# El panorama regulatorio cada vez más complejo de la ciberseguridad en Chile

El grave incidente de ciberseguridad que afectó a Banco Estado a principios de septiembre ha revivido las voces que —desde variados sectores— requieren de forma urgente que el Ejecutivo y el Legislativo tomen medidas tendientes a mejorar el estándar de obligaciones de ciberseguridad existente en nuestro país. En el detalle de este requerimiento se repite una consigna que ya se ha hecho costumbre al conocerse la ocurrencia de un incidente de esta clase: se debe avanzar con la tramitación y promulgación de tres iniciativas legales que son fundamentales, a saber, la nueva ley de delitos informáticos, que adecua nuestra legislación nacional al Convenio de Budapest; la nueva ley de protección de datos personales, que nos acerca a un estándar GDPR, y la anunciada nueva ley marco de ciberseguridad, que establecerá las bases de un sistema nacional de ciberseguridad. Todas estas iniciativas son sumamente relevantes en sus respectivos ámbitos y van muy en línea de lo que nuestra "hoja de ruta" en esta materia —Política Nacional de Ciberseguridad— ha dispuesto para alcanzar una infraestructura de la información robusta y resiliente que proteja adecuadamente los derechos de las personas. No obstante la trascendencia que significan estas tres normas, es importante tener en cuenta que en muy poco tiempo hemos visto cómo distintos reguladores sectoriales han utilizado sus facultades para establecer —en sus respectivas industrias— normas que promueven la ciberseguridad. Estas, de cierta manera, tratan de abordar la ausencia de disposiciones de rango legal en esta materia. En efecto, en el área de telecomunicaciones la subsecretaría del ramo (Subtel) recientemente ha publicado la norma técnica sobre fundamentos generales de ciberseguridad para el diseño, instalación y operaciones de redes y sistemas utilizados para la prestación de servicios de telecomunicaciones, que ha sido dispuesta como requisito en las bases del concurso público para la tecnología 5G (Resolución Exenta N° 1318 del Ministerio de Transporte y Telecomunicaciones del año 2020). Desde el ámbito bancario, destaca el nuevo Capítulo 20-10 de la Recopilación Actualizada de Normas (RAN) de la Comisión para el Mercado Financiero sobre gestión de seguridad de la información y ciberseguridad, que fue publicada en julio y que entrará en vigor el 1 de diciembre de este año. Esta norma se integra a los otros capítulos de la RAN ya vigentes relacionados con ciberseguridad, como el Capítulo 20-7, sobre externalización de servicios; el Capítulo 20-8, sobre incidentes operacionales, y el Capítulo 20-9, sobre gestión de la continuidad del negocio. Cabe destacar, a su vez, el nuevo estándar de ciberseguridad para el sector eléctrico, establecido por el Coordinador Eléctrico Nacional también en julio de este año, a partir de lo instruido por la Superintendencia de Electricidad y Combustible. A todo este nuevo grupo de normas debemos incluir el resto de obligaciones vinculadas con el ámbito de la ciberseguridad que ya están vigentes en nuestro ordenamiento, entre ellas, la Ley Nº 21.180 de transformación digital del Estado, el Decreto Supremo Nº 83 sobre seguridad y confidencialidad de los documentos electrónicos en la Administración del Estado, el Decreto Supremo N° 60 sobre infraestructura crítica de telecomunicaciones o el Instructivo Presidencial en Ciberseguridad Nº 8 del año 2018. Por último, no debemos olvidar otros desarrollos normativos sobre ciberseguridad que ya han sido anunciados por la autoridad y que muy probablemente verán la luz en el próximo tiempo. Por un lado, tenemos lo que ocurre en el área de pensiones, donde en agosto la Superintendencia de Pensiones inició un proceso de consulta pública destinado al establecimiento de una norma de ciberseguridad para la gestión de las AFP y la AFC, que tiene por objetivo la implementación de un sistema de gestión de seguridad y ciberseguridad por parte de estas (norma de carácter general N° 387 y 388). Por su parte, un grupo relevante de nuevos desarrollos en este ámbito fue anunciado por el Comité Interministerial de Ciberseguridad hace algunos meses atrás, donde se nombró un posible Instructivo de ciberseguridad en materia de teletrabajo; el reglamento de la Ley Nº 21.180, de transformación digital del Estado, y modificaciones a los Decretos Supremos N° 1 de 2015 y N° 93 de 2006, que mejoran los estándares de ciberseguridad de las instituciones públicas. Del escenario descrito podemos advertir que se está configurando en Chile un panorama regulatorio cada vez más complejo en materias de ciberseguridad, el que se está construyendo de normas de diverso rango legal y cuyo ámbito de aplicación y profundidad es variado. Además, en el corto a mediano plazo este panorama muy probablemente va a cambiar a consecuencia de las iniciativas ya anunciadas y, particularmente, por el avance que pueden tener la nueva ley de delitos informáticos, la nueva ley de protección de datos personales y la ley marco de ciberseguridad.Toda esta situación complejiza un entramado regulatorio que hasta hace un tiempo atrás era bastante escueto en nuestro país, no solo por la cantidad de normas de distinto rango que se están generando, sino también porque, en la práctica, tienen la potencialidad de regular temas similares de manera diferente o de forma poco coherente o compatible entre sí. A esto hay que agregar que la "ciberseguridad" es por sí un concepto de límites difusos y amplios y que, por lo tanto, puede abarcar normativa de muchos sectores que, en principio, podrían no estar muy relacionados. Por lo anterior, es necesario que las empresas, la alta gerencia y, en particular,

