2022

LA REINVENCIÓN FINANCIERA EN LA ERA DIGITAL

DERECHO FINANCIERO

Asobancaria
Acerca la Banca a los Colombianos

ASOBANCARIA:

Presidente
Hernando José Gómez Restrepo

Vicepresidente Jurídico
José Manuel Gómez Sarmiento

Directora Jurídica Normativa
Adriana María Ovalle Herazo

Directora Jurídica Operacional
Ida María Mestre Ordóñez

EDICIÓN: **Mauricio Valenzuela Gruesso**

DISEÑO: **Julián Andrés Rojas Castañeda**

Primera Edición, Septiembre de 2022
ISBN:978-958-9040-85-0

CONTENIDO

PRÓLOGO

La transformación digital implica para la banca, entre otras varias cosas, recoger de forma asertiva los paradigmas culturales en torno al consumo de servicios financieros y, de manera primordial, a la creación pertinente de nuevas formas de servir a los clientes y usuarios a través de productos, servicios y canales que se centren en satisfacer sus reales necesidades financieras de manera eficiente, ágil, con interacciones sencillas, accesibles y seguras.

En efecto, la atención al consumidor financiero ha migrado a plazas digitales, en donde la seguridad y confianza continúan siendo pilares esenciales, ahora con un nuevo eje de desarrollo y sostenibilidad cimentado en la innovación digital. Esta realidad ha exigido nuevas regulaciones e interpretaciones sobre las mejores formas para que el sector financiero adopte las tecnologías emergentes como blockchain, inteligencia artificial, identidad digital, big data y servicios ciudadanos digitales, entre otras.

La Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria, consciente de la necesidad de actualización permanente, par y paso con el ritmo de los avances tecnológicos, tuvo la iniciativa de reunir a reconocidos expertos en los temas abordados en esta obra, quienes, a título de coautores, aceptaron sin vacilaciones esta invitación para compartir su notable conocimiento, con la expectativa de que el lector enriquezca su saber y pueda además contar con elementos que le permitan formarse un juicio sobre la importancia de la apropiación de este tipo de tecnologías.

Como resultado de este esfuerzo conjunto de Asobancaria y de la academia, se ha materializado esta obra que recoge formas posibles de sintonizar un canal eficiente entre el derecho y la tecnología, como un elemento indispensable para la necesaria y retadora transformación de la banca, y pone a disposición de abogados, estudiantes de derecho y otros profesionales amantes de la temática y ligados al sector un compendio de investigaciones, perspectivas, conocimientos y experiencias sobre asuntos particularmente relevantes en materia digital y de innovación relacionados directamente con la banca.

Acompasando los avances tecnológicos a nuestra forma de entender y hacer funcionar el mundo como un colectivo global, se pretende con este libro sumar un esfuerzo para documentar elementos de innovación y nuevas tecnologías en el derecho bancario. Así, teniendo en cuenta que el sector bancario interactúa con todos los sectores de la economía, permeando a la inmensa mayoría de la sociedad, y que es un intermediario por excelencia en los distintos ecosistemas y entornos en que se desenvuelve el mundo, la disrupción tecnológica debe absorberse adecuadamente por este sector y, por intermedio suyo, por la sociedad en la cual tiene injerencia, lo que implica, entre otras responsabilidades, el fortalecimiento de los programas de educación financiera para mitigar los riesgos propios de estos avances.

En efecto, alrededor de una tecnología determinada coexisten diversos grupos de interés, tanto tradicionales -clientes, usuarios, potenciales clientes, establecimientos de crédito, entidades reguladoras y de vigilancia y control, etc.-, como algunos nuevos -científicos de datos, gamificadores de experiencias, ingenieros del Internet of things -IoT-, entre otros-, que buscan conjuntamente nuevos escenarios económicos, en donde el derecho está llamado a ser el puente, no solo entre la tecnología y la sociedad, sino también entre los distintos actores que confluyen en los metaversos multipropósito.

Cerrando estas generales consideraciones acerca de algunas mínimas implicaciones de la evolución tecnológica, a continuación presentamos al lector un entremés de lo que podrá encontrar en esta obra. Al hacer *zoom* en los capítulos del libro, encontrará una base de la tecnología descentralizada para la banca, recordando que esta tecnología tuvo su primer gran auge en 2008, cuando, por cuenta de la crisis económica global, la escasez de dinero permitió la circulación exponencial de los primeros criptoactivos, aun cuando dichas tecnologías ya venían siendo usadas desde finales de los 90.

Los criptoactivos y las finanzas descentralizadas son conceptos que se apalancan en la eliminación de intermediarios dentro de una operación, conservando características de fidelidad de la información y agilidad en los procesos a partir de una o varias cadenas de bloques informáticos -blockchain-, lo que permite crear soluciones escalables y generar riqueza en un mercado digital. En el libro encontrará cómo estas tecnologías están siendo utilizadas por la banca para sus procesos internos y cómo los criptoactivos pueden ser considerados como parte de un patrimonio.

En línea con la aceptación de este tipo de instrumentos 100% digitales, el dinero circulante también se transa de forma digital a través de intermediarios tecnológicos especializados, que ejecutan pagos digitales, los cuales fortalecen la relación de los sectores financiero, productivo y económico. Su ecosistema permite la interacción fluida de distintos actores, así como la exigencia de estar a la vanguardia de la innovación; instrumentos como el *contactless*, QR, *e-wallet*, *biometric payment*, entre otros, son fruto de una constante evolución para cohesionar cada vez mejor distintas puntas de diferentes relaciones comerciales.

Como consecuencia de un conjunto de interacciones entre los distintos grupos de interés, se ha logrado recabar importantes volúmenes de datos, que existen como un activo derivado y cuyo subyacente es el negocio bancario en sí mismo. Estos datos son el principal insumo de diseño y entrenamiento para las inteligencias artificiales, que son empleadas para mejorar la percepción de los comportamientos financieros, propendiendo por tomar decisiones de mejor calidad y prospección de las que podrían ser tomadas por seres humanos, entre otras fortalezas. En este libro se profundizará en estas materias, especialmente las relacionadas con el mejoramiento de la calificación crediticia y el análisis de viabilidad financiera a partir de la inteligencia artificial y ciencias algorítmicas.

El eje central de los avances tecnológicos es mejorar la calidad de vida de la humanidad; por ello, es necesario hacer eficientes los mecanismos de control regulados por seres humanos. En efecto, allí las normas preventivas y correctivas juegan un rol trascendental, como en la protección del consumidor, pues los entornos digitales no pueden dejar desprovisto al consumidor de herramientas para corregir errores o asimetrías. Un reto relevante de este ítem es desafiar la tecnología para adaptarla a los derechos eminentemente humanos y al principio de trato justo que promueve y protege la regulación colombiana.

La identidad de las personas, como parte de los derechos humanos que han evolucionado en la era digital, ha tenido múltiples aristas de desarrollo. Hoy día tenemos identidades enmascaradas, múltiples identidades, con rasgos biométricos, con factores descentralizados, para propósitos bancarios, metaversos, de entretenimiento, laborales, entre otros. Estas identidades pueden estar compuestas de forma básica y rudimentaria por un correo o un número celular, así como también pueden estar basadas en avatares con identificación propia, nombre y personalidad. Así, la identidad digital para el sector financiero puede ser

una mixtura y estar acorde con el apetito de riesgo; por ello, se ahondará en estos aspectos de identidad digital.

Ahora bien, si el cliente de un servicio bancario es digital, ¿qué impide que la entidad financiera sea totalmente digital? Se abre entonces un nuevo espectro y es el de los neobancos o bancos digitales, que, desde entornos disruptivos, entran a competir por un mercado de hábitos de consumo digitales. ¿Podría ello considerarse una ventaja competitiva? o ¿son mercados cuya regulación es asimétrica?

La prestación de servicios financieros por medios no convencionales ha permitido la creación de oficinas y asesores virtuales, así como inteligencias artificiales que asesoran las mejores inversiones o dan el mejor consejo posible sobre un producto financiero. De esta forma, en muchas ocasiones un cliente que usa los canales digitales de una entidad financiera es atendido integralmente por *chatbots* que reciben órdenes de inteligencias artificiales, garantizando incluso una mejor atención y una mayor profundidad en los servicios suministrados respecto de lo que podría ofrecer una persona bajo los modelos tradicionales.

Las experiencias sensoriales han migrado a escenarios digitales; en la misma línea, los servicios y desarrollo de mercados se ejecutan en espacios virtuales diseñados para tal fin. Estos espacios, considerados como metaversos, condensan gran parte de la experiencia humana de forma virtual; sitios como *marketplaces*, centros culturales, bibliotecas, salones de café, cines, entre otros, ahora están disponibles en todo momento en un metaverso, junto con su correspondiente representación de la persona en ese mundo digital: su avatar, que permite disponer del dinero, encontrar inversiones, interactuar con sitios y otras personas: es un nuevo escenario de comportamientos económicos que requieren de una banca organizada y segura para la confianza en este nuevo entorno social y financiero. Cuestiones como ¿cuáles deberían ser las reglas de un banco en el metaverso? se empiezan a abordar en esta nueva realidad.

Esperamos que en este libro el lector encuentre un conjunto de posiciones que sirvan de aproximación hacia la arquitectura legal y la construcción de puentes entre la innovación tecnológica y los servicios financieros. Esta obra es una invitación a una forma de pensar *legaltech*, en la que abogados y facultades de derecho se conminan a entender una innovación social constante, basada en un mundo digital, donde es necesario repensar el derecho como aliado indispensable de la tecnología, que se acopla a su ritmo y entrega a la sociedad una nueva forma de entender y ejercer los derechos.

Para finalizar, debemos expresar un agradecimiento especial al doctor Mauricio Valenzuela Gruesso, por su invaluable colaboración en la coordinación y compilación de este libro, a la Asociación Bancaria y de Entidades Financieras de Colombia -Asobancaria- por su iniciativa y permanente interés y proactividad en torno a temas de interés relevante como los aquí tratados, y a cada uno de los coautores, quienes de forma decidida y generosa han plasmado sus conocimientos, buscando únicamente un beneficio académico, aportando definitivamente en dar claridad al papel de la banca como un intermediario alineado con los avances de la sociedad alrededor de la construcción de un mundo digital justo y equitativo.

Cristina Acelas García
Secretaría General del Banco Caja Social y Presidente del Comité Jurídico de Asobancaria

INTRODUCCIÓN

Los temas de este libro se organizan en torno a tres ejes: las finanzas descentralizadas como nuevo paradigma de la intermediación financiera, el negocio financiero basado en datos y la digitalización en el sector financiero. De esta forma, ofrece una visión integrada de aspectos críticos para dicho sector, tan estrechamente conectados entre ellos que las modificaciones de unos generan necesarias implicaciones en los otros: como fichas de lego o, para sintonizarnos con el lenguaje del libro, como nodos de una blockchain.

Los autores, de reconocida trayectoria y expertos en sus respectivos temas, se esforzaron por escribir en un lenguaje accesible, y en algunos pasajes en los que no fue posible despojarse del vocabulario técnico, procuraron ilustrar con explicaciones y definiciones, conscientes de que los temas tratados conciernen a las entidades financieras pero también resultan del mayor interés de los consumidores, pues impactan directamente su cotidianidad.

Así, Gerardo Hernández analiza la naturaleza y el impacto de los criptoactivos, al igual que la conveniencia de que los bancos centrales emitan monedas digitales. En favor de la decisión, menciona que una moneda digital constituye una alternativa al efectivo, propicia la inclusión financiera y puede utilizarse como un nuevo instrumento de política monetaria. Sin embargo, dependiendo del modelo que se adopte, la decisión tendría importantes efectos en el sector financiero y podría implicar una mayor participación del banco central en los sistemas de pagos; esto último no parece necesario si los objetivos que se persiguen con dicha decisión pueden alcanzarse con una adecuada regulación, sin distraer al banco central de su objetivo principal de preservar la estabilidad de precios. La emisión de una moneda digital requeriría, igualmente, de un mayor esfuerzo del banco central para introducir constantemente nuevas tecnologías y prácticas, algo en lo que el sector privado históricamente ha tenido una ventaja. El autor comenta algunas experiencias internacionales.

Nydia Remolina se ocupa de las finanzas descentralizadas -DeFi- que ofrecen, entre otros, servicios financieros, préstamos y seguros mediante el uso de blockchain y de activos digitales o criptoactivos. Las DeFi se estructuran tecnológicamente a través de aplicaciones descentralizadas -plataformas que se gobiernan sin intermediarios-, característica que las diferencia de las entidades financieras tradicionales que, por naturaleza, son centralizadas. Sin embargo, la autora desmitifica el concepto de descentralización absoluta. Reconoce que las DeFi pueden beneficiar la inclusión financiera y facilitar otras oportunidades para los consumidores, además de favorecer la automatización de ciertos productos financieros y ser un factor clave para el desarrollo de metaversos. Pero también generan desafíos asociados al lavado de activos y financiación del terrorismo, protección al consumidor, gobierno corporativo, transparencia y riesgos de ciberseguridad. Sin duda, las DeFI desafían las infraestructuras tradicionales del sector financiero, pero ¿desaparecerán las entidades financieras como las conocemos?

Dionisio Machuca relata el proceso de adopción del bitcoin como moneda de curso legal en El Salvador, adicional al dólar. El autor responde las preguntas de: ¿por qué ahora? ¿por qué en El Salvador? y ¿por qué bitcoin? Menciona algunos hechos que precedieron la decisión, en particular la experiencia de Bitcoin Beach, una playa en ese país en la que turistas extranjeros comenzaron a utilizar bitcoin hasta crear un ecosistema que inspiró la posterior

adopción oficial de la criptomoneda. Comenta los detalles del proceso, el corto tiempo que tuvieron los bancos y la población para prepararse, la entrega a los salvadoreños de una billetera electrónica oficial con el equivalente a US$30 en bitcoin, así como el mecanismo de convertibilidad. También se refiere a los beneficios de esta iniciativa en términos de inclusión financiera y a la aspiración de convertir al país en un centro para la actividad de proveedores y entusiastas de esa criptomoneda.

Juan Pablo García y Andrés Umaña unieron sus conocimientos para ilustrar un tema cada día más presente: la inteligencia artificial, que promete cambiar radicalmente la forma de operar el negocio financiero. En qué consiste la inteligencia artificial y cuál ha sido su desarrollo son aspectos que los autores abordan. Explican las distintas modalidades de IA y analizan cómo su implementación en el sector financiero conduce a mayores niveles de inclusión, al reducir costos operacionales por la utilización de *robo advisors*, generar ofertas personalizadas y mejorar el análisis de riesgo a través de metodologías como *machine learning*, que permite generar perfiles de riesgo a clientes sin historial de crédito. Los autores advierten sobre aspectos que deben atenderse a fin de evitar riesgos jurídicos relacionados con el manejo inadecuado de datos, bien sea por falta de autorización del titular o porque se trate de datos obtenidos a través del raspado de datos -*data scraping*- o por el riesgo de inferencia.

Los datos son un tema transversal en este libro. En su ensayo, Natalia Tovar explica qué es un score de crédito, cómo se calcula, cómo nació esta metodología, cuál es su propósito y cuáles los principios del tratamiento de la información. Asimismo, comenta cómo la construcción de *scores* ha contribuido a expandir el uso de las tarjetas de crédito y el consumo. Describe los grandes beneficios que se derivan de los *scores*, tanto para quienes otorgan crédito como para quienes lo reciben, porque permiten conocer con mayor detalle las preferencias de los consumidores y, por consiguiente, ampliar la oferta y diseñar productos más personalizados. A la par con estos beneficios, la autora analiza los desafíos jurídicos a que se enfrentan los *scores*, tales como su uso ético, la calidad de la información que se utiliza y el cuidado que debe tenerse para evitar ciertos datos que podrían conducir a resultados discriminatorios para algunos segmentos de la población.

Álvaro Montero analiza la actual tendencia a permitir la circulación de los datos de las personas, no solo entre entidades financieras y entre estas y sus aliados, sino también desde otras actividades económicas como telecomunicaciones, servicios públicos y comercio, e incluso del Estado hacia las instituciones financieras y las Fintech. Es lo que se conoce como *Open Banking*, *Open Data* y *Open Finance*. En esa dirección avanzan las regulaciones, algunas imponiendo como obligatoria la apertura de datos y otros autorizándola bajo un esquema voluntario. Al margen de la modalidad adoptada, el principio básico sigue siendo que la titularidad de los datos reside en las personas, como desarrollo del derecho fundamental a la intimidad; por consiguiente, la reserva bancaria continúa siendo un elemento de protección especial de la información de los consumidores. El autor analiza los desafíos en materia de responsabilidad en el tratamiento de los datos y otros retos, así como la regulación recientemente expedida en Colombia.

A partir de la premisa de que las entidades financieras deben contar con un sistema de verificación de identidad y mecanismos fuertes de autenticación, Felipe Noval expone lo relativo a la identidad digital, asociada a un sistema robusto que integra diversas tecnologías para verificar la identidad de los usuarios de manera ágil y sencilla, al tiempo que garantiza la privacidad, seguridad e integridad de la información. El autor explica la diferencia entre

identificación y autenticación, y menciona diversas modalidades delictivas de suplantación, que acompaña de preocupantes cifras sobre el crecimiento del ciberdelito. Describe cómo la identidad digital optimiza recursos y disminuye el riesgo de fraude por suplantación en los procesos de vinculación, autenticación y consultas. Comenta que reemplazar los procesos tradicionales por los digitales mejora la experiencia de los clientes. Por último, el autor ilustra su ensayo con casos de uso de identidad digital en Bélgica y Canadá, junto con los desarrollos realizados en Colombia.

Mauricio Rosillo comenta la irrupción de las Fintech en la actividad financiera a nivel global, lo que ha dado un impulso grande a la oferta de productos y servicios en formas muy convenientes para los consumidores. Estas compañías, inicialmente vistas como competidoras, con el tiempo han llegado incluso a ser aliadas de las entidades tradicionales. El autor advierte sobre los riesgos que implican ciertas actividades desarrolladas por fuera de la vigilancia estatal y sin los controles y el rigor impuestos a las entidades reguladas. Analiza en detalle cada uno de esos riesgos -incluido el riesgo sistémico, por la estrecha relación de las Fintech con el sector financiero tradicional- y aboga por un monitoreo estatal y una regulación que permita administrarlos adecuadamente. También se refiere al interés de las BigTech en los servicios financieros y las ventajas de las que gozan por su amplia presencia internacional y la cantidad de información de sus usuarios de la que disponen.

Juan Sebastián Peredo describe cómo, apoyados en nuevas posibilidades tecnológicas, nacieron los neobancos o bancos digitales, que operan cien por ciento en el mundo digital. Precisa que no es solo un proceso de adaptación tecnológica, sino también la respuesta al cambio cultural experimentado por la sociedad en sus hábitos de consumo. Los bancos digitales desafían el statu quo del sistema financiero, lo que puede manifestarse no solo en retos de innovación sino, por ejemplo, en disminución de tasas de los créditos o eliminación de ciertos costos asociados a productos, debido a la mayor eficiencia de la operación digital; adicionalmente, pueden llegar a todos los rincones del país porque no se necesitan sucursales para ofrecer productos y servicios. El autor insiste en la importancia de que la regulación se diseñe bajo el principio de neutralidad tecnológica y, por supuesto, que se permita la innovación tanto de la tecnología como de los modelos de negocio.

En un recorrido por la regulación, María Fernanda Quiñones muestra cómo los prestadores de servicios de pago digitales dejaron de ser vistos como proveedores de infraestructura para pasar a ser parte del sistema financiero, con capacidad de proveer soluciones eficientes y competitivas para los intercambios económicos. Como articuladores de los distintos agentes de la economía, los proveedores de servicios de pago cumplen un papel fundamental en las dinámicas de consumo de las personas y contribuyen al desarrollo y a la competitividad del país. La autora menciona la incursión de nuevos participantes como las SEDPE y las pasarelas de pagos, y de nuevos instrumentos como los depósitos electrónicos. Destaca el potencial de las Fintech para innovar y desarrollar tecnología financiera, y se refiere al interés del regulador por incentivar la competencia a través de segmentar funciones y estimular la entrada de nuevos agentes al mercado.

Eduardo Arce aborda la protección al consumidor financiero. Reconoce los beneficios del mundo digital, pero advierte sobre algunos efectos negativos de la virtualidad. Las rutinas de acceso a los servicios financieros están diseñadas para que el usuario tome decisiones en segundos, sin que en todos los casos alcance a asimilar las implicaciones, lo que puede

derivar, por ejemplo, en la adquisición de un producto que no lo satisface o en una inversión que no corresponde a su perfil. El autor se refiere a los sesgos cognitivos que afectan las decisiones. De ahí la importancia de la información y la comunicación -dos conceptos diferentes pero complementarios- para neutralizar tales sesgos y contribuir a que el consumidor tome decisiones adecuadas. El ensayo incluye cifras sobre delitos informáticos y analiza la responsabilidad que en tales casos le corresponde a la entidad financiera o al consumidor. Finalmente, formula recomendaciones sobre la regulación de protección al consumidor.

Juan Sebastián Peredo tambien estuvo a cargo de los servicios financieros en el metaverso. Tras advertir que ese universo paralelo no puede verse simplemente como un canal adicional de contacto con los clientes, pues no se trata de abrir sucursales allí como se abren en el mundo físico, el autor invita a abandonar nociones preconcebidas sobre la forma en la que se prestan servicios financieros: los bancos tendrán que competir con un sistema financiero paralelo y descentralizado, que no estará únicamente conformado por actividades reguladas y entidades vigiladas o sucursales bancarias. Sobre todo, si se piensa en las nuevas generaciones nativo-digitales. Explica las características de un metaverso, la relación con la Web3 y las modalidades de centralizado o descentralizado que puede adoptar, con los efectos que de una y otra modalidad se derivan para los consumidores. Igualmente, se detiene en conceptos como los NFTs y en el papel que cumplen los *tokens* y la dirección de criptoactivos en los metaversos.

Por último, agradezco a la Asobancaria la invitación a participar como editor de esta obra, que, sin duda, será de enorme utilidad.

