y estándares de internet protocol (IP) o aquellas que le reem-

la Presidencia,[45] e instructivos presidenciales enfocados principalmente en los ciberriesgos asociados a infraestructura crítica, a la continuidad de servicios que se brindan a través de plataformas y sistemas que hacen uso de sistemas de información y otras consideraciones de defensa nacional.[46]

En efecto, las normas técnicas de seguridad vigentes están pensadas desde el enfoque de la ciberseguridad en determinados soportes electrónicos, sin regular consecuencias especiales en caso de que un incidente afecte a bancos de datos personales con independencia del soporte electrónico en que estos se encuentren. Por ejemplo, el citado Decreto 83 establece criterios y estándares de ciberseguridad para los órganos de la Administración del Estado cuando ocurran incidentes de seguridad respecto de documentos electrónicos, y considera que el jefe del servicio imparta instrucciones para mantener la seguridad de los documentos electrónicos y sistemas informáticos, estableciendo, entre otras materias, los procedimientos para reportar incidentes de seguridad.[47] Sin embargo, estos criterios no son aplicables a situaciones en que se verifique una vulneración en bancos de datos personales que no tienen respaldo en un documento electrónico. Por esta razón, la norma no es comprensiva de todos los ciberriesgos que puedan afectar a los datos personales tratados por los órganos públicos.

---

placen. Todas las redes interconectadas deberán cumplir con las recomendaciones y estándares internacionales emitidos por ISO (International Organization for Standardization), IEEE (Institute of Electrical and Electronic Engineers de los Estados Unidos) y los estándares técnicos que en concordancia emita el Ministerio del Interior».

45. El referido decreto aprueba la norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos. Si bien establece criterios y estándares de ciberseguridad para los órganos de la Administración del Estado cuando ocurran incidentes de seguridad respecto de documentos electrónicos, estos criterios se limitan a la gestión y comunicación de documentos electrónicos, y pese a que la definición de documento electrónico que utiliza permite abarcar la mayoría de los supuestos en que podrían verse vulnerados los datos personales de los administrados, no es una norma comprensiva de todos los ciberriesgos y, dada la antigüedad de su emisión, requiere ser actualizada para reflejar plenamente la variedad de ciberriesgos que enfrentan los órganos. Asimismo, en lo que se refiere a la protección de datos personales frente a dichos riesgos, esta norma técnica tiene su foco en los documentos electrónicos producidos por los órganos administrativos, por lo que no aborda la protección de los datos personales de ciudadanos o usuarios de servicios públicos.

46. Nos referimos al Instructivo Presidencial 8, de 2018, 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, que si bien se refiere a la importancia de asegurar la integridad y confidencialidad de la información en poder de la Administración, incluyendo los datos personales de usuarios y administrados, se limita sin embargo a anunciar la actualización de normativa pertinente y la emisión de guías sobre ciberseguridad y protección de datos que, a la fecha, no han sido publicadas.

47. Artículo 20, letra d) del Decreto Supremo 83. No obstante, esta obligación no especifica a quién debe reportarse los incidentes de seguridad, y si estos incluyen los titulares de datos personales en caso de que el incidente afecte a un banco de datos.

Por otra parte, la Ley 21.180, sobre la Transformación Digital del Estado del Ministerio Secretaría, también regula en forma genérica el principio o los estándares de seguridad de las plataformas electrónicas. En efecto, introduce, como modificación al artículo 19 de la Ley de Bases de Procedimientos Administrativos, lo siguiente:

> Artículo 19. Uso obligatorio de plataformas electrónicas. Los órganos de la Administración estarán obligados a disponer y utilizar adecuadamente plataformas electrónicas para efectos de llevar expedientes electrónicos, las que deberán cumplir con estándares de seguridad, interoperabilidad, interconexión y ciberseguridad.

Sin embargo, con posterioridad establece que, mediante un reglamento dictado por el Ministerio Secretaría General de la Presidencia y el Ministerio de Hacienda, se fijarán los estándares de seguridad, funcionamiento, calidad, protección y conservación de los documentos. Por tanto, continúa pendiente la determinación de los estándares técnicos para cumplir la obligación de seguridad del artículo 11 de la Ley sobre Protección de la Vida Privada cuando los bancos de datos sean tratados por órganos de la Administración, lo que, en definitiva, permitirá a los jueces civiles construir el estándar de diligencia para el caso concreto.

Lo anterior implica, que, ante la ausencia de normas específicas que determinen un estándar de actuación respecto de la obligación de seguridad de la información y los sistemas interconectados que aborde a todos los órganos de la Administración del Estado y todas las dimensiones de sus actuaciones en el ciberespacio, el análisis para imputar responsabilidad —es decir la construcción del estándar de servicio por parte del juez— necesariamente deberá basarse en las circunstancias específicas y hechos concretos que han producido, en definitiva, el daño a la víctima, frente al deber de cuidado que correspondía a la Administración como entidad tratante de datos personales.

