

Minuta Presentación ante la Comisión Asesora Ministerial para implementar la Ley N° 21.719

La Asociación de Bancos valora la creación de la Comisión Asesora Ministerial destinada a implementar la Ley N° 21.719, que regula el tratamiento y la protección de datos personales y crea la Agencia de Protección de Datos Personales, cuyo objeto consiste en asesorar técnicamente al Ministerio Secretaría General de la Presidencia, respecto de todas las acciones necesarias para la adecuada implementación de la referida ley.^{1/}

Al respecto, cabe señalar que la implementación de la Ley de Protección de Datos Personales (LDP) tiene especial relevancia para la industria financiera, en un marco regulatorio donde coinciden los procesos de implementación del **Sistema de Finanzas Abiertas (SFA)** en el marco de la Ley Fintec^{2/} a cargo de la Comisión para el Mercado Financiero (CMF); la **Ley Marco de Ciberseguridad**^{3/} a cargo de la Agencia Nacional de Ciberseguridad (ANCI); y el **Registro de Deuda Consolidada**^{4/}, cuya implementación también corresponde a la CMF.

En este contexto, los principales comentarios y recomendaciones para la adecuada implementación de la LPD son los siguientes:

A.- Ley de Protección de Datos y el Sistema de Finanzas Abiertas.

A.1.- Protección de los datos de los clientes financieros.

- La protección de los datos personales constituye el **eje central** de ambos marcos normativos.
- La LDP regula la forma y condiciones para el **tratamiento y protección de los datos personales de las personas naturales**, en conformidad al artículo 19 N° 4 de la Constitución Política de la República; mientras que el SFA regula el **intercambio** - entre distintos prestadores de servicios - de **información de clientes financieros** que hayan consentido expresamente en ello.

¹ 1.- Realizar un diagnóstico general de las acciones necesarias que el Ejecutivo debe impulsar para el cumplimiento de la ley N° 21.719. 2.- Asesorar al Ministerio en la dictación de las normas reglamentarias necesarias para la implementación y cumplimiento de la ley N° 21.719. 3.- Identificar y proponer al Ministerio todas aquellas materias legales o administrativas que fuere necesario adecuar para la correcta implementación de la ley N° 21.719. 4.- Asesorar al Ministerio, respecto de la dictación de los actos administrativos o la adopción de las acciones de gestión necesarias para la implementación de la nueva institucionalidad que crea la ley N° 21.719.

² Ley 21.521.

³ Ley 21.663.

⁴ Ley 21.680.

- El SFA representa la transformación más importante del sistema financiero chileno de las últimas décadas.
- En términos simples, el SFA permitirá la prestación de los siguientes servicios:

(a) consulta de datos financieros: donde los **clientes autorizan** a los proveedores de servicios basados en información (PSBI) para que consulten la información financiera que mantienen en las instituciones proveedoras de información (IPI), de manera que puedan proveerles distintos servicios; y

(b) iniciación de pagos: donde los **clientes** que sean titulares de cuentas corrientes, cuentas vistas o cuentas con provisión de fondos, **instruyen** a una entidad denominada proveedor de servicios de iniciación de pagos (PSIP), para que en su nombre y ante el banco o la institución financiera proveedora de la cuenta respectiva (IPC), ejecuten órdenes de pago o transferencias electrónicas de fondos, con cargo a sus respectivas cuentas y medios de pago.

