Desafíos jurídicos en la protección de la seguridad y privacidad de los usuarios de servicios fintech en Colombia: hacia un fortalecimiento normativo

Autora:

Ángela Rocío Quiroga Gutiérrez

Universidad Santo Tomás Seccional Tunja

Facultad de Derecho

Maestría en Derecho Privado

Tunja

2025

Contenido

Introducción 8

Capítulo 1. Análisis del marco jurídico colombiano en materia de protección a usuarios fintech 12

Marco constitucional relacionado 12

Régimen de protección al consumidor financiero 16

Normativa sobre protección de datos y seguridad de la información 19

Legislación financiera base 22

Regulación de servicios financieros digitales y de inclusión 25

Vacíos, limitaciones y desafíos del marco regulatorio actual 33

Capítulo 2. Implicaciones jurídicas de las tecnologías emergentes en la protección de usuarios fintech 38

Open Finance 39

Neobancos y Banca Digital 41

Computación en la nube 42

Inteligencia artificial en servicios financieros 42

Big data y analytics 43

Billeteras móviles 44

Biometría y autenticación avanzada 45

Roboadvisors y automatización 46

Blockchain y contratos inteligentes 47

Crowdfunding y Plataformas de Financiación Colaborativa 50

Insurtech (Tecnologías aplicadas a seguros) 51

Desafíos regulatorios de las nuevas tecnologías 51
Capítulo 3. Responsabilidad civil de las empresas fintech 56
Marco jurídico de responsabilidad civil en servicios financieros digitales 56
Determinación de responsabilidades ante incidentes de seguridad 59
Mecanismos de protección y resarcimiento para usuarios 63
Análisis de casos y jurisprudencia relevante 66
Propuestas para fortalecer el régimen de responsabilidad 68
Capítulo 4. Análisis comparado de experiencias regulatorias internacionales 73
Marcos regulatorios internacionales 73
Europa 73
América del norte 76
Latinoamérica 77
Asia 82
Oceanía 84
Síntesis comparativa de regiones 85
Modelos regulatorios de referencia internacional 87
De la regulación rígida a la gobernanza ágil 88
Sandboxes regulatorios como herramienta de innovación 89
Surgimiento de hubs de innovación y RegTech 91
Balance entre protección al consumidor e innovación 92
Co-gobernanza público-privada 94
Armonización internacional y cooperación transfronteriza 96
Adaptación contextual a realidades regionales 98

Modelo Experimental 99
Distinción entre Regulación Integral y Sectorial 100
Mejores prácticas en la protección de la seguridad y privacidad de usuarios fintech 101
Europa 101
América del norte 103
Latinoamérica 105
Asia 109
Oceanía 112
Síntesis comparativa de regiones 114
Capítulo 5. Recomendaciones para el fortalecimiento normativo en Colombia 116
Desarrollo de un marco jurídico específico y consolidado 116
Fortalecimiento y clarificación de competencias supervisoras 116
Desarrollo normativo para tecnologías emergentes 117
Fortalecimiento de la protección de datos específica para fintech 117
Ampliación y fortalecimiento del sandbox regulatorio 118
Regulación proporcional basada en riesgos 118
Mecanismos ágiles de resolución de disputas 119
Fortalecimiento de la educación financiera digital 119
Desarrollo de estándares técnicos de seguridad específicos 119
Implementación integral de finanzas abiertas (Open Finance) 120
Hacia un modelo de co-gobernanza público-privada 120
Conclusiones 122
Referencias 125

Lista de figuras

Figura 1. Tecnologías utilizadas por las Fintech en Colombia 39

Lista de tablas

Tabla 1. Comparación de Marcos Regulatorios FinTech por Regiones 86

Tabla 2. Comparación de Mejores Prácticas de Protección de Seguridad y Privacidad por Regiones 114

Introducción

La tecnología financiera ha revolucionado el panorama financiero global, integrándose en la vida cotidiana a través de servicios como banca móvil y pagos instantáneos. El surgimiento de bancos digitales, plataformas de préstamos *peer-to-peer*[1] y soluciones blockchain[2] ha democratizado el acceso a servicios financieros, ofreciendo alternativas eficientes a los sistemas bancarios convencionales. Las pequeñas y medianas empresas han sido las principales beneficiarias de esta transformación digital, accediendo a servicios personalizados a través de bancos en línea, crowdfunding y plataformas P2P. Sin embargo, este nuevo ecosistema financiero presenta desafíos regulatorios que requieren equilibrar la innovación con una supervisión efectiva, mientras las fintech[3] continúan expandiéndose y remodelando el panorama financiero internacional (Cumming et al., 2023).

En Colombia, el sector fintech ha experimentado un crecimiento exponencial en los últimos años, transformando radicalmente la forma en que los ciudadanos acceden a servicios financieros. Según datos de Colombia Fintech (2024b), la asociación del sector, el país a Julio de 2024 contaba con 369 empresas, de las cuales 269 se encontraban clasificadas en nueve verticalidades[4], siendo el crédito digital y pagos digitales las que representan el 65% de ellas. Este crecimiento ha traído consigo una serie de desafíos regulatorios y jurídicos, particularmente en lo que respecta a la protección de los derechos de los usuarios.

---

[1] Es una red donde todos los participantes se conectan directamente entre sí y funcionan tanto como servidores como clientes, sin necesidad de un servidor central.

[2] Es una base de datos digital distribuida y descentralizada que almacena información en "bloques" conectados entre sí de forma cronológica, donde cada nuevo bloque contiene un registro de las transacciones previas que no puede ser alterado sin modificar todos los bloques posteriores.

[3] Es una empresa que utiliza la tecnología para innovar, mejorar o automatizar servicios y procesos financieros

[4] Las verticalidades comprenden: crédito digital, pagos digitales, finanzas empresariales, crypto y blockchain, Regtech, PFM & Wealtech, Crowdfunding, Neobancos, Insurtech y otros.

En la literatura académica se han abordado los desafíos regulatorios en la seguridad y privacidad de los usuarios Fintech desde diferentes perspectivas. En casos internacionales Prayuti (2024) destacó la necesidad de fortalecer los marcos regulatorios para proteger a los consumidores de fraudes y violaciones de datos y, aunque no profundiza en aspectos de responsabilidad civil por violaciones de seguridad y privacidad, identificó debilidades como la falta de especificidad en las regulaciones, supervisión inconsistente y vacíos en la protección de datos personales. De manera similar, Bongomin & Ntayi (2020) identificaron desafíos aplicables al contexto colombiano como la falta de transparencia, seguridad cibernética insuficiente, riesgos operativos y técnicos en los servicios financieros móviles, enfatizando más en aspectos generales de protección al consumidor como mecanismos de reclamación y compensación.

En Colombia, Pertuz (2021) analizó el sandbox regulatorio como mecanismo de supervisión, enfatizando sus limitaciones para proteger a los usuarios, mientas que Arias & Lis (2024) abordaron de manera más general los desafíos regulatorios del sector fintech en Colombia, incluyendo aspectos de ciberseguridad y protección de datos. A su vez, Guzmán (2024) abordó temas como seguridad de datos y prácticas abusivas en relación a la protección al consumidor por medio de instituciones de supervisión.

Por su parte, las investigaciones de González (2024) y Anaya (2020) establecieron la necesidad de fortalecer la protección del consumidor financiero frente a los nuevos canales digitales en Colombia; el primero, enfatizó en el desarrollo de principios y mandatos de optimización para resolver conflictos contractuales, el segundo, profundizó en la responsabilidad civil de las entidades financieras frente a fraudes electrónicos, destacando que los bancos deben asumir la carga de la prueba y demostrar que actuaron con la debida diligencia en casos de violaciones de seguridad.

Los estudios de Gutiérrez & Moreno (2023) y Albarracín (2023) convergen en identificar que la regulación fintech en Colombia, aunque fundamentada en el artículo 335 constitucional y complementada con normativas sobre protección de datos (Ley 1581 de 2012) y delitos informáticos (Ley 1273 de 2009), presenta limitaciones sustanciales. Sus principales hallazgos resaltan la existencia de un marco regulatorio parcial orientado a la protección del interés público y la gestión de riesgos en ciberseguridad y prevención del fraude.

Estas tendencias en investigación coinciden en la ausencia de una legislación integral específica para fintech, particularmente en materia de responsabilidad civil por violaciones a la seguridad y privacidad de usuarios. La presente investigación confirma hallazgos en esta dirección, pero profundiza su análisis en las posibilidades de fortalecimiento normativo considerando la emergencia de nuevas tecnologías y sus implicaciones jurídicas, la responsabilidad civil de las fintech en casos de violaciones a la seguridad y privacidad de los usuarios, y recomendaciones basadas en experiencias exitosas de regulación fintech.

Si bien existen regulaciones generales aplicables, la falta de un marco legal especializado crea incertidumbre sobre el alcance y la efectividad de la protección de los derechos de los usuarios en estas plataformas financieras digitales. Por lo tanto, cuando se interponen procesos por responsabilidad civil contractual y extracontractual por vulneraciones a la protección y seguridad de datos; existe inseguridad jurídica por la dificultad de su resolución por medio de un juez.

En este contexto, surge la necesidad de analizar cómo el marco jurídico colombiano puede evolucionar para proteger efectivamente los derechos de los usuarios de servicios fintech, sin obstaculizar la innovación que está transformando el panorama financiero del país. Este análisis debe considerar no solo la legislación existente y propuesta, sino también las mejores prácticas internacionales y las particularidades del mercado colombiano. De esta manera, la presente

monografía responde a la siguiente pregunta de investigación: ¿Cuáles son los principales desafíos jurídicos para proteger la seguridad y privacidad de los usuarios de servicios fintech, considerando el marco regulatorio actual, el impacto de las tecnologías emergentes y las experiencias regulatorias internacionales?

Como objetivo general, esta monografía se propone analizar los desafíos jurídicos en la protección de la seguridad y privacidad de los usuarios de servicios fintech en Colombia, considerando el marco regulatorio actual, las tecnologías emergentes y las experiencias internacionales, que permitan el fortalecimiento normativo. Esto implica cuatro objetivos específicos, cada uno abordado en los capítulos que constituyen este trabajo: 1) Identificar los vacíos y limitaciones del marco jurídico colombiano vigente en materia de protección a usuarios de servicios fintech; 2) Examinar las implicaciones jurídicas del uso de tecnologías emergentes utilizadas por las fintech en la protección de datos y privacidad de usuarios fintech; 3) Evaluar los mecanismos jurídicos existentes para la determinación de responsabilidad civil de las empresas fintech ante incidentes de seguridad; 4) Proponer mejoras al marco regulatorio colombiano a partir del análisis de experiencias internacionales en protección de usuarios fintech.

Metodológicamente, esta investigación adopta un enfoque cualitativo de tipo documental, fundamentado en la revisión sistemática y análisis de fuentes primarias (normatividad vigente, jurisprudencia y documentos oficiales de entidades reguladoras) y secundarias (literatura académica especializada, informes técnicos y análisis comparativos). El procesamiento de la información seguirá tres fases: una descriptiva para identificar los elementos del marco regulatorio actual, una analítica para examinar críticamente las implicaciones legales y la efectividad de las regulaciones existentes, y una propositiva para desarrollar recomendaciones que fortalezcan la protección de los derechos de los usuarios fintech en Colombia.

Capítulo 1. Análisis del marco jurídico colombiano en materia de protección a usuarios fintech

El marco jurídico colombiano en materia de protección a usuarios fintech se sustenta en una estructura regulatoria multinivel que parte desde la Constitución Política de 1991, pasando por leyes estatutarias y ordinarias, hasta decretos y circulares de las entidades supervisoras. Esta arquitectura normativa aborda aspectos fundamentales como la protección de datos personales, la seguridad de la información, los derechos del consumidor financiero y la regulación de servicios financieros digitales, estableciendo un balance entre la promoción de la innovación tecnológica y la salvaguarda de los derechos de los usuarios. Sin embargo, el marco actual presenta tanto fortalezas como desafíos significativos en su objetivo de proporcionar una protección integral a los usuarios de servicios financieros digitales.

Marco constitucional relacionado

La Constitución Política de Colombia de 1991 establece diversos principios fundamentales que sustentan y enmarcan la regulación de las fintech en el país. El artículo 15 constituye uno de los pilares esenciales al garantizar el derecho fundamental a la intimidad personal y familiar, así como el derecho de los individuos consultar, modificar y corregir sus datos personales almacenados en repositorios informáticos. Este derecho resulta particularmente relevante en el contexto de la economía digital, donde las empresas fintech procesan grandes volúmenes de datos personales y financieros de sus usuarios para ofrecer servicios personalizados y evaluar riesgos crediticios.

El artículo 333 reconoce la libertad de actividad económica e iniciativa privada dentro de los límites del bien común, lo que permite el desarrollo de nuevos modelos de negocio en el sector

financiero, siempre que se ejerzan responsablemente. Este artículo también establece que el Estado debe evitar cualquier abuso de posición dominante en el mercado, lo cual es particularmente relevante en el contexto de la innovación financiera y la competencia con instituciones tradicionales. La disposición constitucional equilibra la libertad empresarial con la responsabilidad social, estableciendo un marco que fomenta la innovación mientras protege los intereses colectivos.

La intervención estatal en el sector financiero encuentra su base en el artículo 335, que define la actividad financiera como de interés público y establece que solo puede ser ejercida con previa autorización del Estado, conforme a la ley. Este artículo es fundamental para justificar la regulación específica de las fintech y la supervisión por parte de entidades como la Superintendencia Financiera. La naturaleza de interés público de la actividad financiera implica una responsabilidad especial para las empresas tecnológicas que ofrecen servicios financieros, requiriendo un equilibrio entre innovación y estabilidad del sistema.

El artículo 334 otorga al Estado la dirección general de la economía y le obliga a intervenir para promover la democratización del crédito, lo cual se alinea con los objetivos de inclusión financiera que persiguen muchas fintech. Esta disposición cobra especial relevancia en el contexto de la transformación digital del sector financiero, donde las nuevas tecnologías pueden servir como herramientas para ampliar el acceso a servicios financieros en poblaciones tradicionalmente excluidas. Complementariamente, el artículo 78 determina que los productores y comerciantes de productos y servicios son responsables por acciones que perjudiquen la salud, seguridad o el suministro apropiado para los consumidores, fundamentando la protección del consumidor financiero en el entorno digital.

El artículo 20, que garantiza el derecho a la información, y el artículo 58, que protege la propiedad privada, completan el marco constitucional relevante para las fintech. El primero sustenta la obligación de transparencia y divulgación adecuada sobre productos y servicios financieros digitales, mientras que el segundo respalda la seguridad de las transacciones y activos digitales. Estas disposiciones, junto con las anteriormente mencionadas, conforman una base constitucional robusta que permite el desarrollo del sector fintech mientras asegura la protección de los derechos fundamentales de los usuarios y la estabilidad del sistema financiero en su conjunto.

La Corte Constitucional se ha pronunciado en referencia a la protección de los usuarios en que adquieren servicios financieros, con implicaciones en las fintech. El primer pronunciamiento relevante se dio en la Sentencia SU-157 de 1999, donde estableció un precedente fundamental al reconocer el acceso al sistema financiero como un derecho fundamental. Esta sentencia exige al Gobierno proporcionar garantías que aseguren condiciones equitativas y objetivas tanto para acceder a la actividad bancaria como para la obtención de créditos.

Posteriormente, en la Sentencia C-955 de 2000, la Corte profundizó su postura estableciendo que las operaciones de intermediación financiera en el contexto colombiano no constituyen un ejercicio de libre albedrío, sino que conllevan compromisos concretos y un rol social que exige el cumplimiento de deberes particulares. Este pronunciamiento fue crucial pues estableció claramente que la libertad de las entidades financieras está restringida y dirigida por el Estado, fundamentando esta intervención en los artículos 334 y 335 de la Constitución.

Una década después, mediante la Sentencia C-640 de 2010, la Corte amplió su interpretación sobre la intervención estatal en la actividad financiera. Este pronunciamiento fue particularmente relevante pues estableció que la intervención del Estado se fundamenta en la

obligación de brindar certidumbre y protección a los usuarios, puesto que esta operación involucra la administración de sus fondos. El Tribunal destacó que los sectores financiero, bursátil y de seguros resultan esenciales para el crecimiento económico, y su efectividad requiere normativas apropiadas y fiscalización especializada y competente.

En años más recientes, a través de las Sentencias C-793 de 2014 y C-331 de 2020, la Corte ha reafirmado y consolidado su doctrina sobre el factor de interés público como criterio ordenador de la actividad financiera. Dichas decisiones han consolidado el imperativo de la participación gubernamental en el ámbito financiero para salvaguardar los intereses de todas las partes implicadas, estableciendo que esta supervisión debe realizarse a través de la Superintendencia Financiera, cuya propósito es preservar el orden en el mercado y asegurar que todos los agentes participen bajo circunstancias equitativas y con claridad informativa.

La Sentencia T-584 de 23 de la Corte Constitucional colombiana establece un precedente fundamental en la protección de usuarios de servicios financieros digitales (fintech), específicamente en el contexto de aplicaciones de préstamos. Al examinar las prácticas abusivas de cobranza de Lukiao App S.A.S., que incluyeron acoso digital, intimidación física y exposición pública de información personal, la Corte determinó que la innovación financiera digital no puede desarrollarse a costa de los derechos fundamentales de los usuarios. La sentencia equilibra el legítimo derecho de las fintech a cobrar sus acreencias con la protección constitucional de la intimidad, honra, buen nombre y habeas data de los usuarios, estableciendo parámetros claros para el sector en un momento crucial de su expansión.

Régimen de protección al consumidor financiero

La protección al consumidor financiero en Colombia se ha fortalecido significativamente a través de diversas leyes que establecen un marco regulatorio integral. La Ley 1328 de 2009 sentó las bases fundamentales al establecer los principios y reglas que rigen la protección de los consumidores financieros, incluyendo aspectos clave como la transparencia, la libertad de elección y el manejo adecuado de conflictos de interés.

En materia de transparencia informativa, las instituciones financieras están obligadas a proporcionar información clara, suficiente y oportuna sobre sus productos y servicios. Esto incluye la divulgación del Valor Total Unificado de las operaciones, que debe expresarse en términos porcentuales efectivos anuales, según lo establecido por la Ley 1748 de 2014. Esta medida permite a los consumidores comprender mejor los costos totales de los servicios financieros.

En cuanto a los derechos específicos de los consumidores, la Ley 1555 de 2012 introdujo importantes beneficios como la posibilidad de realizar pagos anticipados en operaciones de crédito sin penalizaciones, para créditos hasta 880 SMMLV. Por su parte, la Ley 1793 de 2016 fortaleció la protección en el ámbito de las cuentas de ahorro, eliminando la obligación de mantener saldos mínimos, limitando los cobros por inactividad a solo 60 días y estableciendo la obligación de las entidades financieras de reconocer un porcentaje mínimo de rendimiento financiero en todos los depósitos de ahorro, sin importar el monto de los fondos depositados.

El Decreto 1357 de 2018 estableció el marco regulatorio para la actividad de financiación colaborativa (crowdfunding), incluyendo medidas específicas para proteger a los aportantes, como la obligación de informar los riesgos de las inversiones, la prohibición de asegurar retornos, y la necesidad de contar con mecanismos para la resolución de controversias. Esta normativa también

exige que las plataformas de crowdfunding implementen políticas de tratamiento de datos personales y procedimientos para prevenir el lavado de activos.

La Ley 2009 de 2019 complementa este marco regulatorio estableciendo medidas específicas para la protección financiera del consumidor en términos de costos y servicios. Esta ley garantiza el acceso a un paquete mínimo de productos y servicios financieros sin costo adicional para los usuarios que pagan cuotas de manejo, además de prohibir el cobro por operaciones fallidas en cajeros electrónicos y por consultas de saldo en plataformas electrónicas, lo que beneficia especialmente a los usuarios de servicios financieros digitales.

En materia de sistemas de pago, el Decreto 1692 de 2020 fortaleció la protección al consumidor al establecer requisitos de transparencia en las tarifas y comisiones cobradas por los diferentes actores del sistema de pagos de bajo valor. La norma exige que las entidades administradoras de sistemas de pago publiquen información clara sobre costos, requisitos de vinculación y plazos para la acreditación de pagos, además de prohibir prácticas discriminatorias en el acceso a estos servicios.

La innovación financiera y la protección al consumidor se conjugan en el Decreto 1234 de 2020, que creó el espacio controlado de prueba (sandbox regulatorio) para actividades de innovación financiera. Esta normativa establece como uno de sus objetivos principales velar por la protección de los consumidores financieros, exigiendo que las empresas participantes informen claramente a sus usuarios que están participando en un ambiente de prueba y los riesgos asociados.

En cuanto a la protección de datos financieros, la Ley 2157 de 2021 (Ley de Habeas Data) fortaleció los derechos de los consumidores en relación con su información crediticia. La ley establece plazos máximos de permanencia para la información negativa, requisitos de comunicación previa al reporte negativo, y mecanismos de protección contra la suplantación de

identidad. Además, implementa un sistema de alertas para nuevas obligaciones crediticias y establece la gratuidad en la consulta de la información financiera por parte del titular.

De manera compilatoria, la Circular Básica Jurídica de la Superintendencia Financiera de Colombia establece un marco integral para la protección del consumidor financiero, estructurado principalmente en torno a tres pilares fundamentales. El primero se centra en garantizar el acceso y la transparencia de la información, exigiendo que las entidades financieras proporcionen información clara, comprensible y oportuna sobre sus productos y servicios, incluyendo condiciones específicas sobre publicidad, régimen de horarios y gestión de cobranza. El segundo pilar establece mecanismos concretos de atención al consumidor a través del Sistema de Atención al Consumidor Financiero (SAC) y la Defensoría del Consumidor Financiero, creando canales efectivos para la presentación y gestión de quejas y reclamos (Superintendencia Financiera de Colombia, 2014).

El tercer pilar se enfoca en la prevención de prácticas abusivas y la promoción de prácticas justas en la prestación de servicios financieros, regulando aspectos como cláusulas contractuales, condiciones de los productos y transparencia en las operaciones. Esta estructura se complementa con disposiciones transversales que aparecen en diferentes secciones de la circular, abarcando aspectos como la gestión de productos específicos, reglas sobre publicidad, y obligaciones de reporte y seguimiento, todo ello orientado a asegurar una adecuada protección de los derechos de los consumidores en el sistema financiero colombiano (Superintendencia Financiera de Colombia, 2014).

Normativa sobre protección de datos y seguridad de la información

La protección de datos personales y la seguridad de la información en el entorno fintech en Colombia tiene sus bases fundamentales en tres leyes principales que se han desarrollado cronológicamente para adaptarse a las necesidades del sector financiero y tecnológico. Inicialmente, la Ley 1266 de 2008 estableció las disposiciones generales del hábeas data, regulando específicamente el manejo de la información financiera, crediticia y comercial. Esta ley fue pionera en establecer los principios de veracidad, finalidad, circulación restringida y temporalidad de la información, siendo particularmente relevante para las instituciones financieras y las empresas fintech que manejan datos crediticios de los usuarios.

En materia de seguridad y protección de datos financieros, la Ley 1357 de 2009 fortaleció el marco normativo al modificar el Código Penal, estableciendo sanciones más severas para quienes realicen captación masiva y habitual de dinero sin autorización. Esta ley es especialmente relevante para el sector fintech, ya que establece penas de 120 a 240 meses de prisión y multas significativas para quienes capten dinero del público sin autorización, incluyendo el uso de medios de comunicación social u otros de divulgación colectiva, lo cual es particularmente aplicable a las plataformas digitales financieras.

La evolución del marco regulatorio continuó con la Ley 1581 de 2012, que estableció el régimen general de protección de datos personales, complementando y ampliando el alcance de la Ley 1266. Esta ley introdujo principios fundamentales como el de libertad, transparencia, acceso restringido, seguridad y confidencialidad, que son cruciales para las operaciones fintech. Además, estableció categorías especiales de datos, incluyendo los datos sensibles, y definió claramente las facultades de quienes son dueños de los datos, junto con las responsabilidades que deben cumplir aquellos que administran y procesan la información.

En el ámbito de la seguridad operacional, las leyes establecen requisitos específicos para la protección de la información. Las empresas fintech deben implementar medidas técnicas, humanas y administrativas para garantizar la seguridad de los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado según lo establecido en la Ley 1581 de 2012. Esto se complementa con las disposiciones de la Ley 1266 de 2008, que requiere sistemas de seguridad robustos para la administración de datos financieros.

La regulación también establece mecanismos de vigilancia y control específicos para el sector. La Superintendencia de Industria y Comercio y la Superintendencia Financiera tienen facultades para supervisar y sancionar a las entidades que incumplan las normas de protección de datos, con multas que pueden alcanzar los 2,000 salarios mínimos mensuales legales vigentes. En el caso específico de las fintech, dependiendo de su naturaleza y servicios, pueden estar sujetas a la supervisión de ambas superintendencias, especialmente cuando manejan datos financieros y realizan actividades de intermediación.

En cuanto a la transferencia internacional de datos, aspecto crucial para muchas fintech que operan globalmente, la Ley 1581 de 2012 establece restricciones específicas, prohibiendo el traslado de información personal hacia naciones que carecen de estándares suficientes de seguridad informativa, exceptuando casos específicos como el consentimiento expreso del titular o la necesidad de la transferencia para ejecutar un contrato. Esto es particularmente relevante para las fintech que utilizan servicios en la nube o procesan datos en diferentes jurisdicciones.

La Circular Externa 029 de 2014, que contiene el compendio normativo que rige la Superintendencia Financiera de Colombia, determina los criterios específicos que deben seguir las entidades vigiladas para garantizar la seguridad y calidad en la realización de operaciones financieras, incluyendo definiciones y estándares mínimos que deben cumplirse. La normativa

aborda aspectos fundamentales como la conservación de documentos, el manejo de la reserva bancaria y el tratamiento de información confidencial de los usuarios. Además, incorpora estos elementos como parte esencial del sistema de control interno de las entidades, estableciendo directrices para la gestión tecnológica y la protección de datos. La circular enfatiza la importancia de mantener la confidencialidad, integridad y disponibilidad de la información en todas las operaciones del sistema financiero, definiendo las responsabilidades de las entidades vigiladas en la implementación de medidas de seguridad adecuadas y en el correcto manejo de la información de sus usuarios.

La Circular 007 de 2018 estableció los primeros lineamientos robustos en materia de ciberseguridad, exigiendo a las entidades financieras implementar políticas y procedimientos específicos para proteger la información de los consumidores en el ciberespacio. Esta normativa requiere que las instituciones cuenten con una unidad especializada en seguridad de la información y ciberseguridad, además de establecer protocolos de prevención, detección y respuesta ante incidentes cibernéticos.

Con el creciente uso de tecnologías digitales, la Circular 005 de 2019 introdujo regulaciones específicas para la utilización de servicios de computación en la nube, permitiendo a las entidades financieras soportar sus procesos misionales en estos servicios, siempre que cumplan con estrictos estándares de seguridad. Esta normativa exige que los proveedores de servicios en la nube mantengan una disponibilidad mínima del 99.95% y cuenten con certificaciones internacionales como ISO 27001, además de establecer mecanismos para garantizar la independencia y el cifrado de la información de los clientes.

La protección contra el lavado de activos y la financiación del terrorismo se fortaleció significativamente con la Circular Externa 027 de 2020, que implementó el SARLAFT 4.0. Esta

actualización modernizó los procedimientos de conocimiento del cliente, permitiendo la vinculación digital y el uso de nuevas tecnologías para la verificación de identidad. La normativa también introdujo un enfoque basado en riesgos más sofisticado, permitiendo a las entidades aplicar medidas simplificadas o reforzadas según el perfil de riesgo del cliente, adaptándose así a las nuevas realidades del entorno fintech.