Mauricio Valenzuela Gruesso

PARTE 1

LAS FINANZAS DESCENTRALIZADAS: NUEVO PARADIGMA DE LA INTERMEDIACIÓN

CAPÍTULO 1

La revolución de los criptoactivos y las monedas digitales de los bancos centrales

Gerardo Hernández Correa[1]

Resumen

En los últimos años la revolución digital ha llevado al uso masivo de nuevas tecnologías en el sistema bancario y de pagos. El desarrollo fintech y de activos digitales descentralizados -criptoactivos- ha generado preguntas sobre su sostenibilidad y su impacto en el sector financiero tradicional. El nuevo entorno muestra una tendencia en donde las nuevas tecnologías se vienen asociando con la actividad bancaria tradicional en beneficio de los clientes. Lo mismo sucede con la regulación y operación de las cripto en las que ha variado la aproximación de los reguladores. De hecho, algunas especies de ellas -*digital stable coins*- ya han sido aceptadas como un activo financiero por parte de los reguladores de Basilea. A lo anterior se suma la discusión sobre la conveniencia de que los bancos centrales emitan una moneda digital propia y las implicaciones que ello tendría para la política monetaria, los sistemas de pagos y el sistema financiero. Este ensayo busca mostrar de manera sencilla el desarrollo de las cripto y los avances en las discusiones sobre la moneda digital del banco central y su posible aplicación en Colombia.

[1] Vicepresidente Jurídico del Banco de Bogotá. ExCodirector de la Junta Directiva del Banco de la República y ExSuperintendente Financiero de Colombia. Las opiniones y errores son de su absoluta responsabilidad y no comprometen al Banco de Bogotá.

1. Introducción

El uso intensivo de la tecnología digital en todas las áreas de la actividad humana ha sido calificado como una verdadera revolución. Los avances de la tecnología de la información permiten que el individuo sea el centro de la innovación con cambios profundos en actividades tan diversas como la medicina, la salud y la producción de bienes y servicios. La utilización de herramientas como la del big data o la inteligencia artificial han transformado antiguos paradigmas con enormes beneficios para el bienestar y el desarrollo de la sociedad.

Los servicios financieros, que se prestaron por décadas sin cambios sustanciales en su regulación y operación, no han sido ajenos a esta revolución. Sus prestadores vienen en un proceso acelerado de transformación, con inversiones cuantiosas en tecnología y cambios en los modelos de negocio en donde se reemplazan los canales directos por el uso de plataformas digitales y su desarrollo se centra en las necesidades de los consumidores financieros. Este proceso se ha dado en un marco de mayor competencia motivada por la aparición de nuevos vehículos y aplicaciones, algunos regulados y otros no, que prestan servicios con un alto contenido tecnológico y usan un acervo de información diferente a la tradicional, por ejemplo, para el otorgamiento del crédito o para la cobertura mediante una póliza de seguro. En Colombia ya hay instituciones financieras cuya operación recae totalmente en procesos digitales y es posible la aprobación de un crédito sin que medie la presencia física, en tiempos de espera de minutos.

Con ocasión de la pandemia del Covid-19 y la decisión de las autoridades de ordenar el confinamiento de la población en todo el mundo, el uso de plataformas digitales permitió que la economía siguiera cumpliendo con sus necesidades básicas. El sector financiero volcó todos sus esfuerzos para que sus consumidores pudieran realizar sus pagos y transacciones sin la presencia física en sus instalaciones. Esta situación dio un empuje a la digitalización y mostró un camino que no tiene retorno.

Este nuevo escenario de innovación no solo presenta retos para la industria financiera sino también para los reguladores y los bancos centrales. La prestación de servicios financieros ha sido objeto de una fuerte intervención del Estado en la medida que su actividad usa dineros del público para dar crédito a los hogares o a las empresas o para administrarlos de manera profesional financiando actividades de terceros. La regulación financiera se ocupa de establecer reglas para prevenir la toma de riesgos excesivos, exigiendo un capital adecuado y suficiente para realizar sus operaciones.

Como regla general los servicios financieros solo son prestados por instituciones que han recibido la autorización previa del Estado, para lo cual se evalúa su capacidad financiera y operativa. Estas entidades solo pueden prestar los servicios que han sido expresamente autorizados y su actividad se hace en un marco intensamente regulado bajo la estricta vigilancia de entidades públicas de alta capacidad técnica cuya tarea es supervisar que esas reglas, denominadas prudenciales, se cumplan. La confianza del público en las instituciones financieras es fundamental para que el sistema como un todo funcione adecuadamente.

En un marco de innovación los reguladores se enfrentan a la disyuntiva de permitir los cambios manteniendo reglas prudenciales que protejan a ahorradores e inversionistas. Es un delicado balance ya que una regulación inadecuada puede impedir el cambio tecnológico o exacerbar los riesgos, caldo de cultivo para una futura crisis. De allí la necesidad de que el regulador entienda los cambios introducidos por la tecnología y conozca de primera mano la forma como la industria los está adoptando en sus modelos de negocio.

Igual sucede con los bancos centrales -en Colombia, el Banco de la República- que en la gran mayoría de jurisdicciones están encargados de asegurar el buen funcionamiento de los sistemas de pagos. En esta área se han presentado los mayores desarrollos con la aparición de nuevas tecnologías como blockchain y las denominadas criptomonedas, que se han constituido en alternativas a los sistemas de pagos tradicionales. De nuevo, el reto de los reguladores es el de establecer las reglas que permitan sistemas de pagos más eficientes y menos costosos en un ambiente de competencia y con las condiciones de seguridad suficientes para que los pagos se realicen oportunamente.

En este nuevo contexto los bancos centrales vienen estudiando la conveniencia de emitir monedas digitales -*Central Bank Digital Currencies,* CBDC- como alternativa al efectivo y como instrumento para facilitar el funcionamiento de los sistemas de pagos. El Banco Central de Hungría comparó la emisión de este tipo de monedas con la llegada del hombre a la Luna por los enormes efectos que puede traer en la vida cotidiana y, naturalmente, en el sistema financiero y en los sistemas de pagos.

Este trabajo está dividido en tres secciones. La primera, relacionada con el desarrollo de la industria de criptomonedas o criptoactivos y su efecto en distintas políticas públicas. La segunda presenta la discusión y avances respecto a la posible adopción de monedas digitales por parte de los bancos centrales. (En este trabajo se utilizará el acrónimo en inglés de CBDC, como son conocidas estas monedas en la literatura especializada). El tercer capítulo presenta algunas conclusiones para el caso colombiano.

2. La revolución de las cripto: desarrollos recientes y su regulación

La crisis financiera internacional desatada con la quiebra de Lehman Brothers en 2008 llevó a que las autoridades económicas revisaran la regulación y supervisión financiera y propusieran reformas para hacer más estrictas las condiciones de operación de las entidades financieras, en especial de los bancos. Las reformas exigieron mayores niveles de capital y de liquidez y establecieron estrictos criterios para evaluar los riesgos. Así mismo, reconocieron que los sistemas financieros están interconectados y, en esa medida, que algunas entidades tienen la característica de ser sistémicas, es decir, que sus problemas afectan al sistema en su conjunto. También fortalecieron los esquemas de gobierno corporativo y procuraron una mayor información a disposición de los consumidores financieros. Las reformas recomendadas por el Comité de Basilea[2] han sido adoptadas por casi todos los países, incluido Colombia.

[2] El Comité de Basilea o Comité de Supervisión Bancaria de Basilea tiene por objeto recomendar las mejores prácticas sobre temas de regulación y supervisión financiera. Si bien sus recomendaciones no son obligatorias en la práctica son seguidas por los países en la medida que organismos internacionales como el Fondo Monetario Internacional las utiliza en la evaluación periódica de la situación del sistema financiero en los países. Igualmente, las calificadoras de riesgo utilizan el cumplimiento de estos estándares para su trabajo.

Estas reformas tuvieron un efecto inmediato de hacer más costosa la operación de los bancos y, en un principio, limitaron los volúmenes de crédito disponibles al público. De otra parte, se presentó lo que en la literatura se conoce como efectos no esperados de la regulación, que consistió, en este caso, en la aparición de alternativas de financiación por parte de entidades no reguladas, distintas a los bancos y al mercado de capitales. Dichas entidades entraron a participar en la financiación de manera masiva utilizando tecnologías digitales y desarrollando un nuevo mercado menos costoso sin supervisión financiera. Estos vehículos se focalizaron en atender sectores que por su nivel de riesgo quedaron por fuera de la financiación tradicional y que fueron los principales afectados por la crisis global[3].

A lo anterior se sumaron nuevas plataformas y aplicativos con metodologías alternativas -Fintech- que permitieron agilizar operaciones y pagos y medir riesgos financieros utilizando big data e inteligencia artificial. De esta manera, se amplió la competencia llevando a los bancos a dar prioridad a la innovación. Si hay alguna forma de caracterizar la situación actual del sector financiero es de alta innovación y competencia en beneficio de los usuarios.

2.1 Los criptoactivos

En este nuevo marco de competencia surgieron los criptoactivos[4] como una alternativa para invertir y pagar obligaciones sin la participación de los bancos y sin la utilización de las monedas legalmente reconocidas por los Estados. Se puede afirmar que aparecieron como una reacción frente a la crisis económica, al sector financiero y a la intervención considerada intrusiva del Estado. El nuevo esquema basado en la tecnología blockchain permitió la creación de una moneda sin la intervención estatal -creación descentralizada- y de carácter anónimo, lo que colmó las expectativas de un número importante de personas que no estaban satisfechas con los servicios prestados en el marco tradicional del sistema financiero y de pagos.

Desde su aparición, los criptoactivos han motivado una intensa discusión y análisis. Y no puede ser de otra manera ya que constituyen una disrupción frente a los sistemas tradicionales de pagos, dadas las características en su creación y operación. Algunos de estos interrogantes, que siguen siendo materia de estudio, surgen de: (i) el hecho de que su creación no sea centralizada como ocurre con la moneda legal que es emitida por un banco central; (ii) que no tenga un activo relacionado que sustente su valor; (iii) que su valor se determine por movimientos de oferta y demanda que no dependen de factores fundamentales de la economía y que, por lo tanto, hacen el activo muy volátil; (iv) que tenga el carácter de anónimo; (v) que su creación se haga en un ambiente tecnológico novedoso basado en blockchain; (vi) que su negociabilidad solo sea posible dentro de un determinado ambiente tecnológico y conforme a protocolos que no son regulados por las autoridades, y (vii) que sean instrumentos negociables como cualquier otro activo.

[3] Hernández Gerardo. ¿Cuál es el futuro de los criptoactivos? XXV Encuentro de la Jurisdicción de lo Contencioso Administrativo. Septiembre 2019.
[4] Para efectos de este documento utilizaré la denominación de "criptoactivos" dadas las limitaciones legales y prácticas para que estos instrumentos de pagos puedan considerarse como moneda.

2.2 ¿Son los critopactivos una moneda?

La discusión de política pública se centró, en primera instancia, en definir si los criptoactivos tenían los atributos para ser considerados una moneda. En palabras del presidente del Banco Internacional de Pagos, Agustín Carstens:

> *el dinero o la moneda de un país es un acuerdo o convención social sobre un activo representativo de una obligación del emisor, usualmente el banco central, y que goza de aceptación general para hacer pagos, ser depósito de valor, fungir como unidad de cuenta y tener poder liberatorio ilimitado para liquidar las obligaciones entre los agentes de la economía. La base de esta convención es la confianza. Y ella le está dada por el respaldo de una institución estatal de elevada reputación (el banco central), un marco legal y unas políticas públicas consistentes. Esto es lo que garantiza unos altos estándares de seguridad, aceptabilidad y estabilidad en su poder adquisitivo*[5].

Los criptoactivos no cumplen con estos atributos para ser considerados una moneda. No son una obligación de un agente público o privado, no tienen poder liberatorio ilimitado y, dada su volatilidad, no constituyen un depósito de valor. Lo anterior llevó a que las autoridades económicas y financieras internacionales recomendaran no hablar de criptomonedas y a utilizar, en su lugar, la expresión criptoactivos.

Sin embargo, las autoridades no han podido ponerse de acuerdo sobre la naturaleza jurídica de ese activo, aspecto fundamental para su tratamiento regulatorio y para hacer exigibles las obligaciones de contratos. Por esa razón, en distintos países los han calificado como mercancías, medios de pago, activos financieros o, incluso, valores, buscando encajarlos dentro de los marcos regulatorios existentes. Ante esa diversidad de opciones, ha correspondido a los jueces definir en cada caso concreto las normas aplicables.

La regulación colombiana siguió el criterio según el cual los criptoactivos no son moneda. La ley 31 de 1992, que regula el funcionamiento del Banco de la República y las funciones de su junta directiva como autoridad monetaria, cambiaria y crediticia, indica que la unidad monetaria y unidad de cuenta del país es el peso emitido por el Banco de la República. El artículo 8 de la citada ley precisa que el peso es el único medio de pago de curso legal con poder liberatorio ilimitado. A lo anterior se suma la previsión constitucional que indica que el Banco de la República ejerce de manera exclusiva e indelegable el atributo estatal de emitir la moneda legal.

En igual sentido, el banco central ha considerado, conforme a las recomendaciones internacionales, que los criptoactivos no son una divisa que pueda utilizarse para realizar operaciones cambiarias[6] y, de manera consecuente, que los agentes autorizados para realizarlas -Intermediarios del Mercado Cambiario- no están autorizados para emitirlos o venderlos[7]. Por su parte, la Superintendencia Financiera de Colombia ha manifestado que los criptoactivos no constituyen un valor y que, en consecuencia, no les es aplicable la regulación que rige el mercado de valores[8].

[5] Carstens A. Money in the digital age: what role for central banks? Abril 2018.
[6] La Junta Directiva del Banco de la República tiene definido cuales monedas extranjeras pueden utilizarse para realizar operaciones cambiarias, para ese propósito tiene un listado de monedas consideradas divisas.
[7] Ver comunicado de prensa del Banco de la República del 1 de abril de 2014 y respuestas de la Secretaría de la Junta Directiva del Banco de la República a consultas, en especial el JDS-01933 de 2017.
[8] Ver Cartas Circulares 29 de 2014, 78 de 2016, 52 de 2017 de la SFC.

2.3 Desarrollo reciente de los criptoactivos

El consenso de las autoridades económicas a nivel global, en el sentido de determinar que los criptoactivos no son una moneda legal, no limita de ninguna manera la discusión de otros temas muy relevantes para la política pública. Es una opinión generalizada que el uso de los criptoactivos puede impactar positivamente los sistemas de pagos haciéndolos más eficientes y disminuyendo los costos de las transacciones.

A nivel internacional se mencionan también los beneficios de los criptoactivos para mejorar la fluidez de los pagos entre distintos países que en algunos casos tienen restricciones normativas y altos costos. Este aspecto, el de las transferencias transfronterizas, es crucial dada la importancia que han venido adquiriendo los flujos de remesas entre países y la posibilidad de utilizar nuevos instrumentos para apoyos humanitarios a poblaciones vulnerables. Se han venido desarrollando productos que, con tecnología blockchain, están siendo utilizados para pagos transfronterizos, en especial en países con conflictos armados internos, amplios desajustes cambiarios y pérdida de confianza de los ciudadanos en la moneda local.

Estos instrumentos financieros han venido mostrando una dinámica muy importante desde su creación. El Financial Stability Board -FSB-[9] calculaba que en 2021 el mercado de criptoactivos fue de alrededor de $2,6 trillones de dólares[10]; aunque este monto sigue siendo bajo en comparación con la utilización de activos tradicionales, muestra la aceptación de los criptoactivos para la transferencia de recursos y su uso como un activo de inversión, a pesar de sus riesgos y volatilidad.

2.4 Las *stablecoins*

El desarrollo del mercado de criptoactivos permite distinguir entre las denominadas monedas estables (en inglés stablecoins, término que será usado en este escrito)[11] y los cripto tradicionales. Las *stablecoins*, si bien son creadas bajo parámetros similares a los de los cripto tradicionales, se diferencian en que tienen un subyacente, es decir, que están respaldadas por un activo, o atadas a él, constituido normalmente por monedas de reserva o activos líquidos que permite que su negociación sea menos incierta.

No obstante, las autoridades han destacado los riesgos en la negociación de estos instrumentos, en la medida en que los mercados donde operan tienen poca liquidez, lo que dificulta su negociación. Igualmente destacan los riesgos operativos y las posibilidades de ciberataques en los casos en que sus plataformas de negociación no sean robustas[12].

El desarrollo de *stablecoins* ha permitido calificar a los cripto tradicionales como activos puramente especulativos, dada la enorme volatilidad de sus precios. Esta diferenciación ha permitido a las autoridades financieras globales clasificar los criptoactivos de acuerdo con su nivel de riesgo, como se puede apreciar en un reciente documento del Comité de Basilea -Basel Committee on Banking Supervision, 2021- que da a las *stablecoins* el mismo tratamiento de otros activos financieros tradicionales para efectos de exigir determinado

[9] El Financial Stability Board es un órgano internacional creado por el G-20 que persigue el buen funcionamiento y estabilidad del sistema financiero.
[10] Bank of International Settlements. BIS Annual Economic Report. 2022
[11] Para 2021 los stablecoins constituían una proporción pequeña del total de criptoactivos emitidos, llegando a solo el 6% del total (BIS, 2022).
[12] International Monetary Fund. Financial Stability Report. Octubre 2021.

capital a los bancos. Este documento prevé que las cripto tradicionales, que por esencia son especulativas, deben tener requerimientos muy fuertes de capital de 1 a 1 a la exposición de este tipo de activos. Es decir, dada su enorme volatilidad, la carga de capital de las entidades financieras que quieran tener este tipo de criptoactivos en sus balances se hace muy gravosa y desincentiva su uso.

2.5 Los exchanges

Por otra parte, se han venido consolidando plataformas que facilitan las transacciones de los criptoactivos, denominadas exchanges, que operan en el mercado bajo el radar de las autoridades de regulación y supervisión y facilitan la posibilidad de que la banca tradicional pueda operar estos mercados. Los exchanges han hecho enormes esfuerzos para cumplir con las regulaciones de los países, permitiendo una mayor información sobre las transacciones que transan en sus plataformas. Los exchanges se han vuelto el foco de los reguladores que ante la dinámica del mercado de criptoactivos han considerado que estas plataformas pueden proveer controles e información.

Los exchanges son el punto de contacto entre el sistema financiero tradicional y el mercado de los criptoactivos. Estas plataformas correctamente reguladas mitigan el riesgo, ya que facilitan que los bancos, dentro de políticas adecuadas de riesgo, puedan prestar los servicios de entrada y salida de los dineros -*cash in*, *cash out*- de las operaciones realizadas con criptoactivos.

Debe destacarse, también, el uso de aplicaciones financieras que operan bajo tecnología blockchain y que facilitan la transaccionalidad de los criptoactivos. Estas aplicaciones denominadas *Decentralized finance* -DeFi- vienen creciendo de forma paralela con las *stablecoins*. El uso de *contratos inteligentes* permite mantener el récord de las transacciones de manera descentralizada sin que esté en cabeza de un solo agente fiduciario y ejecutar instrucciones o negociaciones cuando hay condiciones predeterminadas que se cumplen, lo que limita también la participación de un tercero. Para el FMI, DeFi tiene el potencial de ofrecer servicios financieros con mayor eficiencia, atrayendo a un número importante de inversionistas en criptoactivos.

2.6 Discusiones de política pública

Las cripto tradicionales siguen presentando para académicos y reguladores interrogantes similares a cuando aparecieron en el mercado. Temas de escalabilidad -uso masivo por parte del público-, volatilidad, opacidad en su creación y negociación y la preocupación relacionada con lavado de activos y financiación del terrorismo, siguen siendo materia de estudio.

Se reconoce, sin embargo, que su uso puede facilitar transacciones a costos menores, en especial en el caso de operaciones transfronterizas. Igualmente, que puede impulsar el proceso de inclusión financiera, tan necesaria en países en desarrollo. Finalmente, atiende a una nueva generación de consumidores financieros a quienes las características de las cripto tradicionales, así como el anonimato de las transacciones, les resulta llamativo.

Qué tanto se extienda su utilización genera retos para la política monetaria, la estabilidad financiera y un impacto ambiental negativo por el uso de energía en su creación. En

cuanto a la política monetaria, el uso de los criptoactivos como medio de pago puede llevar a reemplazar la moneda de curso legal y, por ende, a dificultar la intervención de los bancos centrales que utilizan el manejo de la tasa de interés como una de sus principales herramientas. América Latina tiene muchas experiencias en las que la utilización de una moneda distinta a la emitida por la autoridad estatal limita las acciones de la autoridad monetaria con resultados no siempre positivos[13]. Igualmente, podría tener efectos en la política cambiaria, en cuanto facilitaría el flujo libre y sin controles de los capitales entre los distintos países, agudizando desequilibrios en algunas economías.

Por otra parte, está el efecto en la estabilidad financiera por temas relacionados con información opaca, regulación inapropiada y la excesiva toma de riesgo. Como estos activos operan de manera transfronteriza, aumentan los riesgos de contagio global ante la falla de un agente que pueda considerarse sistémico.

La difícil evaluación de riesgos por parte de los tenedores de esta clase de activos, dada la volatilidad en el precio, presenta uno de los mayores retos para los reguladores financieros. Como ya se mencionó, las cripto tradicionales no están respaldadas por un banco central y su negociación se caracteriza por un mercado poco profundo y con información escasa y asimétrica, lo que puede facilitar la manipulación de los precios. Por esa razón, la educación financiera y la información son indispensables en la protección de los consumidores.

Un efecto muy importante se relaciona con el impacto ambiental de la minería de criptoactivos. Un reciente trabajo con información del Cambridge Center for Alternative Finance muestra que la minería del bitcoin usa más energía que países como Malasia y Suecia y muy cerca a Egipto y Polonia, lo cual hace pensar que no es sostenible en el mediano y largo plazo y que la política pública tendrá que encargarse del tema[14].

Finalmente, persiste la preocupación de las autoridades financieras globales de que, dado el carácter anónimo de los criptos, estos se utilicen de manera abierta para operaciones de lavado y de financiación de terrorismo. Metodologías tradicionales como la de *conozca su cliente* resultan particularmente difíciles de aplicar en el mercado de criptoactivos. Este tema sigue siendo materia de análisis y discusión sin que se haya resuelto en la práctica.

