REVISTA
DE DERECHO ECONÓMICO

VOL. 82 NÚM. 2 (2025) • PÁGS. 55-77 • DOI 10.5354/0719-7462.2025.80599
RECIBIDO: 7/9/2025 • APROBADO: 8/12/2025 • PUBLICADO: 31/12/2025

ARTÍCULOS

Cloud computing y derecho: Notas sobre el nuevo marco jurídico para la migración a la nube de las instituciones financieras

Cloud computing and law: Notes on the new legal framework for financial institutions' cloud migration

Renato Jijena Leiva
Pontificia Universidad Católica de Valparaíso, Chile

RESUMEN Este artículo analiza el paso desde la subcontratación tecnológica tradicional hacia la computación en la nube en el sector financiero chileno y el nuevo marco jurídico que condiciona dicha migración. Con base a la normativa de la Comisión para el Mercado Financiero (capítulos 20-7 y 20-10 de la Recopilación Actualizada de Normas de Bancos) y de las leyes 19628 (reformada en 2024), y 21663 sobre ciberseguridad, se examinan los requisitos habilitantes, los análisis de riesgos y las evaluaciones de impacto en protección de datos personales que deben preceder a la externalización de servicios críticos en plataformas en la nube, gestionadas en mercados altamente concentrados por gigantes tecnológicos. El trabajo aborda, además, el debate sobre la *territorialización* de datos y la localización de infraestructuras a partir del pronunciamiento de la Fiscalía Nacional Económica y del Tribunal de Defensa de la Libre Competencia sobre cláusulas de territorialidad en servicios de nube para el Estado. Finalmente, se estudia el régimen de responsabilidad y solidaridad legal del artículo 15 bis de la Ley 19628 entre bancos responsables del tratamiento y proveedores de nube como encargados, enfatizando los escenarios de brechas de ciberseguridad y los altos costos operativos y sancionatorios asociados. La hipótesis central sostiene que una migración a la nube sin diligencia debida en ciberseguridad y protección de datos genera un entramado de responsabilidades administrativas y civiles para las instituciones financieras y sus proveedores.

PALABRAS CLAVE Computación en la nube, instituciones financieras, ciberseguridad, datos personales, Comisión para el Mercado Financiero.

ABSTRACT This article analyzes the shift from traditional technological outsourcing to cloud computing in the Chilean financial sector, as well as the new legal frame-

work governing such migration. Based on the regulations issued by the Financial Market Commission (chapters 20-7 and 20-10 of the Updated Compilation of Banking Regulations) and on Laws 19628 (as amended in 2024) and 21663 on cybersecurity, the study examines the enabling requirements, risk assessments, and data protection impact assessments that must precede the outsourcing of critical services to cloud platforms, which are managed in highly concentrated markets by major technology companies. The article also addresses the debate on data territorialization and infrastructure localization, drawing on the opinions issued by the National Economic Prosecutor's Office and the Competition Tribunal regarding territoriality clauses in cloud services provided to the State. Finally, it examines the liability regime and statutory joint and several liability established in Article 15 bis of Law 19628 between banks acting as data controllers and cloud providers acting as processors, with particular emphasis on cybersecurity breach scenarios and the significant operational and sanction-related costs involved. The central hypothesis argues that migration to the cloud without due diligence in cybersecurity and data protection gives rise to a complex framework of administrative and civil liabilities for financial institutions and their service providers.

KEYWORDS Cloud computing, financial institutions, cybersecurity, personal data, Financial Market Comission.

Introducción

Frente a la evolución tecnológica de las modalidades de gestión financiera, que ha incorporado a los operadores bancarios en el ámbito de la computación en la nube *(cloud computing)*, la migración desde la subcontratación tradicional *(outsourcing)* hacia ecosistemas oligopólicos de la nube es una realidad. Dicha transformación ha sido abordada por diversas normas jurídicas, cuya fiscalización corresponde a nuevas entidades, y que este estudio se propone sistematizar.

En un contexto mayor, y disruptivo, sobre la regulación jurídica del desarrollo tecnológico,[1] la posibilidad de que una corporación, un servicio público, una empresa de tecnología financiera y ahora un banco, opten por contratar a terceros para la gestión externalizada de las actividades o las funciones que les son propias es una opción practicada desde hace años, pero no en la modalidad de computación en la nube. Dicha externalización responde a diversas causas: incapacidad de asumirlas directamente, querer contar con una mayor eficiencia técnica derivada del análisis económico de sus costos de transacción y para no encarecerlos, o por la especializa-

1. Temas como el manejo de volúmenes masivos de información *(big data)*, la externalización de servicios (en modalidad de computación en la nube), el concatenamiento de información estructurada y gestionada en bloques *(blockchain)*, la gestión de la seguridad de información sin conexión, de la ciberseguridad en línea y la reingeniería (o transformación digital) corporativa, obedecen a un desarrollo tecnológico y jurídico que no está exento de conflictos.

ción de las funciones o servicios encargados (por ejemplo, cobranzas, marketing, *call center*, proveedor de nube, etcétera).

Esta modalidad contractual de prestar servicios en forma electrónica, telemática o digitalmente, a distancia y entre ausentes, siempre se ha enfrentado con al menos cuatro elementos que cuestionan el modelo de la nube. Las robustas y extensas eximentes contractuales de responsabilidad frente a pérdidas de información o una brecha o incidente de ciberseguridad;[2] la exigencia (no cumplida) de que los servicios se presten territorialmente localizados y no descentralizados o en servidores ubicados fuera del país del usuario; que los marcos contractuales se rijan por normas de derecho comparado, mediando prórrogas de derecho aplicable y de jurisdicción, hace que analizar qué normas de derecho civil y de contratos locales les serían aplicables,[3] sea un ejercicio teórico y carente de interés jurídico; y la inevitable aplicación del instituto de la adhesión contractual ante la desigualdad negociadora de las partes, salvo que el cliente que contrata la migración a la nube tenga la envergadura necesaria para pactar modificaciones, por ejemplo, aminorar las eximentes de responsabilidad.[4]

No obstante, la cultura económica y la praxis de la gestión financiera con base en los contratos de subcontratación tecnológica ha cambiado durante los últimos años. Inicialmente solo era una técnica de gestión empresarial usada para externalizar procesos mediante sistemas informáticos a un agente económico especializado. Luego, al aparecer internet, fue implementada de la mano de sistemas de centros de datos *(data centers)*, mediante contratos de alojamiento web y de alojamiento de infraestructura web (bajo el concepto de servicios web), y, actualmente, con los ecosistemas de computación en la nube o de *cloud computing*, que se han instalado como «la modalidad de externalizar» o la tecnología que llegó para quedarse. En este sentido, se alude directamente a la nube como la evolución de la subcontratación tradicional (Mata, 2021: 223). Ahora bien, no hay que olvidar que esta información es gestionada oligopólicamente por proveedores que son gigantes tecnológicos, lo que también se ha cuestionado jurídicamente.[5]

2. La Ley 21663 define incidente de ciberseguridad como todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.

3. La opción contraria, y que ahora se consigna, se puede ver en Severín (2020).

4. Porque si quien externaliza en el sector público es el Servicio de Impuestos Internos, o en el sector privado una compañía transnacional de seguros, el proveedor de la nube debería abrirse a la revisión de su andamiaje contractual.

5. Amazon ha enfrentado demandas relacionadas con presuntas prácticas anticompetitivas como las presentadas por la Comisión Federal de Comercio de Estados Unidos en 2023, por uso de poder monopólico en el comercio minorista y conductas exclusorias; la demanda en México por cláusulas abusivas contra un vendedor; y una acción en Chile por el TDLC debido a exigencias en la adjudicación de servicios de nube.