En materia de transferencias electrónicas, el SARLAFT 4.0 estableció requisitos específicos para las operaciones nacionales e internacionales, exigiendo información detallada sobre ordenantes y beneficiarios, con especial énfasis en las transferencias que utilizan nuevas tecnologías o servicios digitales. Esta regulación también incorporó disposiciones especiales para el monitoreo de operaciones en tiempo real y la implementación de sistemas de alertas tempranas, adaptadas al contexto de las fintech y sus innovadores modelos de negocio.

Legislación financiera base

El marco regulatorio base del sistema financiero colombiano se fundamenta en algunos pilares legislativos fundamentales: La Ley 31 de 1992, que establece la estructura y funciones del Banco de la República como banco central autónomo, regulando sus facultades en materia monetaria, cambiaria y crediticia. La Ley 35 de 1993, que define los parámetros generales bajo los cuales el Gobierno Nacional puede intervenir en las actividades financiera, bursátil y aseguradora, estableciendo un marco de referencia para la protección de los usuarios y la estabilidad del sistema. El Decreto 663 de 1993 (EOSF), que consolida y sistematiza en un solo cuerpo normativo la regulación de las entidades financieras, estableciendo requisitos de constitución, funcionamiento y supervisión de las instituciones del sector. Y la Ley 45 de 1990, que marcó un hito en la modernización del sistema financiero al introducir el concepto de banca múltiple y establecer las

bases para el desarrollo del mercado de valores, aunque varias de sus disposiciones han sido modificadas por normas posteriores, mantiene su importancia como punto de partida de la actual estructura regulatoria del sector financiero colombiano.

Otras leyes han sido relevantes para la regulación general del sistema financiero. La Ley 510 de 1999, fortaleció la regulación del sistema financiero y asegurador estableciendo requisitos más estrictos de capital y supervisión; la Ley 795 de 2003, modernizó el Estatuto Orgánico del Sistema Financiero ampliando las facultades de intervención gubernamental y la protección al consumidor; la Ley 964 de 2005, estableció un marco integral para el mercado de valores y fortaleció la supervisión de la Superintendencia Financiera; la Ley 1314 de 2009, marcó la transición hacia estándares internacionales de contabilidad mejorando la transparencia y competitividad del sector; y la Ley 1340 de 2009, que consolidó el régimen de protección de la competencia otorgando mayores facultades a la Superintendencia de Industria y Comercio para prevenir y sancionar prácticas anticompetitivas en todos los sectores económicos, incluyendo el financiero.

El Decreto 2555 de 2010 establece una serie de regulaciones para el sector financiero colombiano, con el objetivo principal de preservar la credibilidad ciudadana en el sistema y garantizar su evolución bajo parámetros de protección y entorno competitivo. Esta regulación contempla múltiples elementos, como los requisitos patrimoniales que las instituciones crediticias deben conservar (Artículos 2.1.1.1.13, 2.1.2.1.2), la categorización de instrumentos de capital regulatorio (Artículos 2.1.1.1.13, 2.1.1.1.14), y el cociente de solvencia. El decreto también especifica qué organizaciones se consideran establecimientos de crédito, compañías aseguradoras y emisores de valores. Se imponen restricciones a la concentración de riesgos para las entidades

crediticias (Título 3), y se determinan las penalizaciones por infracciones normativas (Artículo 2.1.3.1.5).

En cuanto a la protección de la seguridad y privacidad de los usuarios financieros, el decreto contempla varias disposiciones. Por ejemplo, se establecen requisitos para la apertura de depósitos de bajo monto con trámites simplificados y sin requerir la presencia física del consumidor financiero (Artículo 2.1.6.1.1, 2.1.6.1.4). La normativa también establece los criterios de seguridad y calidad necesarios para la gestión informativa, contemplando medidas contra el blanqueo de capitales y el apoyo económico a grupos terroristas. También se regula el tratamiento de datos personales, exigiendo que las entidades obtengan la autorización previa, expresa e informada de los consumidores financieros. Asimismo, se les exige mantener la reserva bancaria de sus consumidores financieros. Se contempla la existencia de un Defensor del Consumidor Financiero para atender quejas o reclamos. Se establecen reglas para la publicación de información de tarjetas débito y crédito (Título 4) y se menciona la necesidad de que las entidades cuenten con políticas y procedimientos para la administración de conflictos de interés (Artículos 2.1.19.1.1, 2.1.19.1.2, 2.1.19.1.5, 2.36.9.1.14).

La Ley 1870 de 2017 estableció el marco normativo para regular y supervisar los conglomerados financieros en Colombia, definiéndolos como grupos de entidades con un controlante común ("holding financiero") que incluyen dos o más entidades vigiladas por la Superintendencia Financiera. La ley otorgó a esta entidad facultades amplias de supervisión para impartir instrucciones sobre gestión de riesgos, autorizar inversiones y realizar inspecciones, además de establecer instrumentos de intervención relacionados con niveles de capital y límites de exposición al riesgo. También fortaleció los mecanismos de resolución de entidades financieras,

incluyendo procedimientos para la compra de activos y asunción de pasivos en casos de liquidación forzosa administrativa.

Regulación de servicios financieros digitales y de inclusión

En relación con las Fintech o innovaciones y tecnologías financieras, el Decreto 2555 de 2010 introduce el concepto de espacio controlado de prueba para actividades de innovación financiera (Título 7). Este espacio permite probar desarrollos tecnológicos innovadores en la prestación de servicios y productos financieros (Artículos 2.35.7.1.1, 2.35.7.1.3), buscando un equilibrio entre el aprovechamiento de la innovación, la protección de los consumidores y la estabilidad del sistema financiero (Artículo 2.35.7.1.2). Además, se autoriza a las instituciones crediticias para ofrecer sus servicios mediante agentes corresponsales externos vinculados a través de redes de comunicación de datos (Artículo 2.1.6.1.4, Título 9). Se define la actividad de financiación colaborativa (Título 1 del Libro 41), regulando las entidades autorizadas a desarrollarla a partir de una infraestructura electrónica (Artículos 2.41.1.1.1, 2.41.1.1.2, 2.41.3.1.1, 2.41.3.1.2). Igualmente, se autoriza a las entidades de crédito, compañías de servicios financieros y organizaciones de capitalización a tener participación accionaria sin límites en empresas dedicadas a la innovación y tecnología financiera.

La Ley 1735 de 2014 crea las SEDPES (sociedades especializadas en depósitos y pagos electrónicos) son entidades financieras dedicadas únicamente a la recaudación de fondos mediante depósitos y a la ejecución de pagos y movimientos de dinero por medios electrónicos. Se definen sus actividades, la necesidad de mantener los recursos en entidades vigiladas, y la aplicación de normas del Estatuto Orgánico del Sistema Financiero. Las SEDPES no pueden otorgar crédito ni realizar actividades de financiación y se establece que los depósitos estarán cubiertos por el seguro

de depósito. Se permite el uso de corresponsales y se establecen los trámites de vinculación y los límites de saldos y débitos mensuales. Además, esta ley exige que las SEDPES realicen contribuciones a la Superintendencia Financiera y que faciliten el acceso a los datos de identificación de los usuarios, garantizando la protección de datos y el habeas data. Se define el tratamiento regulatorio igualitario entre las SEDPES y otras entidades financieras en el ofrecimiento de servicios y productos, permitiendo que los operadores de información recolecten datos sobre hábitos transaccionales e historial de pagos, siempre con cumplimiento de las leyes de habeas data.

El Decreto 1491 de 2015 realiza una modificación al Decreto 2555 de 2010, estableciendo un marco regulatorio específico para las Sociedades Especializadas en Depósitos y Pagos Electrónicos (SEDPE), buscando así fomentar una mayor inclusión financiera a través de la oferta de servicios transaccionales; esta norma define las condiciones mínimas que deben cumplir los depósitos electrónicos, los diferentes trámites para su apertura, y las directrices para la administración de riesgos y el manejo del efectivo, incluyendo además aspectos como el apalancamiento, el uso de corresponsales y las reglas de competencia en el sector financiero.

En línea con la evolución del sistema financiero colombiano, el Decreto 1357 de 2018 adiciona el Libro 41 al Decreto 2555 de 2010, establece el marco regulatorio para las operaciones de financiamiento colectivo o "crowdfunding" mediante la emisión de títulos valores. Define las entidades de financiación colaborativa como aquellas organizaciones que funcionan como intermediarias conectando a inversionistas con solicitantes que requieren capital para iniciativas productivas.

Se establecen los requisitos para la organización de estas sociedades, así como sus funciones y deberes, incluyendo la gestión de los proyectos, el recaudo y la custodia de los

recursos. Se prohíbe que estas sociedades presten asesoría o administren directamente los recursos de los proyectos, y se obliga a la clasificación de los mismos, con límites para los montos de financiación. Además, se establecen reglas para la información que deben suministrar tanto a aportantes como a receptores, incluyendo los límites de inversión y los tipos de aportantes (calificados y no calificados), así como normas para la emisión y circulación de valores de financiación colaborativa.

En esta misma área del crowdfunding, el Decreto 1235 del 14 de 2020 marcó un primer hito importante al modificar las reglas de emisión de valores, ampliar los montos máximos de financiación en plataformas colaborativas y establecer requisitos de gobierno corporativo en los que se habilita a las SAS (sociedades por acciones simplificadas) a realizar emisiones de instrumentos de deuda en el mercado secundario de valores. Posteriormente, el Decreto 2105 de 2023 complementó esta regulación al introducir cambios significativos en la actividad de financiación colaborativa, permitiendo que estas entidades prestaran servicios a través de corresponsales y estableciendo mecanismos para la publicidad y negociación de valores en sus plataformas. Esta evolución normativa refleja el compromiso continuo del gobierno colombiano por fortalecer el mercado de capitales y ampliar las opciones de financiamiento, especialmente para las pequeñas y medianas empresas, mediante la modernización y flexibilización de los mecanismos de financiación disponibles en el mercado.

Complementando el marco regulatorio de la innovación financiera, el Decreto 2443 de 2018 adiciona un capítulo al Decreto 2555 de 2010, autorizando a las instituciones de crédito, empresas de servicios financieros y entidades de capitalización para realizar inversiones en compañías especializadas en innovación y tecnología del sector financiero (fintech), que se dediquen al desarrollo de tecnologías conexas al sector financiero. Se establecen los porcentajes

de participación y se definen reglas generales para estas sociedades, donde se aclara que estas sociedades no pueden prestar servicios financieros directamente.

Por su parte, el Decreto 222 de 2020, mediante la sustitución del Título 15 del Decreto 2555 de 2010, se enfocó en la reglamentación de los depósitos de bajo monto y ordinarios, y también en los créditos de bajo monto, con el fin de profundizar la inclusión financiera y permitir un mayor acceso a productos y servicios financieros formales. En este decreto se describen las características de los depósitos de bajo monto, incluyendo los inclusivos para personas de bajos ingresos, y se establecen las condiciones para el otorgamiento y seguimiento de créditos de bajo monto, así como el rol de los corresponsales y sus requisitos operativos

El Decreto 620 de 2020 reemplazó el Título 17 del Decreto 1078 de 2015, instaurando directrices básicas para la implementación y funcionamiento de los servicios digitales destinados a la ciudadanía, buscando impulsar la transformación digital del Estado al facilitar la interacción con los ciudadanos y garantizar el uso de medios electrónicos en trámites y servicios públicos. En esta normativa se definieron los servicios ciudadanos digitales fundamentales (interconexión de sistemas, verificación de identidad digital y repositorio digital personal del ciudadano), se reguló el acceso, las obligaciones de los diferentes actores involucrados (Ministerio de Tecnologías de la Información, el Articulador, prestadores y usuarios), y las condiciones para la seguridad y privacidad de la información

El Decreto 1234 de 2020 incorpora el Título 7 al Libro 35 de la Parte 2 del Decreto 2555 de 2010, creando un entorno regulado de experimentación para iniciativas de innovación financiera, comúnmente denominado "sandbox". Este espacio permite experimentar con innovaciones financieras bajo la supervisión de la Superintendencia Financiera. Este mecanismo busca impulsar el desarrollo tecnológico en servicios financieros para aumentar la eficiencia,

resolver problemas que enfrentan los usuarios, promover el acceso a servicios financieros para más personas y optimizar la observancia de las regulaciones. El sandbox opera mediante un Certificado de Operación Temporal que permite a las entidades participantes probar nuevos modelos de negocio bajo condiciones específicas, incluyendo planes de prueba y desmonte, siempre manteniendo la protección al consumidor y la estabilidad del sistema financiero como prioridades fundamentales.

Como desarrollo más reciente de este marco normativo, el Decreto 1297 de 2022 modifica el Decreto 2555 de 2010, enfocándose en la regulación de las finanzas abiertas en Colombia, buscando una mayor competencia e inclusión financiera. Las entidades financieras ahora tienen la posibilidad de ajustar sus modelos para ofrecer productos y servicios a través de ecosistemas propios o de terceros, y se promueve una mayor eficiencia en la prestación de servicios, donde se permite a terceros iniciar pagos con la autorización previa del usuario a través de sistemas de pago de bajo valor. Se establecen reglas para el acceso a estos sistemas y se definen las responsabilidades de los iniciadores de pago. Además, se permite la comercialización de tecnología e infraestructura a terceros por parte de las entidades vigiladas y se establecen normas estrictas para el manejo de datos personales, requiriendo autorización previa de los usuarios y cumpliendo las leyes de protección de datos. Esta norma también crea la figura del corresponsal digital y permite a los establecimientos de crédito invertir en sociedades de innovación financiera.

El artículo 89 de la Ley 2294 de 2023 (Plan Nacional de Desarrollo 2022-2026) establece que tanto entidades públicas como privadas deberán proporcionar acceso a información que facilite el acceso a productos y servicios financieros, buscando promover la competencia y la inclusión financiera. La norma establece que el Gobierno nacional reglamentará los aspectos específicos de este esquema de datos abiertos, incluyendo reglas de funcionamiento, condiciones de acceso y

estándares de seguridad. Todo esto deberá implementarse en el marco del régimen de protección de datos personales establecido por las Leyes 1712 de 2014, 1266 de 2008, 1581 de 2012 y 2157 de 2021.

En las circulares de la Superintendencia Financiera de Colombia (SFC) se puede observar un desarrollo progresivo que inició con un enfoque cauteloso hacia las criptomonedas y ha evolucionado hacia una regulación más integral del ecosistema digital financiero. La SFC comenzó advirtiendo sobre los riesgos de las operaciones con monedas virtuales a través de una serie de cartas circulares entre 2014 y 2017 (Cartas Circulares 029 de 2014, 078 de 2016 y 052 de 2017), estableciendo así una postura inicial de precaución frente a los activos digitales. Paralelamente, se dio un paso importante en la inclusión financiera digital con la regulación de las Sociedades Especializadas en Depósitos y Pagos Electrónicos (Circular Externa 050 de 2016).

Entre 2018 y 2019, la SFC fortaleció el marco de seguridad digital con regulaciones específicas sobre ciberseguridad (Circular Externa 007 de 2018), pasarelas de pago (Circular Externa 008 de 2018), computación en la nube (Circular Externa 005 de 2019) y operaciones mediante códigos QR (Circular Externa 006 de 2019). También se introdujeron normas sobre biometría (Circular Externa 029 de 2019), evidenciando una clara apuesta por la digitalización segura de los servicios financieros.

En el ámbito de regulación de medios de pago y seguridad digital, la Circular 008 de 2018 estableció requisitos específicos para la incorporación de organizaciones que gestionan plataformas de pago y negocios dedicados al comercio digital. La legislación requiere que las instituciones crediticias y administradores de sistemas de pago de valor reducido integren en sus contratos el requisito de obtener certificación PCI-DSS, implementar políticas de protección de datos personales según las Leyes 1581 de 2012 y 1266 de 2008, y establecer procedimientos para

prevenir el lavado de activos, además de realizar campañas informativas sobre medidas de seguridad.

La Circular 006 de 2019 estableció los lineamientos para las operaciones con códigos QR en el sistema financiero colombiano, exigiendo que las entidades se adhieran al estándar internacional EMVCo LLC versión 1.0 EMV® QR Code para sistemas de pago. La regulación requiere que las entidades proporcionen aplicaciones de software para la lectura de códigos QR, faciliten la captura de datos adicionales necesarios cuando se usen códigos QR estáticos, y cumplan con requisitos de seguridad establecidos para internet y banca móvil. Además, para fomentar la compatibilidad entre sistemas, las organizaciones que administran Sistemas de Pago de Bajo Valor tienen la obligación de establecer conjuntamente la estructura de campos para información adicional.

La Circular 026 de 2019 actualizó las instrucciones sobre el uso de dispositivos móviles en oficinas bancarias, derogando la anterior Carta Circular 093 de 2010. La nueva regulación permite que los establecimientos de crédito autoricen el uso de dispositivos móviles a los consumidores financieros dentro de sus instalaciones según su análisis de riesgo, mientras mantienen la restricción para sus funcionarios en áreas donde se realicen depósitos, pagos y retiros. La circular también promueve la transformación digital del sector, instando a los bancos a desarrollar programas de educación financiera sobre el uso de canales digitales y evaluar la implementación de oficinas piloto.

La Circular 029 de 2019 estableció los requerimientos mínimos para la implementación de biometría como factor de autenticación electrónica, requiriendo la verificación de identidad contra las bases de datos de la Registraduría Nacional, operadores de servicios ciudadanos digitales autorizados o bases propias. Para el uso de bases propias, las entidades deben implementar medidas

como el almacenamiento de plantillas biométricas usando sistemas de tokenización o algoritmos de cifrado fuerte, evitar almacenar muestras biométricas salvo autorización explícita, mantener la información demográfica separada, e implementar mecanismos de prueba de vida para fortalecer la confiabilidad del sistema.

El período 2020-2021 marcó un avance significativo en la regulación Fintech con la introducción del SARLAFT 4.0 (Circular Externa 027 de 2020), la regulación de corresponsales móviles y digitales (Circular Externa 002 de 2021), y la normativa sobre crowdfunding (Circular Externa 014 de 2021). Un hito importante fue la implementación del sandbox regulatorio (Circular Externa 016 de 2021), que demuestra la apertura de la SFC hacia la innovación financiera controlada.

La Circular 042 de 2020 reguló los depósitos de bajo monto, estableciéndolos como depósitos a la vista para personas naturales, con un énfasis especial en la inclusión financiera. La norma define los depósitos de bajo monto inclusivos como aquellos dirigidos a personas del nivel 1 del SISBEN, desplazados registrados y beneficiarios de programas estatales. Para su apertura, las entidades solo requieren información básica del documento de identidad, sin necesidad de presencia física del cliente, tarjetas de registro de firmas ni huellas dactilares. La circular también establece que las entidades deben implementar mecanismos especiales de administración de riesgos, pudiendo establecer límites en número y monto de transacciones.

Recientemente, en la Circular Externa 004 de 2024, la Superintendencia Financiera de Colombia estableció instrucciones para la implementación de finanzas abiertas (open finance) y la comercialización de tecnología e infraestructura a terceros por parte de las entidades vigiladas. Define los estándares tecnológicos, de seguridad y procedimientos que deben adoptar las entidades para compartir datos de consumidores financieros con terceros autorizados, siempre con el

consentimiento del consumidor. Establece plazos de implementación (18 meses para estándares principales, 6 meses para otras instrucciones, y 12 meses para comercialización de tecnología), requisitos técnicos específicos (como el uso de API, protocolos de seguridad, y autenticación), y obligaciones sobre el tratamiento de datos personales (Superintendencia Financiera de Colombia, 2024a). El objetivo es promover la interoperabilidad, la competencia en el sector financiero y fomentar la innovación en productos y servicios financieros.

Esta progresión regulatoria refleja cómo la SFC ha pasado de un enfoque inicialmente cauteloso a uno más proactivo y facilitador de la innovación financiera, manteniendo siempre un balance entre la promoción de nuevas tecnologías y la gestión de riesgos asociados. La tendencia actual sugiere un compromiso con la modernización del sistema financiero, priorizando la seguridad, la inclusión y la innovación responsable, en un entorno legal que aún no cuenta con una regulación específica para las empresas Fintech.

Vacíos, limitaciones y desafíos del marco regulatorio actual

El marco regulatorio relacionado con las fintech y la protección de la seguridad y privacidad de los usuarios financieros permite comprender sus vacíos, limitaciones y desafíos. Estos se analizan a continuación de una manera interpretativa, en discusión con hallazgos recientes de la literatura académica.

El marco regulatorio actual presenta una fragmentación significativa, ya que las fintech no cuentan con una ley específica que las regule de manera integral. Si bien existen normas dispersas en diferentes decretos y circulares, esta fragmentación dificulta una supervisión efectiva y puede generar incertidumbre tanto para las empresas como para los usuarios sobre qué normativa aplica en cada caso. Esta situación se alinea con lo señalado por Dávila & Monsalve (2023), quienes

enfatizan que la falta de claridad y los vacíos en las normas que regulan el sector fintech en Colombia constituyen un obstáculo significativo que puede derivar en interpretaciones erróneas y posibles incumplimientos involuntarios que afectan al consumidor.

Un desafío importante surge en la determinación de la autoridad competente para la supervisión. Mientras algunas fintech caen bajo la supervisión de la Superintendencia Financiera, otras pueden estar bajo la Superintendencia de Industria y Comercio, creando potenciales vacíos o superposiciones en la supervisión que podrían afectar la protección efectiva de los usuarios. Esta dualidad supervisora se relaciona directamente con lo que Guzmán (2024) señala sobre la necesidad de fortalecer la supervisión mediante medidas más estrictas, situación que se ve agravada por las limitaciones en las facultades sancionatorias de las entidades supervisoras para controlar las nuevas plataformas tecnológicas (Dávila & Monsalve, 2023).

La regulación actual muestra limitaciones en cuanto al tratamiento de nuevas tecnologías emergentes. Por ejemplo, aunque existen disposiciones sobre computación en la nube y biometría, hay vacíos significativos en la regulación de tecnologías como inteligencia artificial, blockchain o smart contracts, que son cada vez más utilizadas por las fintech. Este vacío en la regulación de tecnologías emergentes se ve reflejado en las preocupaciones sobre vulnerabilidades ante nuevas amenazas como los Deepfakes (Albarracín, 2023), situación que refuerza la necesidad de actualizar constantemente las regulaciones para mantenerlas al día con las rápidas innovaciones tecnológicas (Guzmán, 2024).

Un vacío notable se encuentra en la regulación de la responsabilidad por fraudes o fallos tecnológicos en servicios fintech. Si bien existe un marco general de protección al consumidor financiero, no hay claridad suficiente sobre la atribución de responsabilidades cuando ocurren incidentes de seguridad en el entorno digital, especialmente en casos donde intervienen múltiples

actores en la cadena de servicios. Esta falta de claridad se relaciona directamente con los retos identificados por Pertuz (2021) sobre la protección contra fraudes y ciberataques, y el establecimiento de mecanismos efectivos de protección en las transacciones digitales. Además, como señala Albarracín (2023), existe una inseguridad jurídica significativa en la resolución de procesos por responsabilidad civil cuando ocurren vulneraciones a la protección y seguridad de datos.

La normativa actual también presenta limitaciones en cuanto a la portabilidad de datos financieros. Aunque el Decreto 1297 de 2022 introduce elementos de finanzas abiertas, no establece mecanismos suficientemente robustos para garantizar que los usuarios puedan transferir fácilmente su información entre diferentes proveedores de servicios financieros, lo que puede afectar la competencia y la capacidad de elección de los usuarios. Esta problemática se conecta con las preocupaciones expresadas por Yadav (2020) sobre la seguridad y privacidad de los datos personales, especialmente cuando se utilizan datos alternativos como redes sociales y hábitos de compra en línea para tomar decisiones financieras.

Existe un desafío particular en la regulación de la protección de datos transfronteriza. Muchas fintech operan con infraestructura tecnológica ubicada en diferentes jurisdicciones, pero la normativa actual no aborda adecuadamente los riesgos específicos de la transferencia internacional de datos financieros en el contexto de servicios digitales innovadores. Este desafío se alinea con lo que Gurrea & Remolina (2020) identifican como uno de los principales retos regulatorios internacionales: el manejo de grandes volúmenes de datos y problemas de privacidad, así como la necesidad crítica de coordinación entre diferentes autoridades reguladoras para garantizar una protección efectiva.

La regulación del sandbox regulatorio, aunque innovadora, presenta limitaciones en su alcance y duración. El período de prueba puede resultar insuficiente para algunos modelos de negocio más complejos, y no existe un marco claro para la transición de las empresas que completan exitosamente el período de prueba hacia una operación regular. Estas limitaciones contrastan notablemente con el éxito del modelo británico de la FCA mencionado por Gurrea & Remolina (2020), y se relacionan con lo señalado por Dávila & Monsalve (2023) sobre el desafío de implementar estos espacios controlados para experimentar con nuevas tecnologías financieras mientras se evalúan efectivamente los riesgos.

Un vacío significativo se encuentra en la regulación de la educación financiera digital. Aunque existe un marco general para la educación financiera, no hay disposiciones específicas que aborden los desafíos particulares de la alfabetización digital financiera, necesaria para que los usuarios comprendan y utilicen de manera segura los servicios fintech. Esta carencia se relaciona directamente con lo que Pertuz (2021) identifica como el reto fundamental de asegurar que los consumidores comprendan adecuadamente los nuevos productos y servicios financieros digitales, especialmente en un contexto donde la falta de comprensión puede llevar a decisiones financieras arriesgadas o inadecuadas.

Finalmente, la regulación actual muestra limitaciones en cuanto a los mecanismos de resolución de disputas en el entorno digital. Los procedimientos tradicionales de defensoría del consumidor financiero pueden no ser suficientemente ágiles o adecuados para abordar conflictos específicos del entorno fintech, donde la rapidez y la especialización técnica son cruciales. Esta problemática se alinea con lo señalado por Pertuz (2021) sobre la necesidad de establecer mecanismos efectivos de reclamación y resolución de disputas, y se ve agravada por lo que Arias & Lis (2024) advierten sobre cómo la falta de un marco normativo integral puede exponer a los

usuarios a prácticas abusivas como cobros excesivos de intereses, cláusulas abusivas en contratos y falta de transparencia en la información.

Esta situación se hace más crítica al considerar el contexto internacional, donde como señalan Gurrea & Remolina (2020), existe la necesidad imperante de equilibrar la innovación con la protección al consumidor y la estabilidad financiera, mientras se manejan los desafíos de regular nuevos modelos de negocio que no encajan en los marcos regulatorios existentes. En el caso colombiano, estos desafíos se amplifican por el rápido crecimiento del sector, que según Colombia Fintech (2024b), ya cuenta con 369 empresas, de las cuales un significativo 65% se concentra en crédito y pagos digitales, áreas que requieren una protección especialmente robusta de los derechos de los usuarios.