2.7 La arenera regulatoria[15]

Desde la aparición de los criptoactivos es recurrente la pregunta de hacia dónde debe ir la regulación. La experiencia internacional muestra que, en una primera fase y ante las dificultades de precisar la naturaleza jurídica de los criptoactivos, se les dio tratamiento similar a mercancías, fondos transferibles, instrumentos de pago, unidades de pago susceptibles de ser usadas como medios de pago y activos financieros. Lo anterior con el objeto de aplicar regulación mercantil o financiera ante el vacío de una definición específica. La iniciativa de la Superintendencia Financiera de establecer una arenera regulatoria[16] para transacciones con criptoactivos parece ser la mejor forma de aproximarse a una futura

[13] Casos como el de Argentina con dolarización plena en los años noventa.
[14] Schoar Antoinette, Bitcoin adoption: what regulators need to consider. Princeton Berdheim Center for Finance. Conference.
[15] La arenera regulatoria o "sandbox" consiste en una prueba controlada por el regulador financiero de operaciones que no están autorizadas por la regulación. La arenera permite que de manera temporal ciertos servicios financieros específicos sean prestados en las condiciones definidas por el regulador y bajo su vigilancia con el fin de conocer las características y riesgos.
[16] Ver decreto 1234 de 2020.

regulación. El experimento controlado de la arenera, donde los participantes presentan el modelo de negocio que esperan adelantar, junto con sus riesgos y la forma de mitigarlos, permite el aprendizaje conjunto de los agentes y del supervisor. De manera específica, las pruebas piloto se están adelantando con exchanges de reconocida trayectoria en el mercado para que un número limitado de clientes realicen depósitos y retiros con criptoactivos.

Con la experiencia de la arenera, la Superintendencia Financiera presentó para comentarios una regulación en la cual: (i) define como activo virtual -no financiero- toda representación digital de un activo que se puede comercializar o transferir digitalmente y utilizar para pagos e inversiones; (ii) define a los proveedores de servicios de activos virtuales como toda persona jurídica no vigilada por la SFC que realiza intercambio, transferencia, custodia y administración de activos virtuales y presta servicios relacionados con la oferta de un emisor de activos virtuales y/o venta de una activo virtual; (iii) señala las instrucciones para que las entidades vigiladas tengan vínculos con los proveedores de servicios de activos virtuales; estas instrucciones están relacionadas con temas operativos, controles del sistema de prevención al lavado de activos y de la financiación de terrorismo y cambiarios, y (iv) un régimen reforzado de protección al consumidor.

Adicionalmente, y sin que esto fuera parte de la arenera, se propone que los administradores de fondos de distinta naturaleza puedan realizar inversiones en fondos de inversión extranjera cuyos subyacentes sean activos virtuales, previa adopción de políticas de inversión y de suministrar información a los interesados en este tipo de activos virtuales. También se prevé que las sociedades fiduciarias puedan realizar negocios fiduciarios sobre los mencionados activos.

2.8 ¿Debe expedirse una ley sobre criptoactivos?

La idea de expedir una ley que regule de manera integral el mercado de criptoactivos es sugerida con frecuencia. En Colombia se han presentado algunas iniciativas de origen parlamentario que no han tenido trámite en el Congreso. Estos proyectos de ley tienen la dificultad de que pueden resultar rápidamente inaplicables frente a la dinámica e innovación de ese mercado. De insistirse en estas iniciativas, es indispensable aplicar tres principios: simplicidad regulatoria, neutralidad tecnológica, es decir, que no beneficie o privilegie a un tipo de tecnología frente a otras, y la aplicación de estándares mínimos buscando una mayor posibilidad de que puedan complementarse y conectarse entre sí. Con todo, lo recomendable es tener más información y aprender de lo que sucede en otros países antes de expedir legislación que al poco tiempo pueda ir en contravía de las prácticas del mercado.

En conclusión, la utilización y el desarrollo de los criptoactivos es una realidad que obliga a las autoridades a entender cómo operan y a seguir discutiendo cúal es la mejor forma para regularlos[17]. Los reguladores se han beneficiado de un enorme acervo de trabajos académicos que permiten analizar con herramientas técnicas la dinámica del mercado y su impacto en el sistema financiero internacional. Sin embargo, ese análisis muestra dificultades en la medida en que la información del mercado de criptoactivos disponible es fragmentada y no auditada.

[17] Cuervo Cristina, Morozcova Anastasiia y Nobuyase Sugimoto, Regulation of cryptoassets. Fintech Notes IMF, 2019.

2.9 Una arenera de la vida real: El Salvador

El decreto 57 de 2021 -Ley del Bitcoin- de El Salvador establece que el bitcoin es una moneda de curso legal con poder liberatorio ilimitado, es decir, que si las obligaciones se pagan con bitcoins no es legalmente posible rechazar su pago. A pesar de lo anterior, la misma ley establece una excepción para el caso en que *por hecho notorio y de manera evidente (las personas) no tengan acceso a las tecnologías que permitan ejecutar transacciones en bitcoin*, reconociendo de antemano las dificultades en su uso masivo.

La ley establece incentivos para el uso de la nueva moneda al permitir que los impuestos puedan ser pagados en bitcoin y los intercambios entre el bitcoin y el dólar no estén sujetos a impuestos sobre ganancias de capital. El Estado se compromete a promover la capacitación y los mecanismos necesarios para que la población pueda acceder a transacciones en bitcoin, para lo cual lanzó una billetera electrónica que se llama *Chivo*.

En la práctica esta experiencia está reflejando las dificultades que teóricamente se han señalado para el uso como moneda de los criptoactivos tradicionales. Tal es el caso de la escalabilidad de las operaciones. El uso del bitcoin muestra las dificultades de su uso masivo en un ambiente con baja educación e inclusión financiera. Un segundo tema es el relacionado con los costos de las transacciones y el tiempo requerido para su confirmación. Si bien el consumidor financiero cree que su transacción no tiene costo porque no hay una comisión explícita de la operación, estas transacciones tienen un costo variable que imprime incertidumbre y volatilidad al valor de la transacción y que en este caso beneficia a los *mineros* creadores del bitcoin. El tercer tema es la volatilidad del bitcoin, lo que lo convierte en una mala opción para quienes quieran mantener ahorros de largo plazo. Estudios académicos[18] muestran cómo las variaciones en el precio del bitcoin se correlacionan con anuncios sobre la posibilidad de su uso por agentes financieros formales y cómo existe una enorme concentración de la propiedad de este activo que facilita la manipulación del precio.

Otro tema es el riesgo de lavado de activos que, si bien puede aminorarse con la participación del sistema financiero que aplica metodologías robustas antilavado, puede llevar a que esa jurisdicción sea utilizada masivamente para operaciones relacionadas con actividades delictivas.

Un trabajo reciente[19] muestra los siguientes resultados provisionales de la experiencia en El Salvador: (i) cerca de dos tercios de la población conocen el bitcoin y la posibilidad de negociarlo a través de Chivo; (ii) el mayor número de descargas de Chivo se realizaron con su lanzamiento, motivados en que el gobierno entregó $30 dólares como bono para impulsar su uso; (iii) el mayor número de personas que inicialmente descargaron Chivo, una vez se utilizaron los $30 dólares dejaron de utilizarlo; (iv) reportes del banco central de El Salvador muestran que solo 1.6% de las remesas se hicieron a través de Chivo; (v) solo el 20% de las empresas han utilizado el bitcoin para sus operaciones ordinarias, y, finalmente, (vi) en las transacciones que se realizan con bitcoins, estos son rápidamente convertidos a dólares. La investigación concluye que, *a pesar del estatus de curso legal del bitcoin y los amplios incentivos implementados por el gobierno, esa criptomoneda no es aceptada como medio de pago en El Salvador.* (Traducción propia).

[18] Schoar Antoinette, Bitcoin adoption: what regulators need to consider. Princeton Berdheim Center for Finance. Conference.
[19] Álvarez, Fernando, Argente David y Van Patten Diana. Are cryptocurrencies currencies? Bitcoin as legal tender in El Salvador. National Bureau of Economic Research, Working paper 29968, Abril 2022.

En conclusión, esta experiencia y otras anunciadas recientemente, por ejemplo, en Panamá, que permiten a los ciudadanos acordar el uso de criptoactivos como medio de pago para cualquier actividad civil o comercial, son areneras reales que van a permitir evaluar los aciertos y dificultades para la regulación futura.

2.10 El cripto invierno

El año 2022 ha sido particularmente difícil para la economía del mundo. El rebrote inflacionario producto de la interrupción de las cadenas globales de abastecimiento y el mayor gasto agregado de la economía, impulsado por una política monetaria amplia de los bancos centrales para apoyar a hogares y empresas durante la pandemia, motivó el aumento de las tasas de referencia de dichos bancos. Este aumento en los tipos de interés afecta de manera directa el precio de otros activos, como los valores que se transan en bolsa. Naturalmente, un activo tan volátil como los criptos ha sido uno de los más afectados llevando su valor de mercado a los niveles más bajos desde diciembre de 2020. De igual manera, algunos criptoactivos simplemente desaparecieron dejando cuantiosas pérdidas a los inversionistas, mientras que las *stablecoins* mostraron debilidades en su estructura, tanto que los medios especializados denominaron el primer semestre como el cripto invierno. Cómo se supere este bache en el mercado seguramente definirá, en buena medida, el futuro de las criptomonedas.

3. Las monedas digitales emitidas por bancos centrales -CBDC-

El impacto de nuevas tecnologías en los sistemas de pagos presenta retos enormes para reguladores financieros y bancos centrales, no solo en el campo de la regulación y supervisión financiera sino también en decisiones de política pública. En particular, sobre si los nuevos desarrollos en los sistemas de pagos dan lugar a la intervención directa del Estado, principalmente de los bancos centrales, en cuanto a proveer directamente los servicios de pagos. Algunos bancos centrales han implementado sistemas que permiten el cumplimiento de pagos entre hogares y wcomercios de una manera más rápida y eficiente, como PIX en Brasil y CoDi en México. En este contexto de cambio, caracterizado por un mayor uso de pagos digitales y abandono del efectivo, surge la idea de las monedas digitales emitidas por los bancos centrales -en adelante CDBC-.

3.1 ¿Es necesaria la emisión de CBDC?

El papel del Estado en el buen funcionamiento de los sistemas de pago es un objetivo de política pública. Los sistemas de pagos permiten que las transferencias y pagos de los distintos agentes de la economía se cumplan de una manera segura y eficiente. Los bancos centrales juegan un papel fundamental en la medida en que emiten la moneda y aseguran que las transacciones se cumplan. En palabras sencillas, el banco central es el intermediario fiduciario -de confianza- que debita la cuenta de los pagadores y acredita los pagos en la cuenta del receptor. Una vez ocurre esto, el pago es final e irrevocable. Esta operación se hace en lo que se conoce como sistemas de pago de alto valor, donde se hace la compensación y pagos de las entidades financieras que tienen cuentas en el banco central.

En la gran mayoría de los países es función de los bancos centrales el desarrollo de los sistemas de pagos, tanto de alto valor como de bajo valor, y su seguimiento -*oversight*-, buscando que los pagos se hagan de manera eficiente y a bajos costos. En Colombia, si bien el Banco de la República tiene dentro de sus atribuciones la de *estudiar y adoptar las medidas monetarias, crediticias y cambiarias para regular la circulación monetaria y en general, la liquidez del mercado financiero y el normal funcionamiento de los pagos internos y externos de la economía*, su función, hoy en día, se circunscribe a los pagos mayoristas entre las instituciones financieras en los sistemas de alto valor[20]. La conveniencia de que el banco central regule solo a este segmento del sistema de pagos será analizada posteriormente, pues puede limitar su participación si decidiera emitir CBDC en el futuro.

Ya se mencionó que la moneda tiene una serie de características: (i) la emisión y circulación proviene de la atribución estatal de hacerlo con respaldo de la ley, por ello se habla de moneda legal; (ii) tiene poder liberatorio ilimitado por su valor nominal, lo que significa que tiene la capacidad de pagar obligaciones en un territorio determinado; (iii) el poder liberatorio nace porque así lo dispone la ley y no por la posibilidad de ser convertido en un bien determinado. Por ello la moneda es de curso legal, con poder liberatorio y su circulación no puede limitarse o interrumpirse.

La moneda emitida por los bancos centrales está usualmente asociada con el efectivo, es decir, los billetes y monedas, con los que se hacen transferencias y se pagan las obligaciones en la economía. Sin embargo, la moneda emitida por los bancos centrales también se usa para la transferencia y pagos entre los bancos -mercado interbancario- en las que no hay un intercambio de efectivo, sino que se refleja a través de registros en la contabilidad de los bancos y del Banco de la República. Igualmente, cuando el cliente de un banco hace un pago a una persona que tiene su cuenta en otra entidad, esa transferencia se hace de manera digital, utilizando un sistema de pagos habilitado para ello. En ese sentido, ya existe una moneda digital usada solo por los intermediarios que realizan operaciones en el banco central. Por ello, Prasad ha señalado que trasladar los potenciales beneficios de la CBDC a las personas del común en sus transacciones del día a día, ya sea reemplazando o complementando el uso de billetes y monedas, constituye una verdadera transformación tanto conceptual como tecnológica[21].

3.2 Modelos de emisión de las CBDC

El Banco de Pagos Internacionales -BIS, en su acrónimo en inglés, que será utilizado en este escrito- define la CBDC como una moneda digital denominada en la unidad nacional de cuenta -pesos, en el caso colombiano- y que constituye un pasivo, es decir, una obligación del banco central[22]. Los trabajos teóricos realizados, especialmente bajo el auspicio del BIS, indican que las CBDC pueden tener diversas formas dependiendo del alcance y tecnología utilizada. En general, aunque se reconoce que el uso de CBDC para mercados mayoristas, como el interbancario, podría implicar mayor eficiencia y menores costos, su impacto no sería apreciable para el público en general.

[20] Hernández Gerardo. Marco legal del Banco de la República, banco central de Colombia. Banco de la República 2020.
[21] Prasad Eswar. The future of money. The Belknap Press of Harvard University Press, 2021.
[22] Bank of International Settlements. BIS Annual Economic Report. 2022.

No ocurre lo mismo con las CBDC que puedan utilizarse en los mercados minoristas -entre las personas y los comercios-. Uno de los modelos consiste en una moneda digital emitida de manera centralizada por el banco central, a la cual se tendría acceso a través de monederos electrónicos. Esta moneda digital se distribuiría en montos limitados, a través de los bancos designados, a cambio de efectivo o transferencias realizadas en las cuentas de los clientes. Así, esta moneda reemplazaría de manera directa al efectivo y circularía a través de una plataforma digital del banco central. Las personas se beneficiarían al hacer sus pagos con dinero electrónico por el que responde el banco central y en un sistema administrado por este.

Un segundo modelo es mucho más innovador y agresivo. Consiste en que los individuos y comercios tengan cuentas en el banco central, privilegio que hoy en día solo tienen las instituciones financieras. Para ello sería necesario que el banco central desarrollara un sistema de pagos especializado que compensaría y pagaría buena parte de las transacciones de la economía. Las personas se beneficiarían en la medida en que sus recursos estarían seguros en el banco central, evitando de esta manera los problemas tradicionales de pérdida de depósitos en las crisis bancarias.

El primer modelo puede ser más fácil de implementar en la medida que se asemeja a tecnologías que ya son usadas en el sector financiero, mientras que el segundo modelo tiene retos mayores no solo técnicos sino también conceptuales. El principal reto sería el efecto directo en el sistema financiero, al cual me referiré posteriormente.

En Ecuador, Uruguay y Suecia se han adelantado pilotos con la emisión de CBDC. Bahamas desde octubre de 2020 -*Sand dollar*- es el primer caso de un *Account based CBDC*[23].

3.3 Pros y contras de la emisión de CBDC

Una reciente encuesta realizada por el BIS a sus países miembros muestra los principales motivos de los bancos centrales para estudiar e iniciar pruebas para la posible emisión de CBDC[24]. Estos motivos van desde el interés en proveer una moneda digital que reemplace el efectivo, dado que en algunos países su uso se ha disminuido de manera importante[25]. En otro sentido, el interés de algunos bancos por reducir el uso de efectivo se asocia con informalidad, corrupción y evasión tributaria. Otra razón que se menciona es que las CBDC pueden complementar el uso de plataformas digitales en los sistemas de pagos, mejorando su seguridad y eficiencia. En los países de menor desarrollo se aduce que las CBDC pueden constituir instrumentos para aumentar la inclusión financiera e incrementar la competencia en los sistemas de pagos de bajo valor. En general, se encuentra que las motivaciones son complementarias.

La emisión de CBDC podría servir como un mecanismo para mantener el rol primordial de los bancos centrales en los sistemas de pagos de la economía, generando mayor confianza en

[23] Prasad (2021) trae un buen recuento de ejemplos de CBDC.
[24] En una encuesta del BIS, el 90% de los países de la muestra, que incluye 81 bancos centrales que comprenden el 76% de la población del mundo y el 94% de la producción económica global, están adelantando algún trabajo relacionado con CBDC. El 62% están realizando trabajos o pilotos avanzados de exploración de los CBDC (BIS,2022).
[25] En Gran Bretaña, por ejemplo, del total del M3, el 97% del total está relacionado con el uso de operaciones digitales, en el Eurosistema, 91% del M3 es digital y en China el 96% (Cechetti, 2021).

los mismos. A la vez podría facilitar el uso de instrumentos tradicionales de política monetaria -tasa de interés del banco central- para afectar los agregados monetarios. El Banco de la Reserva de India mencionó en la encuesta citada del BIS los ahorros que se conseguirían en la producción de efectivo y su distribución, costos que pueden ser significativos en países donde el uso del efectivo es muy importante.

El efecto positivo en la inclusión financiera es un elemento mencionado especialmente por los países en desarrollo. Naturalmente, ese efecto depende en buena medida de factores de otra índole, relacionados con la formalidad de la economía, la existencia de infraestructura que facilite los pagos digitales -por ejemplo, acceso a Internet-, los niveles de educación financiera y el grado de innovación tecnológica. En estos casos, las CBDC podrían aportar una mayor confianza a las personas, pero requerirían a la vez de una mayor intervención, afectando la iniciativa privada que históricamente ha tenido una ventaja frente al sector público en cuanto a introducir nuevas tecnologías y prácticas.

Otro factor es el desarrollo de los sistemas de pagos, en la medida en que las CBDC pueden inducir una mayor competencia y quebrar la estructura oligopolística de estos mercados. Sin embargo, este objetivo de política también puede lograrse mediante una regulación y supervisión adecuada de los sistemas de pagos, reservando la participación del Estado a actividades que lo requieran por presentar fallas de mercado. Como se mencionó, el impacto de las CBDC dependerá del desarrollo de los sistemas de pago.

Un aspecto positivo es que las CBDC permitirían introducir reglas relacionadas con la información de las operaciones. Si bien esto rompe con la regla del anonimato que existe en el efectivo, justamente sería un elemento clave para combatir la corrupción, el lavado de activos y la financiación del terrorismo.

3.4 Temas de política pública

Los trabajos académicos resaltan varios temas de análisis y preocupación respecto a la emisión de CBDC. Se ha identificado que, en la medida que los bancos centrales asuman de manera directa las responsabilidades del ecosistema que se crearía alrededor de la nueva moneda digital, sus riesgos operacionales aumentan considerablemente. Para que la CBDC tenga aceptación o genere confianza en el mercado se necesita que el sistema sea estable y robusto. Basta imaginar que, dadas sus características, un volumen muy importante de los pagos se haría a través de esta. A lo anterior hay que añadir la necesidad de que el sistema mantenga los más altos desarrollos tecnológicos disponibles, lo que puede implicar costos que serían, en principio, cubiertos por el banco central, sin que fueran trasladados al público.

Un efecto estructural se relaciona con su impacto en el sector bancario. En la medida en que la CBDC entre a competir directamente con los depósitos de los bancos, es de suponer que un buen número de usuarios preferirían por razones de seguridad trasladar sus recursos a cuentas en el banco central. Esta situación se puede potenciar en épocas de crisis en las que se presenta el fenómeno de *flight to quality,* consistente en que los depositantes prefieren mover sus recursos a entidades que consideran menos riesgosas, aumentando la posibilidad de corridas bancarias. Tiene igualmente implicaciones grandes en el fondeo bancario al obligarlos a acudir a fuentes menos estables con los consecuentes efectos en las tasas de interés y rentabilidad. En efecto, en la medida que recursos de los depositantes

como los de las cuentas de ahorro o corrientes se trasladen al banco central, la disponibilidad de recursos para el crédito se reducirían, teniendo las entidades que acudir a instrumentos de captación más costosos.

La discusión reciente sobre la emisión de CBDC muestra que la gran mayoría de los bancos centrales están dispuestos a explorar la alternativa en la que se mantiene una participación del sector financiero antes que el modelo que le daría acceso directo a los ciudadanos al banco central. En ese primer modelo, el banco central provee la infraestructura básica y les corresponde a los bancos mantener y contabilizar las operaciones de sus clientes. Este diseño reduce los problemas operacionales del banco central que se han mencionado, y da mayor flexibilidad para futuros desarrollos tecnológicos al tiempo que mitiga los efectos en el sistema financiero. Sin embargo, hay aspectos que aún en ese esquema deben analizarse.

El primero de ellos se relaciona con la interoperabilidad de la CBDC con otros sistemas de pagos y el alcance de la participación del banco central. Como lo ha manifestado la directora del Fondo Monetario Internacional, Kristalina Georgieva, no hay un modelo único aplicable porque las economías son diferentes. En algunos casos CBDC puede ser un paso fundamental para mejorar los sistemas de pagos. En otros casos puede constituirse en un elemento adicional que complemente la infraestructura existente. En países con sistemas de pago maduros, la CBDC puede operar incluso como contingencia ante fallas de los sistemas de pagos de bajo valor.

El segundo aspecto para analizar es si la CBDC se utilizaría como instrumento de política monetaria o si simplemente buscaría reemplazar el efectivo. Dependiendo del objetivo buscado, aspectos como si los depósitos en CBDC reconocerán una tasa de interés o si tendrán límites en los montos depositados deben ser materia de cuidadoso análisis[26].

El tercero es el tratamiento de la información de los depositantes. Si bien hay una tendencia de la regulación financiera para el uso amplio y sin límites de información de los clientes, la información relacionada con quienes utilicen CBDC también constituye un tema de discusión y análisis.

3.5 Marco Legal

La experiencia internacional muestra distintas opciones respecto a la base legal para la emisión de CBDC, dado que las legislaciones que regulan los bancos centrales son previas a la revolución digital.

Un grupo de países considera que no es necesaria la modificación del marco legal, en la medida en que la atribución para emitir es amplia y no limita o distingue entre el efectivo y la moneda digital. Tal es el caso del banco central de Uruguay que adelantó un piloto de seis meses en 2017 emitiendo el e-peso.