- En consecuencia, los proveedores de servicios (PSBI y PSIP) deben **autenticar al titular de los datos y contar con su consentimiento para acceder a su información**, cumpliendo con los requisitos que establece la **Ley Fintec y las normas de la CMF**, y también con los principios, **requisitos y condiciones de la LDP**, considerando que el consentimiento del cliente recae sobre datos personales.
- La Ley Fintec exige que el consentimiento se otorgue **previa y explícitamente** a través de medios o canales electrónicos expeditos y seguros. Además, deberá manifestarse en forma **libre, informada, expresa y específica** en cuanto al **tipo de información financiera**, la **finalidad** y el periodo máximo de **validez** de esa autorización, siendo esencialmente **revocable**.
- Los requisitos del consentimiento que establece el SFA son consistentes con las exigencias de la LPD, la cual establece que el tratamiento de los datos personales es lícito cuando el titular presta su consentimiento en forma **previa e inequívocamente**, de manera **libre, informada y específica** en cuanto a su **finalidad o finalidades**, siendo también de la esencia el derecho del titular para revocar el consentimiento en cualquier tiempo y sin expresión de causa.
- El consentimiento de los titulares de datos financieros en el marco del SFA también debe cumplir con los **principios establecidos en la LDP**, específicamente, con los principios de **finalidad y proporcionalidad**.

(a) **Principio de finalidad:** el consentimiento debe especificar claramente los fines del tratamiento de la información y los datos involucrados, entre otros.^{5/}

(b) **Principio de proporcionalidad:** los datos deben ser los estrictamente necesarios para la finalidad respectiva^{6/} (**principio de proporcionalidad**).

- La Norma de Carácter General N° 514 de la CMF (NCG 514), que regula el SFA, exige que el **consentimiento de los clientes debe cumplir con los principios de finalidad y proporcionalidad**, debiendo acreditarse en el marco de los procesos de fiscalización pertinentes.^{7/}
- Sin embargo, la CMF informó que los **PSBI podrán definir la aplicación de los principios de finalidad y proporcionalidad a su criterio**, y que sólo se contempla un rol de **supervisión ex post**^{8/} en esta materia.

Asimismo, la propuesta normativa de la CMF que modifica la NCG 514 establece que las IPI o IPC, deberán entregar los datos solicitados con la sola autenticación que realicen los PSBI o PSIP y del usuario, **prohibiendo, a los IPI e IPC revisar la licitud de los consentimientos o rechazarlos, en resguardo del principio de proporcionalidad**^{9/}.

- Más aún, la misma norma en consulta **permite que el PSBI o PSIP modifique unilateralmente la finalidad y plazos del consentimiento**, siempre y cuando dicho cambio se enmarque en el conjunto de datos del consentimiento inicial. Esta facultad del PSBI o PSIP simplemente **rompe cualquier equilibrio razonable entre el deber de protección de los clientes y la protección constitucional de los datos personales**^{10/}.
- Lo anterior es relevante, considerando la **asimetría de información que existirá en el SFA**. Los clientes tendrán dificultades para evaluar en tiempo real el cumplimiento de los principios de finalidad y proporcionalidad, exponiéndolos a potenciales **eventos de fraude o mal uso de sus datos financieros**.
- Esta situación difícilmente se mitigará en el marco de un proceso de supervisión, ya que el daño se habrá materializado y, además, el SFA contempla

^{5/} Ley Fintec (N° 21.521); Artículo 23.

^{6/} Norma de Carácter General 514 (NCG 514) de la CMF; Sección III, Letra D), N° 1, letra f) y Ley 19.628 modificada por la 21.719; Artículo 2.- Definiciones y Artículo 3.- Principios.

^{7/} Sección III, Letra D); N° 1, letra f) de la Norma de Carácter General N° 514.

^{8/} Norma en consulta de la CMF: sección IV, N° 8, Letra D), N° 1, letra a) (pág. 23).

^{9/} Norma en Consulta de la CMF; Sección IV, Punto 8. Letra D), N° 1, letra a) (página 23).

^{10/} Norma en Consulta de la CMF; Sección IV, Punto 8. Letra D), N° 1, letra i) (página 25).

cientos de miles de conexiones entre instituciones, lo cual hace operativamente imposible revisar el cumplimiento de los principios de finalidad y proporcionalidad.

- La Ley Fintec^{11/} establece que la **CMF tendrá a su cargo la fiscalización del cumplimiento de las obligaciones de los participantes del SFA**. Sin embargo, la misma ley establece que, lo anterior, debe entenderse **sin perjuicio de los deberes y obligaciones que los participantes del SFA conforme al ordenamiento general**, incluyendo la Ley sobre Protección de los Derechos de los Consumidores, y la **Ley sobre Protección de Datos Personales**.