En este contexto, el juez que conozca la causa sobre la responsabilidad de la Administración del Estado en supuestos de incidentes de ciberseguridad que afecten a datos personales deberá recurrir a las prácticas habituales y estándares establecidos en otras actividades, o estándares de conducta para la Administración establecidos para casos específicos como la seguridad y confidencialidad de los documentos electrónicos, para determinar cuál era el estándar de cuidado razonable en las medidas de ciberseguridad adoptadas por el servicio en cuestión. Es decir, a partir de los estándares vigentes en la industria, de acuerdo con la importancia de la actividad que lleva a cabo la entidad tratante, su relevancia estratégica, su tamaño, el tipo y volumen de información que trata, etcétera, el juez deberá apreciar la culpa del servicio en abstracto, pero aplicado a las circunstancias concretas del incidente. Ello porque, en materia de seguridad cibernética, los órganos administrativos están expuestos a los mismos riesgos que cualquier otra organización, sea de carácter público o privado.

En otros términos, la falta de servicio en materia de ciberseguridad y protección

de datos personales actúa como factor de atribución general de la responsabilidad patrimonial de la Administración, en ausencia de un factor de atribución específico en las normas que determinan las funciones y atribuciones de los órganos administrativos que tratan datos personales, específicamente en aquellos casos en que las normas vigentes y recomendaciones que, en principio, permitirían al juez determinar el estándar de cuidado, no resultan suficientes para su aplicación al caso concreto debido a su especificidad o falta de actualización.

En este sentido, si bien la existencia de un instrumento normativo que expresamente establezca los elementos para construir el estándar de diligencia en el tratamiento de datos personales por organismos públicos no es en estricto rigor necesaria, es, al menos, deseable desde el punto de vista de la certeza jurídica, pues permitiría a los jueces en materia civil mantener una cierta uniformidad en los criterios utilizados para determinar dicho estándar de diligencia.

Desde este punto de vista, el Estado será responsable por los daños causados a aquellos usuarios de servicios públicos por un ciberataque cuando el servicio en cuestión no haya adoptado las medidas de ciberseguridad consideradas estándar en la industria informática, lo que, a su vez, variará en función del tipo de información almacenada y tratada en los sistemas del respectivo servicio y su atractivo para ser blanco de ciberataques. Es este sentido, el estándar de conducta no difiere sustancialmente de aquel exigido a organizaciones de carácter privado, pues el deber de cuidado se construirá a partir de los mismos elementos. A saber, el avance de las ciencias informáticas, las medidas de resguardo y los protocolos de seguridad habituales para el manejo de sistemas similares, etcétera,[48] dirigidas a cumplir con la obligación de seguridad respecto del tratamiento de datos personales.

Además de constituir una garantía para los administrados —reflejando su principio de indemnidad patrimonial—, la responsabilidad de la Administración del Estado puede analizarse desde el punto de vista del control de la gestión de los servicios públicos. De acuerdo con Cordero Vega (2015: 646):

> Desde esta perspectiva, la responsabilidad patrimonial de la Administración aparece como un principio de orden, como un instrumento más de control del poder y del buen funcionamiento de los servicios públicos que sirve para la eficiencia de la Administración, siendo un instrumento idóneo para configurar, modelar y modular la actuación administrativa que enseña a la Administración cómo debe actuar y cómo no, si quiere evitar tener que indemnizar y ayuda en última instancia a evitar daños derivados de la acción pública.

48. Cabe hacer presente que en ningún caso esta conclusión implica afirmar la supletoriedad del derecho civil al estatuto de responsabilidad patrimonial del Estado, controversia que excede el propósito y la extensión de este trabajo.

De este modo, la ocurrencia de un daño a las personas derivado de la fuga de información personal producida por un ciberataque a un servicio público en el que existió una falta de servicio, y la subsecuente persecución de la responsabilidad ante los tribunales por parte de las víctimas, producirá, al menos, la publicidad de la actuación u omisión concreta del servicio público en cuestión y de cómo ha sido en realidad su funcionamiento en materia de ciberseguridad, por lo que se produce naturalmente en la opinión pública la evaluación de la actividad desplegada por la Administración y la valoración respecto de cuál debería haber sido su estándar de funcionamiento. Ello, por supuesto, puede derivar en la activación de otras formas de control de la Administración, por lo que puede producirse como resultado un ajuste o mejora del funcionamiento de ese y otros servicios a fin de evitar incurrir en responsabilidad por este tipo de hechos.