Otro grupo ha considerado necesario modificar la ley para permitir de manera específica la posibilidad de emitir monedas digitales y facultar al banco central para establecer el marco operativo necesario para su uso. Tal es el caso de Bahamas que emitió el *Sand Dollar* luego

[26] En el libro "The future of Money", Eswar Prasad presenta un resumen de las implicaciones en la política monetaria y el posible uso de CBDC en los instrumentos de política de los bancos centrales.

de que la ley de manera expresa le permitiera emitir moneda electrónica -*electronic money*-.

Algunos países están analizando reformas comprensivas de las leyes de sistemas de pagos, considerando a las CBDC como un elemento adicional de su funcionamiento. En estos casos se incluyen facultades para la operación del banco central y la interoperabilidad con otros sistemas de pagos de bajo valor.

3.6 El caso colombiano

El Banco de la República ha señalado:

> *En un contexto de un sistema de pago de bajo valor poco desarrollado, acompañado de obstáculos institucionales y de estructura de mercado para su progreso, la introducción de una CBDC minorista es una opción que vale la pena considerar en Colombia. Sus aspectos de diseño (atributos de rentabilidad y conveniencia) pueden establecerse de tal manera que sustituya principalmente tenencias de efectivo, con un impacto moderado sobre los depósitos bancarios y la intermediación financiera. (Traducción propia)*[27].

En el trabajo citado, el banco descarta la amenaza de lo que denomina *digital dollarisation*, es decir, que se utilicen CBDC emitidas por otros países como medio de pago en Colombia, siempre y cuando se mantenga la credibilidad del esquema de inflación objetivo, una tasa de cambio flexible y un sistema financiero sólido. Igualmente, indica que de adoptarse una CBDC colombiana es necesario estudiar con cuidado su operación transfronteriza y sus efectos en el manejo macroeconómico.

Estas recomendaciones surgen luego de señalar la preferencia de las personas en Colombia por el efectivo, las características de la estructura actual de los sistemas de pagos de bajo valor y la conveniencia de implementar un sistema de pagos inmediatos. En este contexto, pareciera que el Banco de la República está considerando una posible emisión de CBDC dentro de un marco de reformas de los sistemas de pagos, buscando una mayor eficiencia y menores costos. Así las cosas, resulta aconsejable revisar el proyecto de ley denominado *Reforma al mercado de capitales*, en el que se atribuye al Gobierno Nacional la función de regular los sistemas de pagos de bajo valor, para establecer, en su lugar, que sea el banco central quien oficie como regulador exclusivo, tal y como lo están haciendo otros países que están considerando o realizando pilotos de uso de CBDC.

Respecto al marco legal, la ley 31 de 1992 no limita la emisión de moneda digital por parte del Banco de la República; de hecho, y como ya se mencionó, esta se utiliza actualmente en el sistema de pagos de alto valor. Por su parte, el artículo 22 de la mencionada ley indica que el banco central podrá abrir cuentas bancarias o celebrar contratos de depósito con personas públicas o privadas (se subraya), cuando ello sea necesario para realizar las operaciones propias del banco. Lo anterior sugiere que, en principio, podría considerarse viable la opción adoptada en otros países para no adelantar una reforma legal. Sin embargo, dadas las implicaciones de la CBDC en los instrumentos de política previstos en la ley 31, es recomendable una reforma legal que dé flexibilidad a la junta directiva para que defina su uso como instrumento de política. De igual manera, si el CBDC es considerado como un

[27] Vargas Hernando. Some thoughts about the issuance of a retail CBDC in Colombia en: Bank of International Settlements: CBDCs in emerging market economies. Abril 2022.

elemento de una reforma integral del sistema de pagos, sería recomendable una reforma legal.

4. Reflexiones finales

4.1 La revolución digital ha transformado la sociedad en todos sus aspectos y el sector financiero no ha sido excepción. La banca viene adelantando un proceso acelerado de digitalización poniendo a los consumidores financieros en el centro de esta transformación. Este proceso de cambio tecnológico se ha beneficiado de la innovación impulsada por las Fintech en un marco de colaboración y mayor competencia. Estos cambios traen retos no solo al sector financiero sino también a los reguladores y supervisores.

4.2 La adopción de nuevas tecnologías -*big data*, blockchain, inteligencia artificial, entre otras- benefician la operación del sistema financiero y facilitan su labor de intermediación financiera. En el caso de los criptoactivos, su aparición ha dado un impulso enorme al priorizar los temas relacionados con los sistemas de pagos y la necesidad de hacerlos más eficientes y menos costosos.

4.3 La aceptación global de criptomonedas y de sus variantes como *stablecoins* indica que este no es un fenómeno transitorio, sino que es parte del complejo sistema de pagos global. En esa medida el análisis de la forma como funcionan sigue siendo una tarea para los operadores, reguladores y supervisores financieros.

4.4 En el caso de las cripto tradicionales subsisten los interrogantes que se plantearon desde su aparición. Temas sobre la escalabilidad, anonimato y su uso para evadir la prevención de lavado de activos y financiación de terrorismo siguen siendo materia de seguimiento y estudio. A ellos se han añadido preocupaciones diferentes relacionadas, por ejemplo, con el impacto ambiental del uso de energía, que seguramente deberá ser tema de regulación. La experiencia de algunas jurisdicciones en donde se han adoptado como moneda de curso legal ratifican las limitaciones mencionadas por los distintos trabajos académicos.

4.5 El desarrollo de las *stablecoins* ha favorecido que estos instrumentos empiecen a considerarse como variantes de instrumentos financieros tradicionales, facilitando su regulación y supervisión. Igualmente, el foco de los reguladores en las plataformas -exchanges- a través de las cuales se negocian los criptoactivos es una alternativa que permite la trazabilidad de operación y la prevención del lavado de activos.

4.6 La regulación de los criptoactivos debe basarse en tres principios: simplicidad regulatoria, neutralidad tecnológica entre productos financieros y la aplicación de estándares mínimos. La experiencia internacional muestra que dada la dinámica del mercado de criptoactivos es preferible esperar a una mayor estabilidad y maduración antes de una regulación integral.

4.7 La experiencia de la arenera regulatoria por parte de la Superintendencia Financiera es una excelente alternativa para conocer mejor cómo operan los mercados antes de regularlos. Una regulación insuficiente o equivocada puede traer obstáculos a la innovación.

4.8 En el contexto de revolución digital, los bancos centrales han empezado a estudiar la conveniencia de emitir monedas digitales. Las razones para su emisión son variadas y van

desde introducir una alternativa al efectivo y propiciar la inclusión financiera hasta su uso como un nuevo instrumento de política monetaria. Sus posibles efectos son de gran magnitud para el sector financiero dependiendo del modelo adoptado para su implementación. Igualmente, para los sistemas de pagos y para la estabilidad financiera.

4.9 La emisión de CBDC implica una participación mayor de los bancos centrales en los sistemas de pagos. Ese mayor involucramiento debe estudiarse cuidadosamente ya que los objetivos buscados pueden lograrse con una buena regulación por parte del Estado sin distraer a los bancos centrales de su objetivo principal de preservar la estabilidad de precios.

4.10 Los bancos centrales parecen preferir un modelo de dos niveles que tiene menores efectos en el sistema financiero. No obstante, su implementación tiene retos de política pública que deben analizarse con cuidado antes de acometerse.

4.11 El Banco de la República ha señalado que las CBDC son una alternativa que debe estudiarse dada la preferencia del uso del efectivo en Colombia y el desarrollo de los sistemas de pagos de bajo valor. En ese orden de ideas, resulta aconsejable que se revise la decisión tomada al presentar a consideración del Congreso el proyecto de ley denominado Reforma al mercado de capitales, en el que se establece que sea el Gobierno Nacional quien regule los sistemas de pagos de bajo valor. La experiencia internacional muestra que debe ser el banco central el regulador exclusivo de los sistemas de pago.

4.12 La ley 31 de 1992 no limita la emisión de moneda digital por parte del Banco de la República; de hecho, esta se utiliza en el sistema de pagos de alto valor. El artículo 22 de la mencionada ley indica que el banco central podrá abrir cuentas bancarias o celebrar contratos de depósito con personas públicas o privadas, cuando ello sea necesario para realizar las operaciones propias del banco, lo que permitiría usar el modelo de emisión de CBDC en el que el público en general podría tener depósitos en el banco central. Sin embargo, dadas las implicaciones de la CBDC en los instrumentos de política previstos en la ley 31, es recomendable una reforma legal que dé flexibilidad a la junta directiva para su uso como instrumento de política.

Bibliografía

Álvarez, Fernando; Argente, David y Van Patten, Diana. Are cryptocurrencies currencies? Bitcoin as legal tender in El Salvador. *National Bureau of Economic Research, Working paper 29968*, Abril 2022.

Aur Rafael, Cornelli Giulio y Frost, Jon. Rise of the central digital currencies: drivers. Approaches and technologies. *BIS working paper* 880. Agosto 2020.

Auer Rafael; Frost, Jon; Gambacorta, Leonardo; Monnet, Cyril; Rice, Tara y Shin Hyun Song. Central bank digital currencies: motives, economic implications, and the research frontier. *BIS working papers 976*, November 2021.

Bank of International Settlements. CBDCs in emerging market economies. Abril 2022.

Bank of International Settlements. BIS Annual Economic Report. 2021.

Bank of International Settlements. BIS Annual Economic Report. 2022.

Basel Committee on Banking Supervision. Prudential treatment of crypto asset exposures. *Consultative Document*. Junio 2021.

Cecchetti, Stephen y Schoenholtz. Central bank digital currency: the battle for the soul of the financial system. *Voux org*. Julio 2021.

Cuervo, Cristina; Morozcova, Anastasiia y Nobuyase, Sugimoto, Regulation of cryptoassets. *Fintech Notes IMF*, 2019.

Duffie, Darrell; Mathieson, Kelly; Darko, Pilav. Central Bank Digital Currency. Princ

Federal, Reserve. Money and Payments: the US dollar in the age of digital transformation, Enero 2022.

Georgieva, Kristalina. The future of money: gearing up for Central Bank Digital Currency. International Monetary Fund 2022.

Hernández, Gerardo. Marco legal del Banco de la República, banco central de Colombia. *Banco de la República* 2020.

Hernández, Gerardo. Cuál es el futuro de los criptoactivos? XXV Encuentro de la Jurisdicción de lo Contencioso Administrativo. Septiembre 2019.

Hernández, Gerardo. Cinco temas de discusión entorno a los criptoactivos. CLEC VI. Congreso Latinoamericano de Economía y Banca. Quito Ecuador, Septiembre 2016.

International Monetary Fund. Financial Stability Report. Octubre 2021.

Kosse, Anneke y Mattei, Ilaria. Gaining momentum: results of the 2021 BIS survey on central bank digital currencies, *Bank of International Settlements.* Mayo 2022.

Prasad, Eswar. The future of money. *The Belknap Press of Harvard University Press,* 2021.

Schoar, Antoinette, Bitcoin adoption: what regulators need to consider. *Princeton Berdheim Center for Finance.* Conference.

Soderberg, Gabriel. Behind the Scenes of Central Bank Digital Currencies. Fintech Notes. *IMF*, Febrero 2022.

Vargas, Hernando. Some thoughts about the issuance of a retail CBDC in Colombia en: Bank of International Settlements: CBDCs in emerging market economies. Abril 2022.

CAPÍTULO 2

Finanzas descentralizadas: ¿el futuro del sector financiero?

Nydia Remolina[1]

Resumen

Las Finanzas Descentralizadas, conocidas como DeFi por su nombre en inglés -*Decentralized Finance*-, hacen referencia al uso de blockchain y activos digitales o criptoactivos para la prestación de servicios financieros. De esta manera, a través de las aplicaciones DeFi se ofrecen servicios como préstamos, seguros, bolsas de intercambio de criptoactivos, entre otros, que se estructuran a partir de criptoactivos y a través de aplicaciones descentralizadas desde el punto de vista tecnológico. En este capítulo se analiza el concepto de DeFi y cómo este desafía las infraestructuras de mercado tradicionales del sector financiero, pero también se desmitifica esa idea de absoluta descentralización. Dentro de las oportunidades se menciona cómo DeFi podría contribuir a la inclusión financiera, a la automatización de ciertos productos financieros y cómo es un factor clave para el desarrollo de metaversos. En los desafíos se analizan, entre otros, el problema de lavado de activos y financiación del terrorismo en estos mercados, la protección al consumidor financiero, los problemas de gobierno corporativo, la falta de transparencia de estos productos, los riesgos de ciberseguridad y problemas de riesgo sistémico. Finalmente, el capítulo aborda los diferentes modelos regulatorios que han intentado dar respuesta a algunos de estos desafíos.

[1] Profesora asistente de la facultad de derecho de Singapore Management University y líder de industria y del fintech track del Centro de Inteligencia Artificial y Gobernanza de Datos de la misma universidad.

1. Introducción

Las Finanzas Descentralizadas, conocidas como DeFi por su nombre en inglés -*Decentralized Finance*-, hacen referencia al uso de blockchain y activos digitales o criptoactivos[2] para la prestación de servicios financieros[3]. De esta manera, a través de las aplicaciones DeFi se ofrecen servicios como préstamos, seguros, plataformas de intercambio de criptoactivos, entre otros. Las DeFi se estructuran a partir de la idea de descentralización a través del uso de *aplicaciones descentralizadas*[4] -Dapps por su nombre en inglés- y contratos inteligentes o *smart contracts*[5]. Adicionalmente, la implementación de DeFi se hace de forma digital a través del uso de criptoactivos. En síntesis, DeFi se trata de estructurar productos y servicios que imitan la funcionalidad de servicios financieros usando activos digitales y mecanismos que permiten operar de forma descentralizada tecnológicamente. En otras palabras, mientras que las finanzas tradicionales dependen de intermediarios, como los bancos u otras entidades financieras para administrar y procesar los servicios financieros, DeFi opera en un entorno descentralizado, usando la tecnología blockchain.

El concepto de descentralización en DeFi viene precisamente del uso de blockchain. Usualmente, los datos se han almacenado en bases de datos centralizadas[6]. Las bases de datos centralizadas son custodiadas por un administrador central y se almacenan en un único servidor[7]. El administrador es un intermediario al que se le confía el mantenimiento de los datos de acuerdo con las instrucciones de su titular. Por otro lado, los usuarios -*o clientes*- que quieran acceder a los datos almacenados deben enviar una solicitud al administrador del servidor[8]. En contraste, en bases de datos distribuidas, como usualmente se definen aquellas que utilizan la tecnología blockchain, las tareas no están controladas ni coordinadas por un administrador central o por una parte que actúe de intermediario. En ese caso, estas tareas están distribuidas a lo largo de las distintas partes que se coordinan a través de un mecanismo de consenso para registrar los datos. Ese mecanismo de consenso está definido en un protocolo[9]. Las finanzas descentralizadas funcionan bajo este principio en el sentido en que no se requiere un administrador o una parte designada para la ejecución y registro de las operaciones –como un banco, por ejemplo– sino que una serie de reglas consignadas en un protocolo definen cómo se ejecutan y registran transacciones apalancándose en la forma de operación de blockchain.

---

[2] Para efectos de este capítulo, utilizaremos los términos *activos digitales* y *criptoactivos* como sinónimos. No obstante, en otros contextos no necesariamente tienen el mismo significado.

[3] Ver Wharton Blockchain and Digital Asset Project, World Economic Forum, *DeFi Beyond the Hype. The Emerging World of Decentralized Finance* (2021), disponible en: https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf; Dirk Andreas Zetzsche Douglas W. Arner, Ross P. Buckley, *Decentralized Finance* (*DeFi*) (2020) 6 JOURNAL OF FINANCIAL REGULATION 172.

[4] Una aplicación descentralizada o Daap es aquella que puede operar de forma autónoma y opera de forma descentralizada a través de tecnologías como blockchain y el uso de contratos inteligentes. Ethereum, "Introduction to Daaps" (2022), disponible en: https://ethereum.org/en/developers/docs/dapps/ Operar de forma "descentralizada" hace referencia a ejecutar alguna tarea u operación, generalmente, sin necesidad de una entidad a cargo de ejecutar dicha tarea u operación.

[5] Un contrato inteligente o smart contract es un término utilizado para describir un programa o código – en términos computacionales – que ejecuta automáticamente una tarea cuando se cumplen ciertas condiciones predefinidas en el programa. Alfonso Delgado de Molina Rius, Vicente García Gil, *Los contratos inteligentes o smart contracts*, en FINTECH, REGTECH Y LEGALTECH: FUNDAMENTOS Y DESAFÍOS REGULATORIOS, Ed. Nydia Remolina y Aurelio Gurrea-Martinez (Tirant LoBlanch, 2020).

[6] Alfonso Delgado de Molina Rius, *Blockchain: concepto, funcionamiento y aplicaciones*, en FINTECH, REGTECH Y LEGALTECH: FUNDAMENTOS Y DESAFÍOS REGULATORIOS, Ed. Nydia Remolina y Aurelio Gurrea-Martinez (Tirant LoBlanch, 2020).

[7] Un servidor es el lugar donde son almacenados los datos.

[8] Alfonso Delgado de Molina Rius, Blockchain: concepto, funcionamiento y aplicaciones, en FINTECH, REGTECH Y LEGALTECH: FUNDAMENTOS Y DESAFÍOS REGULATORIOS, Ed. Nydia Remolina y Aurelio Gurrea-Martinez (Tirant LoBlanch, 2020).

[9] Ibid.

Los servicios ofrecidos a través de DeFi están generalmente codificados en protocolos de software de código abierto -*open source protocols*- y contratos inteligentes que automatizan las decisiones. De forma similar al blockchain, detrás de las finanzas descentralizadas hay entusiastas que promueven sus potenciales beneficios, tales como mayor eficiencia, transparencia e innovación en la prestación de servicios financieros que podrían mejorar los niveles de inclusión financiera. Sin embargo, un importante número de académicos, reguladores y organizaciones internacionales han sido críticos de las finanzas descentralizadas haciendo hincapié en los riesgos asociados a ellas. Estas críticas se exacerban con cada nuevo ciberataque, fraude o controversia en las que se ven envueltas aplicaciones de esta nueva tecnología.

Este capítulo tiene como propósito explicar el concepto de DeFi y comparar las finanzas descentralizadas con algunos productos financieros tradicionales para aterrizar el concepto. También se desmitificará esa idea de absoluta descentralización, generalmente mencionada en el ámbito de los criptoactivos, desde la perspectiva de toma de decisiones y gobierno de estas aplicaciones descentralizadas. Posteriormente, el capítulo analizará las oportunidades y desafíos de DeFi para consumidores, entidades financieras, nuevos competidores y reguladores financieros. Dentro de las oportunidades se presentará cómo DeFi podría contribuir a la inclusión financiera, a la automatización de ciertos productos financieros y cómo es un factor clave para el desarrollo de metaversos. Como parte de los desafíos, se analizará el problema de lavado de activos y financiación del terrorismo en estos mercados, la protección al consumidor financiero, problemas de gobierno corporativo, la falta de transparencia de estos productos, los riesgos de ciberseguridad y problemas de riesgo sistémico. Finalmente, el capítulo abordará los modelos regulatorios de diferentes jurisdicciones y organismos internacionales que han tratado de dar respuesta a algunos de estos desafíos.

2. Concepto de Finanzas Descentralizadas

2.1 El espectro de la descentralización

En la expresión *finanzas descentralizadas* resulta relativamente fácil saber a qué se refiere la palabra *finanzas*. Es intuitivo concluir que un depósito remunerado con intereses o un derivado, desde el punto de vista funcional, se parecen a un producto financiero así sean estructurados con criptoactivos y bajo la infraestructura ya explicada. En cambio, no resulta tan claro a qué hacemos referencia con *descentralización*.

Particularmente, desde la aparición de Bitcoin en 2008[10] la palabra descentralización se ha popularizado en la terminología asociada a la tecnología blockchain. No obstante, la evolución de blockchain ha mostrado que la descentralización no es tan sencilla de definir, y con la aparición de blockchains privadas[11], sometidas a permiso[12] o cerradas[13], en donde una entidad o un grupo de entidades controlan el gobierno de la red, el concepto de descentralización adquiere diferentes tonalidades.

[10] Satoshi Nakamoto, *Bitcoin*: A *Peer-to-Peer Electronic Cash System* (2008), disponible en: https://bitcoin.org/bitcoin.pdf
[11] Las redes cerradas son aquellas en las cuales sólo los usuarios autorizados pueden unirse a la red. El acceso a una red cerrada puede estar vigilado por un guardián (gatekeeper) de un consorcio. Alfonso Delgado de Molina Rius, *Blockchain: concepto, funcionamiento y aplicaciones*, en FINTECH, REGTECH Y LEGALTECH: FUNDAMENTOS Y DESAFÍOS REGULATORIOS, Ed. Nydia Remolina y Aurelio Gurrea-Martinez (Tirant LoBlanch, 2020).
[12] En las redes sometidas a permiso todas las posibles actuaciones están reservadas a una lista aprobada de usuarios. Ibid.
[13] En una red privada sólo los usuarios autorizados pueden leer los datos de las transacciones registradas en la red. Ibid.

En el mundo DeFi ocurre algo similar. Cada protocolo contiene reglas distintas de gobierno y resolución de conflictos. Por ende, es importante hablar del espectro de la descentralización en lugar de la descentralización como concepto abstracto y totalmente opuesto a la *centralización*, definida esta como la prestación de servicios financieros ejecutados por una entidad financiera. No obstante, a pesar de que la centralización de las finanzas tradicionales implica que una entidad ejecuta las operaciones, por ejemplo, un banco aprueba y desembolsa un crédito, es importante también considerar que las finanzas tradicionales están estructuradas de una forma igualmente compleja en donde muchas partes interactúan y se forman varias relaciones contractuales. No en todos los productos de finanzas tradicionales existen interacciones entre el usuario/consumidor y la entidad financiera que presta un servicio. Por ejemplo, en el mercado de derivados financieros interactúan más actores tales como las cámaras de riesgo central de contraparte, sistemas de negociación, sistemas de compensación y liquidación, entre otros. Por ende, la llamada *centralización* de las finanzas tradicionales tiene también cierta complejidad en el sistema financiero actual.