sus equipos de compliance y de seguridad de la información, tengan ya identificadas estas normas e iniciativas y hagan un monitoreo permanente de los cambios que vienen, de forma de hacer una adecuada evaluación de riesgos y estar preparados para adaptarse tanto en lo técnico como en lo legal. Finalmente, cabe destacar que si bien estamos de acuerdo en que se debe retomar el avance de las tres iniciativas regulatorias señaladas al comienzo de este texto, y las condiciones actuales requieren avanzar rápido, es importante que el regulador mantenga presente que cualquier premura no puede ser óbice para generar obligaciones con una pobre técnica legislativa. En esto incluimos normas que tengan potenciales contradicciones en la misma materia o, derechamente, que generen ineficiencias o gastos innecesarios que, en los tiempos que corren, podrían afectar de sobremanera a las pequeñas y medianas empresas en Chile. Estas reglas, al igual que el derecho en general, debe tener un ideal de trascendencia que mire más allá del problema y la innovación del día o, en este caso, más allá del hackeo o la vulnerabilidad de turno.

* Carlo Benussi Díaz es asociado de Carey y consejero de la Alianza Chilena de Ciberseguridad.

# El panorama regulatorio cada vez más complejo de la ciberseguridad en Chile

"...Es importante que el regulador mantenga presente que cualquier premura no puede ser óbice para generar obligaciones con una pobre técnica legislativa. En esto incluimos normas que tengan potenciales contradicciones en la misma materia o, derechamente, generen ineficiencias o gastos innecesarios que, en los tiempos que corren, podrían afectar de sobremanera a las pequeñas y medianas empresas..."

Lunes, 21 de septiembre de 2020 a las 10:47

Carlo Benussi

El grave incidente de ciberseguridad que afectó a Banco Estado a principios de septiembre ha revivido las voces que —desde variados sectores— requieren de forma urgente que el Ejecutivo y el Legislativo tomen medidas tendientes a mejorar el estándar de obligaciones de ciberseguridad existente en nuestro país.

En el detalle de este requerimiento se repite una consigna que ya se ha hecho costumbre al conocerse la ocurrencia de un incidente de esta clase: se debe avanzar con la tramitación y promulgación de tres iniciativas legales que son fundamentales, a saber, la nueva ley de delitos informáticos, que adecua nuestra legislación nacional al Convenio de Budapest; la nueva ley de protección de datos personales, que nos acerca a un estándar GDPR, y la anunciada nueva ley marco de ciberseguridad, que establecerá las bases de un sistema nacional de ciberseguridad.

Todas estas iniciativas son sumamente relevantes en sus respectivos ámbitos y van muy en línea de lo que nuestra "hoja de ruta" en esta materia —Política Nacional de Ciberseguridad— ha dispuesto para alcanzar una infraestructura de la información robusta y resiliente que proteja adecuadamente los derechos de las personas.

No obstante la trascendencia que significan estas tres normas, es importante tener en cuenta que en muy poco tiempo hemos visto cómo distintos reguladores sectoriales han utilizado sus facultades para establecer —en sus respectivas industrias— normas que promueven la ciberseguridad. Estas, de cierta manera, tratan de abordar la ausencia de disposiciones de rango legal en esta materia.

En efecto, en el área de telecomunicaciones la subsecretaría del ramo (Subtel) recientemente ha publicado la norma técnica sobre fundamentos generales de ciberseguridad para el diseño, instalación y operaciones de redes y sistemas utilizados para la prestación de servicios de telecomunicaciones, que ha sido dispuesta como requisito en las bases del concurso público para la tecnología 5G (Resolución Exenta N° 1318 del Ministerio de Transporte y Telecomunicaciones del año 2020).