Capítulo 2. Implicaciones jurídicas de las tecnologías emergentes en la protección de usuarios fintech

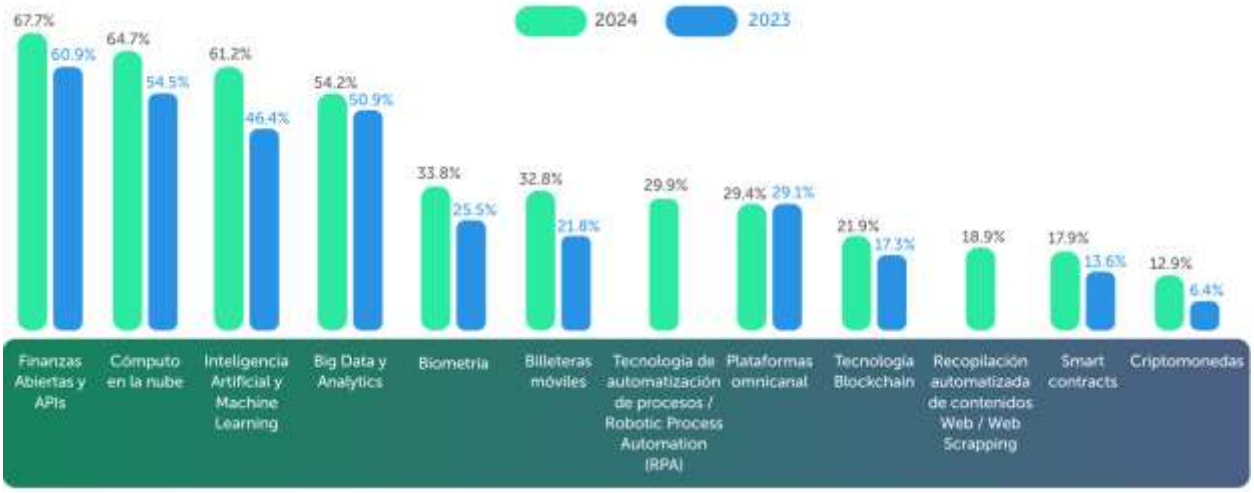
El ecosistema financiero digital se apalanca en un diverso repertorio de tecnologías transformadoras que redefinen la operación e intermediación financiera. La computación en la nube (cloud computing) constituye la infraestructura base para la mayoría de modelos Fintech, permitiendo escalabilidad y reducción de costos fijos. Las tecnologías de registro distribuido (DLT) y blockchain implementan mecanismos descentralizados de consenso que facilitan transacciones sin intermediarios centralizados. La inteligencia artificial y machine learning potencian la analítica avanzada para perfilamiento crediticio, detección de fraudes y asesoría financiera automatizada (robo-advisors). Las interfaces de programación de aplicaciones (APIs) habilitan la interoperabilidad entre sistemas y el desarrollo de modelos de open finance. La biometría transforma los procesos de identificación y autenticación de usuarios. Complementariamente, las finanzas descentralizadas (DeFi) emergen como paradigma disruptivo, apalancadas en contratos inteligentes para la provisión de servicios financieros sin intermediarios tradicionales, representando un horizonte de innovación que desafía los marcos regulatorios establecidos.

En el ecosistema fintech colombiano, la adopción tecnológica muestra una clara tendencia hacia la integración digital y la innovación en servicios financieros. Las Finanzas Abiertas y APIs lideran como las tecnologías predominantes, con una tasa de adopción que alcanza el 67.7% en 2024, superando el 60.9% del año anterior. Le sigue de cerca el Cómputo en la Nube con un 64.7% de implementación, mientras que la Inteligencia Artificial y Machine Learning experimentaron un crecimiento sustancial del 11.1%, llegando al 61.2%. Estas tecnologías, junto con el aumento en métodos de seguridad biométrica y billeteras móviles, responden a la necesidad de crear productos

financieros basados en datos alternativos para evaluar riesgos crediticios, mejorar la seguridad y facilitar transacciones eficientes (ver figura 1).

Figura 1

Tecnologías utilizadas por las Fintech en Colombia



Nota. Tomado de (Finnovista, 2024)

Como se puede observar, el avance tecnológico en el sector fintech ha ido migrando hacia el uso de finanzas abiertas, computación en la nube, inteligencia artificial, bigdata, biometría, billeteras móviles y automatización de procesos. Estas tecnologías tienen implicaciones jurídicas para la protección de los usuarios de estos servicios en Colombia, las cuales se describen a continuación.

Open Finance

El Plan Nacional de Desarrollo ha incorporado la propuesta de una política pública en materia de Open Finance, pendiente de regulación, que puede impactar el ecosistema fintech del país. La Ley 2294 de 2023, a través de su artículo 89, establece obligaciones para entidades públicas y privadas relacionadas con el acceso y suministro de información que facilite la inclusión

financiera y crediticia, promoviendo así la competencia e innovación. Esta disposición, aunque todavía requiere desarrollo regulatorio detallado, podría crear condiciones favorables para la implementación de tecnologías basadas en registros distribuidos y otras innovaciones financieras que dependen del intercambio fluido de datos entre instituciones (Carvajal & Garzón, 2024). Complementariamente, el Decreto 1297 de 2022 ha contribuido al fortalecimiento tanto de los neobancos como del Open Finance en Colombia, poniendo especial énfasis en la iniciación de pagos como actividad fundamental dentro del ecosistema de operaciones fintech, lo que demuestra el interés regulatorio por impulsar esta dimensión de la innovación financiera.

Por su parte, La Resolución Externa No. 6 de 2023 del Banco de la República establece un marco normativo integral para la interoperabilidad en los sistemas de pago de bajo valor inmediatos (SPBVI) en Colombia. Esta regulación determina las condiciones técnicas y operativas que deben cumplir las entidades administradoras de estos sistemas (EASPBVI) para garantizar que los usuarios puedan realizar transferencias de fondos en tiempo real entre diferentes entidades financieras. Las implicaciones jurídicas para la protección de usuarios fintech son significativas, pues la normativa exige que las EASPBVI implementen mecanismos de seguridad para la autenticación mediante "Llaves" y códigos QR, establece directorios federados y centralizados para la verificación de identidades, y obliga a las entidades a adoptar procedimientos específicos para la gestión de fraudes y reclamos. Además, prohíbe prácticas discriminatorias entre operaciones dentro del mismo sistema o entre diferentes sistemas, lo que fomenta un entorno competitivo que beneficia al consumidor financiero mientras impone responsabilidades claras a los participantes del ecosistema de pagos inmediatos bajo la supervisión de la Superintendencia Financiera.

Neobancos y Banca Digital

La normativa colombiana aborda los riesgos tecnológicos en el entorno fintech principalmente a través de exigencias específicas para los neobancos y plataformas digitales financieras. La Circular Externa 029 de 2014 de la Superintendencia Financiera establece requisitos de seguridad que buscan generar un ambiente más equitativo entre los bancos tradicionales y los neobancos, fijando estándares mínimos de seguridad digital. Entre los requisitos destacados figuran: la obligación de contar con mecanismos de autenticación de dos factores para operaciones monetarias y no monetarias, implementar cifrado fuerte de extremo a extremo para información confidencial cuando las operaciones monetarias superen los dos salarios mínimos mensuales legales vigentes, y adoptar medidas que garanticen la atomicidad de las operaciones para evitar su duplicidad debido a fallas en la comunicación ocasionadas por problemas como la calidad de la señal o el traslado entre celdas (Superintendencia Financiera de Colombia, 2014). La Circular Externa 014 de 2021 también permite a las sociedades autorizadas para realizar operaciones de crowdfunding prestar servicios adicionales, pero exigiendo mecanismos que permitan identificar claramente los diferentes tipos de crowdfunding, lo que indirectamente contribuye a la seguridad operativa de estas plataformas.

Adicionalmente, la Superintendencia Financiera tiene un grupo de trabajo dedicado a asuntos fintech, lo cual permite un enfoque hacia la supervisión de los riesgos tecnológicos, especialmente en los proyectos presentados a los sandboxes regulatorios y de supervisión (Carvajal & Garzón, 2024).

Computación en la nube

La Circular Externa 005 de 2019 establece normas específicas que las entidades financieras deben cumplir al implementar servicios cloud, incluyendo requisitos de seguridad de datos, confidencialidad y continuidad operativa. Esta regulación busca proteger a los usuarios finales mediante la imposición de estándares mínimos para el procesamiento y almacenamiento de información financiera en entornos virtualizados. Simultáneamente, estos servicios están sujetos a las disposiciones de protección de datos personales establecidas en la Ley 1581 de 2012, que impone obligaciones estrictas sobre el tratamiento transfronterizo de datos, especialmente relevante considerando que muchos proveedores de cloud computing operan desde jurisdicciones extranjeras. La intersección de estas normativas crea un entorno donde las empresas fintech deben equilibrar la innovación tecnológica con la responsabilidad de salvaguardar la información de sus usuarios, implementando medidas técnicas y organizativas que garanticen el cumplimiento simultáneo de las regulaciones financieras y de protección de datos.

Inteligencia artificial en servicios financieros

Aunque Colombia no dispone de un marco regulatorio específico para la inteligencia artificial, el sistema jurídico nacional cuenta con las leyes estatutarias 1266 de 2008 y 1581 de 2012 sobre protección de datos personales. Estas normativas fueron concebidas con un enfoque tecnológicamente neutral, permitiendo que sus disposiciones se apliquen al procesamiento de información independientemente del método utilizado. Las plataformas fintech, al igual que los sistemas de IA, deben observar principios esenciales como la veracidad, calidad y transparencia en el manejo de datos financieros de los usuarios. Las autoridades reguladoras han reconocido que los procesos de inteligencia artificial comprenden numerosas operaciones con información

personal que deben ajustarse a los parámetros legales establecidos. Para garantizar una protección efectiva, es necesario que los desarrolladores implementen evaluaciones previas sobre impactos en privacidad y adopten robustas medidas de seguridad informática para evitar vulneraciones a los derechos de quienes utilizan servicios financieros digitales (Sentencia T-323 de 2024).

En cuanto a regulación general de IA, recientemente se discutió en el Congreso un proyecto de ley para regular los desarrollos de inteligencia artificial, pero fue archivado por asuntos de procedimiento (Carvajal & Garzón, 2024). Específicamente, Colombia avanza en la regulación de la Inteligencia Artificial a través de dos proyectos clave en el Congreso: el Proyecto 091 de 2023, que establece principios éticos para el uso responsable de la IA, ya aprobado en Comisión Sexta; y el Proyecto 130 de 2023, enfocado en proteger derechos laborales frente a la automatización. En agosto de 2024 se creó una comisión accidental para coordinar estos y otros proyectos relacionados, buscando una legislación unificada que equilibre innovación tecnológica y protección de derechos fundamentales (Bermúdez, 2025).

Big data y analytics

El CONPES 3920 establece lineamientos concretos para fortalecer la seguridad jurídica en la explotación de datos en Colombia. Entre las acciones prioritarias, propone la simplificación de las clasificaciones legales de datos para reducir la confusión sobre su nivel de publicidad y tratamiento, tarea encomendada a la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio. Asimismo, el documento recomienda la creación de una instancia con capacidad ejecutiva que materialice un nuevo marco de gobernanza de datos, articulada con autoridades existentes, pero con mayor alcance que las comisiones anteriores. En

materia de protección al ciudadano, plantea la actualización del marco jurídico para responder a los desafíos de la datificación, considerando la revisión de principios como autorización, información, necesidad y finalidad. También contempla el desarrollo de un marco ético mediante mesas de trabajo multisectoriales y el establecimiento de criterios para garantizar la transparencia, explicabilidad y auditabilidad de los proyectos de explotación de datos en entidades públicas (CONPES, 2018).

Este escenario requiere enfocar la intervención estatal en los usos permitidos de los datos, independientemente del consentimiento previo, definiendo claramente las responsabilidades para proteger estos bienes jurídicos en el contexto fintech, donde la datificación de transacciones financieras exige mayor atención regulatoria. Las entidades financieras enfrentan la responsabilidad legal de garantizar que estas herramientas, capaces de procesar enormes volúmenes de información para evaluar riesgos crediticios, operen dentro de parámetros éticos y transparentes (Colombia Fintech, 2024a). La velocidad con que las organizaciones adopten estas tecnologías determinará no solo su competitividad, sino también su capacidad para cumplir con las obligaciones legales de protección al consumidor financiero.

Billeteras móviles

La operación de plataformas estructuradas como "billeteras electrónicas" en Colombia conlleva estrictas implicaciones jurídicas para la protección de usuarios fintech. El ordenamiento jurídico colombiano establece que estas plataformas, cuando se relacionan con actividades exclusivas de entidades vigiladas por la Superintendencia Financiera, deben operar bajo responsabilidad de dichas entidades o con su participación mediante modalidades autorizadas. El Decreto 222 de 2020, reglamentado por la Circular Externa 002 de 2021, instituye la figura de

corresponsalía digital, permitiendo que entidades vigiladas presten servicios a través de terceros —ya sea física, móvil o digitalmente— bajo su plena responsabilidad. Esta normativa constituye un mecanismo para garantizar que los recursos captados sean depositados en entidades debidamente vigiladas, proporcionando así una capa de protección a los consumidores financieros (Superintendencia Financiera de Colombia, 2021).

La ausencia de regulación específica sobre billeteras virtuales no exime a estos servicios de control estatal. Por el contrario, las actividades relacionadas con captación de recursos del público están reservadas exclusivamente para entidades sometidas al control y vigilancia estatal, so pena de incurrir en el delito de captación masiva y habitual tipificado en los artículos 316 y 316A del Código Penal. Adicionalmente, el Decreto 1692 de 2020 modifica el marco regulatorio de los sistemas de pago de bajo valor, incluyendo diversos roles dentro del concepto de proveedores de servicios de pago (Superintendencia Financiera de Colombia, 2021). Esta normativa complementa el ecosistema regulatorio que busca proteger a los usuarios fintech, asegurando que cualquier entidad que administre recursos para pagos o transferencias cuente con la debida autorización y supervisión.

Biometría y autenticación avanzada

En Colombia, la implementación de tecnologías biométricas para la autenticación de usuarios en el sector fintech representa un avance importante para la seguridad digital. La Circular Externa 029 de 2019 establece directrices específicas sobre el uso e implementación de identificadores biométricos en los servicios financieros, proporcionando un marco regulatorio para estas tecnologías emergentes. Los sistemas de autenticación avanzada no solo cumplen con los requisitos legales de protección de datos personales establecidos en la Ley 1581 de 2012, sino que

también fortalecen la confianza del consumidor al reducir el riesgo de fraude y suplantación de identidad. Las entidades fintech deben equilibrar la adopción de estas tecnologías innovadoras con el cumplimiento estricto de las normas de ciberseguridad, especialmente considerando que la información biométrica constituye datos sensibles bajo la legislación colombiana. La evolución de este marco normativo demuestra el compromiso de los reguladores por adaptarse a los desafíos tecnológicos del sector financiero.

Adicionalmente, la Circular Externa 033 de 2020 establece instrucciones respecto a la Taxonomía Única de Incidentes Cibernéticos (TUIC), actualizando los protocolos de seguridad de la información y ciberseguridad. Estas normativas se complementan con la Circular Externa 005 de 2019 sobre el uso de servicios de computación en la nube y la Circular Externa 006 de 2019 que establece normas relacionadas con las transacciones con códigos QR, conformando un marco regulatorio integral para las tecnologías de autenticación y seguridad digital en el sector financiero colombiano. Este enfoque regulatorio demuestra la importancia que otorgan las autoridades financieras colombianas a la seguridad digital como componente esencial para el desarrollo de las fintech en el país.

Roboadvisors y automatización

La inteligencia artificial en el ámbito financiero colombiano ha tenido cierto desarrollo normativo, particularmente en el caso de los robo-advisors. El Decreto 661 de 2018 estableció el marco regulatorio para esta tecnología, indicando que las recomendaciones proporcionadas mediante sistemas automatizados deben cumplir con las obligaciones de la actividad de asesoría. Esta normativa contempla una particularidad importante: los clientes tienen derecho a solicitar que la recomendación automatizada sea complementada por un asesor profesional certificado.

La Circular Externa 019 de 2021 complementó esta regulación al establecer directrices específicas para entidades financieras que utilizan robo-advisors en el mercado de valores, incluyendo la obligación de establecer áreas responsables para el diseño e implementación de la tecnología, y definir estrategias para la gestión de riesgos asociados. Esta normativa busca garantizar que, a pesar de la automatización, las recomendaciones profesionales mantengan estándares de idoneidad y transparencia. De acuerdo con el Decreto 661 de 2018, incorporado en el Decreto 2555 de 2010, las entidades deben implementar sistemas que clasifiquen productos como simples o complejos, asegurando así que los inversionistas reciban servicios acordes a sus necesidades y objetivos particulares.

Blockchain y contratos inteligentes

La tecnología blockchain, caracterizada por su naturaleza de inalterabilidad de la información, brinda mayor seguridad en las transacciones financieras mediante cadenas de bloques de información que incluyen las operaciones realizadas. Sin embargo, esta misma característica plantea desafíos respecto a derechos como la intimidad, el habeas data y otros derechos fundamentales contemplados en el ordenamiento constitucional, particularmente cuando se trata de datos personales almacenados en bases inmutables (Valderrama, 2025). Los contratos inteligentes, como protocolos informáticos que se ejecutan automáticamente, deben cumplir con estrictos requisitos técnicos y jurídicos para garantizar la autenticidad, integridad y rastreabilidad de la información, especialmente cuando gestionan datos sensibles de usuarios financieros. En el contexto colombiano, la aplicación de estas tecnologías está sujeta a la normativa de protección de datos personales, y las entidades fintech deben asegurar que sus implementaciones tecnológicas no solo faciliten transacciones ágiles y seguras, sino que también respeten los principios de

neutralidad tecnológica y garanticen que la información transmitida mantenga su confidencialidad, autenticidad, integridad y no repudiación (Valderrama, 2025).

El uso de tecnologías blockchain en Colombia no cuenta con una regulación específica, aunque existe un creciente interés tanto en el sector público como privado por su implementación; no obstante, las autoridades financieras han ido estableciendo posiciones claras al respecto. La Circular Externa 052 de 2017 de la Superintendencia Financiera de Colombia prohíbe a las entidades supervisadas intermediar con criptomonedas o permitir el uso de sus plataformas para operaciones con estos activos. Por su parte, el Banco de la República ha emitido comunicados donde establece que las criptomonedas no son reconocidas como moneda de curso legal al no contar con respaldo de ningún banco central. Mientras tanto, la DIAN ha definido las criptomonedas como activos intangibles susceptibles de valoración monetaria, considerándolas activos para efectos fiscales aunque no constituyan monedas legales (Carvajal & Garzón, 2024). Esta postura regulatoria refleja la cautela de las autoridades colombianas frente a estas tecnologías emergentes, sin llegar a prohibirlas completamente sino estableciendo límites claros para su operación dentro del sistema financiero tradicional.

El Ministerio de Tecnologías de la Información y las Comunicaciones (2020) ha propuesto a una metodología estructurada que incluye capacitación del ecosistema, levantamiento de requerimientos funcionales, análisis y diseño, desarrollo de aplicaciones, validación y evaluación de impacto. También ofrece una matriz de priorización para evaluar proyectos potenciales, considerando factores como el trabajo con activos digitales, la eliminación de intermediarios y la creación de registros permanentes. Adicionalmente, recomienda generar un marco normativo adecuado, desarrollar procesos de transferencia de conocimiento y garantizar que los participantes

comprendan la tecnología, advirtiendo que no es apropiada para el almacenamiento de grandes volúmenes de información.

Por su parte, el Banco de la República ha mantenido acercamientos con desarrolladores de estas soluciones, transformando el panorama jurídico de la protección al usuario fintech, creando un entorno donde la trazabilidad y transparencia de las operaciones financieras adquieren nueva dimensión. El caso del primer bono blockchain en Colombia, impulsado por el Grupo BID y Banco Davivienda, ilustra cómo los contratos inteligentes pueden fortalecer los marcos regulatorios existentes al permitir un registro inmutable de transacciones (Banco de la República, 2021). Esta innovación resalta la necesidad de adaptar las normativas actuales para garantizar que la protección al inversionista no se vea comprometida, mientras se aprovechan las ventajas que ofrece la tecnología descentralizada en términos de seguridad y eficiencia operacional.

Estos acercamientos, aunque preliminares, indican una percepción positiva hacia esta tecnología por parte de los organismos reguladores. La experiencia más concreta se dio en 2020 con un proyecto piloto en LaArenera orientado a crear un sistema para administrar e intercambiar garantías en operaciones de derivados OTC usando tecnología blockchain, aunque este no derivó en una regulación específica. Carvajal & Garzón (2024) indican que los principales bancos del país y algunos proveedores de servicios tecnológicos ya utilizan estas tecnologías para su operación interna, pero no ha habido proyectos públicos recientes para su desarrollo normativo.

La legislación colombiana otorga validez jurídica plena a los contratos electrónicos según la Ley 527 de 1999, que establece tres requisitos esenciales: consentimiento expreso para contratar electrónicamente, mecanismos de autenticidad e integridad, y disponibilidad permanente del contrato (Dávila & Monsalve, 2023). El principio de equivalencia funcional, confirmado por la Corte Constitucional en la Sentencia C-831 de 2001, reconoce que los mensajes de datos tienen el

mismo valor legal que los documentos físicos. Para prevenir suplantaciones, el sistema legal colombiano reconoce tres modalidades de firmas electrónicas: digital certificada, electrónica simple y electrónica certificada, establecidas en el Decreto 2364 de 2012 y reforzadas por las directrices de la Superintendencia de Industria y Comercio (2019). Sin embargo, según Padilla (2020), la intersección entre blockchain, contratos inteligentes y servicios financieros crea espacios regulatorios difusos donde la desintermediación genera riesgos específicos relacionados con la inmutabilidad de las transacciones y la dificultad para integrar el "derecho al olvido", planteando desafíos regulatorios que protejan a los usuarios sin obstaculizar la innovación.

Crowdfunding y Plataformas de Financiación Colaborativa

El crowdfunding en Colombia ha sido objeto de regulación específica, principalmente a través del Decreto 1357 de 2018, posteriormente modificado por el Decreto 1235 de 2020 y complementado por el Decreto 2105 de 2023. Este marco normativo ha creado la figura de las Sociedades de Financiación Colaborativa (SOFICO), entidades con objeto social exclusivo para operar plataformas de financiación colaborativa que deben ser previamente autorizadas por la Superintendencia Financiera. La regulación establece límites máximos de inversión para los aportantes (20% del ingreso anual o del patrimonio total) y de recaudación para los proyectos financiados (hasta 58,000 SMMLV con inversionistas profesionales o 19,000 SMMLV con clientes inversionistas). Sin embargo, Carvajal & Garzón (2024) señala una importante laguna regulatoria: mientras el crowdfunding basado en valores está claramente normado, el crowdfunding tradicional de préstamos o el basado en recompensas y donaciones no está regulado y podría enfrentar limitaciones legales al ser potencialmente considerado como "captación masiva y habitual de dineros del público", actividad restringida a entidades financieras autorizadas.

Insurtech (Tecnologías aplicadas a seguros)

Las tecnologías insurtech en Colombia se encuentran en fase de exploración por parte de las compañías aseguradoras, que están enfocándose principalmente en aspectos de cumplimiento normativo, protección de datos, gestión de riesgos y desarrollo de productos personalizados. Aunque no existe una regulación específica para insurtech, Carvajal & Garzón (2024) mencionan que en 2019 y 2020 se realizaron proyectos piloto en LaArenera relacionados con la vinculación simplificada de consumidores a entidades aseguradoras para la toma de seguros de daños. Estas iniciativas fueron relevantes para establecer prácticas de prevención de lavado de activos, que posteriormente se incorporaron en la Circular Externa 027 de 2020, pero no derivaron en una regulación específica para las insurtech.

La Circular Básica Jurídica de la Superintendencia Financiera contiene un capítulo dedicado a la regulación de corresponsales digitales (aplicaciones móviles, sitios web) a través de los cuales las aseguradoras prestan servicios digitales (Superintendencia Financiera de Colombia, 2014). En los últimos años, diversas aplicaciones como Rappi, Seguros Bolívar y Segurapp han comenzado a ofrecer la posibilidad de adquirir seguros completamente por vía digital (Carvajal & Garzón, 2024).

Desafíos regulatorios de las nuevas tecnologías

El ecosistema Fintech enfrenta una configuración distintiva de riesgos que, aunque comparten naturaleza con los del sector financiero tradicional, presentan matices particulares en su manifestación e impacto. El riesgo operacional y de ciberseguridad adquiere dimensiones críticas ante la mayor exposición a ataques cibernéticos derivada del intercambio intensivo de

datos entre múltiples participantes de la cadena de valor. Los riesgos de conductas de mercado se transforman cuando los productos y servicios operan sin interacción humana, requiriendo controles específicos para la transparencia y adecuación en entornos digitales. Emergen además riesgos sistémicos relacionados con la concentración de poder, comportamientos anticompetitivos por parte de BigTechs que subsidian costos para ganar mercado, y riesgos de contagio entre entidades interconectadas. La dependencia tecnológica genera vulnerabilidades ante interrupciones del servicio que pueden desencadenar crisis de confianza con implicaciones para la estabilidad financiera.

El marco regulatorio colombiano enfrenta el reto fundamental de equilibrar la innovación tecnológica con la protección del sistema financiero tradicional. Esto se evidencia en el enfoque adoptado por los reguladores, que han priorizado evaluar la viabilidad de implementar modelos específicos de fintech antes de establecer regulaciones exhaustivas, permitiendo así un desarrollo controlado que favorece ciertos avances mientras mantiene salvaguardas prudenciales.

Un caso paradigmático es el de los criptoactivos, donde a pesar de no existir regulación específica, distintas autoridades como la Superintendencia Financiera, el Banco de la República y la DIAN han emitido pronunciamientos que definen estos activos, pero sin proporcionar un marco normativo completo (Carvajal & Garzón, 2024). Carvajal & Garzón (2024) también destaca el uso de "sandboxes" o areneras regulatorias como LaArenera (Sandbox de Supervisión creado en 2018) y el Sandbox Regulatorio (operativo desde 2020), que funcionan como espacios controlados donde se pueden probar innovaciones financieras con ciertas dispensas regulatorias. Según lo planteado por estos autores, Colombia ocupa el tercer lugar en Latinoamérica en desarrollos fintech, con una representación del 13% de los desarrollos de la región, lo que subraya la importancia de continuar actualizando el marco regulatorio para responder a esta creciente industria.

Las tecnologías emergentes como DLT/Blockchain presentan grandes desafíos jurídicos en la protección de usuarios fintech. La falta de marcos regulatorios específicos genera incertidumbre tanto para proveedores como para consumidores de estos servicios. En Colombia, si bien la Ley 1712 de 2014 establece parámetros sobre el acceso a la información pública que pueden aplicarse a los registros distribuidos, existe un vacío normativo sobre aspectos cruciales como la validez legal de los contratos inteligentes o la responsabilidad en caso de fallos técnicos. Como señala el documento, una adecuada implementación requiere "generar un marco normativo para que la tecnología DLT/Blockchain pueda ser implementada en el sector público". Esta necesidad se hace patente especialmente en sectores sensibles como el financiero, donde la Superintendencia Financiera y el Banco de la República deberían participar activamente en cualquier iniciativa que implique la creación de activos digitales que representen moneda de curso legal (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020).

La protección de datos representa otro desafío regulatorio crítico para las fintech colombianas. Las empresas deben navegar un complejo entramado normativo que incluye la Ley 1581 de 2012 y la Ley 1266 de 2008, además de cumplir con restricciones específicas sobre transferencias internacionales de datos. Esta situación se complica cuando los modelos de negocio fintech dependen de procesamiento transfronterizo de información o utilizan servicios de computación en la nube, requiriendo evaluaciones minuciosas de cumplimiento normativo.