Conclusiones

La adopción de medidas de ciberseguridad suficientes y oportunas por parte de los servicios públicos constituye una exigencia que, en la actualidad, forma parte del buen funcionamiento de la Administración del Estado. Cuando los órganos administrativos responsables de bancos de datos personales de alguna manera incumplen este estándar de ciberseguridad y producto de dicho incumplimiento la entidad sufre un ciberataque que afecta directamente el derecho a la autodeterminación informativa y protección de los datos personales, los usuarios del servicio, titulares de estos datos, pueden hacer responsable al Estado por la falta de servicio del órgano en cuestión, pues, en efecto, se ha producido un funcionamiento deficiente o subestándar del servicio que habilita la imputación de responsabilidad bajo el concepto de falta de servicio.

Los criterios para determinar el estándar de ciberseguridad que debió haber observado el órgano afectado, sin embargo, no difieren en forma sustancial de aquellos que definen el que deben observar entidades privadas en el mismo ámbito, sino que, en uno y otro caso, el juez deberá atender a la naturaleza de los datos tratados por el órgano y el atractivo de estos para potenciales ciberatacantes. En este sentido, cuando las personas ven afectado su derecho a la privacidad o a la protección de sus datos personales por una inadecuada implementación de medidas de ciberseguridad, la responsabilidad civil derivada de ciberataques debe ser construida en iguales términos para el Estado y para los privados, y son determinantes únicamente las circunstancias específicas del caso, no la calidad de ente público o privado de la organización responsable de los datos.

En reconocimiento de la ausencia de estándares reglados de ciberseguridad de aplicación general para la Administración el Consejo para la Transparencia ha precisado algunos de los elementos y herramientas que los servicios públicos deberían

adoptar con miras a disminuir los riesgos cibernéticos a los que están expuestos. Conforme con la interpretación y recomendaciones del Consejo para la Transparencia, el órgano público responsable del tratamiento de datos necesariamente debe adoptar todas las medidas de seguridad que sean pertinentes según la naturaleza de los datos personales tratados. En otras palabras, pese a que el referido Consejo recomienda la adopción de ciertas medidas técnicas y organizativas en materias de seguridad informática, la construcción del estándar de funcionamiento adecuado del servicio del que se trate en lo concerniente a la ciberseguridad y, por consiguiente, a la protección de los datos personales de los ciudadanos, debe atender a la naturaleza de los datos y del tratamiento llevado a cabo por dicho servicio, lo que equivale a reconocer que la determinación del nivel de servicio que establece el límite entre la correcta provisión del mismo y su provisión incorrecta o deficiente —es decir, que permite determinar cuándo ha habido falta de servicio— se debe realizar en el caso concreto, bajo los criterios que, desde la perspectiva de las ciencias informáticas y la industria, deberían adoptarse según las características específicas de la organización en cuestión, sus sistemas y la naturaleza de los datos que trata.

Todo lo anterior da cuenta de que en nuestro país queda bastante camino por recorrer para garantizar normativamente un adecuado nivel de ciberseguridad en el tratamiento de datos personales, ya sea en el sector público o en el privado. Por esta razón, mientras no se apruebe una nueva ley de datos personales que mejore el estándar de protección de este derecho constitucional, la regulación sectorial y las medidas que los propios organismos públicos adopten para resguardar la seguridad de sus bancos y bases de datos serán esenciales para que no le sea imputable responsabilidad al Estado por falta de servicio. A su vez, mientras no exista una norma que fije los niveles de seguridad de la información que deben adoptar las entidades públicas, que permita distinguir el nivel de diligencia exigido en virtud de la naturaleza de los datos tratados, la responsabilidad del Estado por revelación, publicación o fuga de datos personales de los ciudadanos solo podrá determinarse contrastando las medidas adoptadas u omitidas por la Administración con las prácticas generales de ciberseguridad vigentes en la industria informática y el daño causado a sus titulares.

Por lo mismo, teniendo en consideración los valores de certeza jurídica y la confianza del ciudadano en los organismos públicos, se propone que el marco normativo continúe avanzando en dirección a la construcción de un estándar de diligencia adecuado en seguridad de datos personales a nivel normativo, sin distinguir el soporte en el que se encuentre almacenado, tomando especial consideración de los perjuicios que puede sufrir un titular, según la naturaleza de los datos personales vulnerados. Esto es, mediante una determinación general en una futura «ley de ciberseguridad», complementada por las modificaciones que espera introducir el proyecto de ley sobre la protección de los datos personales.

Referencias

Álvarez Valenzuela, Daniel (2020). «La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa». *Revista Chilena de Derecho y Tecnología*, 9 (1): 1-4. DOI: 10.5354/0719-2584.2020.57777.