En este trabajo nos convoca un tema revisado por el Tribunal de Defensa de la Libre Competencia (TDLC) y sobre el cual la Fiscalía Nacional Económica (FNE) ha manifestado su opinión, ya que la externalización contractual con sede en la nube se proyecta a diversos ámbitos, lo que implica que existirán diversos marcos jurídicos aplicables (generales, particulares o sectoriales) para el uso de la nube. Por ejemplo, se ha regulado expresamente en otras jurisdicciones como la Ley de *Cloud*, en Aragón, España, de 2023; se ha habilitado y recomendado, mediante la formulación de directrices, desde la administración de la plataforma de Compras Públicas del Ministerio de Hacienda como el caso de Chile; o se ha regulado y condicionado desde la Comisión para el Mercado Financiero (CMF) como ocurrió en 2017 cuando se modificó la norma 20-17 de la Recopilación Actualizada de Normas de Bancos (RAN).

Jurídicamente, entre las muchas tensiones inherentes al uso de sistemas en la nube,[6] esta investigación presenta como hipótesis de trabajo lo que se debe implementar con base en los capítulos 20-7 y 20-10 de la RAN, en razón de las nuevas exigencias de ciberseguridad y de la aplicación de la modificada Ley de Protección de Datos Personales, las leyes 21663 y 19628, respectivamente, al proyectarse las categorías de la nube para la migración de instituciones financieras.

Particularmente, respecto de la ciberseguridad y, en la medida que la migración a la nube involucre el tratamiento de datos personales de cuentacorrentistas y tarjetahabientes, la pérdida de su control efectivo y las posibles brechas y sanciones serán de un alto costo operativo. Lo anterior, especialmente si no se ha cumplido con: i) las exigencias de auditoría al proveedor; ii) la doble exigencia normativa para el cumplimiento de deberes de confidencialidad;[7] iii) la necesidad de realizar una evaluación de impacto previa a la migración;[8] iv) la obligatoriedad de celebrar un contrato de encargo de tratamiento, muy lejano a un simple contrato de mandato general; v) las exigencias para adoptar medidas técnicas y administrativas de ciberseguridad tras-

6. Algunas serían: i) la provisión de servicios vulnerándose las normas de libre competencia; ii) las exigencias para externalizar el tratamiento de datos personales; iii) la externalización en el sector público; iv) el uso de modelos de nube para el licenciamiento de programas de computación; v) las exigencias de ciberseguridad; y, v) el uso de sistemas de nube en la banca, en las empresas de tecnología financiera y en las compañías de seguros.

7. Doble, en primer lugar, por la exigencia general de confidencialidad del actual artículo 7 de la Ley 19628 y, en segundo lugar, por las obligaciones de secreto y de reserva bancaria que establece el artículo 154 de la Ley General de Bancos, alusivas a que las instituciones financieras deben mantener la confidencialidad de los depósitos y de las captaciones de sus clientes.

8. La nueva Ley de Protección de Datos Personales establece la obligatoriedad de realizar evaluaciones de impacto en protección de datos cuando se identifiquen tratamientos de datos de alto riesgo, como los que involucren el uso de nuevas tecnologías, la recopilación masiva de datos o el tratamiento de datos sensibles, y es la forma en que una organización puede probar que ha evaluado y gestionado adecuadamente los riesgos de la vulneración de la integridad, la confidencialidad o la disponibilidad inherentes a sus operaciones.

pasadas al proveedor de la nube en calidad de mandatario del banco mandante; vi) el cumplimiento de las exigencias del nuevo artículo 15 bis, bajo apercibimiento de surgir responsabilidades legales solidarias para el encargo de tratamiento de datos personales; y, vii) los ineludibles procesos de certificaciones, sea con base en estándares de mercado como las normas ISO 27001 y siguientes o en conformidad a los que haya definido la Agencia Nacional de Ciberseguridad.[9]

El análisis, o la hipótesis de trabajo, busca mostrar que pueden surgir múltiples responsabilidades si la externalización no se verifica con la diligencia debida o con la adopción de medidas de ciberseguridad, respetándose las restricciones de la Ley de Protección de Datos Personales. Un ejemplo es la generación de una brecha de seguridad en la banca, en los sistemas de la matriz internacional de una filial bancaria nacional donde la responsabilidad, partiendo de la base de un consentimiento mal otorgado para migrar la información a sistemas de la nube instalados fuera de Chile, será exclusiva de la corporación que decidió migrar la información a los servidores de la nube de su matriz y fuera del país de residencia de sus clientes.

En 2026 todo este andamiaje regulatorio se activará con la concurrencia de cuatro órganos posibles legitimados para fiscalizar y sancionar: la Agencia Nacional de Ciberseguridad,' la nueva Agencia de Protección de Datos Personales, la Comisión para el Mercado Financiero y el Servicio Nacional del Consumidor, de la mano de posibles acciones colectivas.

Conceptos, características y clasificaciones de los sistemas de computación en la nube

La computación en la nube se define como un modelo de prestación de servicios de carácter tecnológico que hace posible el acceso bajo demanda, mediante la red, a un conjunto de recursos de carácter compartido (López, 2013: 694). Podemos definir a la nube como una infraestructura computacional que permite que los usuarios accedan de manera remota y bajo demanda a sus productos y servicios computacionales, por ejemplo, correos electrónicos empresariales, páginas web, sistemas de ofimática y espacios de almacenamiento, sin la necesidad de que sean propietarios de servidores locales ubicados dentro del territorio nacional del consumidor o usuario, o arrendatarios corporativos de un centro de datos.

9. El artículo 8 alude a deberes específicos de los llamados operadores de importancia vital y dispone que todos deberán, en primer lugar, implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar los riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional del servicio; en segundo lugar, la certificación de sus planes de continuidad operacional o ciberseguridad; y, en tercer lugar, en conformidad al artículo 28, deberán obtener otras certificaciones de ciberseguridad que señala la ley y las que determine la Agencia mediante reglamento.

Los servicios de la nube se basan en una arquitectura cliente-servidor donde internet es el canal principal y permiten al proveedor tecnológico hacerse cargo de mantener sistemas y arquitecturas, ofrecer servicios y recursos informáticos bajo demanda (hardware, software, datos, correos, etcétera) con prescindencia de una arquitectura tecnológica determinada, de recursos físicos propios como un centro de datos y de un espacio físico para ubicarse. La ganancia para el cliente, usuario o consumidor viene de la facilidad de conectarse y acceder a los servicios, en base a sus necesidades reales para procesos tecnológicos. En esencia hay *escalabilidad* y *pago por uso* porque los recursos o servicios se obtienen en un momento determinado y en forma permanente (24/7), y porque el pago al proveedor es concreto y proporcional al uso.

El ecosistema de las plataformas de la nube se caracteriza por la externalización de grandes volúmenes de información para hacer más ágiles las labores de almacenamiento y procesamiento de datos y documentos. Así, quedan de lado, presionadas por las diferencias de costos con el uso externalizado de centros de datos tradicionales, las dudas o reservas respecto a la viabilidad de confiar las aplicaciones a proveedores de servicios, pues conllevan una dependencia de terceros y una cierta intangibilidad en las garantías de seguridad, confidencialidad, disponibilidad e integridad de los datos si son personales.[10]

Las proyecciones del ecosistema de la nube son diversas. El mercado de servicios de computación en la nube se ha consolidado como una industria presente en la vida cotidiana,[11] por lo que el giro comercial de los proveedores de la nube constituye una parte esencial de la economía digital, se diferencian de las formas de gestión de almacenamiento y procesamiento de información anteriores y permiten utilizar funcionalidades para almacenar información de forma colaborativa.