A su vez, Carvajal & Garzón (2024) establecen distinciones importantes entre el consumidor general y el consumidor financiero, lo que impacta directamente en los regímenes de protección aplicables. La regulación colombiana distingue claramente entre ambas figuras: el consumidor general está protegido por la Ley 1480 de 2011, mientras que el consumidor financiero se rige por la Ley 1328 de 2009, la cual regula específicamente las relaciones derivadas entre

consumidores y entidades vigiladas por la Superintendencia Financiera. Esta distinción determina qué normas se aplican a las plataformas fintech según su categorización; por ejemplo, las plataformas de trading de criptoactivos, al no estar vigiladas por la Superintendencia Financiera, se rigen por el régimen general de protección al consumidor establecido en la Ley 1480 de 2011, y no por el Estatuto del Consumidor Financiero, lo que podría impactar la forma en que se gestionan los datos personales y la privacidad.

La interoperabilidad entre sistemas financieros tradicionales y nuevas plataformas tecnológicas constituye un desafío adicional, como se observa en la reciente regulación del Banco de la República sobre la interoperabilidad de servicios de pago de bajo valor. Los reguladores deben diseñar normas que faciliten la integración de estos sistemas sin comprometer la seguridad o la estabilidad del ecosistema financiero en su conjunto.

La Superintendencia Financiera de Colombia (2024b) en su Guía externa para la supervisión de las entidades con enfoque digital mantiene los principios fundamentales de la supervisión tradicional pero incorpora criterios complementarios adaptados a su realidad operativa. La proporcionalidad emerge como principio rector, ajustando las exigencias según el nivel de madurez digital y la materialidad de las actividades tecnológicas dentro del modelo de negocio. La regulación reconoce distintas categorías de entidades con enfoque digital (Fintech independientes, Fintechs diversificadas y BigTechs), adaptando sus requerimientos a la complejidad organizacional de cada una. Se observa mayor énfasis en la evaluación de planes de resolución y contingencia ante inviabilidad del modelo de negocio, particularmente para entidades de reciente creación. Asimismo, los requisitos para juntas directivas y alta gerencia se extienden a conocimientos específicos en ciberseguridad, transformación digital y arquitectura empresarial, elementos no prioritarios en la supervisión de entidades tradicionales.

No obstante, los núcleos de supervisión deben adaptar sus metodologías para abordar modelos de negocio en constante evolución, caracterizados por ciclos de innovación acelerados y estructuras organizacionales complejas. La ubicación geográfica dispersa de miembros de juntas directivas y alta gerencia complica el seguimiento efectivo, exigiendo mecanismos de comunicación permanente. Adicionalmente, la tercerización de funciones críticas en estas entidades difumina los límites de responsabilidad y control, obligando a los supervisores a evaluar no solo la entidad vigilada sino también la solidez de sus proveedores tecnológicos y alianzas estratégicas, especialmente cuando se integran con BigTechs o ecosistemas Fintech más amplios (Superintendencia Financiera de Colombia, 2024b).

Capítulo 3. Responsabilidad civil de las empresas fintech

El vertiginoso avance de la tecnología financiera ha transformado radicalmente la manera en que los individuos y las empresas interactúan con sus recursos económicos, creando un nuevo paradigma que desafía los esquemas jurídicos tradicionales. Las empresas fintech, caracterizadas por su innovación disruptiva y agilidad operativa, han generado importantes cuestionamientos sobre la atribución de responsabilidades ante incidentes, la protección efectiva del consumidor digital y la aplicación de principios jurídicos consolidados a realidades tecnológicas emergentes. Este capítulo examina el marco normativo colombiano actual que regula la responsabilidad civil de estas entidades, analiza los mecanismos jurídicos disponibles para la determinación de responsabilidades, identifica las vías de resarcimiento para los usuarios afectados y presenta propuestas para fortalecer un sistema que debe equilibrar la protección del consumidor con el fomento de la innovación tecnológica en el sector financiero.

Marco jurídico de responsabilidad civil en servicios financieros digitales

El ecosistema Fintech ha transformado la operación financiera tradicional, lo cual se refleja en aspectos jurídicos relacionados con la responsabilidad civil. Esto se fundamenta en las obligaciones que la normativa impone a los intermediarios financieros: proporcionar información clara y completa sobre los productos y servicios, actuar con diligencia protegiendo los intereses del cliente, implementar controles internos, mantener personal debidamente formado y operar con transparencia en todas las transacciones (Nur, 2023).

En Colombia, la responsabilidad civil por operaciones financieras digitales se enmarca primordialmente en el Código de Comercio, particularmente en las disposiciones del contrato de depósito irregular y las normas sobre medios de pago. El artículo 1391 del Decreto 410 de 1974

establece la responsabilidad de las entidades financieras por la custodia de los recursos confiados, aplicándose por analogía a las operaciones electrónicas. La normativa desarrollada para prevenir actividades ilícitas como el lavado de activos (Ley 800 de 2003, Ley 985 de 2005 y Ley 1273 de 2009) constituye un marco jurídico relevante para evaluar casos potenciales de responsabilidad civil en el sector financiero digital (Díaz et al., 2024).

La regulación incluye también disposiciones del Decreto 663 de 1993 (Estatuto Orgánico del Sistema Financiero), especialmente los artículos 72 y 98 que establecen los principios de buena fe y servicio al interés público. La Ley 1328 de 2009 sobre protección al consumidor financiero complementa este marco al determinar la debida diligencia como obligación de las entidades del sector. Adicionalmente, la Circular 052 de 2007 de la Superintendencia Financiera establece requerimientos mínimos de seguridad para las operaciones electrónicas.

Paralelamente, las Fintech operan bajo el esquema general de responsabilidad civil extracontractual establecido en Colombia, particularmente bajo las disposiciones del artículo 20 de la Ley 1480 de 2011, que regula la responsabilidad por productos defectuosos. Este artículo establece que el productor y el expendedor serán solidariamente responsables de los daños causados por los defectos de sus productos, lo cual aplica a las plataformas tecnológicas de servicios financieros cuando sus sistemas presentan fallas. El artículo 6 de la Ley 1480 complementa este marco al establecer que todo productor debe asegurar la idoneidad y seguridad de los bienes y servicios que ofrece, lo que traslada una responsabilidad directa a las empresas Fintech respecto al funcionamiento adecuado de sus algoritmos y sistemas automatizados.

Estas normativas, junto con el Decreto 2555 de 2010 y la Ley 964 de 2005, establecen los criterios para determinar las obligaciones de los intermediarios financieros y las empresas tecnológicas que prestan servicios de asesoría automatizada, conocidos como robo advisors. La

regulación contempla que estos asesores automatizados deben cumplir con estándares similares a los intermediarios tradicionales, incluyendo obligaciones de diligencia, transparencia y protección al consumidor financiero (Nur, 2023).

Las operaciones financieras digitales operan bajo un régimen de responsabilidad que tiende a la objetivación. Esto implica que las entidades financieras responden por las pérdidas que se produzcan en los depósitos de los usuarios, salvo que demuestren la culpa exclusiva del cliente. Los tribunales han reconocido que la actividad financiera no se considera peligrosa pero sí profesional y especializada, lo que implica obligaciones de resultado en cuanto a la custodia y restitución de fondos (Arenas, 2019).

En lo relacionado con la protección de datos personales y la responsabilidad civil, la normatividad vigente incluye la Ley Estatutaria 1266 de 2008, que dicta disposiciones sobre el hábeas data y regula el manejo de información contenida en bases de datos personales. Esta ley constituye un pilar fundamental para la protección de datos en el ámbito financiero, estableciendo obligaciones para las entidades que manejan información sensible de los usuarios. El Decreto 1727 de 2009 complementa este marco al determinar la forma en que los operadores de bancos de datos de información financiera, crediticia y comercial deben presentar la información de los titulares. Asimismo, el Decreto Reglamentario 2952 de 2010 profundiza en la reglamentación de los artículos 12 y 13 de la Ley 1266, fortaleciendo los mecanismos de protección.

La normativa colombiana actual incluye disposiciones de la Ley 1581 de 2012 sobre protección de datos personales, pero carece de un marco específico para las amenazas y riesgos digitales propios del sector Fintech. Esta situación ha llevado a que la responsabilidad civil se construya sobre principios generales del derecho colombiano, aplicando por analogía normas existentes en materia bancaria y de protección al consumidor financiero. Como señala Gaona &

Solano (2021), las empresas que operan en el sector financiero digital deben reparar los perjuicios causados por vulneraciones a los derechos relativos al tratamiento de datos de usuarios y consumidores, en el marco del régimen general de responsabilidad extracontractual .

La supervisión de estas normativas recae en entidades como la Superintendencia Financiera de Colombia, que mediante circulares como la Externa 023 de 2004 y la Externa 033 del mismo año, ha establecido directrices sobre el uso adecuado de la información crediticia en centrales de riesgo y el cumplimiento de obligaciones en la actividad crediticia.

El conjunto de estas disposiciones configura un entramado normativo que busca garantizar la seguridad jurídica en las operaciones financieras digitales, estableciendo claramente las responsabilidades de las entidades financieras hacia los usuarios.

Determinación de responsabilidades ante incidentes de seguridad

En el contexto de los servicios financieros digitales, la determinación de responsabilidades ante incidentes de seguridad presenta complejidades específicas. Las entidades financieras responden bajo un régimen de responsabilidad objetivada fundamentado en la teoría del riesgo creado. Esta teoría sostiene que quien se beneficia de una actividad que genera riesgos debe asumir las consecuencias negativas derivadas de la misma (Parra, 2010). Los bancos y Fintech adquieren responsabilidad por el manejo habitual y lucrativo del dinero ajeno, asumiendo las contingencias propias de su actividad especializada. La jurisprudencia colombiana, especialmente a través de sentencias como la SC18614-2016 de la Corte Suprema de Justicia, ha establecido que las instituciones financieras deben responder por las transacciones fraudulentas realizadas mediante instrumentos electrónicos, a menos que se demuestre la culpa exclusiva del usuario.

Para determinar responsabilidades se analizan tres elementos fundamentales: la culpa de la entidad financiera, el perjuicio para el usuario y la relación causal entre ambos (Tamayo, 2018). En las operaciones electrónicas, la entidad puede exonerarse únicamente si prueba que el depositante incumplió sus obligaciones de cuidado y custodia de credenciales o dispositivos. Sin embargo, el nivel de sofisticación de los métodos de defraudación hace que para el usuario medio sea prácticamente imposible detectar ataques antes de la sustracción de dinero, lo que fortalece la responsabilidad de las instituciones (Sentencia SC18614-2016).

En relación con lo anterior, Ariza (2022) indica que, para determinar la responsabilidad ante fallas o vulneraciones, resulta necesario analizar factores como:

1. El grado de diligencia empleado por el proveedor del servicio en la implementación de mecanismos de seguridad
2. El cumplimiento de los estándares técnicos exigidos por los organismos de supervisión
3. La conducta del usuario y su posible contribución al incidente
4. Las obligaciones contractuales asumidas por cada parte

En este contexto, las entidades Fintech deben desarrollar políticas y procedimientos internos que les permitan utilizar adecuadamente los datos personales de sus clientes, así como establecer protocolos claros para la gestión de incidentes de seguridad y la asignación de responsabilidades.

Los tribunales examinan si la entidad implementó las medidas técnicas adecuadas para prevenir fraudes, considerando estándares de seguridad vigentes en la industria. La carga probatoria recae principalmente en la institución financiera, que debe demostrar el cumplimiento de sus obligaciones de seguridad y la intervención culposa del usuario en caso de pretender exonerarse (Arenas, 2019). La investigación realizada por Baquero & Prieto (2019) señala que la

seguridad de los sistemas Blockchain, utilizados por muchas fintech, depende en gran medida de la inmutabilidad de la información garantizada por la tecnología Hash. Sin embargo, existen vulnerabilidades no asociadas a la tecnología misma sino al uso que hacen las personas de estas plataformas, como el manejo inadecuado de claves de acceso o la pérdida de dispositivos (Díaz et al., 2024).

Por su parte, los intermediarios de valores que utilizan herramientas como los robo advisors mantienen su responsabilidad legal incluso cuando tercerizan funciones a través de estas plataformas automatizadas. Esta responsabilidad no puede ser transferida completamente al proveedor tecnológico, pues según la normativa financiera aplicable, como la Ley 964 de 2005, el Decreto 2555 de 2010 y la normativa complementaria de la Autorreguladora del Mercado de Valores, el intermediario debe garantizar la seguridad y protección de los datos e información de sus clientes.

Los incidentes pueden originarse por diversos factores que incrementan la impredecibilidad de los sistemas automatizados, como errores en los modelos algorítmicos, volatilidad del mercado no anticipada, fallos técnicos, limitaciones en la personalización del servicio o vulnerabilidades de ciberseguridad. Cuando estos eventos generan daños económicos a los usuarios, la responsabilidad contractual objetiva recae principalmente sobre el intermediario de valores que contrató el servicio automatizado (Nur, 2023).

En caso de violaciones de datos personales o incidentes de seguridad, tanto el intermediario financiero como el proveedor tecnológico pueden ser considerados responsables, dependiendo de las circunstancias específicas. La evaluación del nexo causal entre el daño sufrido y la falla en el sistema resulta esencial para determinar la responsabilidad, y el régimen propuesto no permite

eximir de responsabilidad alegando haber actuado con debida diligencia si el daño se materializa (Palmerini, 2017).

Respecto a sistemas de inteligencia artificial incorporados en el sector financiero, no existe un régimen específico de responsabilidad contractual y extracontractual, y Londoño (2024) propone clasificar los riesgos asociados a estos desarrollos en tres categorías: riesgos principales o directos, riesgos secundarios o colaterales, y riesgos no previsibles. Los riesgos directos se relacionan con la funcionalidad misma del sistema, como fallos en su calidad o defectos que impidan su correcta utilización, mientras que los riesgos secundarios, aunque no forman parte del objeto principal del contrato, pueden ocasionar incumplimientos por uso irresponsable o inseguro de los sistemas. Los riesgos no previsibles, por su naturaleza o por el estado actual del conocimiento y la técnica, no pueden anticiparse razonablemente durante el diseño, implementación u operación de los sistemas de IA.

Esta problemática se agudiza especialmente en el ámbito tecnológico, donde los daños suelen caracterizarse por ser en serie, afectar a múltiples partes y presentar carácter permanente. Los intermediarios financieros digitales enfrentan un régimen de responsabilidad que debe considerar tanto su papel como operadores tecnológicos como su función de prestadores de servicios financieros. Esta dualidad complejiza la asignación de responsabilidades, especialmente cuando intervienen múltiples actores en una cadena de prestación de servicios (Castaño, 2021). La responsabilidad en estos casos se complejiza por la opacidad de los algoritmos de aprendizaje automático, que dificulta la comprensión de cómo se llega a determinadas decisiones financieras. Este escenario complica la asignación de responsabilidades y la compensación a los usuarios perjudicados, dado que la regulación actual exige prueba de la culpa y del nexo causal (Londoño, 2024).

Mecanismos de protección y resarcimiento para usuarios

El ordenamiento jurídico colombiano contempla diversos mecanismos para proteger a los usuarios de servicios financieros digitales y permitir el resarcimiento ante pérdidas. El primer nivel de protección lo constituyen las reclamaciones directas ante las entidades, obligadas por la Ley 1328 de 2009 a contar con sistemas de atención al consumidor financiero. Este procedimiento permite resolver controversias de manera expedita sin necesidad de acudir a instancias judiciales. Estas normativas de protección al consumidor financiero establecen obligaciones específicas para los proveedores de estos servicios, como el deber de información, la transparencia en las condiciones contractuales y la implementación de sistemas efectivos de atención al cliente (Ariza, 2022).

La Resolución 2654 de 2019 del Ministerio de Salud y Protección Social de Colombia, aunque enfocada en telesalud y telemedicina, ofrece un marco de referencia aplicable por analogía a los servicios financieros digitales. Esta regulación establece requisitos fundamentales como la autorización previa del usuario, la garantía de identificación de las partes, el tratamiento confidencial de la información y la protección de datos personales conforme a la legislación nacional (Ariza, 2022).

Para los casos en que se produzcan daños derivados de fallas en los servicios Fintech, los usuarios pueden acudir a los mecanismos tradicionales de reclamación, como las quejas ante la entidad, las demandas judiciales por responsabilidad civil o las acciones de protección al consumidor ante la Superintendencia Financiera o la Superintendencia de Industria y Comercio (Ariza, 2022).

Si la reclamación directa no resulta satisfactoria, los usuarios pueden acudir a la Defensoría del Consumidor Financiero, figura creada como mecanismo de resolución de controversias. Sus decisiones, aunque no vinculantes en todos los casos, constituyen un importante filtro previo a instancias judiciales. Paralelamente, la Superintendencia Financiera, a través de su Delegatura para Funciones Jurisdiccionales, tiene competencia para conocer controversias relacionadas con la ejecución y cumplimiento de obligaciones contractuales, incluyendo aquellas derivadas de operaciones electrónicas. Para casos de mayor cuantía, los usuarios pueden acudir a la jurisdicción ordinaria, donde las controversias se dirimen aplicando el régimen de responsabilidad civil objetivada. Este régimen facilita la posición procesal del usuario, pues no debe probar la culpa de la entidad sino únicamente el daño y la relación causal (Arenas, 2019).

Como mecanismo complementario, algunas entidades ofrecen pólizas de seguro que cubren pérdidas por fraudes electrónicos (Arenas, 2019). Sin embargo, estos seguros generan costos adicionales para los usuarios y han sido criticados por trasladar a los clientes riesgos que deberían ser asumidos por las propias entidades. El artículo 87 de la Ley 45 de 1990 permite a los usuarios ejercer acción directa contra las aseguradoras en caso de siniestros cubiertos por las pólizas contratadas por las entidades financieras.

Cuando un usuario sufre daños por el uso de robo advisors, puede solicitar indemnización por los perjuicios causados, incluyendo la pérdida de capital invertido, intereses y costos asociados (Nur, 2023). Para acceder a estos resarcimientos, bajo el régimen tradicional de responsabilidad subjetiva, el usuario debería demostrar que el intermediario no cumplió con su deber de asesoría y que este incumplimiento fue la causa directa de los perjuicios sufridos. Sin embargo, el enfoque de responsabilidad objetiva propuesto eliminaría la necesidad de probar la culpa, bastando con demostrar el daño y el nexo causal (Tamayo, 2018).

La ley colombiana establece que los intermediarios de valores tienen la obligación de contar con seguros de responsabilidad civil profesional y sistemas de administración de riesgos que permitan responder por los daños causados a sus clientes. Además, los organismos reguladores como la Superintendencia Financiera y la Autorreguladora del Mercado de Valores (AMV) supervisan el cumplimiento de estas obligaciones y pueden imponer sanciones administrativas adicionales a las compensaciones económicas que correspondan a los afectados (Nur, 2023).

Es importante destacar que las bases de datos de estas entidades deben estar registradas ante el Registro Nacional de Bases de Datos (RNBD), lo que constituye un primer nivel de protección al permitir la supervisión por parte de autoridades competentes. Las empresas financieras digitales también comparten información con entidades especializadas como la Central de Información Financiera (CIFIN) y la Central de Información Crediticia (DataCrédito), lo que permite mantener un control sobre las operaciones financieras y establecer mecanismos de alerta ante posibles irregularidades.

El Decreto Reglamentario 222 de 2020 ha facilitado el acceso a préstamos de bajo monto para familias de escasos recursos a través de entidades autorizadas, incluyendo sociedades especializadas en depósitos y pagos electrónicos. Esta medida busca contrarrestar prácticas peligrosas como los préstamos "gota a gota", proporcionando alternativas seguras y supervisadas para los usuarios (Díaz et al., 2024).

Adicionalmente, la Circular Básica Jurídica de la Superintendencia Financiera establece límites a los movimientos mensuales (no superiores a 3 salarios mínimos mensuales legales vigentes) y al saldo máximo permisible (no mayor a 8 salarios mínimos mensuales legales vigentes) en cuentas de ahorro de trámite simplificado, lo que constituye un mecanismo de protección ante posibles fraudes de gran escala (Díaz et al., 2024).

Análisis de casos y jurisprudencia relevante

La evolución jurisprudencial sobre responsabilidad en operaciones financieras electrónicas muestra un desarrollo desde la aplicación analógica de las normas sobre cheques hacia un régimen especializado. Durante el período 1989-1999, las controversias se resolvían principalmente por analogía con el pago indebido de cheques, fluctuando entre regímenes de responsabilidad subjetiva y objetiva (Arenas, 2019). Un caso paradigmático fue resuelto por el Tribunal Superior de Bogotá en 2006, donde se estableció que la responsabilidad bancaria debía evaluarse bajo la teoría del riesgo creado. El tribunal concluyó que, si el banco no lograba demostrar la culpa del cuentahabiente, debería asumir el perjuicio derivado de retiros no autorizados, incluso sin haber incurrido en culpa (Tribunal Superior del Distrito Judicial de Bogotá, 2006).

La Corte Suprema de Justicia consolidó esta posición en el fallo de tutela del 11 de marzo de 2010, donde el magistrado Arturo Solarte afirmó que las instituciones financieras están sujetas a un especial régimen de responsabilidad civil frente a los daños sufridos por usuarios de sus servicios. Este fallo aclaró que los principios desarrollados para cheques falsificados podían aplicarse a las formas electrónicas de disposición de recursos (Corte Suprema de Justicia, 2010).

La sentencia SC18614-2016 constituye un punto de inflexión en la materia. En este fallo, el magistrado Ariel Salazar analizó exhaustivamente la responsabilidad bancaria por fraudes electrónicos, concluyendo que se fundamenta en vertientes de la teoría del riesgo (riesgo creado, riesgo provecho y riesgo profesional). La sentencia determinó que los medios tecnológicos desarrollados por las entidades financieras convierten a los usuarios en objetivos de la delincuencia, siendo estos la parte débil del eslabón de seguridad. Esta jurisprudencia ha incentivado a las entidades financieras a implementar medidas técnicas más robustas, pues el

régimen de responsabilidad objetiva traslada a ellas los costos económicos de los fraudes electrónicos, salvo prueba de culpa exclusiva del usuario (Arenas, 2019).

La Superintendencia Financiera de Colombia ha emitido conceptos sobre las criptomonedas y su naturaleza jurídica (Como el concepto No. 2009033065-003 del 11 de junio de 2009 y la Carta Circular 78 de 2016, entre otros), estableciendo que estas no constituyen un medio de pago de curso legal con poder liberatorio ilimitado, por lo que los acreedores no están obligados a recibirlas en cumplimiento de obligaciones. Esta posición, expresada a través del concepto JDS-10625 del 9 de mayo de 2014 del Banco de la República, incide directamente en la responsabilidad civil asociada a transacciones realizadas con estos activos digitales.

La jurisprudencia relacionada con la responsabilidad civil de las fintech en Colombia es aún limitada, debido en parte a la novedad de estos servicios financieros digitales. Díaz et al. (2024) menciona específicamente un caso contra Nequi, resuelto en el Juzgado Segundo Municipal de Pequeñas Causas Laborales de Bogotá (Radicado: 11001 41 05 002 2020 00 280 00). En esta demanda, el accionante Carlos Ernesto Losada Morantes reclamó por la pérdida de $100,000 colombianos previamente depositados en su cuenta. Este caso, aunque de cuantía menor, resulta ilustrativo por la participación de la Superintendencia Financiera de Colombia en la revisión del sistema. Sin embargo, según lo señalado en la investigación, no se encontraron elementos que evidenciaran irregularidades bancarias. Es relevante destacar que este parece ser el único proceso judicial documentado contra Nequi, lo que podría sugerir que la empresa ha operado con corrección y transparencia al menos desde la perspectiva de sus usuarios.

Propuestas para fortalecer el régimen de responsabilidad

El régimen de responsabilidad civil en servicios financieros digitales puede fortalecerse mediante diversas acciones en el plano normativo, tecnológico y educativo. En el ámbito normativo, convendría actualizar el marco regulatorio para contemplar expresamente las nuevas modalidades de servicios financieros digitales, superando la necesidad de aplicaciones analógicas de normas pensadas para operaciones tradicionales (Arenas, 2019).

Nur (2023) propone implementar un sistema de responsabilidad contractual objetiva fundamentado en las teorías del riesgo profesional y riesgo creado. Este enfoque partiría del principio de que las entidades que se benefician económicamente del riesgo inherente a las inversiones deben asumir la responsabilidad por los daños causados, sin necesidad de probar culpa o negligencia. Esta propuesta busca superar las limitaciones del régimen tradicional de responsabilidad subjetiva con culpa probada, que resulta insuficiente para abordar los desafíos que presentan los sistemas automatizados de asesoría financiera. La implementación de un régimen de responsabilidad objetiva simplificaría el proceso de reclamación para los usuarios afectados y proporcionaría mayor seguridad jurídica.

A su vez, Nur (2023) sugiere que el régimen actual contenido en el Decreto 661 de 2018 presenta problemas de efectividad, pues aunque está vigente, resulta ineficaz debido a la falta de reglamentación complementaria que debía emitir la Superintendencia Financiera. Esta situación ha generado inseguridad jurídica tanto para las entidades de vigilancia como para los clientes e intermediarios. No obstante, según el análisis realizado por la Misión Mercado de Capitales en su informe final de 2019, el legislador debe reevaluar la normativa actual sobre la profesión de los intermediarios en el mercado bursátil, pues las nuevas responsabilidades impuestas generan costos

excesivamente altos que dificultan el cumplimiento de metas y objetivos por parte de los intermediarios (Ministerio de Hacienda y Crédito Púbico, 2019).

Entre las propuestas que condensa Ariza (2022) para robustecer este marco normativo se encuentran:

1. Desarrollar una regulación específica sobre criptomonedas y activos digitales que clarifique su naturaleza jurídica y el régimen de responsabilidad aplicable a las transacciones realizadas con estos instrumentos.
2. Establecer estándares mínimos de seguridad informática para las plataformas Fintech, cuyo incumplimiento genere presunciones de responsabilidad en caso de vulneraciones.
3. Crear mecanismos alternativos de resolución de conflictos especializados en disputas tecnológico-financieras, que permitan soluciones ágiles y técnicamente adecuadas.
4. Implementar sistemas de certificación y acreditación para las entidades Fintech, que garanticen niveles adecuados de protección para los usuarios.
5. Desarrollar un régimen de responsabilidad objetiva para ciertos tipos de daños derivados de fallas en sistemas automatizados, equilibrando la necesidad de protección al consumidor con el fomento de la innovación.

Estas propuestas buscan adaptarse a un entorno financiero cambiante, donde la innovación tecnológica debe ir acompañada de un marco regulatorio que proteja adecuadamente los derechos de los usuarios sin obstaculizar el desarrollo de nuevos modelos de negocio que beneficien al mercado y a los consumidores.

La resolución de controversias podría mejorarse mediante la implementación de procedimientos específicos para casos de fraude electrónico. Los llamados mecanismos de SmartSettle o negociación asistida permitirían resolver controversias de pequeñas cuantías de

manera ágil y sin costo para el usuario, atendiendo al problema de microconflictividad que caracteriza estos casos, donde los montos defraudados suelen ser menores a los costos de un litigio (Alzate & Vázquez, 2013).