- Cabe señalar que la CMF argumenta que la **experiencia internacional** muestra que la supervisión del consentimiento se realiza **ex post**. Sin embargo, dicho planteamiento **no responde la pregunta central**, es decir, si dicha estrategia de supervisión será eficaz en la protección de los datos personales de los clientes, teniendo presente la **protección constitucional de los datos personales**. Más aún, la evidencia comparada sugiere que este tema no está resuelto. Por ejemplo:

- JPMorgan (USA) informó que, del total de 1.890 millones de solicitudes de datos realizadas durante junio de 2025 por PSBI, solo el 13% fueron iniciadas directamente por los clientes para ejecutar una transacción específica. El 87% restante correspondió a solicitudes efectuadas por los PSBI con otros fines, que incluían la venta de dicha información.^{12/} Es decir, en este último caso, se trataba de **solicitudes que no cumplían con los principios de finalidad y proporcionalidad**.

- En el sistema de *Open Finance* del Reino Unido se estableció que el plazo máximo para compartir información con los PSBI es de 90 días. Transcurrido dicho período, el usuario debe reconfirmar el consentimiento para mantener habilitado el flujo de información.^{13/} Es decir, en este caso, queda en evidencia que **aún se exploran mecanismos de control efectivos**.

- En Australia, en julio de 2023 se publicó una investigación sobre el proceso de consentimiento, encargada por el *Customer Data Right* (CDR). Uno de sus principales hallazgos fue la **desconfianza de los usuarios** respecto del proceso para autorizar el intercambio de su información dentro del sistema de *Open Finance*, donde menos de la mitad de los usuarios consideró el proceso de consentimiento como “confiable”.^{14/}

¹¹ Art. 27.

¹² <https://www.cnb.com/2025/07/28/jpmorgan-fintech-middlemen-plaid-data-requests-taxing-systems.html>

¹³ <https://standards.openbanking.org.uk/customer-experience-guidelines/account-information-services/account-information-consent/latest/>

¹⁴ [Consent Review Research Report \(Q3 2022, R1-3\)](#)

- El SFA es un proceso nuevo que presenta muchos **desafíos, incertezas y riesgos** que deben resolverse, lo cual exige que el **regulador actúe con prudencia y gradualidad**, particularmente, en el resguardo de los consentimientos y datos personales asociados.
- Por lo tanto, considerando la sensibilidad de este tema, así como los antecedentes expuestos, se sugiere - en esta materia -, que en el proceso de implementación y consolidación del SFA, se establezca un **catálogo amplio, pero definido, de finalidades relevantes y la proporcionalidad de los datos asociados**.

Complementariamente, se solicita que se proponga que en la normativa de la CMF se contemple explícitamente la **responsabilidad de los PSBI y PSIP**, respecto de los datos que reciban desde los IPI e IPC.

A.2.- Diferenciación de estándares de cumplimiento.

- La LPD establece que los estándares o condiciones mínimas que se impongan al responsable de datos para el **cumplimiento de los deberes de información y de seguridad** serán determinados por la Agencia de Protección de Datos, considerando el tipo de dato del que se trata, si el responsable es una persona natural o jurídica, el tamaño de la entidad o empresa de acuerdo a las categorías establecidas en el artículo segundo de la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño, la actividad que desarrolla y el volumen, naturaleza y las finalidades de los datos personales que trata.^{15/}
- Cabe advertir que la infracción del estándar de cumplimiento en materia de seguridad por parte de una empresa de menor tamaño puede **igualmente provocar un impacto sustancial en el SFA** (i.e., en el sistema de pagos).
- Por lo tanto, estimamos conveniente que la Comisión recomiende que **no se establezcan requisitos diferenciados en materia de deberes de información y seguridad, respecto de las entidades que participen en el SFA**.

B.- Ley de Protección de Datos Personales – prevención de fraudes.

