Superintendencia de Industria y Comercio

CIRCULAR EXTERNA No. _____ DE 2025
( )

Para: Entidades vigiladas por la Superintendencia de Industria y Comercio en su rol de Autoridad de Protección de Datos personales.

Asunto: Lineamientos sobre el tratamiento de datos personales en el ecosistema fintech y los modelos de negocio, aplicaciones y procesos que utilizan medios tecnológicos para la prestación de servicios financieros.

Consideraciones

El dinamismo de los modelos de negocio, aplicaciones y procesos para la prestación de servicios financieros agrega valor, refuerza la competitividad y democratiza el acceso a productos financieros. Asimismo, la ampliación del portafolio de productos mediante nuevas infraestructuras tecnológicas permite que los consumidores financieros accedan a más y mejores servicios.

El despliegue de estos modelos de negocio debe realizarse de conformidad con la Constitución Política de 1991 y las leyes aplicables, en especial, las leyes relacionadas con la protección de datos personales.

El cumplimiento de las obligaciones en materia de protección de datos personales y habeas data desarrolla el principio de primacía de los derechos fundamentales, genera confianza en el mercado, promueve un ambiente seguro para el desarrollo de nuevos servicios y funcionalidades y asegura ventajas competitivas sostenibles y globales. Lo anterior, en plena concordancia con el mandato establecido en el artículo 333 de la Constitución, según el cual, "*la empresa, como base del desarrollo, tiene una función social que implica obligaciones*".

El régimen jurídico sobre la protección de datos personales consta, a nivel legal, de dos cuerpos normativos. Ambos son aplicables a las operaciones realizadas por actores que prestan servicios financieros a través de aplicaciones o plataformas tecnológicas. Por un lado, la Ley Estatutaria 1266 de 2008 regula el manejo de la información financiera, crediticia, comercial y de servicios contenida en bases de datos personales. En concreto, es aplicable al tratamiento de datos personales relacionados con el nacimiento, ejecución y extinción de obligaciones dinerarias (literal j, artículo 3, Ley 1266 de 2008). Por otro

lado, la Ley Estatutaria 1581 de 2012 establece el régimen general de protección de datos personales. Esta ley es aplicable a cualquier tratamiento de información personal excluido del ámbito de aplicación de la Ley 1266 de 2008.

La legislación sobre protección de datos personales colombiana reconoce los derechos de las personas en relación con el tratamiento de sus datos personales, establece los principios para dicho tratamiento y asigna a los operadores, fuentes, usuarios, responsables y encargados del tratamiento, el cumplimiento de obligaciones específicas al momento de recolectar, almacenar, tratar y circular los datos personales de terceros. Las leyes estatutarias 1266 de 2008 y 1581 de 2012 son neutrales tecnológicamente y sus mandatos se aplican a todo tratamiento de datos personales que se realice en el marco de los modelos de negocio, aplicaciones y procesos que utilizan tecnología informática para prestar servicios financieros y que conforman el ecosistema y los productos fintech.

La Superintendencia de Industria y Comercio, como Autoridad Nacional de protección de datos personales es la entidad encargada de "*velar por el cumplimiento de la legislación en materia de protección de Datos personales*" (literal a), artículo 21, Ley 1581 de 2012). Ante el crecimiento y expansión del ecosistema fintech y la prestación de nuevos servicios, la Superintendencia de Industria y Comercio ha identificado la necesidad de instruir a los actores que operan en el ecosistema sobre los deberes existentes en materia de datos personales.

Por todo lo anterior, la Superintendencia de Industria y Comercio, en ejercicio de sus facultades de "*impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación* [a la ley] *de las operaciones de los Responsables y Encargados del Tratamiento"* que le confiere la Ley 1581 de 2012 (artículo 21, literal e) y de "i*mpartir instrucciones y órdenes sobre la manera como deben cumplirse las disposiciones* [legales] *relacionadas con la administración de la información financiera, crediticia* [y] *comercial*" que le confiere la Ley 1266 de 2008 (artículo 17, numeral 1), **instruye** a todos los responsables y encargados sobre el tratamiento de datos personales en el ecosistema fintech y los modelos de negocio, aplicaciones y procesos que utilizan medios tecnológicos para la prestación de servicios financieros, en los siguientes términos:

Instrucciones

1. El tratamiento de datos personales en el ecosistema fintech y los modelos de negocio, aplicaciones y procesos que utilizan medios tecnológicos para la prestación de servicios financieros solo puede adelantarse para satisfacer finalidades

constitucionalmente legítimas. Únicamente se puede realizar tratamiento de datos personales durante el tiempo que resulte razonable y necesario, de acuerdo con las finalidades que lo justificaron.