Volviendo al espectro de la descentralización en el mundo de DeFi, la gobernanza se refiere a las formas en que se toman decisiones colectivas, se resuelven conflictos y se implementan cambios en los protocolos. En DeFi, la gobernanza media la actividad entre las aplicaciones y la capa de liquidación subyacente, incluidas decisiones como la modificación de las tasas de interés o las garantías requeridas en las aplicaciones de créditos[14].

Muchos casos de uso en DeFi incluyen un *token* de gobernanza que proporciona derechos de voto sobre ciertas decisiones[15]. En una sociedad tradicional -o *centralizada*, si así se le quiere llamar-, las decisiones son delegadas por los accionistas en los directores y administradores de la compañía. En el caso de DeFi, los tenedores de *tokens* son quienes directamente votan sobre cambios que se quieran implementar y la operatividad de los productos y servicios de la aplicación es gobernada y ejecutada de manera automática por los contratos inteligentes siguiendo las reglas del protocolo escogido. Los tenedores de *tokens* de gobernanza pueden presentar nuevas propuestas de gobernanza o votar por las presentadas por otros miembros de la comunidad de tenedores de *tokens*[16].

Sin embargo, es importante tener en cuenta que la gobernanza de los proyectos de DeFi no recae exclusivamente en las decisiones de los tenedores de *tokens*. En algunos casos, los creadores y operadores de las aplicaciones de DeFi pueden reservarse algunos derechos relacionados con la toma de decisiones[17]. En consecuencia, la gobernanza en el contexto de las DeFi se puede descentralizar parcialmente otorgando a los poseedores de *tokens* derechos de voto limitados: pueden tener poder sobre solo unos pocos parámetros mientras los desarrolladores pueden retener el poder de veto efectivo a través de grandes tenencias

[14] The World Economic Forum, DeFi Policy Maker Toolkit (2021), disponible en: https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf

[15] James Howell, *What Are Governance Tokens And Why Does They Matter?*, 101 Blockchains (2022), disponible en: https://101blockchains.com/governance-tokens/

[16] El funcionamiento es muy similar al de los proyectos basados en blockchain que recaudan fondos con las Initial Coin Offerings u Ofertas Iniciales de Monedas. En una ICO, los tenedores de tokens entregan criptomonedas a los desarrolladores de un proyecto de blockchain para financiar el desarrollo y crecimiento de dicho proyecto. Los tenedores de token tienen unos derechos que se encuentran representados en los tokens. Dependiendo de la estructura del token, los tenedores pueden tener derechos de voto en el proyecto. Ver Aurelio Gurrea-Martinez and Nydia Remolina, Corporate Governance Challenges in Initial Coin Offerings, in Andrew Godwin, Pey Woan Lee, and Rosemary Teele Langford (eds.), TECHNOLOGY AND CORPORATE LAW HOW INNOVATION SHAPES CORPORATE ACTIVITY CORPORATIONS (Edward Elgar Publishing, 2021) pp. 205-226.

[17] Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. Journal of the Association for Information Systems, 19(10), 1; Chohan, Usman W., The Decentralized Autonomous Organization and Governance Issues (2017). Disponible en: https://ssrn.com/abstract=3082055

de *tokens* o no tener la obligación formal de implementar los cambios propuestos por los tenedores de *tokens*[18].

Adicionalmente, como ocurre con los accionistas en algunos mercados de valores, los tenedores de *tokens* pueden delegar en terceros la toma de decisiones en representación suya[19]. Así las cosas, en DeFi se pueden designar personas para implementar cambios según las instrucciones de los tenedores de *tokens*[20]. Esta es una forma de coordinar la toma de decisiones y ahorrar costos de transacción en los procesos de votación.

No obstante, pueden existir mecanismos o diseños en DeFi que se acercan más a ese concepto de *descentralización como sinónimo de operación sin intermediario* o sin una entidad que controle la aplicación. Esto ocurre cuando se utilizan Organizaciones Autónomas Descentralizadas o DAOs, por sus siglas en inglés -*Decentralized Autonomous Organizations*-. Los participantes de una DAO votan sobre los cambios en el protocolo y se alinean a través de incentivos predeterminados y reglas escritas en contratos inteligentes. Las decisiones de gobernanza se ejecutan como transacciones de blockchain, automatizadas y ejecutadas a través de los mecanismos de consenso de la capa de liquidación -en la blockchain-[21]. En esta etapa temprana del desarrollo de las DeFi hay muy pocos o ningún ejemplo de este tipo de implementación en toda la operación de la aplicación. De hecho, los sistemas de votación que hasta ahora se han implementado en el ecosistema DeFi son inmaduros y la participación de los tenedores de *tokens* en procesos de votación es con frecuencia insuficiente[22].

Por ende, no se puede decir que el mundo de las DeFi es realmente descentralizado, al menos no en el sentido jurídico[23], y ni siquiera en el sentido tecnológico, pues la gobernanza de estas aplicaciones no es completamente independiente, automatizada y descentralizada, como ya se explicó. Este controversial concepto de *descentralización* también ha sido ampliamente discutido en otros casos de uso de blockchain[24].

Teniendo esto en cuenta, junto con los riesgos de los que se hablará más adelante, el mundo DeFi todavía tiene bastantes retos que superar y funcionalidades que perfeccionar para realmente competir con una industria financiera madura, debidamente regulada y segura para los consumidores financieros y accionistas de las entidades.

---

[18] The World Economic Forum, DeFi Policy Maker Toolkit (2021), disponible en: https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf

[19] Esto ocurre en mercados de valores tradicionales a través del *proxy voting*. Ver Berdnard S. Black, *Shareholder Activism and Corporate Governance in the United States*, THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW, vol. 3, pp. 459-465 (1998); Bavosa, A, *Delegation and Voting with EIP-712 Signatures* [2020), disponible en: https://medium.com/compound-finance/delegation-and-voting-with-eip-712-signaturesa636c9dfec5e

[20] Esto se hace a través de *claves multisig*, en las que se necesitan múltiples firmas para implementar un cambio. Multisig significa firma múltiple, que es un tipo específico de firmas digitales que hace posible que dos o más usuarios firmen documentos como un grupo. Por lo tanto, se produce una firma múltiple mediante la combinación de varias firmas únicas. La tecnología multisig ha existido en el mundo de las criptomonedas, pero el principio es una que existía mucho antes de la creación de Bitcoin. Binance Academy, ¿Qué es una cartera multisig? (2020). Disponible en: https://academy.binance.com/es/articles/what-is-a-multisig-wallet

[21] Kondova, G., & Barba, R., *Governance of decentralized autonomous organizations* (2019), 15(8) JOURNAL OF MODERN ACCOUNTING AND AUDITING 406.

[22] Sebastian Sinclair, "Uniswap's First Governance Vote Ends in Ironic Failure", Coindesk, (2020). Disponible en: https://www.coindesk.com/uniswaps-first-governance-vote-ends-in-ironic-failure

[23] Se discute en la academia y algunos reportes internacionales (por ejemplo, el World Economic Forum, el FInancial Stability Board y el Banco Internacional de Pagos), qué deberes y tipo de responsabilidad existe en cabeza de los desarrolladores de aplicaciones DeFi respuecto de los tenedores de token. Qué tipo de responsabilidad existe por parte de los que votan en representación de los tenedores de tokens, etc.

[24] Angela Walch, -, en Chris Brummer (Ed.), CRYPTOASSETS, LEGAL, REGULATORY, AND MONETARY PERSPECTIVES (Oxford University Press, 2019). Pg. 39.

2.2 Las diferentes capas de la infraestructura de DeFi

DeFi se diferencia de las finanzas tradicionales en cómo se ejecutan y ofrecen los servicios y productos. Funcionalmente, el producto o actividad suele ser similar a un producto o servicio financiero tradicional -préstamos, seguros, etc.-, pero su forma de ejecución y ofrecimiento es diferente. Las finanzas descentralizadas se ejecutan a través de un conjunto de componentes que usualmente son llamadas DeFi *stack*[25]. En otras palabras, utiliza una infraestructura dividida en múltiples capas. Cada capa tiene un propósito específico. Las capas se construyen unas sobre otras y crean una infraestructura abierta que permite a participantes del ecosistema DeFi construir, repetir o usar partes de las capas en nuevos productos y servicios.

Es importante tener en cuenta que estas capas son jerárquicas. Esto quiere decir que el desempeño de las capas superiores depende de las inferiores. Así las cosas, si, por ejemplo, la capa de liquidación se ve comprometida, todas las capas posteriores no se desempeñarán bien. De manera similar, si la capa base, que usualmente es una red blockchain, como Ethereum, tuviera una estructura más centralizada, cualquier esfuerzo de descentralización en las capas superiores se verá afectado. El siguiente gráfico representa visualmente cómo funcionan estas distintas capas en la infraestructura DeFi.

Fuente: Autor

La capa base o primera capa corresponde a la tecnología que se utiliza para construir la aplicación descentralizada. Actualmente, las aplicaciones DeFi utilizan alguna red blockchain como primera capa[26]. Esto implica que el protocolo nativo de la red blockchain escogida será la base del funcionamiento del caso de uso específico[27]. En esta capa el valor y los

[25] Fabian Schär, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial* (2021), 103.2 THE FEDERAL RESERVE BANK OF SAINT LOUIS OF ST. LOUIS REVIEW 153
[26] Entre las redes de blockchain más usadas para aplicaciones DeFi se encuentran Ethereum, Solana, Cardano, Polygon, Polkadot, Avalanche. Sin embargo, las aplicaciones DeFi más populares en el mercado utilizan como primera capa a Ethereum. Akash Takyar, *Top Blockchains for DeFi*, LeewayHertz (2022), disponible en: https://www.leewayhertz.com/top-blockchains-for-defi/
[27] Por "caso de uso" nos referimos al producto o servicio específico desarrollado. Esto es, préstamos, seguros, derivados, etc.

datos se registran y transfieren a lo largo de cadena de bloques o blockchain de conformidad con el protocolo nativo de la blockchain escogida. Este protocolo es el conjunto de reglas básicas que gobiernan el funcionamiento de cada blockchain[28].

La segunda capa, o capa de activos, consta de todos los activos que se emiten sobre la blockchain[29]. Esto incluye el activo del protocolo nativo, así como cualquier activo adicional que se emita en esta cadena de bloques, generalmente denominados *tokens*. Los activos nativos son los que utiliza la red blockchain escogida para operar. Algunos ejemplos de activos nativos son ETH[30], BTC[31], MATIC[32]. En el ecosistema de los criptoactivos es usual, además, que los desarrolladores creen *tokens* adicionales en las blockchain que cuentan con estándares para crear nuevos criptoactivos. Ejemplos de *tokens* que representan esos estándares son ECR20 o ECR721. Ambos disponibles en la red Ethereum.

La tercera capa corresponde al protocolo que proporciona estándares para casos de uso específicos, como intercambio descentralizado de criptoactivos, mercados de deuda, derivados, gestión de activos, entre otros. Estos estándares generalmente se implementan como un conjunto de contratos inteligentes y cualquier usuario -o aplicación DeFi- puede acceder a ellos. Como tal, estos protocolos son altamente interoperables y pueden ser utilizados posteriormente por otros desarrolladores que quieran construir aplicaciones siguiendo las mismas reglas. Estas reglas son llamadas *smart contracts*, los cuales son públicos con el fin de que sean utilizados y auditados por cualquier interesado[33].

La capa de aplicación implementa los protocolos DeFi en la creación de aplicaciones que se ofrecen a los usuarios de DeFi. Esta es la capa de interacción con el usuario del producto o servicio de finanzas descentralizadas[34]. En otras palabras, la capa de aplicación es la interfaz de usuario que permite a cualquier usuario de DeFi interactuar con la capa de protocolo, independientemente de sus habilidades técnicas. La capa de aplicación es un entorno sin código o programación y suele adoptar la forma de clientes o sitios web a los que se puede acceder a través de cualquier navegador y en los cuales puede operar cualquier usuario.

Por último, la capa de agregación es una extensión de la capa de aplicación. Los agregadores crean plataformas para que los usuarios se conecten a varias aplicaciones y protocolos a la vez. Por lo general, brindan herramientas para comparar y calificar servicios, permiten a los usuarios realizar tareas complejas al conectarse a varios protocolos simultáneamente y combinan información de varias aplicaciones descentralizadas[35].

A continuación presentamos algunos ejemplos de cómo opera este tipo de infraestructura en la práctica.

---

[28] Rauchs, Michel and Glidden, Andrew and Gordon, Brian and Pieters, Gina C. and Recanatini, Martino and Rostand, François and Vagneur, Kathryn and Zhang, Bryan Zheng, *Distributed Ledger Technology Systems: A Conceptual Framework*, The Cambridge Centre for Alternative Finance (2018), disponible en: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf

[29] Buterin, Vitalik. A Next-Generation Smart Contract and Decentralized Application Platform (2013) disponible en:https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[30] Ether (ETH) es el token nativo utilizado por la blockchain Ethereum para verificar transacciones.

[31] BTC es la popular criptomoneda Bitcoin, la cual es la criptomoneda nativa de la red del mismo nombre.

[32] $MATIC es el token nativo de Polygon. Es la criptomoneda de las aplicaciones Polygon que permite a los usuarios interactuar con las dApps que utilizan esa primera capa.

[33] Igor Izraylevych, *What is DeFi: Understanding Decentralized Finance*, SPro Blog (2021), disponible en: https://s-pro.io/blog/what-is-defi#:~:text=Settlement%20Layer&text=The%20settlement%20layer%20is%20formed,to%20real%20estate%20land%20parcels.

[34] The World Economic Forum, DeFi Policy Maker Toolkit (2021), disponible en: https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf

[35] Fabian Schär, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial* (2021), 103.2 THE FEDERAL RESERVE BANK OF SAINT LOUIS OF ST. LOUIS REVIEW 153

Capa	Ejemplo	
Agregadores	Yearn finance: es un grupo de protocolos que se ejecutan en la cadena de bloques de Ethereum que permite a los usuarios optimizar sus ganancias en criptoactivos a través de servicios agregados de préstamos e intercambio de criptoactivos.	
Aplicación (Daap)	Compound	Sushiswap
Protocolo	Compound Tipo de protocolo: préstamos y generación de intereses	En 2020, un usuario llamado Chef Nomi decidió hacer una copia completa del código fuente de Uniswap, y crear una nueva Daap con el nombre de SushiSwap. Esta Daap usaba el mismo protocolo de Uniswap, otra aplicación DeFi. Tipo de protocolo: bolsa de intercambio de criptoactivos descentralizada
Activo	Token nativo: ETH Token de gobernanza: COMP. Este es un token de Ethereum que permite el gobierno comunitario del protocolo Compound.	Token nativo: ETH Token de gobernanza: SUSHI
Ejecución – Liquidación	Ethereum	Ethereum

Fuente: Autor

2.3 Arquitectura abierta de DeFi

La arquitectura abierta significa que hay una amplia disponibilidad del código fuente subyacente para protocolos DeFi y que existen *Application Programming* Interfaces -API- abiertas[36], de la misma forma que existe en los esquemas de banca abierta para servicios financieros tradicionales, para exponer la operabilidad y datos de estas aplicaciones a terceros desarrolladores de otros servicios. Esto permite que el ecosistema DeFi tenga una infraestructura flexible y altamente componible[37]. Este tipo de arquitectura también permite programabilidad, personalización y ampliación dinámica del tipo de aplicaciones, productos o servicios que pueden ser ofrecidos a los usuarios. Esta es una importante diferencia con el mundo de los servicios financieros tradicionales en el que no es usual que el diseño de los productos sea compartido entre varias entidades que incluso pueden ser competidoras.

El uso de código fuente abierto en DeFi permite a los participantes –desarrolladores, usuarios e incluso autoridades financieras y auditores– ver y verificar los protocolos y las reglas de juego de cada aplicación descentralizada directamente. Esta disponibilidad del código también permite crear nuevas aplicaciones simplemente bifurcándolo[38] o crear servicios derivados o competitivos.

[36] Nydia Remolina, *Open Banking: Regulatory Challenges for a New Form of Financial Intermediation in a Data-Driven World*, SMU CENTRE FOR AI & DATA GOVERNANCE RESEARCH PAPER No. 2019/05 (2019).
[37] Que puede componerse o formarse uniendo varios elementos, de acuerdo con el diccionario de la lengua española. Ver https://dle.rae.es/componible
[38] Tomar el código fuente y crear un desarrollo independiente. A través de procesos que se conocen como "forks" un código abierto puede ser bifurcado para crear otra aplicación. Un caso famoso de este tipo de bifurcaciones es Sushiswap, que nació de un fork de Uniswap, otra aplicación descentralizada para intercambio de criptoactivos. Este ejemplo fue mencionado en la subsección anterior de este capítulo.

3. Comparación entre algunos productos financieros tradicionales y su paralelo en DeFi

3.1 Diferencias entre DeFi y productos financieros tradicionales

Funcionalmente, los productos y servicios que se ofrecen a través de DeFi pueden parecer muy similares a productos y servicios financieros tradicionales, como por ejemplo un préstamo o un seguro. Sin embargo, es importante tener en cuenta algunas diferencias funcionales clave entre el mundo de los servicios financieros tradicionales y las finanzas descentralizadas, pues no necesariamente los productos y servicios ofrecidos son sustitutos perfectos[39].

Una primera diferencia tiene que ver con las unidades de cuenta. Los servicios financieros tradicionales están denominados en moneda de curso legal o, en algunos casos, en divisas. Por ejemplo, si un consumidor financiero solicita un préstamo al banco, este préstamo estará denominado en la moneda de curso legal del país o en algunos casos en alguna divisa. Si la entidad financiera aprueba el crédito, desembolsará los recursos con la expectativa de que el deudor cancele su deuda también en moneda de curso legal o en la divisa pactada. En DeFi, el usuario recibe criptoactivos, por lo que igualmente debe pagar el crédito y constituir la garantía con activos digitales.

En segundo lugar, la ejecución de las operaciones en Defi se realiza a través de reglas programadas *ex ante* a través de contratos inteligentes. Los servicios financieros tradicionales dependen para su ejecución de una entidad financiera.

En tercer lugar, el proceso de cumplimiento, compensación y liquidación de las operaciones en DeFi se completa en la red de blockchain o primera capa de la infraestructura DeFi. En los servicios financieros tradicionales, cumplimiento, compensación y liquidación están soportados en la infraestructura relacionada con el servicio o producto específico. Por ejemplo, el sistema de pagos de bajo valor si se trata de transacción con algún medio de pago.

En cuarto lugar, en teoría, cualquier persona podría auditar el código abierto de las aplicaciones DeFi, pues el hecho de ser abierto significa que es accesible para todo el público. No obstante, probablemente la mayoría de usuarios en un mercado minorista o *retail* no tendrían el conocimiento suficiente para realizar dicha auditoría. En el mundo de los servicios financieros tradicionales, la entidad prestadora del servicio financiero requiere de terceras partes que actúen como auditores. Además, si una entidad financiera tradicional usara *smart contracts* para el ofrecimiento de algún producto financiero, seguramente no utilizaría código abierto sino patentado.

En quinto lugar, la interacción y componibilidad con otros servicios en las finanzas tradicionales es generalmente limitada, particularmente si se trata de productos ofrecidos por entidades competidoras. La *composability* o *componibilidad* de DeFi hace referencia a la capacidad de

[39] Los bienes sustitutos perfectos son aquellos que pueden satisfacer la misma necesidad de igual forma. Dos bienes sustitutos perfectos son vistos de la misma forma por el consumidor.

crear aplicaciones y productos nuevos a partir de protocolos y códigos abiertos existentes. Esto está cambiando con algunas tendencias como las finanzas abiertas, también llamadas *Open Finance*. En los esquemas de *Open Finance,* las entidades financieras abren los datos que controlan y/o su infraestructura a terceros desarrolladores para que estos creen nuevos productos financieros apalancándose en las entidades financieras tradicionales[40].

Cabe resaltar que estas diferencias no hacen referencia al cumplimiento regulatorio o la exposición de riesgos a la que se encuentran expuestas las aplicaciones DeFi. Esto será materia de discusión en secciones posteriores de este capítulo.

3.2 Algunos casos de uso de DeFi

3.2.1 Operaciones de crédito

Las operaciones de crédito de DeFi reemplazan la función de intermediación de los proveedores de servicios financieros con reglas automatizadas a través de contratos inteligentes[41]. Esto significa que la aplicación descentralizada ya está programada para asignar una tasa de interés dependiendo del monto del colateral -garantía- entregado por el usuario. Igualmente, la aplicación descentralizada liquida anticipadamente la garantía para asegurar el pago del préstamo cuando el valor de la misma cae en el mercado hasta un monto predefinido. Tanto el colateral como el crédito se encuentran denominados en criptoactivos. Los usuarios entregan activos digitales como garantía -principalmente *stablecoins* y criptoactivos relativamente líquidos y con niveles de capitalización de mercado altos-, y pueden simplemente cobrar intereses sobre el valor de lo entregado o pedir prestado contra lo entregado como una garantía.

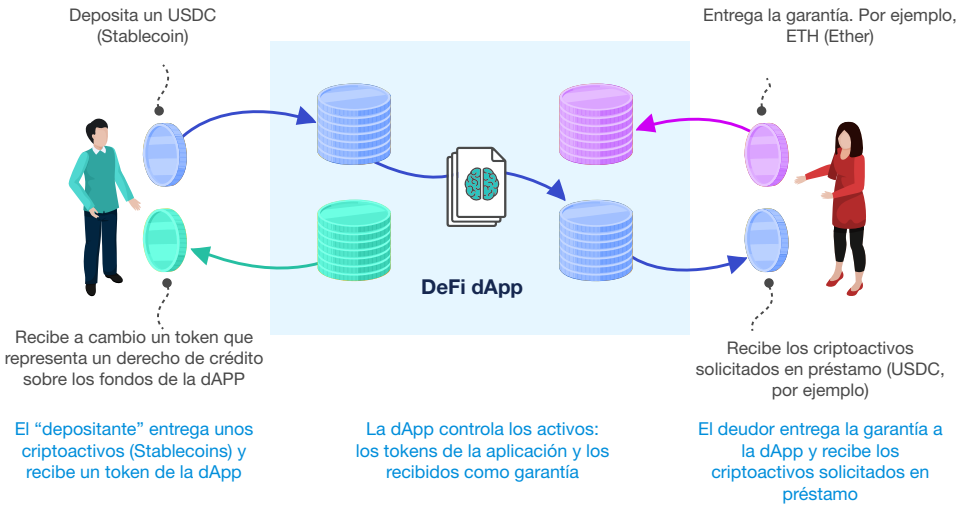
Debido a esta automatización relativamente simple de las condiciones de la operación, en los créditos DeFi no se analiza la información o historia crediticia de un deudor. Esto, aunado a la alta volatilidad de los criptoactivos, conlleva en la práctica que, por regla general, los créditos en DeFi están sobregarantizados. Es decir, la garantía exigida representa un valor más alto que el préstamo[42]. Por ejemplo, una de las DeFi más usadas, Maker, puede pedir hasta 68.966 dólares de DAI[43] contra 100.000 dólares de ETH[44]. Si no se cumple esta relación, la aplicación procede a liquidar la garantía hasta que se cumple una relación del 145%.