Desde el ámbito bancario, destaca el nuevo Capítulo 20-10 de la Recopilación Actualizada de Normas (RAN) de la Comisión para el Mercado Financiero sobre gestión de seguridad de la información y ciberseguridad, que fue publicada en julio y que entrará en vigor el 1 de diciembre de este año. Esta norma se integra a los otros capítulos de la RAN ya vigentes relacionados con ciberseguridad, como el Capítulo 20-7, sobre externalización de servicios; el Capítulo 20-8, sobre incidentes operacionales, y el Capítulo 20-9, sobre gestión de la continuidad del negocio.

Cabe destacar, a su vez, el nuevo estándar de ciberseguridad para el sector eléctrico, establecido por el Coordinador Eléctrico Nacional también en julio de este año, a partir de lo instruido por la Superintendencia de Electricidad y Combustible.

A todo este nuevo grupo de normas debemos incluir el resto de obligaciones vinculadas con el ámbito de la ciberseguridad que ya están vigentes en nuestro ordenamiento, entre ellas, la Ley Nº 21.180 de transformación digital del Estado, el Decreto Supremo Nº 83 sobre seguridad y confidencialidad de los documentos electrónicos en la Administración del Estado, el Decreto Supremo N° 60 sobre infraestructura crítica de telecomunicaciones o el Instructivo Presidencial en Ciberseguridad Nº 8 del año 2018.

Por último, no debemos olvidar otros desarrollos normativos sobre ciberseguridad que ya han sido anunciados por la autoridad y que muy probablemente verán la luz en el próximo tiempo. Por un lado, tenemos lo que ocurre en el área de pensiones, donde en agosto la Superintendencia de Pensiones inició un proceso de consulta pública destinado al establecimiento de una norma de ciberseguridad para la gestión de las AFP y la AFC, que tiene por objetivo la implementación de un sistema de gestión de seguridad y ciberseguridad por parte de estas (norma de carácter general N° 387 y 388).

Por su parte, un grupo relevante de nuevos desarrollos en este ámbito fue anunciado por el Comité Interministerial de Ciberseguridad hace algunos meses atrás, donde se nombró un posible Instructivo de ciberseguridad en materia de teletrabajo; el reglamento de la Ley Nº 21.180, de transformación digital del Estado, y modificaciones a los Decretos Supremos N° 1 de 2015 y N° 93 de 2006, que mejoran los estándares de ciberseguridad de las instituciones públicas.

Del escenario descrito podemos advertir que se está configurando en Chile un panorama regulatorio cada vez más complejo en materias de ciberseguridad, el que se está construyendo de normas de diverso rango legal y cuyo ámbito de aplicación y profundidad es variado. Además, en el corto a mediano plazo este panorama muy probablemente va a cambiar a consecuencia de las iniciativas ya anunciadas y, particularmente, por el avance que pueden tener la nueva ley de delitos informáticos, la nueva ley de protección de datos personales y la ley marco de ciberseguridad.

Toda esta situación complejiza un entramado regulatorio que hasta hace un tiempo atrás era bastante escueto en nuestro país, no solo por la cantidad de normas de distinto rango que se están generando, sino también porque, en la práctica, tienen la potencialidad de regular temas similares de manera diferente o de forma poco coherente o compatible entre sí. A esto hay que agregar que la "ciberseguridad" es por sí un concepto de límites difusos y amplios y que, por lo tanto, puede abarcar normativa de muchos sectores que, en principio, podrían no estar muy relacionados.

Por lo anterior, es necesario que las empresas, la alta gerencia y, en particular, sus equipos de *compliance* y de seguridad de la información, tengan ya identificadas estas normas e iniciativas y hagan un monitoreo permanente de los cambios que vienen, de forma de hacer una adecuada evaluación de riesgos y estar preparados para adaptarse tanto en lo técnico como en lo legal.

Finalmente, cabe destacar que si bien estamos de acuerdo en que se debe retomar el avance de las tres iniciativas regulatorias señaladas al comienzo de este texto, y las condiciones actuales requieren avanzar rápido, es importante que el regulador mantenga presente que cualquier premura no puede ser óbice para generar obligaciones con una pobre técnica legislativa. En esto incluimos normas que tengan potenciales contradicciones en la misma materia o, derechamente, que generen ineficiencias o gastos innecesarios que, en los tiempos que corren, podrían afectar de sobremanera a las pequeñas y medianas empresas en Chile. Estas reglas, al igual que el derecho en general, debe tener un ideal de trascendencia que mire más allá del problema y la innovación del día o, en este caso, más allá del *hackeo* o la vulnerabilidad de turno.