La implementación de contratos inteligentes (Smart Contracts) constituye otra propuesta para automatizar la resolución de controversias. Estos programas informáticos ejecutarían automáticamente las cláusulas correspondientes cuando se cumplan condiciones específicas, evitando acudir a instancias judiciales para la restitución de depósitos en casos de fraude (Chipana, 2019). En efecto, la implementación de *smart contracts* ofrece nuevas posibilidades de resarcimiento automático. Como indica Ariza (2022), la ejecución automatizada de estos contratos permite establecer indemnizaciones predeterminadas que se activan cuando se cumplen ciertas condiciones, lo que reduce la necesidad de intervención humana y agiliza el proceso de compensación. A diferencia de los sistemas tradicionales donde los registros de información de transacciones son almacenados en servidores de entidades intermediarias, la tecnología *blockchain* ofrece mayor seguridad al distribuir la información entre múltiples nodos conectados a la red, dificultando la alteración fraudulenta de los datos (Ariza, 2022).

En materia de aseguramiento, las pólizas de responsabilidad específicas para operaciones electrónicas constituyen una alternativa para distribuir riesgos. Sin embargo, estas deben ser contratadas por las entidades financieras sin trasladar su costo a los usuarios, pues la seguridad constituye un elemento esencial del servicio financiero y no un valor agregado (Narváez, 2015).

Las entidades de supervisión podrían imponer a los prestadores de servicios financieros digitales la obligación de implementar los desarrollos más avanzados en materia tecnológica para mitigar fraudes. Aunque esto representaría costos para las entidades, constituiría una solución

definitiva para los usuarios, pues aumentaría la certeza en las operaciones y dificultaría la exoneración de responsabilidad por parte de las instituciones financieras (Arenas, 2019).

Díaz et al. (2024) señalan la importancia de que las plataformas bancarias digitales trabajen conjuntamente con las centrales de riesgo para garantizar que la información de los usuarios sea correcta y actualizada, ajustándose a la normatividad vigente. Este enfoque permitiría prevenir actividades relacionadas con el lavado de activos mediante la verificación rigurosa de la fuente de los recursos que ingresan al sistema bancario.

En una línea similar, Zabala & Díaz (2020) argumentan que desde las plataformas de inteligencia artificial han surgido productos con altos niveles de seguridad, pero advierten que en aquellas empresas donde existe transferencia de dinero, como Nequi, persiste un riesgo de lavado de activos. Por ello, proponen fortalecer los controles en la colocación física del dinero dentro de los sistemas financieros y en la trazabilidad de las transacciones. Zabala (2021) añade que los Estados deben definir códigos de ética que limiten el alcance de la inteligencia artificial en el uso de datos personales, garantizando el respeto a los principios de privacidad, consentimiento informado y seguridad de la información en todas las operaciones financieras digitales.

Complementariamente, Castaño (2021) plantea la importancia de fortalecer los mecanismos de aseguramiento especializado. Para ello, sería necesario desarrollar productos de seguros que comprendan adecuadamente los riesgos específicos de las operaciones financieras digitales, considerando su potencial impacto masivo y las dificultades en la determinación precisa del daño. Este autor también señala la relevancia de implementar un enfoque preventivo, mediante la adopción de estándares técnicos y operativos que minimicen la probabilidad de incidentes de seguridad, complementando así el régimen de responsabilidad civil con medidas ex ante que reduzcan la necesidad de activar mecanismos de resarcimiento.

La responsabilidad civil de las empresas fintech en Colombia se encuentra en una encrucijada entre la aplicación analógica de normas tradicionales y la necesidad de desarrollar un marco regulatorio especializado que responda a las particularidades de los servicios financieros digitales. El régimen objetivado que ha ido consolidándose a través de la jurisprudencia constituye un avance significativo para la protección de los usuarios, pero requiere complementarse con desarrollos normativos específicos, estándares técnicos robustos y mecanismos ágiles de resolución de controversias. El desafío para los próximos años radica en construir un ecosistema jurídico que, sin obstaculizar la innovación tecnológica, garantice la seguridad de las operaciones, distribuya equitativamente los riesgos inherentes a las plataformas digitales y ofrezca vías efectivas de reparación ante los perjuicios derivados de vulnerabilidades técnicas o fallos operativos. Solo así se consolidará un entorno de confianza que permita el pleno desarrollo del potencial transformador de las fintech en la democratización de los servicios financieros.

Capítulo 4. Análisis comparado de experiencias regulatorias internacionales

Este capítulo ofrece un análisis comparativo de las experiencias regulatorias internacionales en materia de protección de usuarios fintech, estructurado en tres secciones principales. La primera, examina los diversos marcos regulatorios implementados en regiones como Europa, América del Norte, Latinoamérica, Asia y Oceanía, identificando sus características distintivas y enfoques particulares. La segunda, profundiza en los modelos regulatorios de referencia internacional, presentando un análisis de las tendencias globales emergentes, desde la transición hacia gobernanzas más ágiles hasta la implementación de sandboxes regulatorios, finanzas abiertas y enfoques de co-gobernanza público-privada. La tercera, identifica las mejores prácticas en protección de usuarios fintech adoptadas en diferentes regiones y la cuarta sección culmina con recomendaciones específicas para el fortalecimiento normativo en Colombia basadas en experiencias internacionales exitosas.

Marcos regulatorios internacionales

El estudio de los marcos regulatorios internacionales revela diversas aproximaciones normativas en materia fintech. Desde la armonización europea con el GDPR y PSD2, hasta la fragmentación estadounidense o el control gubernamental asiático, cada región ha desarrollado respuestas adaptadas a sus contextos específicos. América Latina muestra una evolución desde enfoques observacionales hacia estructuras más formales en países como México, Brasil y Chile.

Europa

Europa presenta un panorama regulatorio diverso y en constante evolución en materia de tecnología financiera. La Unión Europea ha adoptado un enfoque armonizado a través de regulaciones clave como la Directiva de Servicios de Pago 2 (PSD2) y la Directiva de Mercados

de Instrumentos Financieros II (MiFID II), bajo la coordinación de la Autoridad Bancaria Europea (EBA) que articula la regulación fintech entre los estados miembros (Hutukka, 2024). Este enfoque facilita los requisitos regulatorios para empresas fintech que operan dentro de la UE, aunque puede presentar desafíos para cumplir con estándares que podrían ser más estrictos que en sus países de origen (Zreik & Iqbal, 2024).

El Reglamento General de Protección de Datos (GDPR), implementado en mayo de 2018, constituye una pieza fundamental del marco regulatorio europeo en materia de privacidad y protección de datos, definiendo detalladamente los datos personales y su procesamiento, estableciendo principios de licitud, transparencia, limitación de finalidad, minimización, precisión, limitación de almacenamiento, e integridad y confidencialidad (Alekseenko, 2022). Este reglamento también otorga a los sujetos derechos específicos de acceso, rectificación, olvido, restricción, portabilidad y objeción, incluyendo disposiciones para la aplicación extraterritorial a empresas que procesen datos de ciudadanos de la UE (Alekseenko, 2022).

El Reino Unido destaca como pionero en innovación regulatoria, siendo el primer país en implementar un sandbox regulatorio en 2015 a través de la Autoridad de Conducta Financiera (FCA). Este modelo permite probar modelos de negocio innovadores bajo ciertas condiciones y limitaciones, facilitando la experimentación controlada con productos fintech (Chen, 2022). Adicionalmente, el establecimiento de una "Oficina de Innovación" facilita la comunicación entre reguladores y empresas FinTech, creando un entorno más colaborativo (Chen, 2022). El marco regulatorio británico se caracteriza por un enfoque proactivo que busca equilibrar innovación y gestión de riesgos, posicionando a Londres como un centro fintech líder en Europa (Vijayagopal et al., 2024).

En Europa Central y Oriental, los marcos regulatorios muestran diferentes niveles de desarrollo y madurez. Estonia se posiciona como uno de los países más progresistas, con su autoridad de supervisión financiera Finantsinspektsioon fomentando soluciones tecnológicas innovadoras y un Centro de Innovación para mejorar la comunicación con el sector financiero (Shala & Perri, 2022). Su legislación completa sobre ciberseguridad y protección de datos, junto con la regulación de criptomonedas y crowdfunding, la sitúan en una posición de liderazgo regional (Shala & Perri, 2022).

Lituania ha implementado un sandbox regulatorio bajo la supervisión del Banco de Lituania y un sistema electrónico para gestionar quejas y resolver disputas, además de desarrollar una moneda digital del banco central (CBDC) y establecer una regulación completa para préstamos P2P y crowdfunding (Shala & Perri, 2022). La República Checa ha tomado medidas para controlar los activos digitales desde 2017, reduciendo el anonimato de las transacciones y estableciendo un "punto de contacto fintech" a través del Banco Nacional Checo, además de implementar medidas completas de ciberseguridad y protección de datos (Shala & Perri, 2022).

Otros países de la región como Polonia han creado un Grupo de Trabajo Especial para la Innovación Financiera y un Programa Hub de Innovación y Sandbox Regulatorio (Shala & Perri, 2022). Hungría cuenta con aproximadamente 120 empresas fintech y ha lanzado un Centro de Innovación y Sandbox Regulatorio a través del Banco Nacional (Shala & Perri, 2022). Eslovaquia ha establecido un Centro de Innovación y ha implementado una CBDC, mientras que Letonia ha creado un centro de innovación y sandbox regulatorio a través de la Comisión del Mercado Financiero y de Capitales (Shala & Perri, 2022).

En contraste, Albania, Bosnia y Herzegovina y Kosovo presentan los marcos menos desarrollados de la región, con algunas actividades como préstamos peer-to-peer y crowdfunding

consideradas prohibidas (Shala & Perri, 2022). Albania ha propuesto una ley sobre activos virtuales y tiene la "Agenda Digital para Albania 2015-2020", mientras que Kosovo considera tanto el préstamo P2P como el crowdfunding actividades prohibidas, aunque ha anunciado la intención de crear una Oficina de Innovación (Shala & Perri, 2022).

Rusia ha implementado un enfoque distintivo, con su Ley Federal sobre Datos Personales y un requisito de localización que obliga a los operadores a almacenar datos de ciudadanos rusos en servidores ubicados dentro del país, reflejando un enfoque en mantener el control soberano sobre los datos de sus ciudadanos (Alekseenko, 2022). Su marco regulatorio incluye principios similares al GDPR europeo, pero con diferencias significativas como la prohibición de combinar bases de datos con finalidades incompatibles y una interpretación judicial amplia del concepto de datos personales para incluir cookies, direcciones IP y huellas digitales (Alekseenko, 2022).

América del norte

Estados Unidos se caracteriza por un sistema regulatorio complejo y fragmentado, con múltiples agencias federales y estatales involucradas en la supervisión del sector fintech. Los organismos reguladores clave incluyen la Reserva Federal, la Comisión de Valores y Bolsa (SEC), la Red de Control de Delitos Financieros (FinCEN) y la Oficina del Contralor de la Moneda (OCC), entre otros (Akpukorji et al., 2024). Esta fragmentación regulatoria crea desafíos para las empresas fintech, que deben navegar por una compleja red de requisitos federales, estatales y de autorregulación potencialmente conflictivos (Kalai & Toukabri, 2024).

El enfoque estadounidense implementa regulaciones centradas en la protección del consumidor, prevención del lavado de dinero y seguridad cibernética. Iniciativas como el Financial Charter de la OCC y sandboxes regulatorios a nivel estatal apoyan la innovación mientras

mantienen la supervisión (Vijayagopal et al., 2024). Las regulaciones clave incluyen la Ley Gramm-Leach-Biley (1999), la Ley de Firmas Electrónicas en el Comercio Global y Nacional (2000), la Ley Sarbanes-Oxley (2002) y la Ley Dodd-Frank (2010) (Vijayagopal et al., 2024). Adicionalmente, en 2012 se implementó la Ley JOBS (Jumpstart Our Business Startups), una de las primeras respuestas regulatorias específicas para FinTech, aunque no entró en vigor hasta 2015, lo que demuestra la lentitud del proceso legislativo (Chen, 2022).

A diferencia de su vecino del sur, Canadá ha adoptado un enfoque regulatorio más integrado con un regulador financiero central para las instituciones financieras federales y un sistema consistente de evaluación de riesgos (Kalai & Toukabri, 2024). En 2017, los Administradores de Valores de Canadá (CSA) lanzaron un sandbox regulatorio que proporciona a las empresas fintech un entorno favorable bajo supervisión regulatoria, exento de requisitos regulatorios específicos (Kalai & Toukabri, 2024). Este modelo reduce tanto el costo como el tiempo requerido para el lanzamiento de innovaciones tecnológicas y sirve como atractivo para mayores inversiones en proyectos FinTech (Kalai & Toukabri, 2024).

A pesar de estos avances, se señala que debido a su marco regulatorio, Canadá se queda rezagado respecto a Estados Unidos en la tasa de adopción de tecnologías financieras. La Oficina de Competencia canadiense sugiere que se requiere un formulador de políticas de tecnología financiera unificado que combine experiencia federal, provincial y territorial para facilitar el desarrollo de tecnologías financieras (Kalai & Toukabri, 2024).

Latinoamérica

El panorama regulatorio de la industria Fintech en América Latina presenta un desarrollo heterogéneo, con algunos países estableciendo marcos regulatorios integrales, mientras otros han

adoptado enfoques más fragmentados o se encuentran en etapas incipientes de regulación (Alcázar & Orbezo, 2024; García et al., 2024). La región experimenta un auge fintech impulsado por una creciente clase media y mayor penetración de smartphones, pero se enfrenta a desafíos como la inestabilidad económica y fragmentación regulatoria (Zreik & Iqbal, 2024). Las plataformas como MercadoPago deben navegar requisitos regulatorios que varían significativamente entre países, lo que complica la expansión regional (Zreik & Iqbal, 2024). La región está desarrollando regulaciones de protección de datos inspiradas en el GDPR europeo y medidas de ciberseguridad para abordar amenazas específicas de la región, aunque aún se encuentra en etapas iniciales de desarrollo de marcos regulatorios comprensivos para el sector fintech (Zreik & Iqbal, 2024).

México se posiciona como pionero regional con el marco regulatorio más comprensivo para Fintech, habiendo implementado la Ley para Regular las Instituciones de Tecnología Financiera en 2018. Esta normativa abarca aspectos como financiamiento colectivo, pagos virtuales, operaciones con activos virtuales y modelos novedosos (sandbox regulatorio), complementada con regulaciones secundarias emitidas por la Comisión Nacional Bancaria y de Valores y el Banco de México. Esto ha permitido crear un entorno que promueve la innovación financiera mientras mantiene la protección al consumidor y la estabilidad financiera (López & Melgar, 2024).

Brasil, aunque no cuenta con una ley Fintech específica, ha desarrollado progresivamente un ecosistema regulatorio robusto a través de diversas normativas emitidas por el Banco Central, particularmente en relación a pagos digitales, créditos y sistemas abiertos de finanzas. La implementación del sistema Open Finance representa un avance significativo, siendo considerado referente mundial por su amplio alcance que incluye servicios financieros, inversiones y seguros. Adicionalmente, iniciativas como Drex (moneda digital del Banco Central), y el sistema de pagos

instantáneos Pix, consolidan a Brasil como uno de los mercados Fintech más avanzados en términos regulatorios de la región (Teixeira dos Santos & Figueiredo, 2024).

Argentina presenta importantes avances con la Ley para Desarrollo de Servicios Financieros Tecnológicos emitida en diciembre de 2022, complementada con normativa secundaria para la constitución y registro de compañías Fintech para Crédito Digital, Sociedades Especializadas de Depósitos y Pagos Electrónicos, y Billeteras Electrónicas (Luegmayer & Ocampo, 2024). Este marco regulatorio permite supervisar adecuadamente las nuevas tecnologías financieras mientras se promueve la inclusión financiera y la competencia en el mercado.

Chile ha implementado recientemente un marco regulatorio integral con la Ley 21.521 que entró en vigor en febrero de 2023, estableciendo principios como innovación financiera, promoción de la competencia y protección al cliente financiero. Esta ley regula específicamente servicios como financiamiento colectivo, sistemas alternativos de transacción, intermediación de instrumentos financieros y custodia de instrumentos financieros. Además, establece un sistema de finanzas abiertas que permite el intercambio de información entre distintos prestadores de servicios financieros (Noriega et al., 2024).

Perú ha adoptado un enfoque más segmentado, sin una ley específica para Fintech, pero desarrollando regulaciones sectoriales que han permitido un crecimiento significativo del ecosistema. Destaca la regulación del financiamiento participativo financiero, autorización de empresas 100% digitales, y modificaciones a la normativa aplicable a empresas de préstamos. El ecosistema Fintech peruano continúa en expansión, con un crecimiento anual del 20,9% en el número total de empresas, predominando las verticales de "Préstamos", "Manejo de Inversiones" y "Pagos y Remesas" (Alcázar & Orbezo, 2024).

Uruguay ha avanzado significativamente con regulaciones específicas para plataformas de préstamos P2P, sistema de financiamiento colectivo y, recientemente, con la aprobación de la Ley de Activos Virtuales. Adicionalmente, el Banco Central de Uruguay ha establecido un Nodo de Innovación que funciona como sandbox regulatorio, presentando informes y propuestas en campos como Activos Virtuales, Finanzas Abiertas y Ciberseguridad. Es notable también el enfoque proactivo del regulador en materia de finanzas abiertas, habiendo presentado en 2024 un documento titulado "Hacia un ecosistema de Finanzas Abiertas en Uruguay" (Mailhos & Mercado, 2024).

El Salvador destaca por su enfoque disruptivo al adoptar Bitcoin como moneda de curso legal en 2021, convirtiéndose en el primer país del mundo en hacerlo. Esta iniciativa ha sido complementada con regulaciones adicionales como el Reglamento de Ley Bitcoin y normativas técnicas para facilitar la participación de entidades financieras en el ecosistema Bitcoin. Adicionalmente, en 2022 promulgó la Ley de Emisión de Activos Digitales y diversos reglamentos complementarios, estableciendo un marco regulatorio para activos digitales más allá de las criptomonedas (Arévalo & Bichara, 2024).

Otros países de la región como Guatemala, Panamá, Paraguay, Honduras y Costa Rica se encuentran en etapas más tempranas de desarrollo regulatorio. En Guatemala, las actividades Fintech se han adaptado a la regulación existente sin un marco específico, aunque existe un "SIB Innovation HUB" que funciona como punto de contacto entre reguladores y empresas tecnológicas (García et al., 2024). Panamá ha intentado legislar sobre criptoactivos, pero hasta ahora ninguna propuesta ha prosperado (Sosa & Sanjur, 2024). En Paraguay, las tecnologías Fintech no están ampliamente reguladas, aunque existe un sandbox regulatorio implementado por la Cámara Paraguaya de Fintech (Saavedra & Saavedra, 2024). Honduras cuenta con regulación limitada a

través del Banco Central y la Comisión Nacional de Bancos y Seguros (Pastrana, 2024), mientras que Costa Rica no ha emitido un marco legal específico, aunque cuenta con una Oficina de Innovación Financiera (Ureña & Sandí, 2024).

La regulación de activos virtuales y criptomonedas representa un área de particular interés, con enfoques regulatorios diversos. Mientras El Salvador ha adoptado una postura completamente favorable con la adopción legal del Bitcoin, otros países como México, Uruguay, Perú y Ecuador han comenzado a desarrollar marcos regulatorios para activos virtuales que buscan equilibrar la innovación con la protección al consumidor y la estabilidad financiera (Alcázar & Orbezo, 2024; Arévalo & Bichara, 2024; López & Melgar, 2024; Mailhos & Mercado, 2024; Riofrio & Almeida, 2024).

En materia de protección al consumidor financiero, varios países de la región han desarrollado marcos específicos. México, Argentina, Chile y Uruguay cuentan con normativas específicas para usuarios de servicios financieros, mientras que otros países aplican las disposiciones generales de protección al consumidor (López & Melgar, 2024; Mailhos & Mercado, 2024; Noriega et al., 2024; Riofrio & Almeida, 2024).

El financiamiento colectivo (crowdfunding) ha recibido atención regulatoria en varios países, con enfoques diferenciados según el tipo de crowdfunding (equity, lending, donaciones o recompensas). México, Brasil, Chile, Argentina, Perú y Uruguay han desarrollado marcos regulatorios para modalidades específicas de crowdfunding, estableciendo requisitos para plataformas, límites de inversión y mecanismos de protección al inversor (Alcázar & Orbezo, 2024; López & Melgar, 2024; Mailhos & Mercado, 2024; Noriega et al., 2024; Riofrio & Almeida, 2024; Teixeira dos Santos & Figueiredo, 2024).

Asia

Asia representa una de las regiones más dinámicas en desarrollo fintech, con marcos regulatorios que varían significativamente entre países. China se posiciona como un actor central con un enfoque regulatorio que ha evolucionado considerablemente con el tiempo. Inicialmente, el país adoptó un enfoque de "no hacer nada" hasta 2015 para promover la innovación, permitiendo el desarrollo del sector de préstamos P2P que posteriormente estuvo asociado con esquemas fraudulentos (Chen, 2022). En 2015, el Banco Popular de China (PBOC) junto con otros diez departamentos emitió la "Guía para Promover el Desarrollo Saludable de las Finanzas por Internet", marcando el inicio formal de la regulación FinTech en China (Bu et al., 2022).

La supervisión regulatoria en China se realiza por sectores, sin una ley unificada de fintech. El Banco Popular de China regula empresas fintech relacionadas con monedas, la Comisión Reguladora de Valores de China (CSRC) supervisa inversiones, y la Administración Reguladora Financiera Nacional (NFRA) supervisa otros sectores fintech (Hutukka, 2024). Un aspecto distintivo de la regulación china es la prohibición total de criptomonedas desde 2021 y el desarrollo avanzado de su moneda digital del banco central (e-CNY) (Hutukka, 2024). En materia de protección de datos, China ha implementado la Ley de Protección de Información Personal (PIPL) y la Ley de Seguridad de Datos (DSL), que limitan la capacidad del sector privado para usar datos, aunque con menores restricciones para el gobierno (Hutukka, 2024).

Singapur ha adoptado una postura proactiva creando un ambiente favorable para startups fintech. En 2016, la Autoridad Monetaria de Singapur (MAS) estableció las "Directrices Sandbox Regulatorio FinTech" y el Global FinTech Hackcelerator, posicionándose como un centro líder en innovación fintech (Chen, 2022; Bu et al., 2022). Este enfoque regulatorio proporciona directrices claras para empresas fintech y busca equilibrar la promoción de innovación con una adecuada

gestión de riesgos (Bu et al., 2022). Singapur ha establecido también centros de ciberseguridad específicos para combatir ataques cibernéticos en el sector fintech (Biswas et al., 2024).

Japón ha establecido un marco regulatorio integral para los intercambios de criptomonedas tras una serie de incidentes de hackeo. La industria de intercambio de criptomonedas formó proactivamente una asociación industrial y estableció reglas autorregulatorias (Chen, 2022). Incluso después de que Japón estableciera leyes y regulaciones formales, esta asociación continúa jugando un papel importante, ya que los solicitantes de licencias deben ser nominados por ella, demostrando su significativa función en la gobernanza (Chen, 2022). La Agencia de Servicios Financieros (FSA) supervisa este sector, garantizando la protección del consumidor (Zreik & Iqbal, 2024).

Hong Kong evolucionó de múltiples sandboxes regulatorios a uno único, lo que aumentó significativamente las solicitudes (Chen, 2022). Tailandia implementó un enfoque de sandbox múltiple donde el Banco Central, la Comisión de Valores y la Oficina de Seguros tienen sus propios sandboxes (Chen, 2022). Taiwán creó FinTechSpace, una incubadora apoyada por el regulador financiero FSC que ofrece asesoría legal, servicios de capital de riesgo y construcción de plataformas para conectar bancos con startups (Chen, 2022).

En los Emiratos Árabes Unidos, Abu Dhabi desarrolló Plug and Play Abu Dhabi, apoyado por la Oficina de Inversiones de Abu Dhabi (Chen, 2022). Este programa facilita la comunicación entre startups a través de espacios de coworking, ayudando a formar una atmósfera autorreguladora (Chen, 2022).

La región Asia-Pacífico en su conjunto se proyecta para un crecimiento significativo del sector fintech, con China liderando con una tasa de crecimiento anual compuesta (CAGR) del 27% para 2030, superando a Estados Unidos (Biswas et al., 2024). Este dinamismo está impulsando el

desarrollo continuo de marcos regulatorios adaptados a las características específicas de cada mercado, con un enfoque creciente en la inclusión financiera para poblaciones no bancarizadas y el desarrollo de tecnologías de pago digital avanzadas (Biswas et al., 2024).

Oceanía

La región de Oceanía, representada principalmente por Australia en los documentos analizados, presenta un enfoque regulatorio distintivo en el sector fintech. Australia ha adoptado un marco que combina elementos basados en principios con mecanismos de sandbox regulatorio, buscando un equilibrio entre innovación y protección al consumidor.

A través de la Comisión Australiana de Valores e Inversiones (ASIC), Australia implementó las "Directrices Sandbox Regulatorio" en 2016 y las "Guías Regulatorias 257: Prueba de Productos y Servicios Fintech sin Tener una Licencia AFS o de Crédito" en 2017 (Bu et al., 2022). Estas iniciativas permiten a las empresas fintech probar sus productos y servicios en un entorno controlado con ciertas exenciones regulatorias, facilitando la innovación mientras se mantiene un nivel adecuado de supervisión (Zreik & Iqbal, 2024).

El marco regulatorio australiano para el sector fintech involucra múltiples entidades, incluyendo la Comisión Australiana de Valores e Inversiones (ASIC) y la Autoridad Australiana de Regulación Prudencial (APRA) (Zreik & Iqbal, 2024). Estas instituciones supervisan el sandbox regulatorio y establecen directrices para la operación de empresas fintech en el país.

La Comisión Australiana de Competencia y Consumidores (ACCC) ha desarrollado una política de banca abierta con el objetivo de empoderar a los consumidores, dándoles mayor control sobre su información financiera y fomentando la competencia en el sector bancario (Chaturvedi & Sinha, 2024). Este régimen requiere que los bancos principales compartan datos de clientes a través

de interfaces de programación de aplicaciones (APIs) seguras con proveedores externos autorizados, permitiendo a las empresas fintech crear soluciones financieras innovadoras (Chaturvedi & Sinha, 2024).

En materia de protección de datos, Australia ha implementado un enfoque basado en principios para la privacidad, que incluye requisitos de notificación obligatoria de violaciones de datos y directrices claras sobre el consentimiento del consumidor (Zreik & Iqbal, 2024). El marco regulatorio australiano también especifica varias leyes relevantes para el sector fintech, incluyendo la Ley de Corporaciones, la Ley de Protección al Consumidor, la Ley de Transacciones Electrónicas, la Ley de Privacidad y la Ley de Lucha contra el Lavado de Dinero y Financiamiento del Terrorismo (AML-CTF Act) (Mahalle et al., 2021).

La Comisión de Productividad Australiana de 2008 estableció bases importantes para el desarrollo del marco regulatorio actual, enfocándose en un "marco regulatorio incremental para modelos de negocio iterativos" en la industria de servicios financieros (Mahalle et al., 2021). Este enfoque establece las bases para el crecimiento, escalabilidad y sostenibilidad de los modelos de negocio FinTech en Australia (Mahalle et al., 2021).

Síntesis comparativa de regiones

El mapeo realizado por regiones permite visualizar las diferentes aproximaciones regulatorias, estructuras institucionales y niveles de desarrollo normativo que caracterizan el ecosistema fintech mundial, facilitando la identificación de convergencias y divergencias entre bloques regionales. La tabla 1 presenta un análisis comparativo de los marcos regulatorios para

tecnologías financieras a nivel global, con sus respectivos enfoques para abordar la innovación financiera, la protección al consumidor y la estabilidad del sistema.