Actualmente, la mayoría de los criptoactivos son altamente volátiles. La criptomoneda más popular, bitcoin, ha perdido alrededor del 70% de su valor desde que alcanzó un máximo histórico de aproximadamente US$69,000 en noviembre de 2021. Todo el criptomercado se ha visto afectado por esta tendencia. La capitalización de mercado general de los criptoactivos se ha reducido a menos de US$1 billón desde su pico de 2021 de US$3 billones[45]. Es decir, se ha esfumado un valor mayor al de la economía colombiana, en términos de PIB. Esto aumenta el riesgo de crédito, pues si la garantía es tan volátil, de alguna forma se debe

[40] Nydia Remolina, *Open Banking: Regulatory Challenges for a New Form of Financial Intermediation in a Data-Driven World*, SMU CENTRE FOR AI & DATA GOVERNANCE RESEARCH PAPER No. 2019/05 (2019)
[41] Max Wolff, *Introducing Marble: A Smart Contract Bank* (2018). Disponible en: https://medium.com/marbleorg/introducing-marble-a-smart-contract-bank-c9c438a12890; Ernesto Boado, *Aave Protocol* Whitepaper (v1.0) (2020). Disponible en: https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf.
[42] Gudgeon, Lewis, Sam Werner, Daniel Perez, and William J. Knottenbelt. "Defi protocols for loanable funds: Interest rates, liquidity and market efficiency." *In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pp. 92-112. 2020. DAI es una criptomoneda. Más específicamente una stablecoin cuyo valor está anclado al dólar (USD).
[43] El desarrollador de esta criptomoneda es MakerDAO, una aplicación de finanzas descentralizadas.
[44] ETH es una criptomoneda también llamada Ether. Esta es la criptomoneda de la blockchain Ethereum.
[45] Coinmarketcap. https://coinmarketcap.com/

mitigar el riesgo de impago por parte de la aplicación descentralizada. El riesgo de impago se mitiga gracias a un mecanismo, también automatizado a través de contratos inteligentes, de liquidación anticipada de la garantía[46]. Esto hace que la aplicación liquide la garantía de forma anticipada para pagar el crédito si así se requiere.

Si la automatización funciona de forma correcta, no debería materializarse el riesgo de crédito. A continuación, se muestra en un diagrama un ejemplo ilustrado de un caso de este tipo de operaciones de DeFi.



Fuente: autor y Radix Blog (2022)

Si bien la mayoría de operaciones son sobregarantizadas, en las finanzas descentralizadas también existen préstamos sin garantía, aunque se encuentran en una etapa temprana de desarrollo. Estos son conocidos como *flash loans*, en los cuales los activos se toman prestados y se reembolsan -con intereses- en un solo bloque de la blockchain. De esta forma, tecnológicamente es necesario cumplir la operación en un solo bloque, lo cual elimina el riesgo de impago, pues si el deudor no pudiese devolver los criptoactivos que le han sido entregados en préstamo, nunca quedaría registrada la operación en la blockchain y, en la práctica, al menos desde el punto de vista tecnológico, se podría decir entonces que la operación nunca existió[47].

[46] David McNeil, What is Liquidation in DeFi Lending and Borrowing?, Coinmonks (2021). Disponible en: https://medium.com/coinmonks/what-is-liquidation-in-defi-lending-and-borrowing-platforms-3326e0ba8d0#:~:text=In%20traditional%20finance%2C%20liquidation%20occurs,collateral%20to%20back%20the%20debtdor.

[47] Fabian Schär, *Decentralized Finance*: On Blockchain- and Smart Contract-Based Financial (2021), 103.2 THE FEDERAL RESERVE BANK OF SAINT LOUIS OF ST. LOUIS REVIEW 153.

3.2.2 *Stablecoins*

Debido a la alta volatilidad de los criptoactivos, hace algunos años se empezaron a ofrecer en el mercado las *stablecoins* -monedas estables-, que buscan mantener el valor de un criptoactivo a través de un mecanismo de estabilización. Algunas de las más populares en el mercado de criptoactivos lo hacen atando su valor al valor del dólar estadounidense. Las *stablecoins* que utilizan como mecanismo de estabilización una canasta de activos muy líquidos o divisas no se consideran servicios DeFi en sí mismas, porque implican una custodia centralizada del mecanismo de estabilización, así como un centralizador de la reserva de fondos, ya sea de divisas o de activos líquidos.

Sin embargo, existe otro tipo de *stablecoins* que sí se considera parte del mundo de las finanzas descentralizadas. En primer lugar, están las que utilizan contratos inteligentes para agregar y liquidar activos digitales de forma automatizada. A través de estas operaciones se espera que se estabilice el valor de la *stablecoin*. En segundo lugar, existen las algorítmicas, que se valen de algoritmos a través de los cuales se programan operaciones de contracción y expansión de la *stablecoin*. Mediante el control de la oferta de la *stablecoin* en el mercado, debería poder estabilizarse su valor[48].

3.2.3 Bolsas de criptoactivos descentralizadas

Las aplicaciones de finanzas descentralizadas que ofrecen el servicio de intercambio de criptoactivos permiten a los usuarios intercambiar un critpoactivo por otro sin tener que utilizar el servicio de una bolsa centralizada como Coinbase o Binance. A diferencia de los intercambios centralizados, los protocolos de intercambio descentralizado -también conocidos como DEX- son servicios DeFi porque no toman la custodia de los activos de los usuarios y es posible que no controlen otros aspectos del proceso, como la gestión de compras y ventas de criptoactivos[49].

4. Oportunidades en DeFi

4.1 Inclusión financiera

Uno de los potenciales beneficios que más se citan al hablar del lado positivo de DeFi está relacionado con la inclusión financiera y la capacidad de DeFi para atender a sectores desatendidos de la población, como las pymes. Según los defensores de tales supuestos beneficios, DeFi podría reemplazar algunos servicios bancarios y revisar la inflexibilidad de los procesos actuales, lo que permitiría a las pymes aprovechar una mayor liquidez y oportunidades de crédito alternativas[50].

No obstante, este tipo de argumentos no ha sido comprobado empíricamente. Para que una pyme pueda, por ejemplo, usar un servicio DeFi de préstamos, necesita tener criptoactivos para entregar en garantía, lo que implica estar expuesta a la volatilidad del precio, salvo que

[48] Jarno, Klaudia, and Hanna Kołodziejczyk, *Does the design of stablecoins impact their volatility?*, JOURNAL OF RISK AND FINANCIAL MANAGEMENT 14.2 (2021): 42.
[49] Matthias Funke, *New Decentralised Finance Stacks, Alternatives to Ethereum*, Coinmonks (2021). Disponible en: https://medium.com/coinmonks/new-decentralised-finance-stacks-alternatives-to-ethereum-abe74ecf53f9
[50] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (2022). Disponible en: https://www.oecd.org/finance/why-decentralised-finance-defi-matters-and-the-policy-implications.htm

decida usar *stablecoins* que sean realmente estables. En este escenario, la pyme podría acceder a un crédito de criptoactivos sin necesidad de una evaluación de su perfil de riesgo.

No obstante, esto también implica que la pyme se enfrente a barreras importantes como las relacionadas con tener conocimiento suficiente del mercado de criptoactivos y su tecnología. Así como una comprensión de los servicios DeFi que, en ocasiones, pueden resultar sofisticados para el consumidor financiero promedio.

4.2 Automatización

La automatización a través del uso de algoritmos y contratos inteligentes vista en casos de uso relacionados con servicios financieros es una realidad demostrada en la práctica por los proveedores de servicios de DeFi. El uso de estas tecnologías le resultará útil al sector financiero en general, para hacer más eficiente su operación y reducir costos en el ofrecimiento de servicios financieros.

Adicionalmente, la automatización de algunas operaciones puede ayudar a resolver disputas de una forma más eficiente y, por ejemplo, en operaciones de crédito podría contribuir a mitigar riesgos de contraparte a través de la automatización en la ejecución de algunas operaciones.

4.3 DeFi y el metaverso

El desarrollo de las finanzas descentralizadas tendrá un impacto en la prestación de servicios financieros en el mundo digital. Varios conglomerados financieros a nivel mundial han empezado a explorar cómo se vería ese futuro de las finanzas en un mundo virtual como el metaverso. Las transacciones con activos digitales y criptoactivos serán imprescindibles en un metaverso que pretenda ofrecer servicios financieros y transacciones económicas y jurídicas con los debidos efectos en el mundo real. El mundo de las finanzas descentralizadas de alguna forma ya ha adquirido algo de experiencia sobre cómo realizar transacciones con activos digitales.

No obstante, DeFi está en una etapa temprana de desarrollo y aún quedan muchos desafíos por resolver para que estos y otros potenciales beneficios se vean en la práctica.

5. Desafíos de DeFi

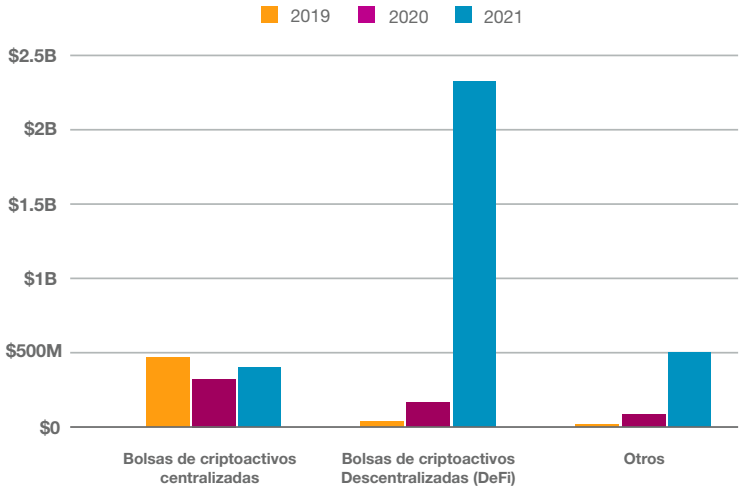
5.1 Lavado de activos y financiación del terrorismo

En 2021, el crimen basado en criptomonedas alcanzó un nuevo máximo histórico, con direcciones ilícitas que recibieron US$14 mil millones en el transcurso del año, frente a US$7,8 mil millones en 2020. No obstante, la regulación en algunos países de las bolsas centralizadas de criptoactivos ha empezado a dar frutos en cuanto a la implementación de políticas de conocimiento del cliente y reporte de transacciones sospechosas en estos mercados.

En contraste con lo que empieza a evidenciarse en el mundo de los proveedores de servicios de criptomonedas que operan de forma centralizada, el mundo DeFi asume un papel más

importante en el lavado de activos y la financiación del terrorismo. En 2021, las cifras mostraron un aumento del 30% en la actividad de lavado de dinero con respecto a 2020. En general, los ciberdelincuentes han lavado más de US$33 mil millones en criptomonedas desde 2017[51].

Valor anual de criptoactivos robados por tipo de víctima (en USD)



Fuente: Chainalysis (2022)

Esto se debe a que la participación en plataformas DeFi solo requiere conexión a una billetera de critpoactivos, y algunas billeteras carecen de controles de conocimiento del cliente para su apertura. Este es un desafío evidente al que se enfrentan reguladores al tratar de mitigar el riesgo de lavado de activos en estos mercados.

Desde el año 2014, el Grupo de Acción Financiera Internacional -GAFI- viene estudiando la interrelación entre el lavado de activos y el mercado de criptomonedas[52]. Las recomendaciones para mitigar dicho riesgo en este contexto van orientadas a exigir a los prestadores de servicios de criptoactivos[53] que identifiquen a quienes realizan transacciones con criptomonedas cuando sea posible, lo que generalmente es cuando el proveedor del servicio tenga la custodia de los activos digitales depositados en las billeteras[54]. Esta aproximación resulta problemática en el mundo de los servicios DeFi si se tiene en cuenta que muchas aplicaciones descentralizadas no son controladas por una persona jurídica. En algunas ocasiones el código de la aplicación es simplemente desarrollado por un programador o desarrollador. La recomendación de GAFI ha estado orientada al licenciamiento de entidades que controlen las DeFi, como desarrolladores o tenedores de *tokens* en algunos casos. No obstante, debido a lo explicado en la sección sobre el espectro de la descentralización, en algunos casos no será posible determinar quién es el proveedor del servicio. En esos casos no habrá posibilidad de identificar a los usuarios de las aplicaciones.

[51] The Chainalysis 2022 Crypto Crime Report.
[52] Financial Action task Force, *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (2014). Disponible en: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.
[53] Virtual Asset Service Providers.
[54] Financial Action task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (2021). Disponible en: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

5.2 Protección al consumidor financiero y a los inversionistas

La falta de transparencia respecto de los derechos de veto que tienen los desarrolladores, la falta de regulación de los servicios DeFi, la poca información disponible sobre los riesgos de mercado -las altas volatilidades-, operacionales -las fallas en los protocolos, en el código abierto o ataques de ciberseguridad-, y la falta de educación financiera y tecnológica sobre el ecosistema DeFi debilitan la protección al consumidor de este tipo de servicios[55].

Igualmente, la falta de supervisión del mundo DeFi permite que algunos de estos prestadores de servicio quiebren sin ningún tipo de liquidación o resolución ordenada, procedimiento que sí está regulado para el sector financiero. Esta circunstancia, aunada a que los sistemas de justicia alrededor del mundo aún no han podido encontrar formas suficientemente eficaces para recuperar los criptoactivos robados en *hackeos* de plataformas o billeteras de usuarios, demuestran que hay todavía mucho camino por recorrer para que en el ecosistema DeFi se proteja efectivamente a los consumidores financieros.

Por último, el colapso de algunos casos de uso de DeFi ha demostrado que la falta de supervisión y reglas claras sobre la operatividad y manejo de riesgos de estas aplicaciones ponen en juego la protección de los consumidores. Un ejemplo reciente es el colapso de algunas *stablecoins* en mayo de 2022, durante lo que se conoció como el *criptoinvierno* o *cryptowinter*. El más famoso fue probablemente el de TerraUSD, una de las *stablecoins* más populares del 2021. En este caso, el algoritmo falló en su tarea de estabilización del precio y nadie pudo detener el colapso –hasta prácticamente llegar a un precio de casi cero–. El colapso ocurrió de forma acelerada debido a la pérdida de confianza en el mecanismo de estabilización por parte del mercado causando una situación muy similar a la de una corrida de depósitos[56]. Este episodio trajo como consecuencia que reguladores en diferentes jurisdicciones y el público en general comprobaran que las *stablecoins* no son tan estables como aseguran los desarrolladores al promocionarlas y ofrecerlas a potenciales compradores, y que si bien el uso de la tecnología puede ayudar en la estabilización del precio, al final del día la confianza del mercado en el sistema, la supervisión financiera y mitigación de riesgos resultan fundamentales.

5.3 Gobierno corporativo

En torno al gobierno corporativo existen varios riesgos debido a la forma como se estructuran las aplicaciones de finanzas descentralizadas. Dada la multiplicidad de actores involucrados en la gobernanza de las aplicaciones –desarrolladores o programadores, tenedores de *tokens*, representantes de los tenedores de *tokens* para votaciones, etc.– resulta compleja la asignación de deberes en las distintas relaciones de agencia que pueden presentarse. Esto sin tener en cuenta la multiplicidad de capas que componen la infraestructura de los servicios DeFi. La misma dificultad se materializa en la asignación de responsabilidades si algo sale mal con la aplicación descentralizada. Problemas de este tipo relacionados con gobierno corporativo ya se han materializado.

[55] En algunos casos el usuario puede ser considerado un inversionista. Por ejemplo, si los criptoactivos o tokens tienen la categoría de valor. Esto dependerá de la definición de valor aplicable en cada jurisdicción.
[56] Zeke Faux y Muyao Shen, *A $60 Billion Crypto Collapse Reveals a New Kind of Bank Run*, Bloomberg Finance (2022). Disponible en: https://www.bloomberg.com/news/articles/2022-05-19/luna-terra-collapse-reveal-crypto-price-volatility.

Por ejemplo, en octubre de 2021, una actualización de la plataforma de préstamos Compound introdujo un error que distribuyó incorrectamente intereses por valor de US$90 millones a algunos usuarios. El fundador de la plataforma publicó en Twitter que *(n)o hay controles administrativos ni herramientas comunitarias para deshabilitar la […]* distribución[57]. En las finanzas tradicionales, las transferencias erróneas podrían impugnarse ante los tribunales y se podría recuperar ese dinero. Este panorama no es claro en el contexto de las finanzas descentralizadas debido a que la recuperabilidad de criptoactivos a través de procesos judiciales es todavía un terreno inexplorado a nivel mundial.

Aunado a lo anterior, ciertos diseños de DeFi y de blockchain favorecen la concentración del poder de decisión en manos de los grandes tenedores de *tokens* y esto puede prestarse para conductas anticompetitivas en la validación de transacciones[58]. En otras palabras, aumenta el riesgo de que una pequeña cantidad de validadores grandes puedan adquirir suficiente poder para alterar la cadena de bloques con el fin de obtener ganancias financieras. Además, los grandes validadores podrían congestionar la cadena de bloques con intercambios artificiales entre sus propias billeteras -intercambios de lavado-, aumentando considerablemente las tarifas que les pagan otros participantes por la validación de transacciones[59].

5.4 Ciberseguridad

El ecosistema DeFi ha perdido más de UD$1,000 millones a manos de *hackers* durante abril y mayo de 2022[60]. Según las últimas estadísticas, en el primer trimestre de 2022 se robaron aproximadamente US$1,600 millones en criptomonedas de las plataformas DeFi. Además, más del 90% de todo lo robado en criptomonedas procede de protocolos DeFi *hackeados*[61]. Esto pone de manifiesto el impacto que la materialización de este riesgo representa para la sostenibilidad del ecosistema.

Una de las razones por las cuales las aplicaciones de DeFi son un blanco atractivo para los ciberdelincuentes es el uso de código abierto. Si bien esto representa ventajas, como la posibilidad de auditar el código por parte de cualquier persona, o la posibilidad de utilizarlo para construir con base en este otros productos y servicios, lo cierto es que también es auditado por delincuentes para encontrarle fallas que puedan aprovechar en ciberataques.

Para evitar esto se requiere elevar los estándares de la industria y determinar responsabilidades sobre quién debe implementar esos estándares más altos, que podrían estar relacionados con, por ejemplo, implementar un mantenimiento y actualizaciones rutinarias del código abierto. Sin embargo, el mantenimiento y las actualizaciones de rutina pueden ser más difíciles de implementar para los servicios descentralizados, o pueden crear vulnerabilidades, especialmente dada la componibilidad de DeFi.

[57] *BIS Quarterly Review 2021*, Banco Internacional de Pagos. Disponible en: https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf
[58] Ibid
[59] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (2022). Disponible en: https://www.oecd.org/finance/why-decentralised-finance-defi-matters-and-the-policy-implications.htm
[60] Elizabeth Gail, *Aumentan los ataques a DeFi - ¿Podrá el sector frenar la oleada?*, Cointelegraph (2022). Disponible en: https://es.cointelegraph.com/news/defi-attacks-are-on-the-rise-will-the-industry-be-able-to-stem-the-tide.
[61] Ibid.

CUANDO TU CÓDIGO ES UN COMPLETO DESASTRE PERO SIGUE FUNCIONANDO

Fuente: Internet

Mitigar el riesgo de ciberseguridad es crucial para el desarrollo exitoso de las finanzas descentralizadas. Sólo en el año 2021, los robos de criptoactivos en aplicaciones DeFi aumentaron 1330% respecto del año anterior[62].

5.5 Riesgo sistémico

Si bien en la actualidad DeFi está en gran medida separado del sistema financiero tradicional, las conexiones podrían aumentar. No obstante, hasta ahora, un enfoque regulatorio conservador ha restringido la participación de los bancos en el ecosistema de los criptoactivos. De hecho, el Comité de Supervisión Bancaria de Basilea ha publicado para comentarios una propuesta de recomendaciones para el tratamiento de las exposiciones a criptoactivos en la ponderación por nivel de riesgo que se utiliza para el cálculo de los requerimientos de capital. Estas recomendaciones en materia prudencial pretenden desincentivar la participación de los bancos en estos mercados altamente volátiles[63].

A pesar de la poca interconexión con el sistema financiero tradicional, el crecimiento de DeFi podría plantear riesgos que afecten la estabilidad financiera si esta situación cambia. La prociclicidad asociada a los cambios en el valor de las garantías y fluctuaciones en los márgenes asociados puede representar un riesgo que afecte la estabilidad del sistema financiero tradicional si las finanzas descentralizadas se conectan más con él. Dado que

[62] The Chainalysis 2022 Crypto Crime Report.
[63] Comité de Supervisión Bancaria de Basilea, Basel Committee publishes second consultation document on the prudential treatment of banks' cryptoasset exposures (2022). Disponible en: https://www.bis.org/press/p220630.htm#:~:text=to%20media%20resources.-,Basel%20Committee%20publishes%20second%20consultation%20document%20on,treatment%20of%20banks'%20cryptoasset%20exposures&text=The%20Basel%20Committee's%20second%20public,consultation%20issued%20in%20June%202021

los precios de las garantías caen y los márgenes aumentan en momentos de dificultad, a menudo surgen espirales descendentes de precios que podrían extenderse al resto del sistema financiero[64]. Debido a la naturaleza en gran medida autónoma de DeFi, los episodios de desapalancamiento rápido hasta ahora han tenido poco efecto fuera de los mercados de criptoactivos.