** Carlo Benussi Díaz es asociado de Carey y consejero de la Alianza Chilena de Ciberseguridad.*

*Análisis jurídico*

Portabilidad financiera y subrogación
**Hernán Corral**
"...Si entendemos la subrogación de la portabilidad financiera como una forma especial de pago por subrogación, podemos concluir que el art. 14 inc. 2º se aplica, pero con la restricción prevista en el art. 18, es decir, en cuanto los términos no sean más gravosos para los terceros garantes, incluyendo el monto del crédito. El mismo criterio debiera aplicarse a las garantías con cláusula de garantía general..."

Demasiada información
**Iñigo de la Maza**
"...La justificación de los deberes de información suele radicarse en la autonomía de las personas (...) A veces, debiésemos ocultarle información porque eso mejorará su bienestar. Por supuesto, el problema es cómo hacer eso y mantener la caja de Pandora del paternalismo jurídico cerrada o, al menos, únicamente entreabierta..."

Miel de Abejas, Miel de Ulmo, Miel Gibson ... camino a "NotMiel"
**Cristóbal Porzio**
"...Todo emprendedor y gerente debiera tener siempre muy claro que, junto con un nuevo producto, se debe pensar muy cuidadosamente en una buena marca, creada y no copiada, además de registrarla, no solo para ser puente entre productor y consumidor, sino que para que en ella se capitalice el esfuerzo enorme que conlleva emprender y lanzar nuevos productos al mercado..."

Caso fortuito, imposibilidad y distribución de riesgos
**Lilian San Martin**
"...La conjugación de las reglas del caso fortuito, con la consecuente imposibilidad sobrevenida del cumplimiento en forma exacta, íntegra y oportuna de la prestación, y las reglas de la llamada teoría de los riesgos, resulta indispensable para comprender cabalmente los efectos del caso fortuito no solo en la relación obligatoria, sino, de manera más amplia, en la relación contractual..."

Luces y sombras de la portabilidad financiera
**Jaime Alcalde**
"...Son muchas las cuestiones de interés, puesto que envuelve aspectos de derecho civil, de consumo, bancario y registral, y donde las realidades de los clientes son muy distintas (...) Desde 2017 se discute una profunda reforma a la institucionalidad sobre protección de datos personales, que debe ser un complemento necesario de esta y otras iniciativas. Sin embargo, no ha tenido avance..."

Ver más

Comentarios Recientes

**Pablo Alarcon** Excelente columna del maestro Nasser
Prexistencias y seguros de salud: falta certeza jurídica para aseguradoras y asegurados · 3 días

**Pablo Fuenzalida** Muy buena columna Álvaro. Interesante tu propuesta de vincular ética jurídica o profesional de la abogacía con las clínicas jurídicas en general y no tan solo respecto de aquellas orientadas a la...
Qué debemos enseñar en las facultades de Derecho y, en especial, el rol en ellas de la Argumentación y la Ética Jurídica · 6 días

**Ricardo Bravo** En este caso los señores Diputados, debieran acusar constitucionalmente al Sr. Ministro, pero como no es mediático el tema, prefieren hacer caso omiso a tan grave denegación de justicia.
Corte eleva a cuatro meses suspensión de ministro Poblete y pide trasladarlo de Santi · 1 semana

**Sebastian Sn** muy buena observación
La (di)símil concepción de la Corte Suprema sobre el control de convencionalidad · 1 semana

**Ronnie Alvear** Felicitaciones profesora, gran valor!!!
Asume nueva directora de la Escuela de Derecho de la U. Finis Terrae · 1 semana

Más Comentados

**Qué debemos enseñar en las facultades de Derecho y, en especial, el rol en ellas de la Argumentación y la Ética Jurídica**
1 comentario · 6 días atrás

**Corte eleva a cuatro meses suspensión de ministro Poblete y pide trasladarlo de Santiatrás**
1 comentario · 1 semana atrás

**Asume nueva directora de la Escuela de Derecho de la U. Finis Terrae**
1 comentario · 1 semana atrás

**El proyecto de ley que suspende los embargos: un adefesio jurídico**
2 comentarios · 2 semanas atrás

**La nueva imagen de las SPAC como vehículo de inversión alternativo**
1 comentario · 2 semanas atrás

Ranking de Comentadores

**Rafael Vargas** · 38 comentarios
**Francisco Balart** · 34 comentarios
**Mario Herrera** · 34 comentarios
**Francisco Castillo** · 32 comentarios
**Rafael Gomez** · 30 comentarios