Tabla 1

Comparación de Marcos Regulatorios FinTech por Regiones

Característica	Europa	América del nort	Asia	Oceanía	América Latina
Enfoque principal	Armonización regulatoria con protección de datos	Fragmentación regulatoria (EE.UU.) vs. sistemas integrados (Canadá)	Control gubernamental con innovación dirigida	Principios basados en riesgo con sandbox estructurado	Desarrollo heterogéneo con énfasis en inclusión financiera y protección al consumidor
Estructura regulatoria	Centralizada (UE) con directivas como PSD2, MiFID II y GDPR	Múltiples agencias sectoriales (EE.UU.) vs. regulador central (Canadá)	Supervisión por sectores sin ley unificada	ASIC y APRA con enfoque basado en principios	Predominio de reguladores financieros tradicionales con adaptaciones para FinTech
Herramientas principales	Sandboxes regulatorios, oficinas de innovación, banca abierta	Licencias estatales (EE.UU.), sandbox nacional (Canadá)	Sandboxes gubernamentales, asociaciones industriales	Sandbox regulatorio, política de banca abierta	Sandboxes regulatorios, hubs de innovación y regulación sectorial
Nivel de desarrollo	Muy avanzado, con diferencias entre Europa Occidental y Oriental	Avanzado en EE.UU./Canadá, emergente en América Latina	Variable: muy avanzado (Singapur, Japón) a dirigido (China)	Avanzado y sistemático	Heterogéneo: avanzado (Brasil, México) a incipiente (Centroamérica)
Legislación específica	GDPR (2018), PSD2, MiFID II	Leyes sectoriales (EE.UU.), CSA sandbox (Canadá, 2017)	PIPL y DSL (China), leyes de cripto (Japón)	Directrices Sandbox (2016), legislación sectorial	Leyes FinTech integrales (México, Chile) vs. regulación fragmentada en otros países
Actitud hacia cripto	Regulada a través de MiCA	Variable por estado (EE.UU.), regulada (Canadá)	Prohibida (China), altamente regulada (Japón)	Regulada con enfoque en protección al consumidor	Diversa: adopción legal (El Salvador) a marcos regulatorios restrictivos
Aplicación territorial	Extraterritorial (GDPR)	Principalmente territorial	Estrictamente territorial	Principalmente territorial	Principalmente territorial con enfoque en mercados domésticos
Innovaciones regulatorias	Primer sandbox (Reino Unido, 2015), derechos digitales amplios	Financial Charter OCC, CSA sandbox (Canadá)	Sistema de "anonimato controlable" (China), autorregulación formal (Japón)	APIs seguras para banca abierta	Sistemas de pagos instantáneos (Brasil), banca digital 100% (Perú), adopción de Bitcoin (El Salvador)
Nivel de integración	Alto en UE, diferencias entre miembros	Fragmentado (EE.UU.), coordinado (Canadá)	Baja integración regional, sistemas nacionales	Coherente a nivel nacional	Baja integración regional, iniciativas nacionales independientes
Autoridades clave	EBA, ESMA, EIOPA, BCE, FCA (Reino Unido)	SEC, OCC, FinCEN, Fed (EE.UU.), CSA (Canadá)	PBOC, CSRC, NFRA (China), MAS (Singapur), FSA (Japón)	ASIC, APRA, ACCC	CNBV (México), BCB (Brasil), CMF (Chile), BCU (Uruguay), SBS (Perú)

Nota. Elaboración propia a partir de la revisión realizada.

El análisis comparativo revela diferentes variaciones en los enfoques regulatorios globales. Europa ha avanzado hacia una armonización regional con iniciativas como PSD2 y MiCA, mientras que Norteamérica presenta un contraste entre la fragmentación regulatoria estadounidense y el enfoque más centralizado canadiense. Asia exhibe modelos divergentes, desde el control estatal dirigido en China hasta enfoques más flexibles pero estructurados en Singapur. Oceanía destaca por su aproximación sistemática basada en principios. América Latina refleja diferentes velocidades de adaptación normativa, con modelos que varían desde regulación integral hasta observación pasiva.

A nivel global, se observa una tendencia hacia el fortalecimiento de marcos regulatorios específicos para fintech, aunque con estrategias diferenciadas que responden a prioridades locales, estructuras institucionales preexistentes y objetivos particulares de política pública, evidenciando que no existe un modelo único de regulación fintech sino aproximaciones adaptadas a los contextos socioeconómicos y jurídicos de cada región.

Modelos regulatorios de referencia internacional

Los modelos regulatorios de referencia internacional evidencian una transformación desde normativas rígidas hacia sistemas más ágiles. Esta evolución se manifiesta en sandboxes regulatorios, hubs de innovación, tecnologías regulatorias (RegTech) y esquemas de co-gobernanza público-privada. Estas aproximaciones buscan equilibrar la protección del consumidor y la estabilidad financiera con la promoción de la innovación, adaptándose a la naturaleza dinámica del sector fintech.

De la regulación rígida a la gobernanza ágil

La evolución de los marcos regulatorios de FinTech refleja un cambio paradigmático desde estructuras normativas rígidas y prescriptivas hacia sistemas de gobernanza más ágiles y adaptativos. Este modelo responde a la naturaleza altamente dinámica y en constante evolución del sector FinTech, donde el ritmo de innovación supera significativamente la capacidad de respuesta de los mecanismos legislativos tradicionales.

Chen (2022) documenta esta transformación como un cambio fundamental en la mentalidad regulatoria, donde los organismos supervisores están transitando desde un enfoque de control estricto hacia un modelo colaborativo que reconoce la necesidad de adaptabilidad. Este cambio no implica una desregulación, sino una reformulación de los mecanismos regulatorios para hacerlos más receptivos a la innovación tecnológica mientras mantienen su función protectora esencial.

La gobernanza ágil se caracteriza por marcos normativos basados en principios en lugar de reglas específicas, permitiendo a los reguladores adaptar sus interpretaciones y respuestas según evolucionan las tecnologías y modelos de negocio. Como señala Vijayagopal et al. (2024), existe una tendencia hacia la regulación adaptativa (AFR - Adaptive Finance Regulation) que permite a los reguladores ajustar su enfoque según evoluciona la tecnología, evitando así la obsolescencia regulatoria que típicamente afecta a marcos más rígidos.

En la práctica, esta transición se evidencia en la creciente adopción de aproximaciones regulatorias más iterativas y experimentales. Por ejemplo, el caso de Estonia ilustra este enfoque, donde Finantsinspektsioon promueve activamente que las empresas financieras adopten nuevas soluciones tecnológicas capaces de manejar controles de riesgo, estableciendo un marco flexible que incentiva la innovación responsable (Shala & Perri, 2022).

En América Latina, esta tendencia se manifiesta en la progresiva formalización regulatoria de actividades FinTech, avanzando desde modelos iniciales de "esperar y ver" hacia marcos más estructurados pero flexibles (Noriega et al., 2024). La evolución busca equilibrar la innovación con la protección al consumidor, la integridad del sistema financiero y la inclusión financiera, aspectos particularmente relevantes en una región con altos niveles de población no bancarizada (López & Melgar, 2024).

Sandboxes regulatorios como herramienta de innovación

Los sandboxes regulatorios representan quizás la innovación más significativa y ampliamente adoptada en la regulación FinTech global. Estos "entornos de prueba" proporcionan espacios controlados donde las empresas pueden experimentar con productos y servicios innovadores bajo supervisión regulatoria, pero con ciertas exenciones o flexibilidades normativas temporales.

Iniciado por la Autoridad de Conducta Financiera (FCA) del Reino Unido en 2015, este modelo ha sido replicado con variaciones en numerosas jurisdicciones. El sandbox británico limita los montos transaccionales anuales y los grupos de usuarios para mitigar riesgos potenciales, permitiendo que las empresas participantes operen con "inversores profesionales" durante "un año" con un límite transaccional de "1 millón de dólares anuales" (Chen, 2022). Adicionalmente, la FCA asigna un experto para asistir a las empresas dentro del sandbox, facilitando tanto la innovación como el cumplimiento regulatorio.

La eficacia de este modelo ha llevado a su adopción global con adaptaciones locales. La Autoridad Monetaria de Singapur (MAS) estableció su sandbox en 2016, posicionando al país como una jurisdicción progresista y favorable a la innovación, atrayendo talento, inversión y

asociaciones globales (Chaturvedi & Sinha, 2024). En Australia, la Comisión Australiana de Valores e Inversiones (ASIC) implementó sus "Directrices Sandbox Regulatorio" en 2016, permitiendo a participantes probar productos sin necesidad de obtener licencias completas (Bu et al., 2022).

Un desarrollo interesante es la evolución de modelos de sandbox específicos. Tailandia implementó un enfoque de sandbox múltiple donde el Banco Central, la Comisión de Valores y la Oficina de Seguros tienen sus propios sandboxes sectoriales (Chen, 2022). En contraste, Hong Kong evolucionó de múltiples sandboxes regulatorios a uno único, lo que aumentó significativamente las solicitudes de participación (Chen, 2022). Estas variaciones reflejan adaptaciones a contextos regulatorios y mercados específicos.

La importancia de los sandboxes trasciende la mera flexibilidad regulatoria. Como señala Kalai & Toukabri (2024), estos entornos reducen tanto el costo como el tiempo requerido para el lanzamiento de innovaciones tecnológicas y sirven como un imán atractivo para mayores inversiones en proyectos FinTech. En economías emergentes, los sandboxes han sido particularmente valiosos para catalizar la inclusión financiera, permitiendo a las startups experimentar con productos financieros novedosos adaptados a poblaciones desatendidas (Akpukorji et al., 2022).

Varios países latinoamericanos han implementado sandboxes regulatorios como complemento a sus enfoques regulatorios principales. México, Brasil, Colombia y Perú cuentan con estos espacios controlados de experimentación que permiten probar nuevos modelos de negocio bajo supervisión regulatoria, pero con ciertas flexibilizaciones normativas (López & Melgar, 2024; Teixeira & Figueiredo, 2024; Alcázar & Orbezo, 2024). Los sandboxes facilitan la innovación y proporcionan a los reguladores información valiosa sobre nuevos modelos de

negocio antes de definir marcos regulatorios permanentes, aunque su alcance suele ser limitado a pocas empresas y por periodos acotados (Mailhos & Mercado, 2024).

Surgimiento de hubs de innovación y RegTech

Complementando a los sandboxes regulatorios, los hubs o centros de innovación han emergido como espacios institucionales donde las empresas FinTech pueden interactuar con los reguladores para obtener orientación sobre cómo navegar el marco normativo. A diferencia de los sandboxes, que ofrecen entornos de prueba con exenciones específicas, estos hubs funcionan como puntos de contacto y canales de comunicación que facilitan el entendimiento mutuo entre innovadores y supervisores.

Estonia estableció un Centro de Innovación a través de Finantsinspektsioon para facilitar la comunicación entre la autoridad supervisora y las empresas que aplican innovación en el sector financiero (Shala & Perri, 2022). De manera similar, la República Checa creó un "punto de contacto fintech" a través del Banco Nacional Checo, mientras que Polonia estableció un Grupo de Trabajo Especial para la Innovación Financiera (Shala & Perri, 2022). Estos mecanismos permiten a los reguladores comprender mejor los modelos de negocio emergentes y a las empresas navegar requisitos regulatorios complejos.

Paralelamente, la Tecnología Regulatoria (RegTech) representa una tendencia creciente en el panorama regulatorio global. RegTech utiliza tecnologías emergentes como blockchain, computación en la nube, aprendizaje automático e interfaces de programación de aplicaciones (API) para mejorar la eficiencia y eficacia de la regulación y el cumplimiento (Bu et al., 2022). El Reino Unido sobresale en este ámbito, siendo el país con mayor número de empresas RegTech (90 según el informe de Bu et al., 2022).

La implementación de RegTech facilita la supervisión de riesgos en tiempo real, permite análisis predictivos de potenciales violaciones normativas y automatiza procesos de reporte regulatorio, reduciendo la carga administrativa tanto para reguladores como para entidades supervisadas. Como señala Biswas et al. (2021), este enfoque se centra en mejorar el cumplimiento normativo mediante sistemas automatizados, utilizando análisis de datos avanzados para aumentar la eficiencia y reducir costos asociados con el cumplimiento regulatorio.

Estas iniciativas están transformando la relación tradicional entre reguladores y regulados, estableciendo un diálogo bidireccional que favorece tanto la innovación como el cumplimiento normativo efectivo. Los reguladores obtienen mayor visibilidad sobre desarrollos tecnológicos emergentes, mientras que las empresas FinTech reciben orientación temprana sobre potenciales desafíos regulatorios, creando un círculo virtuoso de colaboración.

Los países latinoamericanos han ido desarrollando instrumentos regulatorios cada vez más sofisticados, incluyendo hubs de innovación que complementan los sandboxes y facilitan la comunicación entre reguladores y empresas FinTech (Alcázar & Orbezo, 2024; Teixeira & Figueiredo, 2024). Esta tendencia se corresponde con un incremento en la cooperación entre reguladores y sector privado, elemento clave para el desarrollo de marcos normativos adaptativos en la región (Mailhos & Mercado, 2024).

Balance entre protección al consumidor e innovación

Un desafío central en la regulación FinTech es encontrar el equilibrio óptimo entre fomentar la innovación que puede expandir el acceso a servicios financieros y garantizar la protección adecuada para consumidores y estabilidad sistémica. Esta tensión fundamental ha dado

lugar a modelos regulatorios que buscan calibrar cuidadosamente las exigencias normativas según el nivel de riesgo.

Chaturvedi & Sinha (2024) identifican una tendencia creciente hacia marcos regulatorios basados en principios que priorizan la flexibilidad, la innovación y la supervisión basada en riesgos. Este enfoque permite a los reguladores responder a dinámicas y tecnologías de mercado cambiantes rápidamente, ajustando sus intervenciones según la naturaleza y magnitud de los riesgos identificados. Por ejemplo, la Comisión Australiana de Competencia y Consumidores (ACCC) desarrolló una política de banca abierta que equilibra el empoderamiento del consumidor mediante mayor control sobre su información financiera con salvaguardas organizacionales y técnicas robustas para proteger los datos (Chaturvedi & Sinha, 2024).

En la Unión Europea, el Reglamento General de Protección de Datos (GDPR) y la Directiva de Servicios de Pago 2 (PSD2) establecen marcos que promueven tanto la innovación como la protección del consumidor. El GDPR garantiza derechos amplios para usuarios mientras que PSD2 impulsa la competencia a través de la banca abierta, introduciendo requisitos de seguridad más estrictos como la autenticación reforzada de clientes (Hutukka, 2024). Este equilibrio permite el desarrollo de nuevos servicios financieros mientras mantiene altos estándares de seguridad y privacidad.

Estados Unidos presenta un enfoque distinto, con un sistema regulatorio más fragmentado pero que enfatiza requisitos robustos de ciberseguridad y normativas AML/KYC estrictas (Vijayagopal et al., 2024). La implementación de licencias bancarias nacionales de propósito especial permite a las empresas FinTech operar bajo un marco regulatorio adecuado a sus necesidades específicas, manteniendo altos estándares de seguridad y privacidad (Akpukorji et al., 2022).

Este equilibrio no es estático sino dinámico, evolucionando con la madurez del mercado. Como ilustra el caso chino, inicialmente se adoptó un enfoque permisivo para promover la innovación, pero tras casos problemáticos como Ezubao, los reguladores implementaron controles más estrictos (Chen, 2022). Esta calibración continua refleja un aprendizaje regulatorio que busca mantener un balance óptimo entre apertura a la innovación y controles proporcionados al riesgo.

En la región latinoamericana, este balance se manifiesta en distintos modelos regulatorios. El Modelo de Regulación Integral, adoptado principalmente por México y Chile, establece leyes marco específicas que ofrecen mayor certeza jurídica y reglas claras tanto para emprendedores como para consumidores (López & Melgar, 2024). En contraste, el Modelo de Observación Pasiva adoptado en varios países centroamericanos y Paraguay permite mayor flexibilidad para la experimentación e innovación, aunque genera incertidumbre regulatoria y puede presentar mayores riesgos para los consumidores (García Sáenz et al., 2024; Ureña & Sandí, 2024).

Co-gobernanza público-privada

Uno de los desarrollos más significativos en la regulación FinTech es la transición desde modelos puramente gubernamentales hacia esquemas de gobernanza compartida que involucran tanto a reguladores públicos como a actores privados. Esta co-gobernanza reconoce que la complejidad y el ritmo de cambio en el sector FinTech requieren aprovechar la experiencia y capacidades de múltiples partes interesadas.

Chen (2022) identifica claramente esta evolución desde la supervisión gubernamental tradicional hacia modelos de co-gobernanza público-privada. Este cambio se refleja en el surgimiento de asociaciones industriales con funciones autorregulatorias, agencias de calificación crediticia y aceleradoras vinculadas a gobiernos. Por ejemplo, en el Reino Unido, la asociación

industrial de préstamos P2P (P2PFA) jugó un papel autorregulador importante antes de la intervención formal de la FCA, estableciendo estándares que luego influyeron en la regulación formal (Chen, 2022).

El caso japonés ofrece un ejemplo particularmente ilustrativo. La industria de intercambio de criptomonedas formó proactivamente una asociación industrial y estableció reglas autorregulatorias. Incluso después de que Japón estableciera leyes y regulaciones formales, la asociación de la industria sigue desempeñando un papel crucial, ya que los solicitantes de licencias deben ser nominados por esta asociación, demostrando su función significativa en la gobernanza (Chen, 2022).

Modelos similares se observan en aceleradoras vinculadas a gobiernos, como el Global FinTech Hackcelerator en Singapur, Plug and Play Abu Dhabi en los Emiratos Árabes Unidos, y FinTechSpace en Taiwán. Estas iniciativas combinan recursos y experiencia tanto pública como privada, proporcionando tutoría, espacios de trabajo, consultas con expertos de la industria y acceso a financiamiento (Chen, 2022).

Alekseenko (2022) destaca el fomento creciente de la autorregulación y autocontrol por parte de la industria, combinado con mecanismos formales de supervisión gubernamental. Esta tendencia refleja un reconocimiento de que los reguladores por sí solos no pueden seguir el ritmo de la innovación, mientras que la industria por sí sola podría priorizar el crecimiento sobre la protección del consumidor.

La co-gobernanza ofrece varias ventajas, incluyendo mayor flexibilidad, capacidad de respuesta rápida ante nuevos desarrollos, y aprovechamiento del conocimiento especializado del sector privado. Sin embargo, también presenta desafíos relacionados con conflictos de interés

potenciales y la necesidad de mecanismos de rendición de cuentas efectivos. El éxito de estos modelos depende de un equilibrio cuidadoso entre autonomía industrial y supervisión pública.

América Latina muestra una tendencia creciente hacia la cooperación entre reguladores y sector privado, elemento fundamental para el desarrollo de marcos normativos adaptativos (Mailhos & Mercado, 2024). Esta co-gobernanza es particularmente evidente en el Modelo de Regulación Sectorial ejemplificado por Brasil, donde el Banco Central ha desarrollado normativas particulares para diferentes verticales FinTech en colaboración con representantes de la industria (Teixeira & Figueiredo, 2024).

Armonización internacional y cooperación transfronteriza

La naturaleza inherentemente global de las operaciones FinTech está impulsando esfuerzos significativos hacia la armonización regulatoria internacional y la cooperación transfronteriza. Esta tendencia responde a la realidad de que las plataformas digitales financieras operan fácilmente a través de fronteras, creando desafíos para marcos regulatorios tradicionalmente definidos por límites jurisdiccionales nacionales.

Alekseenko (2022) identifica la armonización internacional como una tendencia dominante debido al carácter transfronterizo de FinTech. Observa principios comunes emergentes entre jurisdicciones, como el consentimiento libre, específico, informado e inequívoco; limitación de la finalidad del procesamiento de datos; precisión y relevancia de datos; seguridad y confidencialidad; y control del usuario sobre sus datos. Esta convergencia de principios facilita operaciones multinacionales y reduce la fragmentación regulatoria.

Existe una tendencia creciente hacia la aplicación extraterritorial de leyes nacionales, especialmente evidente en el GDPR europeo, que se aplica a cualquier entidad que procese datos

de ciudadanos de la UE independientemente de su ubicación (Alekseenko, 2022). Este enfoque incentiva la adopción de estándares regulatorios más elevados a nivel global, ya que las empresas que operan internacionalmente deben cumplir con los requisitos más estrictos de las jurisdicciones donde tienen presencia.

La cooperación regulatoria transfronteriza se manifiesta cada vez más a través de acuerdos bilaterales y multilaterales entre autoridades supervisoras. Un ejemplo es el memorando de entendimiento entre la Agencia Supervisora de Servicios Financieros de Croacia y la Autoridad de Valores de Israel para colaboración en temas fintech (Shala & Perri, 2022). Estos acuerdos facilitan el intercambio de información, mejoran la supervisión coordinada y promueven enfoques regulatorios consistentes.

Zreik & Iqbal (2024) destacan que la cooperación regulatoria transfronteriza busca abordar desafíos regulatorios globales, garantizar estándares consistentes y promover la armonización y convergencia regulatoria. Esta colaboración es particularmente importante para combatir el fraude transnacional, el lavado de dinero y otros riesgos que trascienden fronteras nacionales.

Sin embargo, la armonización plena enfrenta obstáculos significativos, incluyendo diferencias en sistemas legales, prioridades políticas y niveles de desarrollo económico. Como resultado, observamos un proceso gradual de convergencia más que una estandarización completa, con esfuerzos para establecer principios comunes mientras se mantiene flexibilidad para adaptaciones locales.

La región está avanzando hacia cierta armonización, con países desarrollando regulaciones de protección de datos inspiradas en el GDPR europeo, aunque adaptadas a las realidades regionales (Zreik & Iqbal, 2024). Sin embargo, persisten importantes diferencias entre los enfoques nacionales, como evidencia el caso único de El Salvador con su Modelo Experimental

marcado por la adopción del Bitcoin como moneda de curso legal, implementando cambios regulatorios disruptivos que lo posicionan como pionero en nichos específicos (Bichara & Arévalo, 2024).

Adaptación contextual a realidades regionales

A pesar de las tendencias globales hacia cierta convergencia en principios regulatorios, persiste una marcada adaptación de los modelos regulatorios a las realidades sociales, económicas y culturales específicas de cada región. Esta diversificación refleja diferentes prioridades, capacidades y contextos en los que opera la tecnología financiera.

Vijayagopal et al. (2024) observan que mientras los países desarrollados como EE.UU. y Reino Unido tienden a enfocarse en una amplia gama de innovaciones fintech, los países en desarrollo como India ponen mayor énfasis en la inclusión financiera y los pagos digitales. Esta diferencia de enfoque se manifiesta en los marcos regulatorios, con India implementando iniciativas gubernamentales como Digital India, UPI (Interfaz de Pagos Unificada) y Aadhaar que priorizan el acceso financiero para poblaciones anteriormente excluidas.

Incluso dentro de regiones aparentemente homogéneas como Europa Central y Oriental, existen variaciones significativas. Estonia, Lituania y Eslovaquia presentan marcos regulatorios avanzados con sólidos sistemas de identidad digital, mientras que Albania, Bosnia y Herzegovina y Kosovo muestran desarrollos regulatorios más incipientes (Shala & Perri, 2022).

Esta adaptación contextual no contradice la tendencia hacia cierta convergencia global en principios fundamentales, sino que refleja la necesidad de implementaciones diferenciadas que respondan a realidades locales específicas. El éxito de los marcos regulatorios fintech depende en

gran medida de su capacidad para balancear principios universales con soluciones adaptadas a contextos particulares.

Este aspecto es particularmente relevante en América Latina, donde se identifican enfoques específicos como el Modelo de Adaptación Normativa implementado en países como Perú, Uruguay y Argentina. Este modelo busca adaptar la regulación existente para acomodar los nuevos modelos de negocio FinTech, complementándola con normativas específicas para ciertas verticales (Alcázar & Orbezo, 2024; Mailhos & Mercado, 2024; Riofrio & Almeida, 2024). La ventaja de este enfoque es su pragmatismo, permitiendo la operación de empresas FinTech sin necesidad de una reforma integral del marco financiero, aunque puede generar incertidumbre regulatoria en ciertos segmentos de la industria (Saavedra & Saavedra, 2024).

Modelo Experimental

El Salvador representa un caso sin precedentes a nivel global con su Modelo Experimental, caracterizado principalmente por la adopción del Bitcoin como moneda de curso legal. Este enfoque regulatorio disruptivo posiciona al país como pionero en la integración de criptomonedas al sistema financiero formal, asumiendo riesgos regulatorios significativamente mayores que otras jurisdicciones (Bichara & Arévalo, 2024). A diferencia de los modelos incrementales predominantes en otras regiones, El Salvador ha optado por un cambio radical que redefine fundamentalmente la relación entre monedas digitales y el sistema financiero tradicional.

Esta aproximación puede generar ventajas competitivas en segmentos específicos, atrayendo inversiones e impulsando la innovación en tecnologías blockchain, aunque simultáneamente conlleva mayores riesgos sistémicos y desafíos de protección al consumidor al implementar sistemas sin precedentes regulatorios comparables (Bichara & Arévalo, 2024). Este

modelo diverge significativamente de los enfoques más cautelosos adoptados en otras regiones como Europa, Asia o Norteamérica, donde las criptomonedas son generalmente tratadas como activos o instrumentos financieros específicos, pero no como moneda de curso legal con todas sus implicaciones para el sistema financiero y la economía en general.

Distinción entre Regulación Integral y Sectorial

América Latina ha desarrollado dos aproximaciones regulatorias particularmente definidas que representan polos opuestos en el espectro de formalización normativa: el Modelo de Regulación Integral y el Modelo de Regulación Sectorial. El primero, adoptado principalmente por México y Chile, se caracteriza por la creación de leyes marco específicas para la industria fintech. México, pionero regional con su Ley para Regular las Instituciones de Tecnología Financiera de 2018, estableció un marco comprensivo que abarca diversas verticales fintech bajo un mismo cuerpo normativo, incluyendo crowdfunding, pagos virtuales y activos virtuales (López & Melgar, 2024). Este enfoque ofrece mayor certeza jurídica y establece reglas claras tanto para emprendedores como para consumidores, facilitando el desarrollo del ecosistema con una visión holística, aunque puede resultar menos ágil para adaptarse a innovaciones no contempladas inicialmente.

En contraste, el Modelo de Regulación Sectorial, ejemplificado por Brasil, se caracteriza por la emisión de regulaciones específicas para cada vertical fintech, sin una ley marco integral. El Banco Central de Brasil ha desarrollado normativas particulares para pagos digitales, instituciones de crédito fintech, sistemas de financiamiento colectivo y Open Finance, entre otros (Teixeira & Figueiredo, 2024). Esta aproximación permite mayor adaptabilidad a las características específicas de cada vertical y facilita la actualización normativa ante nuevos

desarrollos tecnológicos, aunque puede generar cierta fragmentación regulatoria y complejidad para empresas que operan en múltiples verticales (Alcázar & Orbezo, 2024). Esta distinción nítida entre enfoques integrales y sectoriales representa una característica distintiva del panorama regulatorio latinoamericano, ofreciendo diferentes modelos de gobernanza para el desarrollo fintech según las prioridades y capacidades regulatorias de cada país.