- La Ley 20.009, que establece el régimen de limitación de responsabilidad por fraudes con medios de pago (Ley de Fraudes), dispone que las entidades que intervienen o prestan servicios asociados a pagos y transacciones electrónicas, deben adoptar las **medidas de seguridad necesarias para prevenir la comisión de los ilícitos descritos en dicha ley**.^{16/}

¹⁵ Art. 14 septies.

¹⁶ Art. 6.

- En dicho contexto, la Ley de Fraudes establece que los emisores u operadores deberán considerar, entre otras, (i) contar con **sistemas de monitoreo** que tengan como objetivo detectar operaciones que no corresponden al comportamiento habitual del usuario; (ii) implementar **procedimientos internos para gestionar las alertas** generadas por dichos sistemas de monitoreo; o (iii) **identificar patrones de potenciales fraudes**.
- **Contar con bases de datos personales comunes a la industria bancaria** contribuirá en la prevención, detección y análisis de conductas que puedan corresponder a fraudes financieros. Esta información, junto con otros mecanismos que emplea la industria, permiten no sólo dar cumplimiento a los requerimientos normativos, sino que también fortalecen el normal funcionamiento del sistema de pagos y la estabilidad financiera.
- En consecuencia, y sin perjuicio de lo dispuesto en la Ley de Fraudes, para fines de mayor certeza jurídica, solicitamos que la Comisión Asesora Ministerial proponga al Ministerio SEGPRES, el envío de un proyecto de ley que modifique la Ley de Fraudes, que **autorice a los emisores de pago para establecer y compartir bases de datos comunes, cuyo propósito específico y exclusivo sea la prevención, detección y análisis del fraude financiero, y del lavado de activos**. Para estos efectos, dichas entidades deberán adoptar las más altas medidas de seguridad, tanto técnicas como organizativas, para resguardar la confidencialidad, integridad y disponibilidad de la información contenida en ellas, de acuerdo con los estándares que establezca la Agencia de Protección de Datos Personales.

C.- Distintos requisitos para acceder a la información en la Ley que crea el Registro de Deuda Consolidada, Ley de Protección de Datos Personales, el Sistema de Finanzas Abiertas, y el Reglamento sobre Análisis de Solvencia Económica e Información a los Consumidores.

- La Ley que crea el **Registro de Deuda Consolidada**^{17/} establece que el acceso a la información requerirá del **consentimiento** del cliente, pero únicamente con la finalidad de **evaluar el riesgo comercial, riesgo crediticio y para realizar gestión de riesgos** para operaciones específicas.

Sin embargo, no se requiere el consentimiento en los siguientes casos: (i) deudores vigentes de cada institución, (ii) información anonimizada de grupos de personas, y (iii) cuando los reportantes cuenten con otra fuente de licitud de conformidad con el Título III de la Ley sobre Protección de Datos Personales, pero

¹⁷ El REDEC contiene información positiva (deuda vigente) y negativa, (deuda vencida o en mora).

en este último caso, la norma de la CMF restringe la fuente de licitud exclusivamente a la información reportada al Boletín Comercial.^{18/}

- Por su parte, la **Ley sobre Protección de Datos Personales** establece que el tratamiento de los datos personales requiere el **consentimiento** del titular.

Sin embargo, **no se requiere dicho consentimiento**, entre otros casos, cuando el tratamiento esté referido a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial y se realice de conformidad con las normas del Título III de esta ley (cumplimientos e incumplimientos), incluidos los datos referidos a la situación socioeconómica del titular.

- El **Sistema de Finanzas Abiertas** permite la **consulta de la información financiera de los clientes previo consentimiento de estos últimos**.
- El artículo 17 N incorporado por la ley N° 21.398 a la ley N° 19.496, establece que, antes de la celebración de una operación de crédito de dinero, los proveedores deberán **analizar la solvencia económica del consumidor** para cumplir las obligaciones que de ella se originen, sobre la base de información suficiente obtenida a través de medios oficiales destinados a tal fin, y deberán informarle el resultado de dicho análisis.