En un entorno de computación en la nube la gestión de la información estaría, de forma virtual, en manos y bajo la responsabilidad del cliente que contrata los servicios de la nube (similar a la antigua idea de los contratos de alojamiento de infraestructura web), que la maneja a través de internet accediendo, por ejemplo, a soluciones o herramientas de bases de datos, de correo electrónico, o de cualquier tipo de aplicaciones de acuerdo con sus necesidades.[12]

---

10. Boletín e-Gobierno Red de Líderes de Gobierno Electrónico de América Latina y el Caribe, «E-gobierno en la nube», Red Interamericana de Gobierno Digital, octubre de 2016, p.2, disponible en https://tipg.link/mbjL.

11. CeCo UAI, «Mercado del *cloud computing*: El nuevo estudio de la Autorité francesa», *Centrocompetencia.com,* 5 de julio 2023, disponible en https://tipg.link/m8lq.

12. En función del modelo utilizado los datos pueden no estar realmente en manos del contratista porque el mantenimiento y la gestión del soporte físico, de los procesos y de las comunicaciones pueden encontrarse en manos de terceros subcontratados. Sobre la deslocalización, que es esencial e inherente a los servicios de la nube, se nota en que un proveedor puede operar desde, prácticamente, cualquier lugar del mundo.

Lo más relevante, desde el punto de vista jurídico y contractual, es la determinación de las responsabilidades de las partes. En principio, el prestador de servicios que asume el cumplimiento del contrato para que su contraparte contractual externalice la gestión, el procesamiento, el tratamiento si se trata de datos personales o el almacenamiento de información y documentos, debiera asumir la mayor carga de responsabilidades. Sin embargo, es común que estos contratos se estipulen haciendo aplicación de la autonomía y de la libertad contractual, pero jurídicamente cuestionables, incluyendo cláusulas eximentes de responsabilidad robustas y radicales.

Respecto a la externalización de servicios se argumenta que no se puede realizar sin una previa clasificación de los activos de información, no solo digitales o informáticos,[13] y concurrentes, porque al identificarlos y clasificarlos con una organización concreta se puede comprender mejor su valor y su impacto en el negocio.[14] Esto es importante, tanto en los entornos tradicionales como en la nube o en los servidores de la nube, y en estos últimos la clasificación de activos lo es aún más, porque son entornos complejos y siempre más dinámicos que los tradicionales.[15] Cuando se trabaja en migración a la nube hay que considerar las posibles vulnerabilidades de los sistemas y aplicaciones instalados en entornos que suelen ser más complejos que los tradicionales y más difíciles de proteger.[16] En efecto, solo una vez que se hayan clasificado los activos se puede desarrollar un plan de acción para mitigar el riesgo que debe incluir medidas concretas como la implementación de controles de seguridad, mecanismos de autenticación (para asegurar el origen legítimo de la gestión de clientes y empleados), bases de datos, etcétera.

Clasificaciones conceptuales y esenciales

Las tecnologías en la nube ofrecen tres modelos de servicios que en el ecosistema no han cambiado por años. El primero se denomina «software como servicio» y al cliente o usuario se le da la posibilidad de que las aplicaciones que su proveedor su-

13. La Ley 21663 de Ciberseguridad los define como toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.

14. Diego Ferruz R., «La importancia de clasificar los activos en la nube», *Trendtic.cl*, 21 de noviembre 2023, disponible en https://tipg.link/mE6o.

15. Los activos en la nube pueden estar distribuidos en varias regiones y plataformas e incluso pueden estar en distintos proveedores de nube (es el caso del llamado *multicloud*), lo que dificulta su seguimiento y protección.

16. El artículo 2 de la Ley 21663 define una vulnerabilidad como la debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas. Dentro de las más comunes que pueden surgir, entre otros, durante la migración a la nube se incluyen, i) la «inatención a los activos», o el olvidarse de algunos activos; cabe revisar y evitar que no existan ii) configuraciones incorrectas (por ejemplo, cuando una contraseña débil permite que se acceda a un recurso y se use como bisagra para llegar a otros activos más críticos); o iii) una falta de supervisión.

ministra corran en una infraestructura en la nube (Joyanes, 2012: 40), y se accede al servicio contratado a través de un proveedor que asume el alojamiento, hospedaje, mantención y seguridad de la aplicación.[17] El consumidor no maneja o controla la infraestructura de la nube subyacente, incluyendo la red, servidores, sistemas operativos, etcétera y el modelo ofrece a los clientes beneficios como la reducción de costos en hardware y software (pago por uso), conectividad en cualquier momento y lugar (mediante conexión internet). En este caso, todo el soporte, actualizaciones y mejoras están controladas por el proveedor.

La segunda se denomina «plataforma como servicio» y permite a los inscritos desplegar aplicaciones propias, adquiridas o desarrolladas por el propio usuario en la infraestructura de la nube de su proveedor, el cual ofrece la plataforma de desarrollo y las herramientas de programación. El cliente tiene un control parcial sobre las configuraciones del entorno y las aplicaciones, ya que la infraestructura y recursos siempre dependen del proveedor que las despliega. En base a ello «desde el punto de vista de la seguridad, esta es compartida entre el proveedor y el cliente, aunque las aplicaciones desarrolladas o alojadas en la plataforma contractualmente corren por parte o son responsabilidad del cliente» (Quiroz, 2016: 11) o mandante que contrata la externalización.

Por último, está la llamada «infraestructura como servicio», donde el proveedor ofrece al usuario recursos, es decir, infraestructura computacional (capacidad de almacenamiento, procesamiento o comunicaciones) y, además, le entrega al cliente la libertad de poder realizar cualquier acción como si se tratara de una infraestructura propia, como tener servicios corriendo, desarrollo de aplicaciones, alojamiento, almacenamiento de datos, servicios de correos, etcétera, sin la necesidad de preocuparse por la gestión de los servidores físicos. Por lo tanto, la «finalidad de este servicio es evitar la compra de infraestructura por parte de los clientes, buscando reducir costos de equipos, mantención y personal de tecnologías de la información, dado que todo esto es proporcionado por la empresa proveedora» (Quiroz, 2016: 12).

En cuanto a las formas de desplegar y operar una estructura en la nube, es decir, las modalidades de implementación de computación en la nube, la clasificación estandarizada distingue según el control y la gestión que exista de los entornos informáticos y nos centraremos en cuatro tipos: nube pública, privada, comunitaria e híbrida.[18]

17. Así, por ejemplo, el sistema de nube lo puede ofrecer Amazon Web Services y Telefónica la operatoria concreta.

18. Estas categorías fueron definidas por Peter Mell y Timothy Grance en el documento «The NIST definition of cloud computing» del National Institute of Standards and Technology, septiembre de 2011, disponible en https://tipg.link/mE8G.

Con la nube privada la infraestructura es proporcionada para el empleo exclusivo de una organización madre que comprende a múltiples consumidores o unidades de negocio, la que puede ser poseída, manejada o administrada por la organización, por un tercero, o por alguna combinación de ellos. En una nube pública, la infraestructura es proporcionada para el empleo abierto a cualquiera, sin exclusividad, y la plataforma de la nube puede ser poseída, manejada o administrada por una empresa, institución o una organización del gobierno, o alguna combinación de ellos.

