EL MERCURIO Legal

Versión para imprimir El Mercurio.com

Telecomunicaciones y reporte de ciberincidentes: un ataque, muchas regulaciones

"...La implementación de estos deberes puede ser un desafío importante para los operadores. Estos deberán interactuar con varios órganos del Estado y titulares de datos personales. Además, algunos órganos requerirán varios reportes (...). Las regulaciones norman de manera distinta los incidentes que generan deberes de reportar, los contenidos de los informes y sus plazos, entre otras materias. Entender las acciones específicas que son exigidas por cada regulación requerirá tiempo y paciencia..."

Viernes, 13 de junio de 2025 a las 18:00

Lucas MacClure y Lucas Sierra

Como consecuencia de un cúmulo de regulaciones, los operadores de servicios de telecomunicaciones necesitan preocuparse de reportar los incidentes que afectan o ponen en riesgo su ciberseguridad. ¿Cuáles son estas reglas y cómo podría el Estado facilitar su cumplimiento?

La respuesta a los ciberincidentes es una materia de creciente importancia tanto para los operadores de telecomunicaciones como para el interés público. Casos recientes así lo demuestran. En Chile, a fines del año 2023, el operador de servicios de telecomunicaciones GTD sufrió un incidente de ciberseguridad por el ataque de un *ransomware* que afectó parte de sus plataformas. Esto significó que los sitios web de sus clientes, entre los que había algunos servicios estatales, dejaran de estar disponibles al público[1].

Otro caso se conoció en Estados Unidos el año pasado: un grupo de *hackers* accedió a sistemas informáticos de, al menos, nueve empresas de comunicaciones norteamericanas, entre ellas, proveedores de internet (ISPs) y de servicios telefónicos, como AT&T, Verizon y T-Mobile. Los *hackers* accedieron a listas de personas que eran objeto de escuchas por parte del Departamento de Justicia (con fines de contra-espionaje); asimismo, a metadatos de más de un millón de personas que trabajan en Washington D.C. (tal como sus números telefónicos). El ataque fue atribuido a un grupo de *hackers* asociados al Ministerio de Seguridad de China[2]. Un senador estadounidense se refirió al ciberincidente

como "el peor *hackeo* de telecomunicaciones en la historia de nuestra nación"[3]. Chile también es vulnerable a ciberincidentes originados en China por, entre otras razones, la proliferación en nuestro país de routers de la marca TP-Link (de origen chino).

Los ciberincidentes dirigidos a las empresas de telecomunicaciones pueden afectar la privacidad de sus usuarios y su acceso a los servicios de telecomunicaciones contratados, la reputación corporativa, la confianza pública hacia el sistema de persecución penal y su efectividad, y la contrainteligencia. Además, estos ataques pueden tener implicancias geopolíticas.

En caso de sufrir un incidente de ciberseguridad, los operadores de telecomunicaciones en Chile tienen deberes de reporte. Ello es positivo, porque la transparencia en esta materia puede contribuir a que otros operadores —y actores en otras industrias— reaccionen mejor frente a amenazas específicas. Además, la publicidad de incidentes genera riesgos para la reputación corporativa y ese riesgo es un incentivo para que los operadores mejoren sus medidas de ciberseguridad.

Ahora bien, el marco regulatorio chileno de los deberes de reporte de los operadores de telecomunicaciones es complejo y está creciendo. Veamos.