Mejores prácticas en la protección de la seguridad y privacidad de usuarios fintech

Las mejores prácticas en protección de usuarios fintech reflejan un creciente consenso sobre principios fundamentales adaptados regionalmente. Europa destaca con mecanismos como consentimiento informado y autenticación reforzada; Estados Unidos implementa supervisión sectorial y monitoreo avanzado; Asia desarrolla sistemas como el "anonimato controlable" chino; Oceanía enfatiza evaluaciones continuas de riesgo. Estas experiencias proporcionan referentes valiosos para fortalecer el marco normativo colombiano.

Europa

Europa ha desarrollado algunas de las prácticas más avanzadas en materia de protección y seguridad para usuarios de servicios financieros digitales. La implementación del Reglamento General de Protección de Datos (GDPR) estableció un estándar global para la protección de información personal, creando un marco integral que va más allá del sector fintech pero que tiene implicaciones significativas para este (Alekseenko, 2022). A continuación, se describen las principales prácticas:

Transparencia y consentimiento informado: Una de las prácticas distintivas implementadas en la Unión Europea es el requisito de consentimiento claro y específico antes del procesamiento

de datos. El GDPR exige que las empresas fintech obtengan un consentimiento explícito, específico e informado de los usuarios antes de recopilar y procesar sus datos personales (Alekseenko, 2022). Esta aproximación ha transformado la manera en que las aplicaciones financieras interactúan con los usuarios, priorizando la transparencia y la autonomía del consumidor.

Derechos digitales amplios: El marco europeo otorga a los usuarios un conjunto amplio de derechos sobre sus datos: acceso, rectificación, eliminación (derecho al olvido), restricción, portabilidad y objeción. Esta estructura fortalece significativamente la posición del usuario frente a las empresas fintech, permitiéndole mayor control sobre su información personal y financiera (Alekseenko, 2022). La portabilidad de datos es particularmente relevante en el contexto fintech, ya que facilita la movilidad entre proveedores de servicios.

Autenticación reforzada y seguridad técnica: La Directiva de Servicios de Pago 2 (PSD2) introdujo la autenticación reforzada de clientes (SCA) para pagos en línea, estableciendo un estándar de seguridad más exigente. Este sistema requiere verificación a través de al menos dos factores independientes entre algo que el usuario conoce (contraseña), posee (dispositivo móvil) o es (biometría) (Hutukka, 2024). La combinación de estos elementos ha reducido significativamente el fraude en transacciones electrónicas.

Evaluaciones de impacto y enfoque preventivo: Una práctica innovadora es el requisito de evaluaciones de impacto de privacidad para tecnologías de alto riesgo. Este enfoque preventivo obliga a las empresas fintech a evaluar los riesgos potenciales para los derechos y libertades de los individuos antes de implementar nuevas tecnologías o procesos que involucren datos personales (Alekseenko, 2022). Esta aproximación proactiva ha incentivado la integración de principios de "privacidad por diseño" en el desarrollo de soluciones fintech.

Supervisión independiente: Europa ha establecido autoridades independientes de supervisión en cada Estado miembro, creando un sistema de vigilancia especializado con poderes reales de investigación y sanción. En el Reino Unido, la FCA asigna expertos específicos para asistir a las empresas dentro del sandbox regulatorio, equilibrando orientación con supervisión (Chen, 2022). Este modelo de supervisión activa pero colaborativa facilita tanto la innovación como el cumplimiento de estándares de seguridad.

Banca abierta con salvaguardas: La implementación de la banca abierta bajo PSD2 permite a los consumidores compartir datos financieros con terceros de manera segura, a través de interfaces de programación de aplicaciones (APIs) estandarizadas y seguras (Hutukka, 2024). Este enfoque equilibra la innovación con la seguridad, permitiendo el desarrollo de nuevos servicios financieros sin comprometer la privacidad y protección del usuario.

El enfoque europeo hacia la protección y seguridad en fintech se distingue por su carácter integral, preventivo y centrado en el usuario. La combinación de requisitos técnicos robustos, derechos amplios para los usuarios y supervisión efectiva ha establecido un estándar de referencia global, influyendo en los marcos regulatorios de otras regiones que buscan un equilibrio similar entre innovación y protección.

América del norte

En el continente americano, las prácticas de protección y seguridad muestran contrastes significativos entre el enfoque fragmentado pero riguroso de Estados Unidos y el sistema más integrado de Canadá. A continuación, se describen las principales prácticas:

Supervisión multicapa con enfoque sectorial: Estados Unidos implementa un sistema de supervisión con múltiples capas regulatorias que, a pesar de su fragmentación, establece estándares

elevados para la protección del consumidor. Este enfoque sectorial proporciona protecciones específicas para distintos tipos de datos: financieros, médicos y de comunicaciones (Alekseenko, 2022). La ventaja de esta aproximación es la adaptación precisa a los riesgos particulares de cada segmento del mercado financiero.

Monitorización avanzada de riesgos cibernéticos: Las entidades financieras estadounidenses han desarrollado sistemas sofisticados para la monitorización de riesgos cibernéticos, particularmente relevantes ante la exposición a riesgos descentralizados como la vulnerabilidad de datos de clientes a través de tecnologías de interfaz (Kalai & Toukabri, 2024). Estos sistemas incluyen el análisis de comportamiento de usuarios, detección de anomalías y respuesta automatizada a amenazas potenciales.

Supervisión rigurosa de terceros: Un elemento distintivo del modelo estadounidense es el énfasis en la supervisión de proveedores externos. Los bancos que se asocian con empresas tecnológicas deben implementar mecanismos robustos para monitorear y gestionar a terceros, lo que requiere mayor diligencia debida y costos continuos de monitorización (Kalai & Toukabri, 2024). Esta práctica es crucial en un ecosistema donde las instituciones financieras tradicionales frecuentemente colaboran con startups fintech.

Enfoque basado en divulgación: La Ley Gramm-Leach-Biley establece requisitos detallados para que las instituciones financieras proporcionen avisos de privacidad, implementando un modelo de protección basado en la divulgación transparente de políticas y prácticas (Vijayagopal et al., 2024). Este enfoque complementa las medidas técnicas de seguridad con un componente informativo que busca empoderar al consumidor mediante el conocimiento.

Regulación preventiva del fraude: La implementación de normativas como la Regla de Custodia (2013) establece mecanismos específicos para proteger los activos de los clientes,

previniendo el fraude financiero (Vijayagopal et al., 2024). Estas regulaciones preventivas se complementan con requisitos estrictos de verificación de identidad (KYC) que ayudan a reducir el riesgo de actividades fraudulentas.

Sandbox con supervisión continua (Canadá): El sistema de sandbox regulatorio canadiense proporciona a las empresas un entorno favorable pero con supervisión constante de las autoridades reguladoras, asegurando que las innovaciones sean probadas bajo vigilancia para garantizar la protección del consumidor (Kalai & Toukabri, 2024). Este enfoque constante pero no intrusivo permite mantener altos estándares de seguridad sin obstaculizar la innovación.

El panorama americano muestra una evolución hacia sistemas más sofisticados de protección y seguridad, con Estados Unidos priorizando un enfoque basado en reglas específicas y supervisión sectorial y Canadá optando por un sistema más integrado con supervisión continua.

Latinoamérica

La implementación de tecnologías financieras en América Latina ha venido acompañada de diversos mecanismos para salvaguardar la integridad del sistema financiero y proteger a los usuarios. Estas prácticas varían entre jurisdicciones, pero es posible identificar tendencias regionales que constituyen puntos de referencia para el desarrollo de un ecosistema Fintech seguro y confiable. Más allá de los marcos regulatorios formales, estas mejores prácticas representan estándares operativos que equilibran la innovación con la adecuada protección del consumidor financiero y la estabilidad sistémica. A continuación, se describen las principales prácticas:

Requisitos de Capital y Garantías para Plataformas Fintech: Una práctica extendida en la región es el establecimiento de requisitos patrimoniales mínimos para empresas Fintech,

particularmente para aquellas que manejan fondos de terceros. En Brasil, las compañías de crédito directo (SCD) y las compañías de préstamos P2P (SEP) deben mantener un capital mínimo de BRL 1 millón, mientras que los requisitos aumentan para entidades que ofrecen servicios de pago (Teixeira & Figueiredo, 2024). En Perú, existen requerimientos similares para las sociedades administradoras de plataformas de financiamiento participativo financiero (Alcázar & Orbezo, 2024). Esta exigencia busca asegurar la solvencia de las empresas y minimizar riesgos para los usuarios.

Segregación de Fondos de Clientes: La separación estricta entre fondos propios de las plataformas Fintech y los recursos de los usuarios representa una práctica esencial adoptada por varios países. En Brasil, los fondos mantenidos en cuentas de pago están legalmente segregados de los activos de las instituciones de pago, lo que significa que no son responsables directas de las deudas de la entidad y no pueden ser embargados por acreedores, incluso en casos de quiebra (Teixeira & Figueiredo, 2024). Medidas similares se observan en México y Argentina, garantizando que, ante insolvencia de la plataforma, los fondos de los usuarios permanezcan protegidos (López & Melgar, 2024; Riofrio & Almeida, 2024).

Debida Diligencia sobre Proyectos e Inversores: Las plataformas de financiamiento colectivo en varios países deben implementar procesos de debida diligencia sobre los proyectos e inversores. En Uruguay, las plataformas de crowdequity deben verificar la existencia legal, viabilidad financiera e historial de negocios de los proyectos antes de permitir su publicación (Mailhos & Mercado, 2024). En Chile y Perú existen disposiciones similares, exigiendo a las plataformas implementar metodologías para evaluar y determinar el grado de riesgo de sus posibles solicitantes (Noriega et al., 2024; Alcázar & Orbezo, 2024). Esta práctica proporciona mayor transparencia y reduce riesgos de fraude.

Límites de Inversión y Exposición: Para proteger a inversores minoristas y prevenir concentraciones excesivas de riesgo, varios países han establecido límites de inversión en plataformas Fintech. México implementa un sistema de clasificación de inversores (institucionales, calificados, no calificados) con límites proporcionales a su nivel de sofisticación (López & Melgar, 2024). En Perú, existen límites específicos según el tipo de inversión y perfil del inversor (Alcázar & Orbezo, 2024). Uruguay establece topes de inversión por proyecto y por plataforma, con excepciones para inversores institucionales (Mailhos & Mercado, 2024). Estas restricciones previenen pérdidas excesivas para pequeños inversores mientras permiten mayor participación a actores más sofisticados.

Gestión de Riesgos Tecnológicos y Ciberseguridad: América Latina está desarrollando regulaciones de protección de datos inspiradas en el GDPR europeo, adaptándolas a las realidades regionales (Zreik & Iqbal, 2024). Estas iniciativas incluyen implementación de medidas de ciberseguridad específicamente diseñadas para abordar amenazas regionales, requisitos de transparencia para empresas fintech, y colaboración regional para combatir el fraude financiero transfronterizo (Zreik & Iqbal, 2024). En Perú, la Superintendencia de Banca, Seguros y AFP ha emitido el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aplicable a entidades supervisadas (Alcázar & Orbezo, 2024). Brasil exige que los proveedores de servicios de pago mantengan programas de ciberseguridad y sistemas de respuesta a incidentes (Teixeira & Figueiredo, 2024). Estas medidas buscan prevenir vulneraciones de datos y ataques informáticos que podrían comprometer tanto la estabilidad de las plataformas como la información de los usuarios.

Transparencia e Información al Usuario: La obligación de proporcionar información clara y suficiente sobre riesgos, costos y características de los servicios financieros representa una

práctica ampliamente adoptada. México exige que los proveedores de servicios de activos virtuales informen a los clientes que estos no son moneda de curso legal ni están respaldados por el gobierno (López & Melgar, 2024). En Argentina, las plataformas deben advertir los riesgos tecnológicos, cibernéticos y de fraude inherentes a las operaciones (Riofrio & Almeida, 2024). Esta transparencia empodera a los usuarios para tomar decisiones informadas sobre los productos y servicios financieros que utilizan.

Interoperabilidad de Sistemas de Pago: La promoción de interoperabilidad entre diferentes sistemas de pago representa una práctica emergente en la región. Brasil ha sido pionero con su sistema de pagos instantáneos Pix, que facilita transferencias entre diferentes instituciones financieras (Teixeira & Figueiredo, 2024). Perú ha establecido requerimientos de interoperabilidad para las empresas emisoras de dinero electrónico (Alcázar & Orbezo, 2024). Estas iniciativas fomentan la inclusión financiera y reducen costos transaccionales, permitiendo mayor competencia y beneficiando a los usuarios finales.

Protección de Datos Personales: La implementación de políticas robustas de protección de datos personales constituye una práctica esencial. Las plataformas Fintech en México deben cumplir con la Ley Federal de Protección de Datos Personales, estableciendo medidas técnicas, físicas y administrativas para salvaguardar la información (López & Melgar, 2024). En Perú, las entidades que operan en el ecosistema Fintech deben observar la Ley de Protección de Datos Personales y su reglamento (Alcázar & Orbezo, 2024). Estas medidas garantizan el adecuado tratamiento de información sensible y previenen usos no autorizados.

Prevención de Lavado de Activos y Financiamiento del Terrorismo: Los requisitos de cumplimiento en materia de prevención de lavado de activos y financiamiento del terrorismo (PLAFT) representan una constante en la región. Entidades como proveedores de servicios de

activos virtuales en Perú deben registrarse ante la Unidad de Inteligencia Financiera y cumplir con normas específicas (Alcázar & Orbezo, 2024). En Uruguay, las plataformas de financiamiento participativo financiero están sujetas a normativas de prevención de LA/FT (Mailhos & Mercado, 2024). Estas disposiciones buscan prevenir el uso de nuevas tecnologías financieras para actividades ilícitas, alineando la innovación con estándares internacionales de integridad financiera.

Las mejores prácticas identificadas en materia de protección y seguridad en el ecosistema Fintech latinoamericano reflejan un esfuerzo progresivo por equilibrar la promoción de la innovación con la adecuada gestión de riesgos. Si bien estas prácticas se implementan con diferentes niveles de sofisticación según la madurez del marco regulatorio de cada país, representan en conjunto una hoja de ruta para el desarrollo seguro del sector. A medida que el ecosistema Fintech continúa evolucionando en la región, es previsible que estas prácticas se refuercen y estandaricen, consolidando un entorno que fomente simultáneamente la innovación, la inclusión financiera y la protección de los usuarios.

Asia

La región asiática ha desarrollado enfoques distintivos para la protección y seguridad en el sector fintech, con variaciones significativas entre sus principales economías. A continuación, se describen las principales prácticas:

Control de flujos de datos con anonimidad controlada (China): China ha implementado un modelo único de "anonimato controlable" en su moneda digital del banco central (e-CNY). Este sistema permite que las partes permanezcan anónimas para el público mientras el Banco Popular de China puede rastrear transacciones para combatir actividades ilícitas (Hutukka, 2024). Esta

aproximación equilibra cierto nivel de privacidad para los usuarios con capacidades de supervisión robustas para las autoridades.

Protección estricta de datos personales: La Ley de Protección de Información Personal (PIPL) y la Ley de Seguridad de Datos (DSL) de China establecen un marco integral para la gestión de datos personales y la seguridad informática. Estas regulaciones limitan la capacidad del sector privado para utilizar datos personales y establecen requisitos estrictos para su procesamiento, aunque con menos restricciones para entidades gubernamentales (Hutukka, 2024).

Licencias específicas para servicios de pago: China ha implementado un sistema de licencias de servicios de pago para proveedores no financieros, estableciendo un control regulatorio específico para este segmento del mercado fintech (Hutukka, 2024). Este requisito asegura que incluso las plataformas no bancarias cumplan con estándares mínimos de seguridad y protección al consumidor cuando ofrecen servicios de pago digital.

Marco proactivo de ciberseguridad (Singapur): Singapur ha establecido un marco proactivo para la ciberseguridad a través de la Autoridad Monetaria de Singapur (MAS), con directrices claras sobre protección de datos de clientes y prácticas de seguridad (Zreik & Iqbal, 2024). Estos estándares incluyen requisitos específicos para la gestión de incidentes, evaluaciones de vulnerabilidad y protección de infraestructuras críticas financieras.

Verificación robusta y diligencia debida: En Singapur, los requisitos rigurosos de KYC y diligencia debida establecen procesos exhaustivos de validación de identidad y evaluación de riesgos (Zreik & Iqbal, 2024). Estos procedimientos están diseñados específicamente para detectar y prevenir fraudes financieros en un entorno digital, adaptándose a los riesgos particulares del ecosistema fintech de la región.

Seguridad reforzada para intercambios de criptomonedas (Japón): Tras varios incidentes graves de hackeo, Japón ha implementado requisitos estrictos de seguridad para intercambios de criptomonedas (Zreik & Iqbal, 2024). Estos incluyen la segregación obligatoria de fondos de clientes, mantenimiento de reservas, evaluaciones periódicas de seguridad y protocolos detallados para gestión de brechas de seguridad (Chen, 2022).

Autorregulación con supervisión oficial: Un aspecto distintivo del enfoque japonés es el papel significativo que continúan desempeñando las asociaciones industriales incluso después de la implementación de regulaciones formales. Los solicitantes de licencias para operar intercambios de criptomonedas deben ser nominados por la asociación industrial, creando un filtro adicional que complementa la supervisión gubernamental (Chen, 2022).

Asociaciones estratégicas público-privadas: En varios países asiáticos, incluyendo Singapur y Hong Kong, se han establecido colaboraciones estratégicas entre entidades gubernamentales y el sector privado para mejorar la detección y respuesta a amenazas de seguridad. Estos esfuerzos incluyen ejercicios conjuntos de simulación de ciberataques, compartición de inteligencia sobre amenazas y desarrollo colaborativo de estándares de seguridad (Zreik & Iqbal, 2024).

El enfoque asiático para la protección y seguridad en fintech se caracteriza por un fuerte control gubernamental sobre los datos y flujos financieros, complementado con mecanismos de autorregulación industrial y colaboración público-privada. Esta combinación refleja tanto las prioridades culturales y políticas de la región como la respuesta pragmática a amenazas específicas que han afectado a sus mercados financieros digitales.

Oceanía

La región de Oceanía, principalmente representada por Australia en la investigación sobre fintech, ha desarrollado un conjunto distintivo de prácticas de protección y seguridad que complementan su marco regulatorio basado en principios. A continuación, se describen las principales prácticas:

Notificación obligatoria de violaciones de datos: Australia ha implementado un sistema de notificación obligatoria de violaciones de datos que requiere que las empresas fintech informen a los usuarios y reguladores cuando se producen brechas de seguridad significativas (Zreik & Iqbal, 2024). Esta práctica fomenta la transparencia y permite una respuesta rápida para mitigar posibles daños, además de incentivar mejores medidas preventivas de seguridad.

Consentimiento estructurado y detallado: Las prácticas australianas de protección de privacidad ponen énfasis en directrices claras sobre el consentimiento del consumidor, requiriendo que las fintech obtengan aprobación explícita para la recopilación y uso de datos (Zreik & Iqbal, 2024). Este sistema va más allá de la mera conformidad legal, promoviendo un enfoque sustantivo que asegura que los consumidores comprendan realmente cómo se utilizará su información.

Evaluaciones regulares de vulnerabilidad: Un elemento destacado del enfoque australiano es la implementación de evaluaciones periódicas de vulnerabilidad y cumplimiento (Zreik & Iqbal, 2024). Estas revisiones sistemáticas buscan identificar proactivamente posibles fallos de seguridad antes de que puedan ser explotados, creando un ciclo de mejora continua en la protección de datos y sistemas.

APIs seguras para banca abierta: La política de banca abierta desarrollada por la Comisión Australiana de Competencia y Consumidores (ACCC) requiere que los bancos principales compartan datos de clientes a través de interfaces de programación de aplicaciones (APIs) seguras

con proveedores externos autorizados (Chaturvedi & Sinha, 2024). La implementación de estas APIs incluye salvaguardas técnicas robustas como encriptación avanzada, control de acceso basado en roles y autenticación multifactor.

Transparencia en la recopilación y uso de datos: Las prácticas australianas enfatizan la obtención del "consentimiento del cliente" para utilizar múltiples fuentes de datos, comunicando claramente las fuentes de información, los métodos analíticos empleados, los detalles que se intentan identificar y el propósito del uso de los datos analizados (Mahalle et al., 2021). Esta transparencia permite a los usuarios tomar decisiones informadas sobre compartir sus datos.

Restricciones para transferencias internacionales: Australia ha implementado controles específicos para transferencias de fondos internacionales, incluyendo restricciones para transferencias a países bajo sanciones y medidas para prevenir la transferencia de divisas a paraísos fiscales (Mahalle et al., 2021). Estos controles ayudan a mitigar riesgos relacionados con el lavado de dinero y financiamiento ilícito.

Mecanismos estructurados de resolución de quejas: Un componente importante del enfoque australiano es el establecimiento de plataformas dedicadas y personal especializado para manejar las quejas de los clientes, con marcos de tiempo específicos (acuerdos de nivel de servicio) para la resolución de problemas (Mahalle et al., 2021). Estos mecanismos formales aseguran que los usuarios tengan acceso a vías efectivas para resolver disputas y problemas de seguridad.

El enfoque de Oceanía, principalmente a través de las prácticas australianas, se distingue por su énfasis en la transparencia, evaluación continua de riesgos y mecanismos estructurados de protección al consumidor. Estas prácticas reflejan un equilibrio entre promover la innovación financiera y establecer salvaguardas efectivas para proteger a los usuarios y mantener la confianza en el sistema financiero digital.

Síntesis comparativa de regiones

La tabla 2 ofrece una visión panorámica de las mejores prácticas en materia de protección, seguridad y privacidad implementadas en los ecosistemas fintech globales. El análisis aborda aspectos cruciales como consentimiento y transparencia, derechos de usuarios, autenticación y protección de datos, entre otros, permitiendo identificar diferentes aproximaciones regionales para salvaguardar la integridad del sistema financiero y proteger a los usuarios de servicios fintech, considerando las particularidades culturales, tecnológicas y socioeconómicas de cada región.

Tabla 2

Comparación de Mejores Prácticas de Protección de Seguridad y Privacidad por Regiones

Característica	Europa	América del nort	Asia	Oceanía	América Latina
Consentimiento y transparencia	Consentimiento explícito, específico e informado (GDPR)	Enfoque basado en divulgación de políticas de privacidad	Comunicación clara de propósitos, especialmente en Singapur	Consentimiento estructurado y detallado sobre uso de datos	Enfoque en transparencia informativa sobre riesgos y condiciones, con obligaciones de divulgación detallada
Derechos del usuario	Amplio espectro: acceso, rectificación, eliminación, portabilidad	Variables según leyes estatales/federales en EE.UU.	Limitados en China, más amplios en Singapur y Japón	Enfoque en accesibilidad y comprensibilidad	Heterogéneos según país, con mayor desarrollo en México, Brasil y Chile, incluyendo acceso, rectificación y cancelación
Autenticación	Autenticación reforzada (SCA) con múltiples factores bajo PSD2	Verificación robusta de identidad y monitoreo de transacciones	Sistemas avanzados en Singapur, verificación biométrica en China	Combinación de factores adaptada al contexto	Multifactor en desarrollo, con énfasis creciente en biometría y verificación digital de identidad
Protección de datos	Evaluaciones de impacto preventivas para tecnologías de alto riesgo	Protecciones sectoriales específicas (EE.UU.), sistema integrado (Canadá)	Control estricto gubernamental (China), marco proactivo (Singapur)	Notificación obligatoria de violaciones de datos	Segregación obligatoria de fondos de clientes, con segmentación entre activos propios y de usuarios
Supervisión	Autoridades independientes con poderes reales en cada Estado miembro	Supervisión multicapa (EE.UU.), sistema centralizado (Canadá)	Supervisión gubernamental directa con autorregulación complementaria	Evaluaciones regulares de vulnerabilidad y cumplimiento	Predominio de reguladores financieros tradicionales con iniciativas de hubs de innovación financiera
Banca abierta/APIs	APIs estandarizadas y seguras bajo PSD2	En desarrollo, variable por jurisdicción	Desarrollo avanzado en Singapur, controlado en China	APIs seguras con salvaguardas técnicas robustas	Avanzado en Brasil (Open Finance), en desarrollo en México, Perú y Uruguay, con orientación a interoperabilidad

Gestión de incidentes	Notificación obligatoria de violaciones y planes de respuesta detallados	Protocolos de respuesta sectorial, requerimientos de divulgación	Protocolos estrictos en Japón y Singapur	Sistema formal de notificación con plazos definidos	Requisitos de reporte a reguladores financieros, con protocolos específicos para entidades supervisadas
Criptomonedas	Protecciones específicas bajo MiCA	Variables por estado (EE.UU.), seguridad estricta (Canadá)	Prohibidas (China), alta seguridad (Japón)	Medidas similares a productos financieros tradicionales	Altamente variadas: adopción legal (El Salvador), requisitos PLAFT (Perú, Uruguay), advertencias sobre riesgos (México)
Educación y empoderamiento	Programas extensivos de alfabetización digital financiera	Enfoque en divulgación de riesgos (EE.UU./Canadá)	Programas gubernamentales (Singapur), limitados (China)	Campañas regulares de educación al consumidor	Obligaciones de información sobre riesgos y advertencias en plataformas, con énfasis en inclusión financiera
Transferencias internacionales	Marco formal para transferencias con protecciones equivalentes	Control exhaustivo de transacciones transfronterizas	Restricciones significativas, especialmente desde China	Controles específicos para países de alto riesgo	Enfoque en prevención de lavado de activos y financiamiento del terrorismo con estándares GAFI
Innovaciones específicas	Privacidad por diseño como principio técnico y organizativo	Análisis avanzado de comportamiento de usuarios	Sistema de "anonimato controlable" en e-CNY de China	Divulgación clara de términos y condiciones	Establecimiento de límites de inversión progresivos según perfil de inversor y sistemas de pagos instantáneos (Brasil)

Nota. Elaboración propia a partir de la revisión realizada.

El panorama global de prácticas de protección y seguridad en fintech evidencia diferentes filosofías regulatorias y prioridades regionales. Europa ha consolidado un enfoque centrado en amplios derechos digitales bajo el GDPR, mientras Norteamérica presenta un sistema más fragmentado con énfasis en la divulgación de riesgos. Asia exhibe contrastes entre el modelo de control estatal directo de China y aproximaciones más flexibles en Singapur y Japón. Por su parte, Oceanía destaca por su sistema formal estructurado con foco en la notificación de incidentes. América Latina implementa prácticas pragmáticas como segregación de fondos, límites de exposición y transparencia informativa. Esta diversidad de aproximaciones evidencia que las prácticas de protección y seguridad responden a realidades socioeconómicas, infraestructuras tecnológicas y marcos jurídicos particulares de cada región, aunque con tendencias convergentes hacia la autenticación multifactor, la gestión estructurada de incidentes y los requerimientos de transparencia, adaptados a diferentes contextos de desarrollo fintech.

Capítulo 5. Recomendaciones para el fortalecimiento normativo en Colombia

El análisis del panorama regulatorio internacional y su contraste con la situación colombiana permiten proponer un conjunto de recomendaciones para fortalecer el marco normativo nacional en materia de protección de seguridad y privacidad de usuarios fintech. Colombia ha avanzado significativamente en la regulación sectorial, pero aún requiere un enfoque más integral y adaptado a las realidades tecnológicas emergentes.