Cuando se alude a una nube comunitaria, la infraestructura es proporcionada para el empleo exclusivo de una comunidad de usuarios específica que se ha organizado para servir a una función o propósito común; se puede tratar de una o varias organizaciones, pero que comprendan objetos comunes como su misión, políticas, seguridad o necesidades de cumplimientos regulatorios. Por último, estamos ante una nube híbrida cuando la infraestructura es una composición de dos o más infraestructuras de nube distintas (privada, comunitaria o pública) que pueden ser, a su vez, propias, compartidas o públicas, permitiendo portar datos o aplicaciones entre ellas.[19]

Prerrequisitos para la migración a la nube y exigencias en materia de riesgos y protección de datos personales

Si para el sector público las restricciones al migrar a la nube son esenciales, para las instituciones financieras se debieran seguir criterios similares. En el caso de Chile un enorme caudal de datos personales son tratados con sistemas de *big data* o de manejo de volúmenes masivos de información. Un ejemplo es el caso de la pretendida externalización de la gestión de los pasaportes o documentos públicos de identidad por el Servicio de Registro Civil hacia los sistemas y servidores en línea de una empresa estatal china, y que, desde diciembre de 2026, estarán sujetos por ley a evaluaciones de impacto y sancionados en caso de que no se cumpla con ellas.

Esto demuestra cómo, a pesar de estar involucrados derechos fundamentales, se desarrollan regularmente tratamientos o cesiones de datos personales sin evaluaciones de impacto previas, sin competencias legales expresas, sin la verificación del ámbito del tratamiento, por ejemplo, con la participación de un encargado y cesionario y sin que se contemplen estándares idóneos de protección de datos personales o, al menos, sin la habilitación previa de una autoridad de control y de protección de datos personales.

19. Técnicamente con la combinación de ambas estructuras se puede mantener la alta seguridad de una nube privada y, al mismo tiempo, aprovechar la escalabilidad y los recursos bajo demanda de una nube pública para momentos de sobrecarga.

Las exigencias del capítulo 20-7 de la Recopilación Actualizada de Normas de Bancos

El capítulo 20-7 de la RAN alude ampliamente a las contrataciones por parte de las instituciones bancarias de proveedores de servicios externos para que realicen una o más actividades operativas, las cuales podrían ser también efectuadas internamente por la entidad con sus propios recursos, tanto humanos como tecnológicos. Atendido lo anterior, sus disposiciones no son aplicables a servicios que una entidad no puede proveerse a sí misma, como servicios básicos o aquellos donde una ley ha definido que deban ser prestados por entidades de giro exclusivo.

Esto habilita a los bancos a externalizar servicios como el procesamiento de datos y almacenamiento en la nube, no solo en un proveedor de la nube, sino también en una empresa de tecnología financiera. La externalización de servicios también se ve afectada por riesgos estratégicos, reputacionales, de cumplimiento, de país, de concentración y legal, entre otros, sobre todo porque los contratantes tienen la libertad de seleccionar para el almacenamiento de datos una nube pública, privada o un híbrido de las dos, dependiendo de sus necesidades.

En general, permite establecer controles permanentes, asegurar el cumplimiento de compromisos con los clientes y realizar auditorías independientes; establece que se deben exigir informes periódicos de auditoría interna por parte del proveedor, documentación actualizada de los procedimientos, consideración de los riesgos en las cadenas de servicios externalizados, y especificaciones claras en los contratos respecto a responsabilidades y obligaciones en caso de subcontratación; señala qué deberá incorporar el banco en sus reportes de riesgo operacional, información sobre la gestión de riesgos de externalización, incluyendo cambios relevantes y exposición a servicios críticos; y dispone que los datos y tecnologías utilizadas en la externalización se deben ubicar en sitios de procesamiento específicos y en una jurisdicción definida y conocida.

Los imprescindibles análisis de riesgos y las evaluaciones de impacto en función a la Ley 19628, modificada en 2024

Una evaluación de impacto consiste en un análisis de riesgos que se realiza en el momento previo a la implementación de un tratamiento de datos personales, especialmente cuando este implica su comunicación a los servidores de una empresa proveedora de servicios en la nube. Dicho análisis se efectúa desde la fase de diseño del tratamiento y permite establecer medidas técnicas y organizativas adecuadas para prevenir, mitigar o reducir los efectos de eventuales incidentes.

Una evaluación de impacto en la protección de datos y la gestión del riesgo son actividades integradas, la primera forma parte indivisible de la gestión de riesgos y se

debe ejecutar en el marco de la misma. Una evaluación de impacto será obligatoria cuando exista una probabilidad de alto riesgo en el tratamiento de datos personales. En tales casos, se trata de un proceso que amplía los requisitos de la gestión del riesgo, debe traducirse en acciones positivas para la implementación de medidas y garantías para la gestión del riesgo y, además, constituye una herramienta para demostrar cumplimiento normativo.

El ya referido artículo 15 ter de la modificación a la Ley de Protección de Datos Personales refiere a la evaluación de impacto en sede de protección de datos personales. Es un supuesto esencial de procedencia que dispone que, cuando sea probable que en un tipo de tratamiento que por su naturaleza, alcance, contexto, tecnología utilizada o fines, pueda producir un alto riesgo para los derechos de las personas titulares de los datos personales, el responsable del tratamiento deberá realizar (es un imperativo) una evaluación del impacto previo al inicio de las operaciones del tratamiento.

Despejando dudas interpretativas, se dispone que la evaluación de impacto en la protección de datos se requerirá siempre en casos de: i) evaluación sistemática y exhaustiva de aspectos personales de los titulares de datos, basada en el tratamiento o decisiones automatizadas, como la elaboración de perfiles, y que produzcan en ellos efectos jurídicos significativos; ii) tratamiento masivo de datos o gran escala; iii) tratamiento que implique observación o monitoreo sistemático de una zona de acceso público; y iv) tratamiento de datos sensibles y protegidos especialmente en las hipótesis de excepción del consentimiento.

Restricciones a la deslocalización de los datos: Los criterios de la Fiscalía Nacional Económica

En 2017 la CMF cambió el criterio de los borradores de la nueva norma RAN 20-7 que, inicialmente, exigía la operación no deslocalizada (con base en servidores instalados en un solo territorio) solo mediante servidores instalados en Chile.[20] A la fecha de escritura de este artículo, la norma *territorializa* la gestión externalizada cuando señala que los datos, plataformas tecnológicas y aplicaciones a utilizar en la externalización de los servicios, «deben encontrarse en sitios de procesamiento específicos y para el caso de procesamiento en el extranjero, en una jurisdicción definida y conocida».[21]

20. Antes de su aprobación como norma de la RAN, y en el marco de una consulta pública, en 2017 la industria de proveedores —agrupados gremialmente en la Asociación Chilena de Empresas de Tecnologías de Información o como empresa Microsoft en particular— planteó diversas consideraciones que la autoridad acogió.

21. Además de la jurisdicción se debe conocer la ciudad donde operan los centros de datos.

Para esto sirve comparar con el debate generado para los servicios públicos. El tema que convoca son las exigencias a los proveedores de operar con servidores localizados o con centros de datos instalados localmente. Si se trata de externalizar la gestión pública a servidores de computación en la nube, en el Estado ha existido conformidad solo con liberar una guía de recomendaciones no obligatorias y depender de un instructivo presidencial general de 2018,[22] lo que ha significado permitirse exprofeso, al no regular legalmente, que la información de los chilenos se gestione y almacene masivamente en servidores deslocalizados fuera del país.

Si se legislara, por ejemplo, para exigir que se encripten todos los tratamientos de datos personales en los servicios públicos, la primera consecuencia sería mantener la exigencia de que se opere solo con servidores ubicados dentro del territorio de Chile y que contractualmente no se acepten eximentes de responsabilidad. Es, por cierto, una postura diametralmente opuesta a la de los proveedores comerciales de la nube como Microsoft, Amazon o Google, donde lo más seguro es que el debate se desarrolle de la misma manera en que esas empresas agrupadas en los gremios de la industria de tecnologías de la información y la comunicación, que se levantaron para objetar y establecer que no se exigiera un criterio de territorialidad.[23]

En los convenios de colaboración celebrados entre el Gobierno de Chile y empresas de gigantes tecnológicos proveedoras, como Amazon Web Services (AWS),[24] se ha recurrido al TDLC para consultar sobre algunas licitaciones en las que se exige tener centros de datos fijos localizados en el país ya que, según la empresa, con esta opción se le excluiría arbitraria e injustificadamente de participar.