Primero, los operadores tienen deberes de reporte bajo la regulación sectorial de las telecomunicaciones. De acuerdo a la Resolución Exenta 1318, de 2020, del Ministerio de Transportes y Telecomunicaciones (RE 1318/2020 MTT), los operadores de redes y sistemas declarados como infraestructura crítica, entre otros operadores "relevantes", deben reportar ciberincidentes a la Subsecretaría de Telecomunicaciones (Subtel) y al "CSIRT de referencia" (actualmente es el CSIRT Nacional, que es parte de la autoridad de ciberseguridad, como se explica abajo; "CSIRT" quiere decir *Cyber Security Incident Response Team*). La RE 1318/2020 MTT regula los operadores obligados, tipos de incidentes que deben ser reportados, contenidos, plazos, tipos de reportes (inicial, intermedios y final), medio de comunicación y destinatarios indirectos, entre otras materias. La Subtel debe fiscalizar el cumplimiento del deber de reporte y sancionar a los infractores. Esta regulación sectorial explica que GTD, tras el ciberincidente que sufrió en 2023, haya informado "a las autoridades de la Subtel y al CSIRT, y a los cerca de 350 clientes con afectación"[4].

Además, la regulación sectorial exige que los operadores informen al Ministerio Público y eventualmente ejerzan acciones judiciales cuando "un operador detecte que sus redes y sistemas fueron utilizados como medio para la comisión de algún delito informático" (RE 1318/2020 MTT). Cumplir esta obligación supone tener en cuenta la legislación penal, en especial la Ley Nº 21.459, sobre delitos informáticos.

Segundo, los operadores deben cumplir con los deberes de reporte de la Ley Nº 21.663 Marco de Ciberseguridad (LMC) y su regulación infralegal. La LMC entró en vigencia a principios de este año; sus normas sobre reporte han sido complementadas por el Reglamento de reporte de incidentes de ciberseguridad de la Ley Nº 21.663 (Decreto 295 de 2024, del Ministerio del Interior), la Resolución Exenta 7, de 2025, de la ANCI, que regula una taxonomía de incidentes de ciberseguridad, y la Resolución Exenta 2, de 2025, del mismo órgano, que autoriza la publicidad de alertas tempranas, avisos e información sobre riesgos e incidentes de ciberseguridad.

Esta enjundiosa regulación exige que los operadores de servicios de telecomunicaciones —en tanto "servicios esenciales"— reporten ciberincidentes que puedan tener "efectos significativos". Deben reportar a la Agencia Nacional de Ciberseguridad (ANCI), específicamente a su CSIRT Nacional. Tal como ocurre en la regulación sectorial, la normativa general de ciberseguridad regula varios aspectos del deber de reporte, desde los tipos de ciberincidentes que generan un deber de reportar hasta las

sanciones aplicables a quienes omiten hacerlo.

Tercero, la futura Ley sobre Protección de Datos Personales (LPDP), que entrará en vigencia el 1 de diciembre de 2026, exigirá que los responsables del tratamiento de datos personales reporten ciberincidentes que afecten esos datos. El reporte se deberá realizar a la futura Agencia de Protección de Datos Personales (APDP) y, en algunos casos, también a los titulares. La LPDP establece cuándo se debe reportar y las sanciones por incumplimiento, pero deja otras materias sin definir, o las regula de manera vaga. Así, los plazos contenidos en el informe y otras materias necesarias para la implementación del deber deberán ser desarrollados por la APDP. Es probable que el deber sea aplicable a los operadores de telecomunicaciones, pues estos frecuentemente realizan tratamiento de datos personales en tanto responsables.

Finalmente, también es necesario tener en cuenta la regulación del mercado financiero. Esta exige que las sociedades anónimas reporten "hechos esenciales" a la Comisión para el Mercado Financiero (CMF). Hay muchos operadores de telecomunicaciones que son sociedades anónimas y se podría argumentar que ciertos ciberincidentes son hechos esenciales. Aunque el deber de estos operadores de reportar ciberincidentes a la CFM no ha sido regulado expresamente a nivel legal ni infralegal, no sería sorprendente que el reciente desarrollo de la regulación general de ciberseguridad bajo la LMC motive a la CFM a tomar cartas en el asunto respecto de las sociedades anónimas, tal como ya lo ha hecho respecto de bancos, aseguradoras y otros actores del mercado financiero.