2. El tratamiento de datos personales en el ecosistema fintech y los modelos de negocio, aplicaciones y procesos que utilizan medios tecnológicos para la prestación de servicios financieros debe limitarse a aquellos datos que sean pertinentes, adecuados y necesarios para cumplir las finalidades constitucionalmente legítimas para la cual hayan sido recolectados. Los actores del ecosistema fintech deben aplicar criterios para minimizar el tratamiento de datos personales. Las aplicaciones por medio de las cuales se accede al servicio o producto no deben solicitar acceso a información innecesaria como la galería de imágenes del dispositivo o la lista de contactos.

3. El tratamiento de datos personales en el ecosistema fintech debe incluir procedimientos que aseguren, de manera previa a la recolección de los datos, la obtención de la autorización del titular para dicho tratamiento. Asimismo, se debe informar al titular sobre cuáles son los datos personales que serán recolectados y las finalidades específicas que justifican su tratamiento. Por tanto, en las aplicaciones disponibles para descarga, es el titular quien debe decidir si otorga acceso a su información personal, como, por ejemplo, el acceso a la ubicación o a la cámara. En dicho sentido, deberá informarse de manera clara la finalidad de cada acceso, a fin de que el titular pueda tomar una decisión informada sobre el uso de sus datos.

4. La autorización para el tratamiento de datos personales la puede expresar el titular de la información por escrito, por un mensaje de datos, de forma oral o mediante conductas inequívocas que permitan determinar de forma razonable que se otorgó la autorización. Para el tratamiento de datos sensibles no procede la autorización mediante conductas inequívocas. Los actores del ecosistema fintech deben contar con evidencia de que el titular de la información efectivamente otorgó su autorización para el tratamiento de sus datos personales. La autorización debe estar disponible para la consulta del titular.

5. En los casos en que se solicite autorización para el tratamiento de datos personales con finalidades adicionales a aquellas estrictamente necesarias para la prestación del servicio, dicha autorización deberá otorgarse de manera diferenciada. Para solicitar la autorización en estos casos, se sugiere usar palabras sencillas y

expresiones breves, que sean comprensibles por los titulares. Se podrían señalar, entre otras, las siguientes finalidades diferenciadas: para perfilamiento y mejor conocimiento de los gustos y necesidades; para activar alianzas con comercios aliados; para compartir con entidades vinculadas con fines comerciales y/o publicitarias; para realizar contacto con fines comerciales y/o publicitarios.

El titular tiene el derecho a autorizar, de forma libre, previa e informada, únicamente aquellos tratamientos con los que esté de acuerdo y excluir aquellos que no desee autorizar. El responsable del tratamiento deberá asegurar que el mecanismo de recolección de la autorización permita al titular seleccionar de manera diferenciada cada una de las finalidades no necesarias, sin que la negativa a autorizarlas impida la prestación del servicio principal.

6. Está prohibido condicionar la realización de actividades financieras o el acceso a servicios y productos financieros a través de medios tecnológicos al suministro de datos personales sensibles, en especial, al suministro de datos biométricos. Cuando se realice tratamiento de datos sensibles, el responsable deberá contar con medidas de seguridad adicionales que garanticen la protección de la información. Asimismo, deberá obtener por escrito o mediante un mensaje de datos la autorización del titular.

7. La recolección y el tratamiento de datos personales sensibles, en especial de datos biométricos, requiere una diligencia reforzada por parte del responsable del tratamiento. Por eso, al momento de la recolección que en todo caso deber ser excepcional, el responsable del tratamiento deberá informar al titular:
    a. Que por tratarse de datos sensibles no está obligado a autorizar su tratamiento; y
    b. Cuáles de los datos que serán objeto de tratamiento son sensibles y cuáles son las finalidades específicas de dicho tratamiento, por cada tipo de dato personal sensible.