En efecto, en el escrito presentado a fines de 2023, de conformidad a lo dispuesto en los artículos 18-2 y 31 del Decreto Ley 211 de 1973, se solicitó iniciar un procedimiento no contencioso con el objeto de que se resolviera si era o no contrario a la libre competencia que los órganos de la administración del Estado puedan exigir que la infraestructura o los datos deban ubicarse en territorio chileno en contrataciones de servicios de «infraestructura como servicio en nube pública» a efectuarse bajo el Convenio Marco 2239-5-LR22 de la Dirección de Compras y Contratación Pública.[25]

22. Véase *Instructivo presidencial 1: Uso de servicios de la nube*, Secretaría de Gobierno Digital, 12 de enero 2018, disponible en https://tipg.link/mB6b.

23. De eso se trata una política de Estado, de ponderar, de tratar de equilibrar y, de no poder hacer algo, de optar sobre las condiciones de orden público que permitirán a los operadores económicos autorizados a contratar servicios de nube al momento de legislar, porque en Chile una mera política de recomendaciones no es un aporte regulatorio al gobierno. Mirando al derecho comparado, el estudio de la Ley *Cloud* de Aragón, aprobada en 2023, podría generar alguna sorpresa intelectual que ayude a construir una política de Estado real en cualquier país de Latinoamérica.

24. «Amazon inicia su expansión en Chile y firma acuerdo con el Ministerio de Hacienda», *Diario Financiero*, 2 de marzo 2017, disponible en https://tipg.link/mBD5.

25. Disponible en https://tipg.link/mEEI.

El TDLC, por resolución de 4 de enero de 2024, dio inicio al procedimiento contemplado en el artículo 31 del Decreto Ley 211 en autos caratulados «Consulta sobre si la exigencia de territorialidad de la infraestructura o datos en Chile por parte de los órganos públicos bajo convenio marco de la Dirección de Compras y Contratación Pública es o no acorde con la normativa de libre competencia» bajo el rol C 526-23. La magistratura ordenó oficiar a diferentes organismos a fin de que estos, así como quienes tuvieran interés legítimo, aportaran antecedentes dentro del plazo de veinte días hábiles contados desde la publicación en el *Diario Oficial*. Con base en la solicitud de AWS y la información que se aportara en el proceso, el TDLC resolvería si era o no contrario a la libre competencia que en esas contrataciones de «infraestructura como servicio» los órganos de la administración del Estado pudieran exigir que la infraestructura o los datos deban ubicarse en el territorio chileno, en el contexto de las compras públicas a efectuarse bajo el convenio marco.

Al respecto, los criterios informados por la FNE son relevantes por ser los primeros emanados de un ente fiscalizador y porque afectan a las instituciones financieras. En el contexto de la libre competencia, la entidad concluye que las restricciones de territorialidad no tienen el potencial de afectarla porque permiten el concurso de varios proveedores en igualdad de condiciones, y analiza la industria de los servicios en la nube. En su razonamiento, la FNE considera que para determinar si las restricciones de territorialidad establecidas infringen o no el Decreto Ley 211, se debe considerar la jurisprudencia sobre los requisitos que deben verificarse para que las condiciones sobre bases de licitación o solicitudes de cotización puedan ser consideradas contrarias a esa normativa, las cuales califica de consistentes:

> Las solicitudes de cotización de los órganos del Estado para la adquisición de servicios de nube pública abren un proceso competitivo entre las empresas adjudicadas, de la misma forma en que cualquier licitación pública lo haría para los oferentes de un determinado bien o servicio, por lo que los criterios jurisprudenciales para analizar licitaciones públicas son aplicables de forma equivalente a las cotizaciones (FNE, 2024: 10).

La FNE concluye que dichos requisitos no concurren en forma copulativa, a saber: i) que el órgano cotizante cuente con poder de compra en el mercado relevante del producto que se pretende adquirir; ii) que las exigencias puedan o tiendan a alterar el proceso competitivo del mercado en el cual se enmarca la licitación; y, iii) que las exigencias no tengan una justificación objetiva o razonable (FNE, 2024: 10-11).

Las conclusiones del informe pueden resumirse en lo siguiente: «Las restricciones de territorialidad establecidas por los órganos de la administración del Estado en la adquisición de servicios de nube no tienen el potencial de afectar la libre competen-

cia» (FNE, 2024: 18);[26] en segundo lugar, «conforme a los antecedentes recabados por la Fiscalía, tanto de organismos públicos sectoriales, como de empresas de la industria, la exigencia de territorialidad de la infraestructura y de los datos podrían justificarse por razones de latencia, de sensibilidad de la información que se quiere almacenar, y de ciberseguridad»; y en tercer lugar una recomendación, más bien obvia, que dice:

> Con todo, atendiendo a la necesidad de que se fomente la rivalidad entre los oferentes en los procesos de licitación y los procesos competitivos como los que se abren con las cotizaciones en el Convenio Marco 2022, es necesario recomendar a los servicios públicos que las exigencias técnicas que se establezcan, entre ellas, la de territorialidad, sean adoptadas en virtud de antecedentes que las justifiquen (FNE, 2024: 18).

Sin embargo, porque la recurrente optó por accionar caso a caso o licitación a licitación de cada servicio público, por resolución de 22 de mayo de 2024, y a petición de la consultante, el TDLC tuvo por retirada la consulta.[27] Ahora bien, los medios de prensa cubrieron el caso a nivel nacional e internacional y catalogaron la acción, apuntando a lo esencial del modelo, como «una estrategia en la batalla por la territorialidad de la nube».[28]

El cumplimiento diligente de las exigencias de ciberseguridad

Un elemento o eje transversal a todo ámbito donde se celebren contratos de computación en la nube, además de la eventual responsabilidad por la prestación de servicios con negligencia de los proveedores de nube, son las exigencias de seguridad y, muy especialmente, de ciberseguridad que se le deben imputar o exigir al proveedor.

Dicha ciberseguridad es desarrollada por la norma RAN 21-10 de la CMF y regulada por la Ley 21663, para los activos de información en general, y la Ley 19628, bajo apercibimiento de multas, para el activo de información datos personales o nominativos, que están a cargo o son tratados por los responsables de datos personales, de forma personal o mediando encargos de tratamiento. Además, es necesario entender o visualizar dos contextos. Uno, el de la responsabilidad de la institución financiera que opta por externalizar o migrar a la nube sin las prevenciones necesarias o en forma negligente y, por otro lado, el de la eventual responsabilidad contractual del proveedor de servicios de nube.

---

26. Agrega el informe que «lo anterior, debido a que no se cumple ninguno de los tres requisitos copulativos establecidos por el Honorable Tribunal para que las bases de licitación infrinjan el Decreto Ley 211».

27. Véase la resolución en https://tipg.link/mBYA.

28. «Amazon Web Services busca pronunciamiento sobre cláusula de territorialidad de servicios cloud de Chile», *Americaeconomia.com*, 9 de enero 2024, disponible en https://tipg.link/mBZK.

Por cierto, si los sistemas del proveedor de nube son accedidos dolosamente (léase hackeados) podrá imputarse una responsabilidad personal y penal al sujeto activo del ilícito, pero esta arista no eludirá la imputación y la posible determinación de algún grado de falta de diligencia previa, por ejemplo, por no haberse encriptado o anonimizado la data de los clientes del banco, tanto por el responsable de datos personales, como por su encargado de tratamiento, mandatario y proveedor comercial de nube.