En breve, ante un ciberincidente los operadores de servicios de telecomunicaciones pronto tendrán que prestar atención al menos a tres conjuntos de regulaciones —la sectorial de telecomunicaciones, la general de ciberseguridad y la general de protección de datos personales— con el fin de determinar si necesitan reportar incidentes y cómo cumplir con estos deberes, y, potencialmente, a la regulación del mercado financiero. Los operadores podrían verse enfrentados al desafío de reportar un mismo incidente a la Subtel, la ANCI —por la vía del CSIRT Nacional—, la APDP, los titulares de datos personales, el Ministerio Público y la judicatura penal, y la CFM.

La implementación de estos deberes puede ser un desafío importante para los operadores. Estos deberán interactuar con varios órganos del Estado y titulares de datos personales. Además, algunos órganos requerirán varios reportes: por ejemplo, la regulación contempla tres reportes para la Subtel (inicial, intermedio y final), y entre tres y cinco reportes para la ANCI (alerta inicial, segundo reporte y final, y, eventualmente, de situación en el momento y sobre plan de acción de operador de importancia vital). El total podría superar los diez reportes. Más allá del número de órganos y reportes involucrados, las regulaciones norman de manera distinta los incidentes que generan deberes de reportar, los contenidos de los informes y sus plazos, entre otras materias. Entender las acciones específicas que son exigidas por cada regulación requerirá tiempo y paciencia, y, todo esto, al tiempo que el equipo de ciberseguridad de un operador debe ejecutar acciones urgentes para contener un incidente.

¿Cómo podría el Estado facilitar el cumplimiento de los deberes de reporte de ciberincidentes de los operadores de telecomunicaciones? Se debería buscar armonizar la regulación, en la medida de lo posible. La armonización de la regulación ya está contemplada, en parte, en la LMC. Esta ley le ordena a la ANCI que se coordine con otras autoridades que son destinatarias de reportes de ciberincidentes ——como la Subtel o la APDP— para proporcionar "un sistema de ventanilla única que permita notificarlas simultáneamente" (art. 9). Respecto de otras materias, se podrían utilizar las reglas generales sobre coordinación regulatoria de la LMC (especialmente en su art. 25)[5]. Además, aquí la futura APDP puede jugar un rol importante y positivo, ella tendrá la tarea de concretizar el deber de reporte que se encuentra regulado, de manera breve y con lagunas, en la LPDP. Es recomendable que la APDP lo haga

teniendo en cuenta las regulaciones que ya establecen deberes de reporte de ciberincidentes.

** Lucas MacClure Brintrup y Lucas Sierra Iribarren son abogados y socios de Lupa Legal.*

[1] Así lo reportan dos *Alerta de Seguridad de la Información IOC Ransomware en Empresa de Telecomunicaciones*, que emitió el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) del Ministerio del Interior y Seguridad Pública, con fecha 24/10/2023, disponibles aquí y aquí. Asimismo, en su *Memoria* correspondiente al año 2023, GTD reconoce este incidente. Ver GTD, "GTD Memoria 2023", 2024, pp. 28 y 122.

[2] Sobre este ciberincidente ver David E. Sanger et. al., "Emerging Details of Chinese Hack Leave U.S. Officials Increasingly Concerned", The New York Times, 23 de noviembre de 2024, sec. U.S.; Sabrina Tavernise et al., "How China Hacked America's Phone Network", The New York Times, 12 de diciembre de 2024, sec. Podcasts; "2024 United States Telecommunications Hack", en Wikipedia, 1 de abril de 2025.

[3] Ellen Nakashima, "Top Senator Calls Salt Typhoon 'Worst Telecom Hack in Our Nation's History'", The Washington Post, 21 de noviembre de 2024.

[4] GTD, "GTD Memoria 2023", 2024, pp. 28.

[5] Sobre estas reglas de coordinación puede verse Lucas Sierra y Lucas MacClure, "Regulaciones de ciberseguridad y de telecomunicaciones: un contacto virtuoso", El Mercurio Legal, 13 de mayo de 2025.