8. Los actores del ecosistema fintech deberán garantizar la transparencia en el uso de tecnologías automatizadas en sus procesos de tratamiento de datos personales. En particular, deberán informar de manera clara y suficiente a los titulares de los datos personales sobre la utilización de este tipo de tecnología. Esta información deberá estar disponible desde el momento de la recolección de los datos en la Política de Tratamiento de la Información, así como en los términos y condiciones y/o mediante

mensajes específicos durante el proceso de registro o solicitud del servicio, transmitidos en un lenguaje comprensible para el usuario promedio.

9. Ningún titular podrá ser objeto de una decisión basada exclusivamente en el tratamiento automatizado de sus datos personales sin haber sido debidamente informado sobre ello. Asimismo, los titulares tendrán el derecho a impugnar una decisión automatizada a través de los canales dispuestos para la presentación de peticiones o reclamos, especialmente cuando dicha decisión tenga consecuencias negativas o determinantes, como la negación de un crédito o el rechazo en la apertura de un producto o servicio financiero. Cuando corresponda, los responsables y encargados del tratamiento deberán tener en cuenta lo dispuesto en la Circular Externa No. 002 del 21 de agosto de 2024 de esta entidad, sobre "Lineamientos sobre el Tratamiento de Datos Personales en Sistemas de Inteligencia Artificial".

10. Los actores del ecosistema fintech deben garantizar la seguridad de los datos personales sometidos a tratamiento. Por tanto, deben adoptar medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole para evitar la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información. Las medidas de seguridad implementadas deben registrarse y revisarse de manera periódica, adaptándose a la evolución de los riesgos y al estado del arte en materia de seguridad de la información. Las medidas de seguridad implementadas deben estar documentadas y ser apropiadas al tipo y nivel de riesgo, así como ser auditables por las autoridades para su evaluación y mejora permanentes.

11. Los actores del ecosistema fintech deben establecer mecanismos sencillos y ágiles que se encuentren permanentemente disponibles a los titulares con el fin de que estos puedan acceder a sus datos personales y ejercer sus derechos. Se reitera el deber y la importancia de anunciarlos en la Política de Tratamiento y en cualquier otro medio que facilite su ubicación y conocimiento por parte de los titulares. Debe garantizarse en todo momento el derecho fundamental al habeas data de los titulares, esto es, el derecho a conocer, rectificar, actualizar y suprimir sus datos personales, en los términos del artículo 15 de la Constitución, la Ley 1266 de 2008, la Ley 1581 de 2012 y la jurisprudencia constitucional.

12. Los actores del ecosistema fintech deben implementar procedimientos que garanticen el mantenimiento de registros detallados sobre las solicitudes de acceso a datos personales por parte de terceros autorizados por el titular. Dichos registros

deberán incluir, como mínimo, la identidad del solicitante, el origen de los datos, el destinatario, la finalidad del acceso y las fechas en que se realizaron dichas acciones. Estos registros deberán conservarse por un período razonable, definido conforme a los principios de necesidad y proporcionalidad, y deberán ser puestos a disposición de los titulares y de las autoridades competentes, cuando así se requiera.

13. Los responsables y encargados deberán implementar estrategias de diseño legal orientadas a mejorar la comprensión del titular sobre el uso de su información personal. Estas estrategias podrán incluir la presentación por capas, siempre que cumplan con los requisitos legales y faciliten la comprensión clara y gradual de la información relevante para el ejercicio de los derechos del titular. Asimismo, deberán habilitarse, de forma visible e intuitiva, mecanismos que permitan a los titulares gestionar sus preferencias de privacidad y decidir sobre la entrega de sus datos personales a terceros. El tratamiento de los datos personales deberá observar el principio de transparencia y el deber de informar al titular, garantizando que reciba información clara y suficiente sobre los terceros que tendrán acceso a sus datos, indicando la calidad en la que actúan (responsables, encargados o terceros autorizados). Destinar recursos a este tipo de estrategias e implementarlas con efectividad podrá ser valorado en el contexto del cumplimiento del principio de responsabilidad demostrada.