Adicionalmente, se puede pensar en las eventuales responsabilidades que podrían surgir en materia civil, por ejemplo, contractual o extracontractualmente. Así, en el caso de que el proveedor de servicios de la nube en una relación de empresa a empresa esté domiciliado legalmente en Chile y mantenga contratos con clientes o proveedores, ante un ciberataque o un incidente de ciberseguridad que le impidan que asuma sus obligaciones, será responsable civilmente por los daños y perjuicios causados si se acredita su negligencia al momento de prevenir en sede de ciberseguridad la diligencia del servicio que presta. De igual manera, podría ser responsable derivado de un hecho ilícito (extracontractualmente) cuando, sin existir un contrato previo, la responsabilidad derive, por ejemplo, de un ciberataque que cause daños a terceros, sin haberse adoptado preventiva y diligentemente medidas de seguridad,[29] o porque se produce una filtración de datos personales. Ambas, ejemplos de casos reales, podrían generar responsabilidad civil por daños morales o patrimoniales a los afectados.[30]

A esta fecha, la premisa de análisis sostiene que el cumplimiento de las medidas de ciberseguridad no es una decisión libre y que, conforme a la disciplina de la gestión de vulnerabilidades, está muy lejos de ser solo un problema tecnológico. La RAN número 20-10 alude expresamente a la gestión de seguridad de la información y ciberseguridad. El concepto base de trabajo de estas normas dictadas por el fiscalizador es el Sistema de Gestión de la Seguridad de la Información, un conjunto de diversos componentes para la prosecución de un fin específico que, proyectado a diversos ámbitos (bancario, de salud, previsional, tributario, etcétera), siempre mantendrá las mismas características esenciales. Cualquier opción en materia del Sistema de Gestión de la Seguridad de la Información de la banca o las entidades financieras siempre debe tener en consideración el cumplimiento de estos estándares mínimos, estando los esenciales ya recogidos.

Por lo mismo, son disposiciones basadas en buenas prácticas (léase, estándares) que deben ser consideradas como lineamientos mínimos a cumplir por las entidades

29. Sería el caso de implementar protocolos de respuesta o políticas frente a incidentes porque la gestión de un ciberataque siempre requiere de acciones inmediatas para detener la intrusión y contener los daños.

30. Véase el artículo 23 de la Ley 19628 de 1999, vigente hasta fines de 2026, disponible en https://tipg.link/mBcI.

para la gestión de la seguridad de la información y ciberseguridad, que son conceptos de diverso alcance.[31] Para la correcta contextualización de la norma, se define que la debida adhesión a los lineamientos dispuestos será parte de la evaluación de gestión que se realiza a los bancos en el ámbito de sus riesgos operacionales, atendiendo al volumen y complejidad de sus operaciones.

Respecto a la prevención de fraudes, el artículo 4.2 de la RAN número 1-7 decreta una carga de gestión que establece que los bancos:

> Deberán contar con sistemas o procedimientos que permitan identificar, evaluar, monitorear y detectar en el menor tiempo posible aquellas operaciones con patrones de fraude, de modo de marcar o abortar actividades u operaciones potencialmente fraudulentas, para lo cual deberán establecer y mantener, de acuerdo a la dinámica de los fraudes, patrones conocidos de estos y comportamientos que no estén asociados al cliente.[32]

Entre los puntos que se deben cumplir se consideran elementos generales de gestión y procesos específicos de gestión de riesgos de seguridad de la información y ciberseguridad,[33] los que deben considerar como mínimo, identificación, análisis, valoración, tratamiento y aceptación o tolerancia de los riesgos a que están expuestos los activos de información de la entidad, así como su monitoreo y revisión permanente.[34]

El andamiaje normativo establecido y fiscalizado por la CMF se debe entender complementario al de la Ley 21663 Marco de Ciberseguridad, al menos para las ins-

31. La seguridad se define como el conjunto de acciones para la preservación de la confidencialidad, integridad y disponibilidad de la información de la entidad. Y la ciberseguridad comprende o alude al conjunto de acciones para la protección de la información presente en el ciberespacio y de la infraestructura que la soporta, y tiene como objetivo evitar o mitigar los efectos adversos de riesgos y amenazas inherentes que puedan afectar la seguridad de la información y la continuidad del negocio de la institución.

32. En palabras simples, toman especial importancia los riesgos que amenazan la ciberseguridad en un entorno creciente de conectividad y dependencia de los servicios otorgados a clientes a través de plataformas tecnológicas, lo que significa que las entidades deben asegurar la adecuada calidad y disponibilidad de los sistemas utilizados para la prestación de dichos servicios y que enfrenten una progresiva exposición a los riesgos, especialmente cuando se asumen en el ciberespacio.

33. Dentro de la estructura organizacional definida se cuenta con una función de gestión de riesgos, independiente de las áreas generadoras de riesgos, encargada del diseño y mantención de un sistema adecuado de identificación, seguimiento, control y mitigación de los riesgos en materia de seguridad de la información y ciberseguridad. Asimismo, se han aprobado niveles mínimos de disponibilidad para asegurar que los servicios otorgados a través de plataformas tecnológicas y los activos de información de la entidad cuentan con un resguardo adecuado en términos de la seguridad física y ambiental, etcétera.

34. Y más específicamente, aspectos como la identificación de sus activos, de acuerdo con la definición y alcance contenido en la política de seguridad de la información y ciberseguridad, la evaluación de los controles existentes de manera de conocer su efectividad y suficiencia, etcétera.

tituciones financieras, conceptualmente prestadores de servicios esenciales y operadores de importancia vital. El artículo 8 consigna, extensamente, los deberes específicos de estos últimos, que se desarrollan en el resto del articulado de la ley y en sus reglamentos subordinados. El artículo 9 es el que detalla y regula la obligación, quizás, más importante, el deber de reportar un incidente de ciberseguridad. Específicamente, sobre implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar los riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional del servicio. Por lo mismo, la CMF establece como exigencia que el Sistema de Gestión de la Seguridad de la Información permita evaluar tanto la probabilidad como el potencial impacto de un incidente de ciberseguridad.

Sobre mantener un registro de las acciones ejecutadas que compongan el Sistema de Gestión de Seguridad de la Información para cada uno de los activos que se determinen en el inventario de activos, y de conformidad a lo que señale el reglamento, estos registros son importantes porque permiten demostrar y preacreditar la diligencia debida. En cuanto a elaborar e implementar planes de continuidad operacional y ciberseguridad certificados en los centros de certificación exclusivos que se establezcan, en conformidad al artículo 28,[35] deben ser sometidos a revisiones periódicas, ya que se deben adaptar a las condiciones imperantes por parte de los sujetos obligados con una frecuencia mínima, por regla general, de dos años.[36]

El artículo 8 de la Ley 21663 establece como deber especial de ciberseguridad, dentro de las obligaciones para los bancos que sean operadores de importancia vital, pruebas de penetración o de hackeos blancos, y realizar preventiva y continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y otros, para detectar acciones o programas informáticos que comprometan la ciberseguridad. Más en detalle, son obligados a i) aplicar, de manera permanente, las medidas para prevenir, reportar y resolver incidentes de ciberseguridad (de naturaleza tecnológica, organizacional, física o informativa); ii) implementar medidas de

35. El artículo 28 agrega perentoriamente que los operadores de importancia vital deben obtener las certificaciones de ciberseguridad que señale la ley y las que determine la agencia mediante reglamento, y solo «los organismos que sean parte del registro de entidades certificadoras autorizadas a cargo de la agencia», estarán habilitados para emitir certificaciones válidas. Se agrega que para formar parte de este registro bastará acreditar el cumplimiento de los requisitos que establezca el reglamento y, para mantenerse, cumplir con los requisitos referidos. Adicionalmente, la agencia podrá homologar certificaciones técnicas internacionales o extranjeras sobre ciberseguridad mediante resolución fundada de su director o directora.