Desarrollo de un marco jurídico específico y consolidado

Colombia necesita avanzar hacia la creación de un marco jurídico unificado para las fintech, siguiendo ejemplos como México y Chile que han desarrollado leyes integrales. Este marco debería consolidar las diversas normativas sectoriales existentes en un cuerpo legal cohesivo que abordó específicamente las particularidades de los servicios financieros digitales y establezca claramente las responsabilidades y derechos de todos los actores del ecosistema. La fragmentación normativa actual genera incertidumbre tanto para empresas como para usuarios, dificultando el desarrollo del sector y la efectiva protección de los derechos. Un marco unificado facilitaría la interpretación y aplicación de las normas, proporcionando mayor seguridad jurídica y previsibilidad para todos los participantes del ecosistema fintech.

Fortalecimiento y clarificación de competencias supervisoras

Es imperativo establecer una delimitación clara de competencias entre la Superintendencia Financiera y la Superintendencia de Industria y Comercio, evitando vacíos y superposiciones en la supervisión de las fintech. Podría implementarse un modelo de supervisión coordinada con protocolos específicos de colaboración entre ambas entidades, o alternativamente, valorar la

creación de una unidad especializada en fintech dentro de la SFC, con personal técnico cualificado en tecnologías financieras emergentes. Esta especialización supervisora debe complementarse con mecanismos efectivos de coordinación internacional, particularmente relevantes dada la naturaleza transfronteriza de muchos servicios fintech. Colombia podría beneficiarse de acuerdos de cooperación con autoridades supervisoras de referencia como la FCA británica o la MAS singapurense.

Desarrollo normativo para tecnologías emergentes

El marco regulatorio actual muestra limitaciones significativas respecto a tecnologías emergentes como inteligencia artificial, blockchain o contratos inteligentes. Es necesario desarrollar regulaciones específicas que aborden los riesgos y oportunidades de estas tecnologías, considerando experiencias internacionales como la regulación japonesa sobre criptoactivos o el enfoque europeo hacia la IA. Este desarrollo debe seguir un enfoque de neutralidad tecnológica y basado en principios, que permita la flexibilidad necesaria para adaptarse a la evolución constante de estas tecnologías sin necesidad de reformas continuas. Los principios rectores deberían incluir la transparencia algorítmica, la transparencia algorítmica de decisiones automatizadas y la responsabilidad por los resultados de sistemas autónomos.

Fortalecimiento de la protección de datos específica para fintech

Aunque Colombia cuenta con un marco general de protección de datos, es necesario desarrollar normativas específicas para el contexto fintech que aborden cuestiones como la portabilidad de datos financieros, el uso de datos alternativos para evaluaciones crediticias y la transferencia internacional de información financiera. La experiencia europea con el GDPR ofrece lecciones valiosas, particularmente en aspectos como el consentimiento explícito, los derechos de

acceso y rectificación, y la evaluación de impacto para tecnologías de alto riesgo. Colombia podría adaptar estos principios a su contexto particular, considerando las particularidades del ecosistema fintech nacional y los desafíos específicos de inclusión financiera.

Ampliación y fortalecimiento del sandbox regulatorio

El sandbox regulatorio colombiano, aunque ha representado un avance significativo, presenta limitaciones en términos de alcance y duración. Es recomendable ampliar su capacidad, flexibilizar los criterios de ingreso para startups innovadoras y establecer mecanismos claros para la transición desde la fase experimental hacia la operación regular bajo marcos normativos adaptados. Esta ampliación debería complementarse con la creación de un hub de innovación fintech, siguiendo ejemplos como Estonia o el Reino Unido, que sirva como punto de contacto permanente entre reguladores y empresas, facilitando la orientación regulatoria continua y la retroalimentación sobre desafíos emergentes.

Regulación proporcional basada en riesgos

El principio de proporcionalidad debe guiar el desarrollo regulatorio, estableciendo requisitos diferenciados según el tipo de servicio, volumen de operaciones y riesgos específicos de cada modelo de negocio fintech. Este enfoque evitaría imponer cargas excesivas a startups innovadoras mientras mantiene controles robustos sobre actividades de mayor riesgo. Este modelo podría implementarse mediante un sistema escalonado de licencias o autorizaciones, con requisitos regulatorios que aumenten proporcionalmente con la complejidad y riesgo de las actividades desarrolladas, siguiendo ejemplos como el sistema de licencias escalonadas de Singapur o el enfoque basado en actividades de Reino Unido.

Mecanismos ágiles de resolución de disputas

Es fundamental desarrollar procedimientos específicos y expeditos para la resolución de controversias en el entorno fintech. Los mecanismos tradicionales de defensoría del consumidor financiero podrían complementarse con sistemas digitales de resolución de disputas que aprovechen la tecnología para ofrecer soluciones rápidas y accesibles. Estos sistemas podrían incluir plataformas en línea para la presentación y seguimiento de reclamaciones, procedimientos simplificados para controversias de baja cuantía y mecanismos de mediación digital que faciliten acuerdos sin necesidad de procedimientos judiciales formales, siguiendo modelos como el sistema canadiense de resolución de disputas financieras en línea.

Fortalecimiento de la educación financiera digital

La alfabetización financiera digital constituye un componente esencial de la protección al usuario fintech. Es necesario desarrollar programas específicos que aborden los desafíos particulares de los servicios financieros digitales, incluyendo la evaluación de riesgos, la protección de datos personales y la identificación de señales de fraude. Estos programas deberían implementarse mediante alianzas público-privadas que involucren a entidades educativas, asociaciones fintech y reguladores, aprovechando las capacidades tecnológicas para llegar a diversos segmentos de la población con contenidos adaptados a sus necesidades específicas.

Desarrollo de estándares técnicos de seguridad específicos

Colombia debería establecer estándares mínimos de seguridad informática específicos para el sector fintech, abordando aspectos como autenticación reforzada, cifrado de datos, gestión de

incidentes y continuidad operativa. Estos estándares deberían alinearse con mejores prácticas internacionales mientras se adaptan a las particularidades del contexto colombiano. La adopción de estos estándares podría incentivarse mediante esquemas de certificación reconocidos que proporcionen ventajas competitivas a las empresas que demuestren altos niveles de seguridad, siguiendo modelos como el sistema de certificación de ciberseguridad de Singapur o los sellos de confianza digital europeos.

Implementación integral de finanzas abiertas (Open Finance)

Si bien Colombia ha dado pasos importantes hacia las finanzas abiertas con el Decreto 1297 de 2022 y la reciente Circular Externa 004 de 2024, es necesario desarrollar un marco más completo que establezca estándares técnicos detallados, protocolos de seguridad robustos y mecanismos de supervisión efectivos para la implementación de API abiertas en el sistema financiero. Este marco debería abordar aspectos como la estandarización de formatos de datos, los requisitos técnicos para las interfaces, los mecanismos de autenticación y los procedimientos para la gestión de consentimientos, tomando como referencia experiencias avanzadas como el sistema brasileño de Open Finance o el régimen británico de Open Banking.

Hacia un modelo de co-gobernanza público-privada

Colombia debería avanzar hacia un modelo de co-gobernanza que involucre activamente a representantes de la industria, académicos, defensores de consumidores y reguladores en el desarrollo y evaluación continua del marco normativo fintech. Este enfoque colaborativo permitiría aprovechar el conocimiento especializado del sector privado mientras mantiene el enfoque en el interés público y la protección del consumidor. Este modelo podría implementarse

mediante comités consultivos formales, foros regulares de diálogo y mecanismos transparentes para la retroalimentación sobre propuestas normativas, siguiendo ejemplos exitosos como la colaboración entre asociaciones industriales y reguladores en Japón o el modelo de consulta abierta del Reino Unido.

La implementación efectiva de estas recomendaciones requeriría un esfuerzo coordinado entre diversas entidades gubernamentales, el sector privado y la sociedad civil. El resultado sería un ecosistema fintech más robusto, innovador y seguro, que contribuya efectivamente a la inclusión financiera y el desarrollo económico del país, mientras garantiza la adecuada protección de los derechos fundamentales de los usuarios.

Conclusiones

El análisis del marco jurídico colombiano en materia de protección a usuarios fintech revela un panorama caracterizado por la fragmentación normativa. A pesar de contar con regulaciones aplicables desde el nivel constitucional hasta circulares específicas, Colombia carece de un marco legal integral y especializado para las fintech. Esta situación genera incertidumbre sobre el alcance y la efectividad de la protección de los derechos de los usuarios, especialmente en lo relacionado con la seguridad y privacidad de su información. Las normativas existentes presentan limitaciones significativas para abordar las particularidades de las tecnologías emergentes, como inteligencia artificial, blockchain y contratos inteligentes, que son fundamentales para el desarrollo del sector.

El estudio de las implicaciones jurídicas de las tecnologías emergentes utilizadas por las fintech demuestra que innovaciones como open finance, computación en la nube, inteligencia artificial y biometría plantean desafíos regulatorios específicos. Si bien existen avances como la Circular Externa 005 de 2019 sobre computación en la nube o la Circular Externa 029 de 2019 sobre biometría, persisten vacíos normativos significativos. Estos vacíos son particularmente evidentes en áreas como la regulación de algoritmos de decisión automatizada, la transparencia en el uso de datos alternativos y la atribución de responsabilidad ante fallos tecnológicos. La adopción de tecnologías impulsoras del sector fintech colombiano requiere un marco normativo que equilibre la innovación con la protección efectiva de los usuarios.

En materia de responsabilidad civil de las empresas fintech ante incidentes de seguridad, se identificó que Colombia ha evolucionado hacia un régimen de responsabilidad objetivada, especialmente para operaciones electrónicas. Sin embargo, la aplicación práctica de estos principios enfrenta dificultades debido a la complejidad técnica de los servicios financieros digitales y la multiplicidad de actores involucrados en la cadena de valor. Los mecanismos

existentes para la determinación de responsabilidades y el resarcimiento a usuarios afectados resultan insuficientes ante la sofisticación de las amenazas digitales. Es necesario complementar el marco actual con procedimientos específicos, como soluciones de SmartSettle para pequeñas reclamaciones y sistemas de seguros especializados que no trasladen costos adicionales a los usuarios.

El análisis comparado de experiencias regulatorias internacionales revela tendencias globales hacia modelos de gobernanza más ágiles, que incluyen sandboxes regulatorios, hubs de innovación y enfoques de co-gobernanza público-privada. Regiones como Europa, con su Reglamento General de Protección de Datos (GDPR), y países como Reino Unido, Singapur y México ofrecen referentes valiosos para Colombia. Particularmente relevantes son las prácticas de transparencia y consentimiento informado, autenticación reforzada, evaluaciones de impacto preventivas y mecanismos ágiles de resolución de disputas. La región latinoamericana muestra una evolución hacia marcos más comprensivos, destacando los modelos de regulación integral de México y Chile, así como el enfoque sectorial de Brasil.

A partir de estos hallazgos, se proponen recomendaciones concretas para el fortalecimiento normativo colombiano, incluyendo el desarrollo de un marco jurídico específico y consolidado para las fintech, la clarificación de competencias supervisoras, la regulación específica de tecnologías emergentes, el fortalecimiento de la protección de datos en el contexto fintech, la ampliación del sandbox regulatorio y la implementación de mecanismos ágiles de resolución de disputas. Estas propuestas buscan equilibrar la promoción de la innovación con la protección efectiva de los derechos de los usuarios, contribuyendo así a un ecosistema fintech más robusto, inclusivo y seguro para todos los participantes.

La presente investigación cumple su propósito de analizar comprehensivamente los desafíos jurídicos para la protección de la seguridad y privacidad de los usuarios fintech en Colombia, proporcionando una hoja de ruta para el fortalecimiento normativo basada en las mejores prácticas internacionales y adaptada a las particularidades del contexto colombiano. Este fortalecimiento resulta imprescindible para garantizar que la innovación financiera digital avance de manera sostenible, respetando los derechos fundamentales de los consumidores financieros y contribuyendo efectivamente a la inclusión financiera en el país.

Referencias

Akpukorji, I. S., Nzeako, G., & Akinsanya, M. O. (2024). Theoretical frameworks for regulatory compliance in Fintech innovation: A comparative analysis of Africa and the United States. *Finance & Accounting Research Journal*, *6*(5), 721-730. https://doi.org/10.51594/farj.v6i5.1107

Albarracín, C. G. (2023). *Las fintech en Colombia, desarrollo legislativo, vacíos jurídicos y retos del legislativo* [Artículo de Grado, Universidad Católica de Colombia]. https://repository.ucatolica.edu.co/entities/publication/a6d27b36-a04d-4f9d-a04e-1ee08aa26e72

Alcázar, R., & Orbezo, A. (2024). Perú. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 186-200). Lloreda Camacho & Co. https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

Alekseenko, A. P. (2022). Privacy, Data Protection, and Public Interest Considerations for Fintech. En H.-Y. Chen, P. Jenweeranon, & N. Alam (Eds.), *Global Perspectives in FinTech* (pp. 25-49). Springer International Publishing. https://doi.org/10.1007/978-3-031-11954-5_3

Alzate, R., & Vázquez, E. (2013). *Resolución de disputas en línea (RDL): Las claves de la mediación electrónica*. Editorial Reus.

Anaya, C. P. (2020). Protección del consumidor financiero en Colombia, en el uso de canales electrónicos bancarios. *Vniversitas*, *69*, 1-12. https://doi.org/10.11144/Javeriana.vj69.pcms

Arenas, J. (2019). *La Responsabilidad Civil Objetiva por la emisión y uso de tarjetas débito en Colombia* [Tesis de Maestría, Universidad Nacional de Colombia]. https://repositorio.unal.edu.co/handle/unal/77381

Arévalo, A., & Bichara, R. (2024). El Salvador. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 102-114). Lloreda Camacho & Co. https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

Arias, Y. J., & Lis, S. (2024). *Desafíos regulatorios, financieros y tecnológicos que enfrentan las fintech en el panorama financiero colombiano.* [Tesis de Especialización, Universidad EAN]. http://hdl.handle.net/10882/13979

Ariza, R. A. (2022). Nuevas perspectivas del uso de la tecnología en el ámbito del contrato de seguro. *Revista Ibero-Latinoamericana de seguros*, *31*(57), 15-47. https://doi.org/10.11144/Javeriana.ris57.nput

Banco de la República. (2021). *El Banco de la República participa en lanzamiento de primer piloto de un bono blockchain en Colombia | Banco de la República*. Banco de la República. https://www.banrep.gov.co/es/el-banco-republica-participa-lanzamiento-primer-piloto-bono-blockchain-colombia

Baquero, C. C., & Prieto, M. Y. (2019). *Activos financieros en Colombia respaldados con tecnología blockchain* [Tesis de Grado, Universidad Piloto de Colombia]. http://repository.unipiloto.edu.co/handle/20.500.12277/4850

Bermúdez, K. (2025, febrero 6). *¿En qué va la Inteligencia Artificial en Colombia?* Senado de la República. https://www.senado.gov.co/index.php/el-senado/noticias/6176-en-que-va-la-inteligencia-artificial-en-colombia

Biswas, R., Saha, P., Paul, G., & Saha, A. (2024). *Regulatory Outlook in Fintech: A Review*. *5*(6), 7100-7108.

Bongomin, G. O. C., & Ntayi, J. M. (2020). Mobile money adoption and usage and financial inclusion: Mediating effect of digital consumer protection. *Digital Policy, Regulation and Governance*, *22*(3), 157-176. https://doi.org/10.1108/DPRG-01-2019-0005

Bu, Y., Li, H., & Wu, X. (2022). Effective regulations of FinTech innovations: The case of China. *Economics of Innovation and New Technology*, *31*(8), 751-769. https://doi.org/10.1080/10438599.2020.1868069

Carvajal, C., & Garzón, S. (2024). Colombia. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 58-75). Lloreda Camacho & Co. https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

Castaño, D. (2021). Introducción. Del Derecho Análogo al Derecho para un Mundo Digital. En C. García, J. C. Henao, & D. Castaño (Eds.), *Derecho, innovación y tecnología: Fundamentos para una lex informática* (Primera edición, pp. 43-74). Universidad Externado de Colombia.

Chaturvedi, Dr. P., & Sinha, Prof. S. K. (2024). Regulation of Fintech Innovations through Policy Frameworks: Ensuring Consumer Protection Whilst Promoting Innovation. *BSSS Journal of Management*, *15*(1), 83-104. https://doi.org/10.51767/jm1506

Chen, H.-Y. (2022). Regulatory Innovation in FinTech. En H.-Y. Chen, P. Jenweeranon, & N. Alam (Eds.), *Global Perspectives in FinTech* (pp. 79-95). Springer International Publishing. https://doi.org/10.1007/978-3-031-11954-5_5

Chipana, J. (2019). Los smart-contracts y el arbitraje. Una introducción. *Cuadernos Jurídicos Lus et Tribunalis*, *05*(05), 85-91. https://doi.org/10.18259/iet.2019006

Colombia Fintech. (2024a). *Big Data y motores de decisiones, entre las tecnologías que continuarán revolucionando el sector financiero en el 2024*. Colombiafintech.

https://colombiafintech.co/lineaDeTiempo/articulo/-big-data-y-motores-de-decisiones-entre-las-tecnologias-que-continuaran-revolucionando-el-sector-financiero-en-el-2024

Colombia Fintech. (2024b). *Fintech Snapshot*. Asociación Colombiana de Empresas de Tecnología e Innovación Financiera.

CONPES. (2018). *CONPES 3920: Política Nacional de Explotación de Datos*. Departamento Nacional de Planeación.

Corte Suprema de Justicia. (2010). *Tutela. Magistrado Ponente. Arturo Solarte Rodriguez.* https://consultajurisprudencial.ramajudicial.gov.co/WebRelatoria/FileReferenceServlet?corp=csj&ext=pdf&file=363167

Cumming, D., Johan, S., & Reardon, R. (2023). Global fintech trends and their impact on international business: A review. *Multinational Business Review, 31*(3), 413-436. https://doi.org/10.1108/MBR-05-2023-0077

Dávila, C. A., & Monsalve, D. F. (2023). *La aplicación de los contratos legales inteligentes en el contrato de mutuo y su incidencia en el mercado Fintech en Colombia.* [Tesis de Grado, Universidad Colegio Mayor de Cundinamarca]. https://repositorio.unicolmayor.edu.co/handle/unicolmayor/6987

Díaz, R., Zabala, T. D., & Romero, H. A. (2024). Análisis del riesgo de mal manejo de bases de datos personales (caso Nequi). *Nuevos desafíos del Derecho, 4*(1), Article 1. https://doi.org/10.15765/fwq7bs19

Finnovista. (2024). *Fintech Radar Colombia. VII Edición*. Finnovista, Mastercard, Galileo. https://www.finnovista.com/wp-content/uploads/2024/05/RADAR-COLOMBIA-ESPANOL-3.pdf

Gaona, T., & Solano, D. (2021). Tratamiento de datos personales y aseguramiento de la responsabilidad derivada de la ocurrencia de amenazas digitales. En C. García, J. C. Henao, & D. Castaño (Eds.), *Derecho, innovación y tecnología: Fundamentos para una lex informática* (Primera edición, pp. 229-263). Universidad Externado de Colombia.

García, C., Ardón, O., Granados, S., & Cofiño, A. (2024). Guatemala. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 115-128). Lloreda Camacho & Co. https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

González, C. A. (2024). Protección del consumidor financiero: Nuevos caminos para la comprensión de los negocios financieros en Colombia. *Jurídicas CUC*, *20*(1), Article 1. https://doi.org/10.17981/juridcuc.20.1.2024.14

Gurrea, A., & Remolina, N. (2020). *Global Challenges and Regulatory Strategies to Fintech* (SSRN Scholarly Paper No. 3576506). Social Science Research Network. https://doi.org/10.2139/ssrn.3576506

Gutiérrez, M., & Moreno, M. J. (2023). *Introducción a las Fintech: Alcance de su concepto y marco legal en Colombia* [Tesis de Grado, Universidad EAFIT]. http://hdl.handle.net/10784/32627

Guzmán, R. S. (2024). *El respaldo legal y financiero de los neo bancos en Colombia: Un análisis de la regulación de las Fintech y la protección para los usuarios* [Tesis de Maestría, Universidad Externado de Colombia]. https://bdigital.uexternado.edu.co/handle/001/16721

Hutukka, P. (2024). Fintech law in the European Union, the United States and China: Regulation of financial technology in comparative context. *Maastricht Journal of European and Comparative Law*, *31*(5), 559-594. https://doi.org/10.1177/1023263X241298416

Kalai, L., & Toukabri, M. (2024). Risks, Regulations, and Impacts of FinTech Adoption on Commercial Banks in the United States and Canada: A Comparative Analysis. *Thunderbird International Business Review*, *66*(6), 609-641. https://doi.org/10.1002/tie.22404

Londoño, C. C. (2024). *La atribución de la responsabilidad civil extracontractual por daños generados por el uso de sistemas de Inteligencia Artificial* [Tesis de Grado, Universidad Pontificia Bolivariana]. https://repository.upb.edu.co/handle/20.500.11912/11872

López, S., & Melgar, M. (2024). México. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 143-157). Lloreda Camacho & Co. https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

Luegmayer, S., & Ocampo, J. (2024). Argentina. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 6-24). Lloreda Camacho & Co. https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

Mahalle, A., Yong, J., & Tao, X. (2021). Regulatory Challenges and Mitigation for Account Services Offered by FinTech. *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 280-287. https://doi.org/10.1109/CSCWD49262.2021.9437631

Mailhos, J., & Mercado, M. (2024). Uruguay. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 201-216). Lloreda Camacho & Co.

https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

Ministerio de Hacienda y Crédito Púbico. (2019). *Misión del Mercado de Capitales*. Banco Mundial. https://documents1.worldbank.org/curated/en/998101621598113254/pdf/Informe-Final.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). *Borrador—Guía para el uso y la implementación de tecnología de registros distribuidos (DLT/Blockchain) en el sector público*. Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/715/articles-149959_recurso_1.pdf

Narváez, J. (2015). *El Contrato de Seguro en el Sector Financiero.* Editorial Ibáñez.

Noriega, F., Lasagna, D., & Domínguez, A. (2024). Chile. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 45-57). Lloreda Camacho & Co. https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

Nur, J. M. (2023). *Régimen de responsabilidad contractual a los intermediarios de valores por violación del deber asesoría frente al robo advisor* [Tesis de Maestría, Universidad Externado de Colombia]. https://bdigital.uexternado.edu.co/handle/001/14771

Padilla, J. A. (2020). Blockchain y contratos inteligentes: Aproximación a sus problemáticas y retos jurídicos. *Revista de Derecho Privado*, *39*, Article 39. https://doi.org/10.18601/01234366.n39.08

Palmerini, E. (2017). Robótica y derecho: Sugerencias, confluencias, evoluciones en el marco de una investigación europea. *Revista de Derecho Privado, 32*, Article 32. https://doi.org/10.18601/01234366.n32.03

Parra, M. F. (2010). *Responsabilidad civil* (Primera edición). Ediciones Doctrina y Ley.

Pastrana, M. (2024). Honduras. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 129-142). Lloreda Camacho & Co. https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

Pertuz, D. (2021). Revisión de la experiencia regulatoria en Colombia sobre las fintech y el desarrollo del sandbox regulatorio. *Misión Jurídica*, *14*(21), Article 21. https://doi.org/10.25058/1794600X.1955

Prayuti, Y. (2024). Evaluation of Legal and Policy Issues in Consumer Protection in Indonesian Fintech Transactions. *LEGAL BRIEF*, *13*(2), Article 2. https://doi.org/10.35335/legal.v13i2.985

Riofrio, C., & Almeida, N. (2024). Ecuador. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 88-101). Lloreda Camacho & Co. https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

Saavedra, M., & Saavedra, J. (2024). Paraguay. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 175-185). Lloreda Camacho & Co. https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

Shala, A., & Perri, R. (2022). Regulatory barriers for fintech companies in Central and Eastern Europe. *Eastern Journal of European Studies*, *13*(2), 292-316. https://doi.org/10.47743/ejes-2022-0214

Sosa, J., & Sanjur, A. (2024). Panamá. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 158-174). Lloreda Camacho & Co. https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

Superintendencia de Industria y Comercio. (2019). *Guía sobre el tratamiento de datos personales para fines de comercio electrónico*. Superintendencia de Industria y Comercio. https://www.sic.gov.co/content/gu%C3%ADa-sobre-el-tratamiento-de-datos-personales-para-fines-de-comercio-electr%C3%B3nico

Superintendencia Financiera de Colombia. (2014). *Circular Básica Jurídica (C.E. 029/14)*. Superfinanciera. https://www.superfinanciera.gov.co/publicaciones/10083443/normativanormativa-generalcircular-basica-juridica-ce-10083443/

Superintendencia Financiera de Colombia. (2021). *Concepto 2021095181-001. Billeteras electrónicas*. Superintendencia Financiera de Colombia.

Superintendencia Financiera de Colombia. (2024a). *Circular Externa 004 de 2024. Instrucciones relativas a las finanzas abiertas y comercialización de tecnología e infraestructura a terceros*. Superintendencia Financiera de Colombia. https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1069605

Superintendencia Financiera de Colombia. (2024b). *Guía externa para la supervisión de las entidades con enfoque digital*. Superintendencia Financiera de Colombia. https://www.superfinanciera.gov.co/publicaciones/10114248/nuestra-entidadmarco-integral-de-supervisionanexos-marco-integral-de-supervision-

10114248/#:~:text=Gu%C3%ADa%20externa%20para%20la%20supervisi%C3%B3n%20de%20las%20entidades%20con%20enfoque%20digital

Tamayo, J. (2018). *Tratado de responsabilidad civil* (Segunda edición ; corregida y aumentada). Legis.

Teixeira dos Santos, M., & Figueiredo, P. (2024). Brasil. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 26-44). Lloreda Camacho & Co. https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

Tribunal Superior del Distrito Judicial de Bogotá. (2006). *Magistrada ponente. Dra. Ana Lucia Pulgarín Delgado.*

Ureña, M., & Sandí, R. (2024). Costa Rica. En Lloreda Camacho & Co (Ed.), *Regulación Fintech en Latinoamérica* (pp. 76-87). Lloreda Camacho & Co. https://www.carey.cl/wp-content/uploads/2024/12/Latam-Fintech-Regulation-Latam-Spanish.pdf

Valderrama, J. (2025). *Consideraciones para la apreciación probatoria al contrato inteligente: Reflexiones en torno a la neutralidad tecnológica y reglas probatorias*. Ediciones Universidad Santo Tomás. https://repository.usta.edu.co/server/api/core/bitstreams/524edcd7-9e45-4dd4-b3fc-ca99fac7e54e/content

Vijayagopal, P., Jain, B., & Ayinippully Viswanathan, S. (2024). Regulations and Fintech: A Comparative Study of the Developed and Developing Countries. *Journal of Risk and Financial Management*, *17*(8), 324. https://doi.org/10.3390/jrfm17080324

Yadav, Y. (2020). Fintech and International Financial Regulation. *Vanderbilt Journal of Transnational Law*, *53*(3), 1109-1146.

Zabala, T. D. (2021). La ética en inteligencia artificial desde la perspectiva del derecho*. *Via Inveniendi Et Iudicandi*, *16*(2), 1-28.

Zabala, T., & Díaz, R. (2020). Lavado de Activos y Financiación del Terrorismo Vs. Desarrollo Económico de Colombia. *Verba luris*, *44*, 4-43. https://doi.org/10.18041/0121-3474/verbaiuris.44.6865

Zreik, M., & Iqbal, B. A. (2024). Navigating the Global Fintech Regulatory Landscape: Balancing Innovation and Protection. En M. S. M. Justin, R. Jalagat, K. Chandar, P. Aquino, & K. Sayari (Eds.), *Advances in Finance, Accounting, and Economics* (pp. 71-102). IGI Global. https://doi.org/10.4018/979-8-3693-3803-2.ch004