14. Los actores del ecosistema fintech que adelanten gestiones de cobranza de forma directa, por medio de terceros o por cesión de la obligación, deberán abstenerse de contactar a las referencias personales suministradas por los consumidores financieros. El incumplimiento de estos deberes es objeto de vigilancia y control por parte de la Delegatura para la Protección de Datos Personales conforme a lo establecido en las leyes 1266 de 2008, 1581 de 2012 y 2300 de 2023, y la Circular Externa 001 del 26 de junio de 2024 de esta Superintendencia.

15. Los actores del ecosistema fintech deberán implementar mecanismos accesibles y continuos para ilustrar e informar a los titulares acerca de sus derechos en materia de protección de datos personales y en los riesgos asociados al tratamiento de su información. Por tanto, se les exhorta a asumir un rol proactivo en la sensibilización de sus clientes y usuarios sobre la importancia de la protección de sus datos personales. La trazabilidad sobre estas acciones podrá evidenciarse a través de indicadores y cualquier otro medio idóneo, los cuales deberán estar disponibles para ser compartidos con la Autoridad. Destinar recursos a este tipo de estrategias e

implementarlas con efectividad podrá ser valorado en el contexto del cumplimiento del principio de responsabilidad demostrada.

16. Los actores del ecosistema fintech deberán definir de manera expresa y documentada sus roles en el tratamiento de datos personales, conforme a lo dispuesto en la Ley 1581 de 2012 y sus normas reglamentarias. Cuando se realicen transmisiones de datos personales, estas deberán ser formalizadas mediante el respectivo contrato de transmisión de datos personales. En los casos en que la comunicación de datos se realice entre responsables del tratamiento, deberán contar con la autorización previa, expresa e informada del titular, salvo las excepciones establecidas en la ley. En todo caso, si se evidencia que un actor del ecosistema fintech, aun cuando haya sido designado formalmente como encargado del tratamiento, determina en la práctica los fines y medios del tratamiento de los datos personales, se considerará responsable del tratamiento. En tal condición, asumirá las obligaciones previstas para este rol en el régimen de protección de datos personales.

17. En caso de que los modelos de negocio, aplicaciones y procesos que utilizan medios tecnológicos para la prestación de servicios financieros realicen transferencias o transmisiones internacionales de datos personales, el responsable ubicado en territorio nacional deberá:
    a. Validar que el encargado o responsable destinatario esté ubicado en un país que cuente con un nivel adecuado de protección de datos personales, conforme al numeral 3.2 del Título V de la Circular Única de la Superintendencia de Industria y Comercio.
    b. En caso de que la transferencia y transmisión se realice a un país que no cuente con un nivel adecuado de protección de datos personales conforme el párrafo anterior, el responsable del tratamiento deberá validar que la operación se encuentre dentro de las excepciones establecidas en el artículo 26 de la Ley 1581 de 2012.
    c. En caso de que no se encuentre dentro de las excepciones de ley, deberá verificar que el país al que se transfieren o transmiten los datos personales cumpla con los estándares fijados en el numeral 3.1 del Título V de la Circular Única de la Superintendencia de Industria y Comercio.
    d. Finalmente, si la transferencia no se encuentra en el escenario anterior, deberá solicitar declaración de conformidad ante la Delegatura para la Protección de Datos Personales, en los términos del numeral 3.3 del Título V de la Circular Única de la Superintendencia de Industria y Comercio.

18. La suscripción de las Cláusulas Contractuales Modelo que se incluyen en la "*Guía de implementación cláusulas contractuales modelo para la Transferencia internacional de Datos personales (TIDP)*" de la Red Iberoamericana de Protección de Datos y su anexo "*Modelo de Cláusulas Contractuales*" constituye una medida apropiada y efectiva para demostrar la implementación del principio de responsabilidad demostrada en las transferencias internacionales de datos personales.

Cordialmente,

CIELO ELAINNE RUSINQUE URREGO
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Elaboró: Daniel Ospina Celis
Revisó: Héctor Barragán / Juan Carlos Upegui
Aprobó: Alejandro Bustos / Juan Carlos Upegui