36. Se agrega que, por excepción, la agencia podrá instruir a uno o más operadores de importancia vital, fundadamente y por motivos sobrevinientes graves, la certificación de sus planes de continuidad operacional o ciberseguridad en un plazo menor al indicado, solo respecto de cada operador de importancia vital siempre que la certificación tenga al menos un año de vigencia.

prevención y gestión de riesgos de ciberseguridad definidas por la Agencia Nacional o por el regulador sectorial; iii) reportar al Equipo Nacional de Respuesta a Incidentes de Seguridad Informática los incidentes de ciberseguridad o ciberataques de que sean objeto; y iv) cumplir con los principios de la ley.

En el ámbito de las acciones de contingencia y para lo referido al deber de adoptar, de forma oportuna y expedita, las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad que se haya verificado, se extiende a la restricción incluso de uso o acceso a sistemas informáticos si fuera necesario. Se previene que se informe a los potenciales afectados en forma simultánea en el hecho y conforme a plazos determinados, en la medida que puedan identificarse y cuando así lo requiera la Agencia sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos.

Por otro lado, el artículo 14 quinquies de la Ley 19628 recoge para Chile la misma norma del Reglamento General de Protección de Datos de la Unión Europea y considera expresamente a las auditorías como medidas técnicas y administrativas a adoptarse. Primero, determina que se considerará el estado de la técnica, los costos de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de los titulares. En segundo lugar, se agrega que una de las opciones puede ser que el responsable (el mandante, un banco) y el encargado del tratamiento (el mandatario, un proveedor de la nube) apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, y dentro de las medidas se menciona, a título meramente ejemplar, un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para alcanzar este objetivo.

En definitiva, son medidas técnicas y organizativas apropiadas, entre otras: la seudonimización y el cifrado de datos personales; la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; y un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.[37]

El marco de solidaridad legal de la Ley 19628 para el encargo de la entidad financiera al proveedor de nube

Jurídicamente esta institucionalidad legal y su incumplimiento va aparejado de multas administrativas. En su inciso primero el nuevo artículo 15 bis de la Ley 19628 dis-

37. La definición es una causal no taxativa o de *numerus apertus*.

pone que un responsable de tratamiento de datos personales o nominativos,[38] que son los que identifican o hacen identificable a una persona natural,[39] lo puede efectuar de dos maneras: en forma directa o a través de un tercero mandatario o encargado,[40] donde la delegación siempre es voluntaria y nunca obligatoria. En este segundo caso, un *encargo de tratamiento* es un acuerdo formal entre un responsable y un encargado del procesamiento, ahora el proveedor de servicios de nube, mediante la externalización de servicios, donde el primero confía al segundo la realización de ciertas actividades de tratamiento de datos personales en su nombre.[41]

Como se precisa, el responsable del tratamiento de datos es la entidad que decide por qué y cómo se procesan los datos personales o determina los fines y los medios del tratamiento. El responsable, entonces, no necesariamente ejecuta el procesamiento de los datos y puede externalizarlo en un procesador de datos, pero es quien toma las decisiones clave sobre el uso de la información personal. Por lo tanto, el encargado del tratamiento asume la obligación de prestar un servicio al responsable, lo que implica el tratamiento de datos personales por cuenta de este. En el caso de que el encargado del tratamiento de datos tenga que delegar o subcontratar parte de sus tareas debe hacerlo en otro encargado o en un coencargado, siempre y cuando haya recibido previa autorización escrita del responsable del tratamiento de datos.

El artículo 15 bis en estudio agrega que el tercero mandatario o encargado debe realizar el tratamiento de datos personales conforme al encargo y a las instrucciones que le imparta el responsable y le queda prohibido su tratamiento para un objeto distinto del convenido con el responsable y su cesión o entrega, en los casos en que el responsable no lo haya autorizado de manera expresa, exclusiva y específicamente para cumplir con el objeto del encargo.[42] Esta norma, ajena a las críticas estructurales

38. Hablar de *tratamiento* es usar un concepto estándar en la institucionalidad comparada y chilena en protección de datos personales de forma más amplia que el simple *procesamiento*. La denominación actual alude a cualquier operación, o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan de cualquier forma recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de datos personales.

39. A esta fecha, y salvo excepciones, los derechos para la autodeterminación informativa no se reconocen como potestades de personas fictas o jurídicas.

40. La letra x) del artículo 2 define al tercero mandatario o encargado como la persona natural o jurídica que trata datos personales por cuenta del responsable de datos.

41. En cuanto acto jurídico bilateral o contrato, y porque el responsable puede efectuar el tratamiento de datos a través de un tercero mandatario o encargado, el primer obligado por el contrato y la delegación deberá realizar —el mandato es imperativo— el tratamiento de datos personales conforme al encargo y a las instrucciones que le imparta el responsable. Por ley, le queda prohibido su tratamiento para un objeto distinto del convenido con el responsable, así como su cesión o entrega en los casos en que el responsable no lo haya autorizado de manera expresa y específica para cumplir con el objeto del encargo.

42. Se trata de hipótesis diversas. La mera entrega o comunicación para cumplir el encargo no es lo

y de fondo que ya se han formulado a la nueva legislación (Marrero, 2025), no hace sino reconocer una opción contractual para facilitar el tratamiento, cotidiano y esencial para los gestores de bases y bancos de datos, que venía regulado en el artículo 28 del Reglamento General de Protección de Datos de la Unión Europea y que ha suscitado una variada jurisprudencia administrativa en sistemas jurídicos donde existen autoridades de protección de datos personales.[43]

Es evidente que el tratamiento de datos a través de un tercero mandatario o encargado, en este caso el proveedor de la nube, se presenta cuando el responsable, quien gestiona la información nominativa y toma decisiones sobre ella, opta por no hacerlo directamente. La importancia del rol está en comprender su alcance, saber cuándo y cómo designarlo adecuadamente permitiría a las organizaciones garantizar una gestión de datos responsable y segura, evitando sanciones y pérdidas de competitividad. En este contexto, el responsable del tratamiento no pierde dicha condición ni sus competencias por el solo hecho de encomendar el tratamiento o comunicar los datos a un encargado, siempre que no exista ánimo de cesión ni de transferencia que le permita operar como nuevo responsable.[44] Así, el responsable podrá encomendar al encargado las funciones de recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales. El caso más simple sería, por ejemplo, la hipótesis de una institución financiera que debe cumplir la obligación o deber de seguridad mediante el respaldo o el almacenamiento de la información de sus cuentacorrentistas o tarjetahabientes en sistemas, redes o servidores externos en forma periódica,[45] que es lo que exige la normativa bancaria y cuyo cumplimiento fiscaliza la Comisión de Mercado Financiero.

Al respecto la ley establece imperativamente que el tercero mandatario o encargado deberá realizar el tratamiento de datos personales. El mandato es perentorio, conforme al encargo y a las instrucciones que le imparta el responsable. Las dos prohibiciones derivadas y explicitadas tampoco admiten cuestionamiento jurídico: un encargado no puede gestionar u operar un tratamiento de datos personales para un objeto distinto del convenido con el responsable, y no puede cederlos o entregarlos si

mismo que una cesión de datos, donde la transferencia a un tercero implica que él pasa a ser el nuevo responsable del tratamiento. Así lo dispone expresamente la Ley 19628.