Esta materia se encuentra regulada en el **Reglamento sobre Análisis de Solvencia Económica e Información a los Consumidores**¹⁹, por lo que, en este caso, la fuente de licitud para el tratamiento de los datos se encuentra en la ley.

- En este contexto, considerando la **multiplicidad de regulaciones en materia de acceso a la información de los titulares**, solicitamos que la Comisión proponga al Ministerio SEGPRES las modificaciones legales o reglamentarias que corresponden para **unificar los requisitos de acceso y tratamiento de la información sin consentimiento del titular**.

D.- Coordinación regulatoria

D.1.- Reporte de incidentes de ciberseguridad.

- La **coordinación regulatoria** entre la Agencia de Protección de Datos Personales, la CMF y la ANCI, representa un gran desafío para la industria bancaria.

¹⁸ La CMF señaló que se habilitaría un registro nominado complementario al Boletín Comercial, pero no existe certeza sobre la información que contendrá dicho registro.

¹⁹ DS N°53 (Economía), de 21 de abril de 2022 (D.O. de 3 de agosto de 2023).

- La dictación de actos administrativos de carácter general de los órganos de la Administración del Estado que tengan efectos en los ámbitos de competencia de otro órgano se rige por el **principio de coordinación regulatoria** de la Ley de Bases de los Procedimientos Administrativos. Sin embargo, la opinión del órgano requerido **no es vinculante**.^{20/}
- El principio de coordinación regulatoria no vinculante se reconoce en la Ley Marco de Ciberseguridad^{21/} (Agencia Nacional de Ciberseguridad y las autoridades sectoriales) y en la Ley que crea el Registro de Deuda Consolidada (CMF)^{22/}.
- En el caso de la Ley Fintec y de la Ley de Protección de Datos Personales se aplica el principio general de la Ley 19.880, sin perjuicio de que la Ley de Protección de Datos Personales establece el principio de coordinación regulatoria entre la Agencia de Protección de Datos Personales y el Consejo para la Transparencia.
- La Comisión Asesora Ministerial debiese **proponer lineamientos para la coordinación entre la CMF y las demás Agencias**, de manera de evitar inconsistencias en sus regulaciones y para evitar reacciones que puedan afectar la estabilidad del sistema financiero, en particular en materia de reporte de incidentes de ciberseguridad:
 - (i) **CMF:** los bancos deben informar a la CMF dentro 30 minutos, al público “oportunamente”.
 - (ii) **ANCI:** los bancos deben enviar una alerta dentro de 3 horas desde que hubiese tomado conocimiento del incidente; segundo informe dentro de 24 horas; 7 días para informar un plan de acción; y 15 días para el informe final;^{23/}.
 - (iii) **Agencia de Protección de Datos Personales:** las vulneraciones a las medidas de seguridad deben reportarse a la Agencia “sin dilaciones indebidas”.^{24/} También deben comunicarse las vulneraciones a los titulares de datos sensibles y datos relativos a obligaciones de carácter económico, financiero, bancario o comercial.

²⁰ Art. 37 bis.

²¹ Art. 25

²² Art. Primero Transitorio.

²³ Título IV del Reglamento (DS 295 de 25/9/2024)

²⁴ Art. 14 sexies.

D.2.- Ley Marco de Ciberseguridad y Ley sobre Protección de Datos Personales. Determinación de las sanciones.

- La LPD establece los **criterios que la Agencia de Protección de Datos Personales deberá aplicar prudencialmente para determinar el monto de las multas.**
- En este contexto, la ley señala que “cuando por unos mismos hechos y fundamentos jurídicos, el infractor pudiese ser sancionado con arreglo a esta ley y a otra u otras leyes, de las sanciones posibles, se le impondrá la de mayor gravedad.”²⁵
- Cabe señalar que el **mismo criterio se encuentra en la Marco de Ciberseguridad.**²⁶
- La Comisión Asesora Ministerial debiese **proponer lineamientos para la coordinación** entre la Agencia de Protección de Datos Personales y la ANCI, para la aplicación de este criterio.

2 de octubre de 2025

²⁵ Art. 37 inc. final.

²⁶ Art. 40.