Por otro lado, las *stablecoins*, especialmente aquellas cuyo uso se pueda extender globalmente, podrían conllevar riesgos para la estabilidad financiera[65]. Si los riesgos concomitantes no se gestionan bien, las *stablecoins* son propensas al mismo fenómeno conocido en el sector bancario como corrida de depósitos, lo que comprometería su capacidad para transferir fondos dentro del ecosistema DeFi. Además, las posibles liquidaciones por parte de una *stablecoin* de sus activos de reserva podrían generar choques para las empresas y los bancos, con un impacto potencialmente grave en el sistema financiero y la economía en general[66]. Estos riesgos se ven agravados por el hecho de que los usuarios usan las *stablecoins* como un medio de pago[67], aunque no son ni dinero del banco central ni dinero de los bancos comerciales.

Dado que los principales desafíos en DeFi se asemejan a los de las finanzas tradicionales, las respuestas regulatorias diseñadas para el sector financiero tradicional pueden ser una guía para mitigar estos riesgos en el ecosistema DeFi. Por supuesto, debería aplicarse el principio básico de *mismos riesgos, mismas reglas*, sobre todo para contrarrestar el arbitraje regulatorio, que también afecta la estabilidad del sistema financiero.

6. Respuestas regulatorias y de supervisión

Las respuestas regulatorias y de supervisión dirigidas específicamente a los servicios DeFi son muy limitadas. Los reguladores y supervisores a nivel mundial apenas están tratando de entender cómo funciona esta nueva forma de ofrecer servicios financieros, o servicios similares a los financieros, y cómo aproximarse a estas aplicaciones para proteger a los consumidores, la estabilidad del sistema y prevenir el lavado de activos.

Las guías de GAFI y reguladores en jurisdicciones como Estados Unidos, la Unión Europea, Singapur, Corea del Sur, Japón, Reino Unido, entre otros, se han encargado de implementar regímenes de licenciamiento para proveedores de servicios de criptoactivos. No obstante, estas normas están generalmente pensadas para proveedores de servicios centralizados como los proveedores de billeteras y las bolsas tradicionales[68] de intercambio de criptoactivos. Adicionalmente, estos marcos normativos generalmente se centran en mitigar los riesgos de lavado de activos y financiación del terrorismo, y algunos de ellos en los riesgos asociados a la ciberseguridad. Pero no es claro si son aplicables o cómo lo serían a las DeFi. Tampoco abordan generalmente los otros tipos de riesgos señalados en la sección anterior.

---

[64] *BIS Quarterly Review 2021*, Banco Internacional de Pagos. Disponible en: https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf
[65] Financial Stability Board, Regulation, *Supervision and Oversight of "Global Stablecoin*" Arrangements (2020). Disponible en: https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/
[66] Douglas Arner, Raphael Auer and John Frost, *Stablecoins: risks, potential and regulation* (2020), FINANCIAL STABILITY REVIEW, BANCO DE ESPAÑA, no 39.
[67] *BIS Quarterly Review 2021*, Banco Internacional de Pagos. Disponible en: https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf
[68] Tradicionales en oposición a las DEX.

A pesar de estas limitaciones, algunas reacciones de organismos internacionales, reguladores y supervisores respecto de la evolución del sector de las finanzas descentralizadas podrían indicar hacia dónde van las respuestas regulatorias a esta innovación. Por un lado, el Comité de Pagos e Infraestructuras de Mercado y la Organización Internacional de Comisiones de Valores -IOSCO- publicaron para consulta en 2021 una guía preliminar que confirma y aclara que las *stablecoins* de importancia sistémica deben observar los estándares internacionales para los sistemas de pago, compensación y liquidación. De acuerdo con este documento, la función de transferencia de una *stablecoin* -la funcionalidad del activo digital gira en torno a servir de medio de transferencia de valor de una parte a otra- es *comparable* a esa misma función realizada por otros tipos de infraestructuras del mercado financiero[69]. No obstante, no es claro si alguna de las *stablecoins* que operan actualmente se considera sistémicamente importante.

Por otro lado, GAFI aclaró en el año 2021 que los creadores, dueños y operadores de las aplicaciones descentralizadas de DeFi, así como las personas que mantienen el control o la influencia suficiente en las aplicaciones DeFi, incluso si parecen descentralizadas, pueden caer bajo la definición de un prestador de servicios de criptoactivos[70]. Esto implicaría que deben solicitar una licencia en la jurisdicción de competencia y cumplir con las obligaciones de conocimiento del cliente y reporte de transacciones sospechosas con el fin de mitigar el riesgo de lavado de activos y financiación del terrorismo.

En 2022, el Financial Stability Board publicó un reporte para el G20 sobre los riesgos de los criptoactivos para la estabilidad financiera e incluyó algunos de los problemas asociados a DeFi. No obstante, no hay aún un marco de recomendaciones para abordar esta problemática[71].

Ahora, algunas jurisdicciones han dado indicaciones sobre cómo deberían regularse ciertos aspectos de las finanzas descentralizadas. No obstante, no hay marcos regulatorios ni propuestas suficientemente comprensivas de todos los riesgos. Por ejemplo, en Estados Unidos, el Grupo de Trabajo del Presidente sobre Mercados Financieros, la Corporación Federal de Seguros de Depósitos -FDIC[72], por sus siglas en inglés- y la Oficina de Control de la Moneda -OCC-[73] por sus siglas en inglés- han manifestado que se debe exigir a los emisores de *stablecoins* que operen cubiertos por el seguro de depósito y sujetos a supervisión federal como una entidad bancaria[74].

Bajo una aproximación similar, el Ministerio del Tesoro de Reino Unido publicó una consulta para comentarios en la que propone que el Banco de Inglaterra adquiera competencia sobre las *stablecoins* en quiebra para evitar que una crisis de criptoactivos afecte la estabilidad financiera. Bajo este supuesto, los emisores de *stablecoins* serían puestos bajo administración especial por parte del Banco para proteger a los consumidores en caso de

[69] Banco Internacional de Pagos, CPMI and IOSCO publish guidance, call for comments on stablecoin arrangements (2021). Disponible en: https://www.bis.org/press/p211006.htm
[70] Financial Action Task Force, *Updated Guidance for a Risk-Based Approach. Virtual Assets and Virtual Assets Service Providers* (2021). Disponible en: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf
[71] Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-assets* (2022). Disponible en: https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/
[72] Federal Insurance Deposit Commission.
[73] Office of the Comptroller of the Currency.
[74] Office of the Comptroller of the Currency, Statement by the Acting Comptroller of the Currency on the Report on Stablecoins (2021). Disponible en: https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-112.html

resolución de la entidad[75].

Adicionalmente, atendiendo las recomendaciones de GAFI en materia de DeFi, Singapur ha impulsado una reforma a su ley de Pagos Digitales. En este cuerpo normativo es donde se encuentra regulada la prestación de servicios de criptoactivos[76].

Por último, algunas jurisdicciones, si bien no se han pronunciado específicamente sobre DeFi, han decidido prohibir todo tipo de actividad o servicio relacionado con criptoactivos. Este es el caso de Egipto, Irak, Qatar, Omán, Marruecos, Argelia, Túnez, Bangladesh y China. Otros cuarenta y dos países, incluidos Argelia, Bahrein, Bangladesh y Bolivia, han prohibido implícitamente las monedas digitales al imponer restricciones a la capacidad de los bancos para tratar con criptomonedas o al prohibir los intercambios de criptomonedas.

7. Conclusiones

En este capítulo se ha abordado en detalle el concepto de DeFi al explicar su infraestructura y comparar los servicios de finanzas descentralizadas con el mundo de los servicios financieros tradicionales. Los servicios DeFi y los servicios financieros tradicionales parecen similares funcionalmente, pero a la vez son tan diferentes funcionalmente que no podrían considerarse sustitutos perfectos. ¿Son entonces las finanzas descentralizadas realmente disruptivas para el sector financiero tradicional? Esa es una pregunta que escapa el análisis de este capítulo, pero lo que sí podemos concluir es que DeFi es una innovación cada vez más utilizada y, por ende, se hace necesario entender de qué se trata para abordar los posibles riesgos a los que estarían expuestos el sistema financiero y los consumidores de ese tipo de servicios.

No obstante, DeFi no sólo conlleva riesgos, sino que también puede potencialmente traer beneficios en materia de innovación, inclusión financiera, reducción de costos, entre otros. Para aprovechar de la forma más eficiente estos beneficios es menester abordar los riesgos y diseñar políticas regulatorias que conduzcan a un adecuado balance entre la promoción de la innovación y la consecución de los objetivos de la regulación financiera. Esta será una tarea difícil para los reguladores a nivel mundial teniendo en cuenta que DeFi es un área nueva y de rápido crecimiento, cuyos servicios operan de forma transfronteriza gracias a la digitalización con una variedad de cuestiones económicas, técnicas, operativas y legales sin resolver. Esperamos que este capítulo contribuya a enriquecer el debate con el fin de construir soluciones eficaces para el futuro.

[75] HM Treasury, Managing the failure of systemic digital settlement asset (including stablecoin) firms: Consultation (2022). Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1079348/Stablecoin_FMISAR_Consultation.pdf

[76] Payment Services (Amendment) Bill. Disponible en: https://www.mas.gov.sg/news/speeches/2021/payment-services-amendment-bill

Bibliografía

Arner, Douglas; Auer, Raphael, and Frost, John, *Stablecoins*: *risks, potential and regulation* (2020), FINANCIAL STABILITY REVIEW, BANCO DE ESPAÑA, no 39.

Banco Internacional de Pagos, *BIS Quarterly Review 2021*, Banco Internacional de Pagos. Disponible en: https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf

Banco Internacional de Pagos, *CPMI and IOSCO publish guidance, call for comments on stablecoin arrangements* (2021). Disponible en: https://www.bis.org/press/p211006.htm

Bavosa, Adam, *Delegation and Voting with EIP-712 Signatures* [2020), disponible en: https://medium.com/compound-finance/delegation-and-voting-with-eip-712-signaturesa636c9dfec5e

Beck, Roman, Müller-Bloch Christoph, & King John Leslie, *Governance in the blockchain economy: A framework and research agenda* (2018), 19(10) JOURNAL OF THE ASSOCIATION FOR INFORMATION SYSTEMS 1

Black, Berdnard S., *Shareholder Activism and Corporate Governance in the United States*, THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW, vol. 3, pp. 459-465 (1998)

Binance, Academy, *¿Qué es una cartera multisig?* (2020). Disponible en: https://academy.binance.com/es/articles/what-is-a-multisig-wallet

Boado, Ernesto, *Aave Protocol Whitepaper* (v1.0) (2020). Disponible en: https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf.

Buterin, Vitalik, A *Next-Generation Smart Contract and Decentralized Application Platform* (2013) disponible en:https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

Chainalysis 2022 Crypto Crime Report.

Chohan, Usman W., *The Decentralized Autonomous Organization and Governance Issues* (2017). Disponible en: https://ssrn.com/abstract=3082055

Comité de Supervisión Bancaria de Basilea, Basel Committee publishes second consultation document on the prudential treatment of banks' cryptoasset exposures (2022). Disponible en: https://www.bis.org/press/p220630.htm#:~:text=to%20media%20resources.-,Basel%20Committee%20publishes%20second%20consultation%20document%20on,treatment%20of%20banks'%20cryptoasset%20exposures&text=The%20Basel%20Committee's%20second%20public,consultation%20issued%20in%20June%202021.

Delgado de Molina, Rius, Alfonso, *Blockchain: concepto, funcionamiento y aplicaciones*, en FINTECH, REGTECH Y LEGALTECH: FUNDAMENTOS Y DESAFÍOS REGULATORIOS, Ed. Nydia Remolina y Aurelio Gurrea-Martinez (Tirant LoBlanch, 2020)

Delgado de Molina, Rius Alfonso, García Gil Vicente Vicente, *Los contratos inteligentes o smart contracts*, en FINTECH, REGTECH Y LEGALTECH: FUNDAMENTOS Y DESAFÍOS REGULATORIOS, Ed. Nydia Remolina y Aurelio Gurrea-Martinez (Tirant LoBlanch, 2020)

Ethereum, "Introduction to Daaps" (2022), disponible en: https://ethereum.org/en/developers/docs/dapps/
Operar de forma "descentralizada" hace referencia a ejecutar alguna tarea u operación, generalmente, sin necesidad de una entidad a cargo de ejecutar dicha tarea u operación.

Faux, Zeke, and Shen Muyao, A $60 Billion Crypto Collapse Reveals a New Kind of Bank Run, Bloomberg Finance (2022). Disponible en: https://www.bloomberg.com/news/articles/2022-05-19/luna-terra-collapse-reveal-crypto-price-volatility

Financial Action task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (2021). Disponible en: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

Financial Action task Force, Virtual Currencies Key *Definitions and Potential AML/CFT Risks* (2014). Disponible en: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-assets* (2022). Disponible en: https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/

Financial Stability Board, Regulation, *Supervision and Oversight of "Global Stablecoin*" Arrangements (2020). Disponible en: https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/

Funke, Matthias, *New Decentralised Finance Stacks, Alternatives to Ethereum,* Coinmonks (2021). Disponible en: https://medium.com/coinmonks/new-decentralised-finance-stacks-alternatives-to-ethereum-abe74ecf53f9

Gail, Elizabeth, *Aumentan los ataques a DeFi - ¿Podrá el sector frenar la oleada?,* Cointelegraph (2022). Disponible en: https://es.cointelegraph.com/news/defi-attacks-are-on-the-rise-will-the-industry-be-able-to-stem-the-tide

Gudgeon, Lewis, Werner Sam, Perez Daniel, and Knottenbelt William J. "Defi protocols for loanable funds: Interest rates, liquidity and market efficiency." *In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pp. 92-112. 2020.

Gurrea-Martinez, Aurelio and Remolina Nydia, Corporate Governance Challenges in Initial Coin Offerings, in Andrew Godwin, Pey Woan Lee, and Rosemary Teele Langford (eds.), TECHNOLOGY AND CORPORATE LAW. HOW INNOVATION SHAPES CORPORATE ACTIVITY CORPORATIONS (Edward Elgar Publishing, 2021) pp. 205-226.

HM Treasury, Managing the failure of systemic digital settlement asset (including stablecoin) firms: Consultation (2022). Disponible en: https://assets.publishing.service.gov.uk/

government/uploads/system/uploads/attachment_data/file/1079348/Stablecoin_FMISAR_Consultation.pdf

Howell, James, *What Are Governance Tokens And Why Does They Matter?*, 101 Blockchains (2022), disponible en: https://101blockchains.com/governance-tokens/

Izraylevych, Igor, What is DeFi: *Understanding Decentralized Finance,* SPro Blog (2021), disponible en: https://s-pro.io/blog/what-is-defi#:~:text=Settlement%20Layer&text=The%20settlement%20layer%20is%20formed,to%20real%20estate%20land%20parcels.

Jarno, Klaudia, and Kołodziejczyk, Hanna, *Does the design of stablecoins impact their volatility?*, JOURNAL OF RISK AND FINANCIAL MANAGEMENT 14.2 (2021): 42.

Kondova, Galia, & Barba, Renato, *Governance of decentralized autonomous organizations* (2019), 15(8) JOURNAL OF MODERN ACCOUNTING AND AUDITING 406.

McNeil, David, *What is Liquidation in DeFi Lending and Borrowing?*, Coinmonks (2021). Disponible en: https://medium.com/coinmonks/what-is-liquidation-in-defi-lending-and-borrowing-platforms-3326e0ba8d0#:~:text=In%20traditional%20finance%2C%20liquidation%20occurs,collateral%20to%20back%20the%20debt

Nakamoto, Satoshi, Bitcoin: *A Peer-to-Peer Electronic Cash System* (2008), disponible en: https://bitcoin.org/bitcoin.pdf

OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (2022). Disponible en: https://www.oecd.org/finance/why-decentralised-finance-defi-matters-and-the-policy-implications.htm

Office of the Comptroller of the Currency, Statement by the Acting Comptroller of the Currency on the Report on Stablecoins (2021). Disponible en: https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-112.html

Payment Services (Amendment) Bill. Disponible en: https://www.mas.gov.sg/news/speeches/2021/payment-services-amendment-bill

Rauchs, Michel; Glidden, Andrew; Gordon, Brian; Pieters, Gina; Recanatini, Martino; Rostand François; Vagneur, Kathryn, and Zhang, Bryan Zheng, Distributed Ledger *Technology Systems: A Conceptual Framework, The Cambridge Centre for Alternative Finance* (2018), disponible en: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf

Remolina, Nydia, Open Banking: *Regulatory Challenges for a New Form of Financial Intermediation in a Data-Driven World*, SMU CENTRE FOR AI & DATA GOVERNANCE RESEARCH PAPER No. 2019/05 (2019)

Schär, Fabian, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial* (2021), 103.2 THE FEDERAL RESERVE BANK OF SAINT LOUIS OF ST. LOUIS REVIEW 153
Sinclair, Sebastian, “Uniswap’s First Governance Vote Ends in Ironic Failure”, Coindesk,

(2020). Disponible en: https://www.coindesk.com/uniswaps-first-governance-vote-ends-in-ironic-failure

Takyar, Akash, *Top Blockchains for DeFi, LeewayHertz* (2022), disponible en: https://www.leewayhertz.com/top-blockchains-for-defi/

Walch, Angela, *Deconstructing "Decentralization"*, en Chris Brummer (Ed.), CRYPTOASSETS, LEGAL, REGULATORY, AND MONETARY PERSPECTIVES (Oxford University Press, 2019). Pg. 39.

Wharton, Blockchain and Digital Asset Project, World Economic Forum, *DeFi Beyond the Hype. The Emerging World of Decentralized Finance* (2021), disponible en: https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf

Wolff, Max, *Introducing Marble: A Smart Contract Bank* (2018). Disponible en: https://medium.com/marbleorg/introducing-marble-a-smart-contract-bank-c9c438a12890

The World Economic Forum, DeFi Policy Maker Toolkit (2021), disponible en: https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf

Zetzsche, Dirk Andreas, Arner Douglas W., Buckley Ross P., *Decentralized Finance* (*DeFi*) (2020) 6 JOURNAL OF FINANCIAL REGULATION 172.

CAPÍTULO 3

Bitcoin: el proyecto que sigue transformando a El Salvador y lo ha puesto en la mira del mundo

Dionisio Ismael Machuca Massis[1]

Resumen

Este ensayo describe el proceso de adopción del bitcoin como moneda de curso legal de El Salvador, adicional al dólar. Relata la experiencia de Bitcoin Beach como proyecto piloto con el que entusiastas del bitcoin iniciaron una pequeña operación en una playa salvadoreña, la posterior expedición de la Ley Bitcoin, la entrega de la billetera electrónica Chivo a los salvadoreños con el equivalente en bitcoins a US$30, la relevancia del ecosistema construido en torno a la Ley, el efecto de inclusión financiera y el más reciente proyecto anunciado por el Gobierno que incluye una emisión de bonos -*Volcano bonds*-, de la cual una parte se destinará a inversión en el proyecto denominado Bitcoin City y otra a inversión en bitcoins, con un esquema de *tokenización* para poner el bono a disposición de criptoinversionistas. Adicionalmente, este ensayo da cuenta de cómo las personas han incorporado a su vida diaria el manejo del bitcoin, así como la participación de los bancos y los mecanismos de convertibilidad entre las dos monedas, como elemento de mitigación de la volatilidad del precio del bitcoin.

[1] Vicepresidente Jurídico y Secretario General de Banco Agrícola en El Salvador -Grupo Bancolombia- y Director Secretario de la Gestora de Fondos de Inversión Banagrícola. Ha estado al frente del desarrollo de los habilitadores jurídicos para la transformación digital del banco, siendo uno de los líderes del proyecto Bitcoin BA, la primera integración que permite a un banco aceptar pagos en cripto moneda.

1. Introducción

El 9 de junio del 2021, El Salvador se convirtió en el primer país en adoptar el bitcoin -BTC- como moneda de curso legal. Cuatro días antes, el presidente de la República lo había anunciado a través de un video presentado por Jack Mallers -fundador de Zap Solutions y CEO de Strike- en el marco de la conferencia Bitcoin 2021 en Miami. Simultáneamente, las ediciones digitales de CNBC y Coindesk lo anunciaron al mundo. La Ley Bitcoin se publicó y de inmediato comenzó a regir.

Una decisión de tal envergadura suscita al menos tres interrogantes: ¿Por qué ahora?, ¿Por qué bitcoin? y ¿Por qué en El Salvador? Un recorrido que nos lleva de Bitcoin Beach a Bitcoin City nos ayudará a comprender mejor lo que ha sucedido en El Salvador y a dar respuesta a estas inquietudes.

El punto de partida es el proyecto con el que un grupo de entusiastas del Bitcoin -pero más entusiastas y comprometidos con el desarrollo de las personas- iniciaron una pequeña operación de apoyo a una comunidad muy necesitada en una playa salvadoreña durante la pandemia Covid-19. Y el punto de llegada es el más reciente proyecto anunciado por el Gobierno, que incluye una emisión de bonos -*Volcano bonds*-, que en parte se destinarán a inversión en el proyecto denominado Bitcoin City y en parte a inversión en bitcoin, incluyendo un posible esquema de *tokenización* que dota a los bonos de las características de una criptomoneda, es decir, sin representación material y con la posibilidad de fraccionamiento que permite inversiones de montos pequeños para ponerlo al alcance de todo tipo de inversionistas.

Esperamos poder ilustrar cómo, pese a que la aprobación de la Ley Bitcoin y la adopción de este como moneda de curso legal han acaparado los titulares y las principales inquietudes de las personas alrededor del tema, lo más relevante es el ecosistema creado con ocasión de esta ley, los proyectos puestos en marcha y el impacto en los salvadoreños, así como la inclusión financiera generada y los aprendizajes que de esta experiencia se pueden aprovechar a nivel mundial.

2. De Bitcoin Beach a Bitcoin City -más que la Ley Bitcoin, la creación de un ecosistema

2.1 Bitcoin Beach

Bitcoin Beach se ha convertido en un proyecto emblemático en muchos sentidos, tanto para El Salvador como para la comunidad Bitcoin, al ser denominado como el primer proyecto de economía circular –sostenible- sobre dicha criptomoneda. Sin embargo, a la base de lo que a primera vista parecería un proyecto de características tecnológicas e innovadoras está la preocupación por las personas, particularmente por las más necesitadas y la labor que Missionsake viene desarrollando por medio de diversas actividades en la comunidad del Zonte, una comunidad en el litoral salvadoreño. Por más de 15 años, Missionsake[2] y su Hope House se han dedicado a empoderar a las comunidades a través de la formación de sus líderes, ayudando en el desarrollo mental, espiritual, físico y de salud relacional de la

[2] https://missionsake.com

comunidad misionera; el Proyecto Bitcoin Beach ha sido su programa de empoderamiento financiero con especial impacto en la comunidad a partir de los meses más difíciles y de restricción de movilidad de la pandemia Covid-19 durante el año 2020.