Álvarez Valenzuela, Daniel y Alejandro Hevia Angulo (2020). «Protección legal para la búsqueda y notificación de vulnerabilidades de ciberseguridad en Chile». *Revista Chilena de Derecho y Tecnología*, 9 (2): 1-4. DOI: 10.5354/0719-2584.2020.60658.

Barros Bourie, Enrique (2006). «Responsabilidad del Estado». En *Tratado de responsabilidad extracontractual*. Santiago: Jurídica de Chile.

Benussi Díaz, Carlo (2020). «Obligaciones de seguridad en el tratamiento de datos personales en Chile: Escenario actual y desafíos regulatorios». *Revista Chilena de Derecho y Tecnología*, 9 (1): 227-279. DOI: 10.5354/0719-2584.2020.56660.

Bermúdez Soto, Jorge (2002). «La responsabilidad extracontractual de la Administración del Estado por falta de servicio y por el daño ambiental». *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, 23: 253-264. Disponible en bit.ly/35PDq5z.

Cordero Vega, Luis (2010). *La responsabilidad de la Administración del Estado*. Segunda edición. Santiago: Abeledo Perrot.

—. (2015). *Lecciones de derecho administrativo*. Segunda edición. Santiago: Thomson Reuters.

—. (2017). «De Marín a Pierry: 20 años en el desarrollo de la responsabilidad del Estado en la Corte Suprema». En Juan Carlos Ferrada (coordinador), *Libro en homenaje al profesor Pedro Pierry* (pp. 1-21). Disponible en bit.ly/2U1HCfK.

Enteiche Rosales, Nicolás (2011). «El fundamento de la responsabilidad extracontractual del Estado administrador en Chile: Revisión de la evolución jurisprudencial (1999-2010)». *Actualidad Jurídica*, 23: 109-135. Disponible en bit.ly/3w3SGql.

Garrido Iglesias, Romina y Sebastián Becker Castellaro (2017). «La biometría en Chile y sus riesgos». *Revista Chilena de Derecho y Tecnología*, 6 (1): 67-91. DOI: 10.5354/0719-2584.2017.45825.

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

Jimeno Muñoz, Jesús (2017). *La responsabilidad civil en el ámbito de los ciberriesgos*. Madrid: Fundación Mapfre.

—. (2019). *Derecho de daños tecnológicos, ciberseguridad e insurtech*. Madrid: Dykinson.

López Torres, Jonathan (2020). *Ciberespacio & ciberseguridad: Elementos esenciales*. Ciudad de México: Tirant lo Blanch.

OCDE, Organización para la Cooperación y el Desarrollo Económicos (2020). *Pers-*

pectivas económicas de América Latina 2020: Transformación digital para una mejor reconstrucción. Disponible en bit.ly/3dbPtoZ.

Reusser Monsálvez, Carlos (2018). *Derecho al olvido: La protección de datos personales como límite a las libertades informativas*. Santiago: Der.

Román Cordero, Cristián (2012). «Responsabilidad patrimonial de la Administración por Falta de Servicio (= responsabilidad objetivada)». *Revista de Derecho Público Iberoamericano*, 1: 25-51. Disponible en bit.ly/3gXZkbY.

Salas Retamal, Andrés (2018). «Regulación de privacidad de datos *online* en Chile y Australia: Revisión crítica y desafíos futuros». *Latin American Legal Studies*, 3: 97-134. DOI: 10.15691/0719-9112VOL3A5.

Sánchez Rojas, Emilio (2010). «¿Ciber… qué? La ciberseguridad». *Ejército de Tierra Español*, 837: 136-143. Disponible en bit.ly/3vVoTNo.

Sobre las autoras

Natalia Jara Fuentealba es abogada. Licenciada en Ciencias Jurídicas y Sociales de la Universidad de Chile. Ha cursado el diplomado en Protección de Datos Personales en la Pontificia Universidad Católica de Chile y el diplomado Entendiendo China en el Instituto de Relaciones Internacionales de la Universidad de Chile. Abogada asociada del estudio jurídico Philippi Prietocarrizosa Ferrero DU & Uría en el equipo de energía, mercados regulados y TMT (tecnología, medios y telecomunicaciones). Su correo electrónico es natalia.jara@ug.uchile.cl. https://orcid.org/0000-0001-8419-6431.

Antonia Jorquera Cruz es abogada. Licenciada en Ciencias Jurídicas y Sociales por la Universidad de Chile y bachiller en Humanidades y Ciencias Sociales por la misma casa de estudios. Abogada asociada del estudio jurídico Philippi Prietocarrizosa Ferrero DU & Uría en el equipo de energía, mercados regulados y TMT (tecnología, medios y telecomunicaciones). Su correo electrónico es antonia.jorquera@ug.uchile.cl. https://orcid.org/0000-0003-2928-0563.

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).