43. Para ser más precisos, la figura del encargado de tratamiento se recoge en los artículos 4, 8, 28 y 29, y en el considerando 81 del Reglamento General de Protección de Datos de la Unión Europea.

44. El artículo 15 determina, expresamente, que «una vez perfeccionada la cesión, el cesionario adquiere la condición de responsable de datos para todos los efectos legales». Agrega que «el cedente, por su parte, también mantiene la calidad de responsable de datos respecto de las operaciones de tratamiento que continúe realizando».

45. El concepto «redes y sistemas informáticos» en Chile tiene definición legal. El artículo 2 de la Ley 21663 Marco de Ciberseguridad señala que se entiende por tales al conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.

el responsable no lo ha autorizado de manera expresa y específicamente para cumplir con el objeto del encargo. Un requisito esencial para el encargo es que los tratamientos se hagan por cuenta y riesgo y bajo las instrucciones expresas del responsable, lo que significa que, mediando el encargo contractual, los datos personales siempre se mantienen bajo la esfera de su control.

Como ocurre con toda obligación de cumplimiento solidario establecida por ley, en este caso se busca beneficiar al titular o propietario de los datos personales. El artículo 15 bis considera solo dos hipótesis de solidaridad legal: entre responsable y encargado o entre el encargado y un delegado o subencargado.

Se presenta una causal, que involucra conjuntamente al mandante, si el tercero mandatario o encargado trata los datos con un objeto distinto del convenido o los cede o entrega sin haber sido autorizado en los términos dispuestos en el encargo. A modo de ejemplo: si un banco contrata a un tercero para que gestione sus bases de datos en la nube, y este tercero no cumple con las medidas de seguridad técnicas y administrativas necesarias, tanto el banco, responsable y mandante, como el tercero proveedor de la nube, encargado y mandatario, podrían ser considerados responsables solidariamente ante una brecha de seguridad.[46]

La otra causal legal de solidaridad surge cuando delega parte o la totalidad del encargo a otro subencargado, porque ahora como delegante continuará siendo solidariamente responsable junto con el delegado sobre dicho encargo, sin que pueda eximirse de responsabilidad, argumentando que ha delegado el tratamiento. La consecuencia es que el titular y propietario de los datos podrá exigir el cumplimiento de las obligaciones relacionadas a cualquiera de las partes en su totalidad, y tendrá más opciones de buen resultado para sus pretensiones sin tener que dividir la responsabilidad entre ellas. Es preciso recordar que la solidaridad legal existe en aquellos casos en que dos o más personas están obligadas a cumplir una misma prestación y cualquiera de ellas puede ser exigida por el acreedor para el cumplimiento total de la deuda. La solidaridad nunca se presume, debe estar establecida expresamente en la ley o en el contrato.

Cuando el tema de las responsabilidades, eventualmente solidarias, adquiere mayor importancia, y así lo demuestra la evidencia empírica, es cuando se producen brechas o incidentes de ciberseguridad y ellas acarrean un daño o perjuicio a los titulares. En el caso de que estas sean imputables a la negligencia o falta de cuidado del encargado, por haber actuado a nombre de un mandante, este también debe asumir su cuota de responsabilidad, sobre todo si se ha establecido la solidaridad legal.

46. Este posible incumplimiento también podría imputarse al responsable, por ejemplo, porque no recurrió únicamente a encargados del tratamiento que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento cumpla los requisitos del Reglamento y garantice la protección de los derechos del interesado.

Conclusiones

Una evolución tecnológica paulatina y conveniente de las modalidades de gestión, en particular, pero no exclusivamente financiera, instaló a los operadores en el contexto de la computación en la nube de internet. Al parecer, estos ecosistemas de nube no admiten cuestionamientos tecnológicos, en especial por sus capacidades de procesamiento y de ciberseguridad. Sin embargo, el derecho y las normativas se han ido haciendo cargo de esta realidad, de este mecanismo de externalización y de sus implicancias jurídicas.

En este trabajo se analizaron los puntos relacionados con la ciberseguridad y el tratamiento de datos personales dándole un contexto y aprovechando la regulación para la banca general y particular, en especial, las referencias al nuevo marco jurídico para el encargo de tratamiento de datos entre el banco (mandante) y el proveedor de nube (el mandatario). El estudio explica la necesidad de considerar al capítulo 20-7 de la RAN y las evaluaciones de impacto de la Ley 19628 como requisitos previos para implementar la migración a la nube; y al capítulo 20-10 de la RAN y las leyes 19628 y 21663 como los parámetros necesarios e ineludibles para gestionar, en forma cibersegura, la migración a la nube.

El análisis concluye que pueden surgir múltiples responsabilidades de ser imputables a la negligencia o falta de cuidado del que externaliza si la externalización no se verifica con diligencia, con la adopción de medidas de ciberseguridad y respetando las restricciones de la Ley de Protección de Datos Personales, especialmente cuando se producen brechas o incidentes de ciberseguridad y ellas acarrean un daño o perjuicio a los titulares o cuentacorrentistas.

Referencias

FNE, Fiscalía Nacional Económica (2024). «Informe acerca de las materias consultadas en la presentación de Amazon Web Services, Inc.» Disponible en https://tipg.link/mbjc.

Joyanes, Luis (2012). *Computación en la nube: Estrategias de* cloud computing *en las empresas*. Ciudad de México: Alfaomega.

López, David (2013). «La computación en la nube o *cloud computing* examinada desde el ordenamiento jurídico español». *Pro Jure Revista de Derecho*, 40 (1): 689-709. Disponible en https://tipg.link/mE73.

Marrero, Leocadio (2025). «La Ley de Protección de Datos Personales en Chile: De la ilusión a la oportunidad perdida». *Revista La Ley Privacidad,* 23.

Mata, Miguel Ángel (2021). *Aspectos jurídicos del outsourcing tecnológico*. Valencia: Tirant Lo Blanch.

Quiroz, Alonso (2016). «Guía metodológica para el uso de *cloud computing* en instituciones públicas chilenas». Tesis para obtener el grado de Ingeniero Civil Informático, Universidad Santa María. Disponible en https://tipg.link/mE92.

Severín, Gonzalo (2020). «Contratos de servicios de *cloud storage* público: Cláusulas de privacidad y seguridad del contenido almacenado a la luz del derecho chileno». *Revista Chilena de Derecho y Tecnología*, 9 (1): 121–150. DOI: 10.5354/0719-2584.2020.54688.

Sobre el autor

Renato Jijena Leiva es abogado de la Pontificia Universidad Católica de Valparaíso. Magíster en Derecho Público de la misma universidad. Magíster en Protección de Datos Personales de la Universidad Internacional de La Rioja, España. Magíster en Gobierno Electrónico de la Universidad Tecnológica Metropolitana de Chile. Diplomado en Derecho Informático de la Universidad de Zaragoza, España. Su correo electrónico es renato.jijena@pucv.cl. 0000-0003-4139-6411.

REVISTA DE DERECHO ECONÓMICO

La *Revista de Derecho Económico* es un esfuerzo editorial de profesores del Departamento de Derecho Económico de la Universidad de Chile y de juristas externos que presentan ideas y reflexiones surgidas de sus investigaciones. La revista publica artículos sobre aspectos jurídicos relacionados con microeconomía, macroeconomía, políticas económicas, orden público económico, libre competencia, regulación de servicios públicos, derecho del consumidor, derecho bancario, derecho del mercado de valores, derecho tributario, contabilidad, comercio y finanzas internacionales, derecho del medioambiente y recursos naturales, derecho minero, derecho de aguas, derecho de la energía, derecho internacional económico, análisis económico del derecho y otras temáticas afines.

SITIO WEB
revistaderechoeconomico.uchile.cl

CORREO ELECTRÓNICO
rde@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).