Michael Peterson, uno de los líderes de Missionsake y Bitcoin Beach explica a través de un video[3] la génesis y entrañas del proyecto.

No es nuestra intención definir el concepto ni el contexto del proyecto, pero sí trasladarles los mensajes de Michael desde su experiencia, que nos hicieron reflexionar sobre los impactos y aprendizajes que este esfuerzo concentrado generó para, sin duda, convertirse en la chispa que dio muchas pautas al actual proyecto que, bajo la Ley Bitcoin, se propone al país y a sus relaciones con el mundo. Habiendo sido parte del proyecto de implementación de la Ley Bitcoin para el banco con mayor presencia e impacto en El Salvador, Banco Agrícola miembro del Grupo Bancolombia, nos hace todo el sentido en relación con los retos que también enfrentamos.

La imposibilidad para las personas de salir de sus casas durante la pandemia, no poder trabajar, no poder desplazarse a adquirir sus alimentos, estuvieron a la base de buscar soluciones efectivas para una comunidad que en su generalidad no estaba bancarizada. Por el contrario, quienes teníamos cuenta bancaria, tarjeta de débito o crédito, resolvimos este problema comprando en línea, aprovechando el acelerado desarrollo de los *deliveries* o domicilios, o con opciones de *pick-up* en espacios especialmente adecuados previo pago en línea, transferencia bancaria u otro medio remoto de pago.

Una crisis que estaba afectando al menos dos puntas de una economía fundamentada en el efectivo. El equipo de Bitcoin Beach, que ya tenía un plan piloto con jóvenes a los que habían formado en el uso del bitcoin y de las billeteras electrónicas -*wallets*-, ante la necesidad de las personas en esa comunidad obtuvieron una donación en bitcoins que les permitió, desde su conocimiento de las familias y sus necesidades, hacerles entrega de recursos en esa criptomoneda a través de donaciones semanales, habilitando el uso de una billetera electrónica y desarrollando un ecosistema con los comercios, tiendas -pequeñas despensas- y comerciantes individuales, para que la comunidad pudiese interactuar a través de una llamada telefónica o un mensaje de texto, haciendo sus pedidos, transfiriendo los recursos a la *wallet* del comercio y recibiendo sus productos. Este fue el primer paso para introducir a la comunidad en un sistema de pagos, un ecosistema de interacción y uso de criptomonedas.

En el video, Peterson explica cómo acompañaron a los comercios por lo menos durante los primeros dos meses y los apoyaron para comprender la volatilidad del bitcoin, incluso asumiendo inicialmente las fluctuaciones de precio para evitar el impacto en el monto donado; resolvieron la importancia de la conectividad a través de *hot spots* -accesos de conexión gratuita- en los comercios, pues el costo de la conectividad es un elemento a tener en cuenta en estos proyectos que buscan inclusión.

De igual manera, se preguntaron por la educación versus el uso y concluyeron, a partir de la experiencia, que lo primero debía ser el uso. Si las personas usan la tecnología y con ella resuelven una necesidad, luego se preocupan por entenderla; en cambio, comenzar

[3] https://www.bitcoinbeach.com

por la formación puede resultar un mundo tan distinto al conocido que inhibe lanzarse al uso o la experimentación, por lo que la recomendación de estos amigos fue la de aprender usando, y para ello lo importante era una interfaz amigable –una aplicación que invitara al uso-. En este sentido, decidieron utilizar la billetera de Strike –*proveedor de wallets*- y un protocolo *lightning* que opera como una segunda capa sobre blockchain y que permite mayor velocidad y menores costos en las transacciones, lo que también es importante tanto para facilitar la adopción como para la seguridad de la transacción y su aplicación inmediata.

Eligieron una billetera custodial, es decir, en la que un tercero tiene las llaves de acceso y el usuario cuenta con una contraseña que es fácil de recuperar, pues la custodia la tiene el administrador de la billetera. Actores más sofisticados, en la medida que van conociendo este mundo de las criptomonedas, suelen moverse a billeteras no custodiales, en las que el usuario tiene las claves de acceso de modo que, si las pierde u olvida, no tiene cómo acceder a su dinero o activos. En una etapa inicial, en este proyecto se entendió que era importante que las personas no tuviesen un riesgo de pérdida en caso de extravío de las claves o llaves de acceso y por ello optaron por una billetera custodial que, unida a una interfaz amigable, operara de forma muy similar a cualquier interacción en línea con un comercio o institución financiera.

Otro elemento que se destaca como un hito del proyecto fue la instalación del primer cajero automático en la comunidad, que permitió a los usuarios retirar dólares contra sus fondos en bitcoins. Aunque los beneficiarios de la donación no retiraron ni trasladaron de inmediato sus fondos en bitcoins, la sola posibilidad de poder hacerlo generó tranquilidad y confianza en el ecosistema. Fue otro aprendizaje importante, en cuanto el mecanismo de *cash out* -posibilidad de retirar en efectivo- como elemento clave para el funcionamiento del ecosistema y principalmente para generar confianza en él.

2.2 Ley Bitcoin

Con fecha 9 de junio de 2021 se dio por finalizado el proceso de formación de la Ley Bitcoin[4]. El día D quedó fijado para el 7 de septiembre, es decir, 90 días después de la publicación de la ley.

Noventa días y una ley de tan solo dieciséis artículos podría parecer poco o al menos suscitar inquietudes para un proyecto de tales complejidades, entre ellas la integración tecnológica y financiera que daría paso no sólo a una moneda de curso legal sino, además, a la primera moneda de curso legal sin representación física y cuya titularidad y acceso sólo se hacen efectivos a través de la plataforma y servicios prestados por proveedores especializados. Una transformación a nivel nacional que obligaba a todos los actores económicos a hacer adecuaciones para cumplir con una ley que introdujo la obligación de aceptar pagos en bitcoins, junto con la necesaria inmersión y formación en al menos los aspectos básicos de las criptomonedas: blockchain*, lightning,* bitcoin*,* exchange*,* volatilidad, proveedores de servicios especializados, conocimiento electrónico del cliente -e-KYC-, conocimiento de las transacciones -*KYT, Know Your Transaction*-, entre otras.

Una ley que, desde la perspectiva jurídica, calificamos de disruptiva, pues lejos de regular exhaustivamente las situaciones posibles -como cuando se diseña desde el laboratorio o

[4] Decreto Legislativo No. 57 publicado en el Diario Oficial No. 110, Tomo No. 431.

la cabeza del experto-, apenas dictó el marco y los principios para que lo posible pudiese transformarse en realidad, para diseñar desde la experiencia.

El contenido de la Ley lo explicamos en cuatro apartados: bitcoin como moneda de curso legal; mecanismo de convertibilidad; protección al consumidor y aspectos de orden económico, y responsables de emitir la regulación.

2.2.1 La Ley declara al bitcoin como moneda de curso legal y, como consecuencia natural, establece que no estará sujeto a ganancia a capital; es decir que, a diferencia de los países que lo regulan como un activo, los cambios de valor en el bitcoin y el consecuente incremento en el valor adquisitivo no son hecho generador del impuesto sobre la renta. Asimismo, se declara su uso para el pago de contribuciones tributarias.

Un aspecto, que inicialmente fue controversial pero que con el tiempo tuvo un adecuado dimensionamiento y resultó de gran ayuda para la comprensión y la cobertura de la volatilidad, fue el hecho que la ley establece la obligación de *aceptar* pagos en bitcoins, pero con la aclaración de que *aceptar* no implica la obligación de *recibir*. El mecanismo de convertibilidad previsto para la billetera electrónica oficial permite que el pago se acredite en dólares, si el usuario que recibe el pago así lo decide; por lo tanto, se puede aceptar el pago en bitcoins pero recibir dólares.

La afirmación, de suyo compleja, no solo generó confusión en sus inicios, sino además una serie de etiquetas y memes. Finalmente, las inquietudes se disiparon con el uso de la solución.

La Ley también define que cualquier obligación previa estipulada en dólares de los Estados Unidos de América[5] puede pagarse en bitcoins, de tal manera que el pago en cualquiera de las dos monedas tiene igual validez respecto a la liberación de las obligaciones en dinero.

2.2.2 La Ley prevé un mecanismo de convertibilidad. El Estado se obliga a proveer y garantizar la convertibilidad *automática e instantánea*. Con tal fin crea un fideicomiso a través del Banco de Desarrollo de El Salvador[6], un banco de segundo piso, propiedad del Estado. La Ley indica que el mencionado fideicomiso operará en adición a los mecanismos de convertibilidad que puedan poner a disposición los privados.

A la fecha, algunos privados han contratado servicios de convertibilidad a través de terceros especializados; y aunque la regulación no ha hecho exclusiones, al mecanismo de convertibilidad oficial se accede a través de la billetera denominada Chivo Wallet, de la que sólo pueden ser titulares los salvadoreños, sean personas naturales o jurídicas.

Consideramos que este mecanismo de convertibilidad emula, de alguna manera, el Proyecto Bitcoin Beach en cuanto a la necesidad de acompañar a los usuarios para entender las implicaciones de la volatilidad del bitcoin. En este sentido, provee la posibilidad para el usuario de no asumir los riesgos de las continuas variaciones del bitcoin, dada la opción de conversión que complementa el diseño de la solución Chivo Wallet, y en adición a este

[5] Moneda de curso legal en El Salvador.
[6] Ley de Creación del Fideicomiso Bitcoin, Decreto Legislativo No. 137 de la Asamblea Legislativa de la República de El Salvador, fechado 31 de agosto de 2021. Publicado en el Diario Oficial No. 165, Tomo No. 432, de fecha 31 de agosto de 2021.

mecanismo incorpora la posibilidad de manejar dos gavetas: una en bitcoins y otra en dólares.

Chivo Wallet provee a sus usuarios desde una sola aplicación una cuenta en bitcoins y otra en dólares; esta segunda es similar a la de un emisor de dinero electrónico. La aplicación permite al usuario preseleccionar, para cada tipo de pago o transferencia, en qué moneda quiere recibirlos y de esa manera evitar la volatilidad, por ejemplo, eligiendo siempre recibirlo en dólares. Otra opción es mantenerlos en la moneda que se recibe, e incluso provee la posibilidad de tomar una decisión en cualquier momento respecto de los fondos en cualquiera de las cuentas.

No podemos dejar de mencionar la paradoja que representa este mecanismo de convertibilidad, pues mientras la filosofía tras tecnologías como blockchain y bitcoin proponen eliminar a los terceros de confianza -por ejemplo, el Estado y sus bancos centrales con relación a la emisión de la moneda-, parecería que en El Salvador la inclusión del tercero de confianza a través del mecanismo de convertibilidad oficial y la billetera Chivo, diseñados desde el Estado, fue el elemento que fortaleció la confianza para adoptar el bitcoin en el periodo de los 90 días propuestos.

Sin intención de polemizar, creemos que el caso de El Salvador plantea un panorama retador a los promotores y defensores del bitcoin: ¿Será que la realidad de los sistemas descentralizados no es pura con relación a los terceros de confianza, y quizás una receta posible para continuar masificando su adopción sea una solución híbrida que integre plataforma de confianza y terceros de confianza respecto de los retos naturales de adopción y protección del consumidor?

2.2.3 En materia de orden económico, al que podemos sumar medidas de protección al consumidor, la Ley indica que el tipo de cambio entre el bitcoin y el dólar se establece libremente por el mercado; en el mismo sentido, indica que los precios pueden expresarse en bitcoins y que para fines contables se utilizará el dólar.

Importante recalcar que ninguna interacción económica debe quedar al margen de la protección al consumidor, incluso aquellas que se perfeccionan y realizan a través de plataformas electrónicas o las que no tienen una representación física. En el caso de El Salvador, el apego al derecho de consumo y a la prevención del lavado de dinero ha quedado establecido desde esta ley.

2.2.4 Se delegó al Banco Central de Reserva y a la Superintendencia del Sistema Financiero la emisión de la normativa necesaria para la aplicación de la Ley, lo que supuso que, en los mismos 90 días otorgados para su entrada en vigencia, se preparara, discutiera y aprobara el marco normativo que la acompañaría; sin duda todo un reto.

Buscando la nota positiva, es importante destacar que el corto periodo para que la Ley entrara en vigencia y su marco amplio de acción resultaron ser un facilitador de las integraciones necesarias para hacer realidad este proyecto. Representaron oportunidades para construir, sobre la marcha, los rieles necesarios para los trenes dispuestos a surcar este territorio, novedoso y aún en proceso de ser entendido y conquistado.

2.3 Un proyecto de 90 días

La Ley Bitcoin requirió preparación de todos los actores económicos, con carácter obligatorio, y en ese sentido contar con una solución para aceptar pagos en bitcoins a la entrada en vigencia de la Ley. Las opciones eran desarrollar un proyecto propio que permitiese el cumplimiento del mandato, o adoptar la solución oficial suscribiéndose a la *wallet* Chivo.

El primer camino era el único claro al inicio de esos 90 días; el segundo apenas se fue vislumbrando con el anuncio del lanzamiento de Chivo, la presentación de sus gavetas en bitcoins y dólares, más certeramente con el conocimiento de la propuesta de normas y lineamientos del Banco Central de Reserva -BCR-, y en definitiva en los días previos al 7 de septiembre, cuando se conoció con más detalle la solución de Chivo para los comercios como un elemento distinto a la *wallet* de personas naturales.

Refiriéndonos al sistema financiero, podemos afirmar de manera general que se optó por utilizar la solución oficial, suscribiendo una *wallet* en la versión comercial que permitía a los bancos y entidades financieras aceptar los pagos en bitcoins, para lo cual el cliente que se presenta a una oficina o agencia es dirigido a una caja o punto de atención específico en el que desde su *wallet* puede interactuar con la de la entidad; es decir, no hay una integración en los sistemas del agente económico sino una interacción entre dos usuarios de *wallet* Chivo, utilizando además el mecanismo de convertibilidad oficial para no mantener posiciones en bitcoins.

Algunos comercios de consumo masivo, destacando McDonald´s y Starbucks, entre otros, sí desarrollaron sistemas propios e integraron proveedores especializados que les permitieron desde sus cajas y puntos de venta aceptar pagos en bitcoins de manera integrada a sus sistemas de pago. En este mismo sentido, destacamos el único proyecto de esta naturaleza en el sistema financiero, impulsado por Banco Agrícola, el banco líder en El Salvador con mayor participación de mercado, miembro de Grupo Bancolombia. Por su connotación como primer proyecto de esta naturaleza desde un banco a nivel latinoamericano, consideramos importante incluir este proyecto como una parada relevante en nuestra travesía bitcoin.

Para este banco el plazo del proyecto fue de 82 días. Se inició sin conocimiento de lo que la normativa complementaria podría definir, adelantando en simultáneo una intensa inmersión y formación en la materia, con tres objetivos estratégicos: (i) aceptar bitcoins como forma de pago para créditos y tarjetas de crédito, utilizando cualquier *wallet* en bitcoins con tecnología blockchain o *lightning*, a través de la aplicación de banca móvil y servicio web de *e-banca*; (ii) desarrollar una solución para que empresas y comerciantes pudieran aceptar pagos en bitcoins de sus clientes desde cualquier *wallet*; y (iii) interoperar con la billetera *Chivo*.

Esta solución se integró a una estrategia de *paga y vende como quieras*, ampliando así el abanico de soluciones de pago. Opera de la mano con un proveedor de servicios internacional. Así, cuando un cliente hace un pago en bitcoins, la aplicación y servicio web del banco le muestra la cotización a dólar. Si el cliente acepta la operación, transfiere desde su *wallet* los bitcoins, los convierte de manera inmediata y abona al saldo correspondiente la cantidad equivalente en dólares. De esta manera el cliente se asegura de la cantidad a pagar y el banco *acepta* la transacción en bitcoins, pero *recibe* dólares, sin mantener en ningún momento una posición en la criptomoneda ni exponerse a su volatilidad. De similar manera opera la solución de adquirencia para los comercios a través de la plataforma de Wompi.

La integración con Chivo, en su gaveta en dólares, fue posible para todos los bancos del sistema a través del proyecto Transfer 365, que, desde el Banco Central de Reserva, posibilitó la interconexión en tiempo real de Chivo con todas las entidades financieras reguladas.

3. Normas del Banco Central de Reserva

El BCR expidió dos normas técnicas[7]: la primera, para facilitar la aplicación de la Ley Bitcoin, cuyo objetivo principal es regular las relaciones entre los sujetos regulados[8] y los proveedores a contratar para transacciones y pagos digitales en bitcoins o dólares a través de mecanismos electrónicos. De acuerdo con dichas normas, las entidades que contratan son responsables del cumplimiento del marco jurídico por parte de los proveedores de servicios, entre otros, en lo relacionado con prevención de lavado de dinero y financiamiento al terrorismo, ciberseguridad, derecho de consumo, riesgo operativo, quejas y reclamos de los clientes, y normativa de proveedores bitcoin. Adicionalmente, las entidades que contratan deben obtener de la Superintendencia del Sistema Financiero una manifestación de no objeción al modelo de negocio y autorización del Banco Central de Reserva como nueva operación. Esta propuesta se convirtió en las Normas para facilitar la participación de las entidades financieras en el ecosistema bitcoin[9].

De similar manera, la segunda norma contiene los Lineamientos para la autorización del funcionamiento de la plataforma de la billetera digital para bitcoins y dólares[10]. De forma muy concreta, habilitó como operación bancaria, previa autorización de la plataforma tecnológica por el Banco Central de Reserva, la billetera digital en bitcoins y dólares, de manera que cualquier banco podría estar operando billeteras o *wallets* en bitcoins. A la fecha ninguna entidad financiera cuenta con el producto de billetera en bitcoins.

Varias pueden ser las razones: por una parte, la posición del Comité de Basilea[11], que en sus propuestas contempla exigir a los bancos un alto requerimiento de capital para las posiciones en criptomonedas; y de otra, el hecho de que los bancos están autorizados[12], tanto para fungir como emisores de dinero electrónico como para el manejo de cuentas simplificadas de depósito de ahorro, con requisitos mínimos para su apertura y que operan 100% digitales.

Adicionalmente, se emitió el reglamento de la Ley[13], dirigido a los Proveedores de Servicios de Bitcoin, que incluye la creación de un registro para estos proveedores en el Banco Central. Para los bancos resultó importante que el reglamento les reconociera la posibilidad de proporcionar servicios a estos proveedores, pero que no fuera obligatorio. Adicionalmente, con relación a las billeteras ofrecidas por el Estado, obliga a los bancos a prestar sus servicios

[7] Documentos publicados para consulta, comunicados a través de las circulares 615 y 616 del Banco Central de Reserva, de fecha 17 de agosto de 2021.
[8] Bancos, aseguradoras, sociedades de ahorro y crédito, etc.
[9] Norma NRP-29 aprobada por el Comité de Normas del BCR, CNBCR-12/2021 del 7 de septiembre de 2021.
[10] Esta propuesta se convirtió en la resolución de Consejo Directivo del BCR 29/2021 "Lineamientos para la autorización del funcionamiento de la plataforma tecnológica de servicios con bitcoin y dólares", aprobada el 7 de septiembre de 2021.
[11] Basel Committee on Banking Supervision - Consultative Document - Prudential treatment of crypto asset exposures. Issued for comments by September 10, 2021. June 2021. ISBN 978-92-9259-480-0 (online)
[12] Ley para facilitar la Inclusión Financiera. Decreto Legislativo No. 72 de la Asamblea Legislativa de la República de El Salvador, fechado 2 de septiembre de 2015. Publicado en el Diario Oficial No.160, Tomo No. 408 del 3 de septiembre de 2015.
[13] Reglamento de la Ley para facilitar la Inclusión Financiera. Decreto Legislativo No. 27 de la Asamblea Legislativa de la República de El Salvador. Publicado en el Diario Oficial Tomo No 432 del 27 de agosto de 2021.

como plataforma de intercambio sin generar comisión para el usuario de dichas billeteras. Esta disposición allanó el camino a la conectividad de la billetera de Chivo en dólares con las cuentas del sistema financiero.

Regular de esta manera a los proveedores también arrojó claridad respecto de personas naturales que, ante la pronta entrada en vigencia de la Ley, quisieron anticiparse realizando operaciones de compra de bitcoins por cuenta de terceros. Esas operaciones, que inicialmente generaron alertas como inusuales, quedaron claramente sujetas a un registro previo en el Banco Central. A junio de 2022, el registro de proveedores de servicios bitcoin muestra en su página Web 48 proveedores[14].

Un último elemento en este contexto fue la ley de Creación del Fideicomiso Bitcoin, que estableció las bases de creación del Fideicomiso y su operatividad, así como la conformación de su patrimonio vía transferencia de US$150 millones por parte del Ministerio de Hacienda; igualmente, dispuso los lineamientos para el mecanismo de convertibilidad, el manejo de la billetera oficial y la interoperabilidad.

4. Día D

Llegado el 7 de septiembre, entre la expectativa por la entrada en vigencia de la ley, la incertidumbre y el hecho de ir conociendo casi en simultáneo el marco regulatorio complementario, el día D fue para algunos la espera de entrada en producción de Chivo, y, para los que se lanzaron a innovar con proyectos propios, como el caso particular destacado de Banco Agrícola, de desvelo a la espera de las autorizaciones para operar.

Terminamos un día lleno de muchas satisfacciones, con la sonrisa del deber conquistado al haber no sólo cumplido la ley, sino en el caso de algunos actores hacerlo con el mejor servicio disponible en el mercado, y recibir la retroalimentación de los clientes que se volcaron a probar su efectividad.

Para la billetera oficial y las entidades que acogieron esa solución, la historia fue diferente: la cuenta en Twitter del presidente de la República y la del propio Chivo dieron cuenta del paso a paso y las horas de espera para lograr la disponibilidad y descarga de la aplicación en las diferentes tiendas, las suspensiones de servicio que fue necesario implementar para estabilizarlo, incluidos algunos problemas de suplantación de identidad en la vinculación a la billetera. Finalmente, una curva de aprendizaje razonable de cara a lo que representó para el Gobierno un proyecto masivo, de alta carga tecnológica, implementado a gran escala, en corto tiempo y con intensivo requerimiento de recursos de toda naturaleza. Sin embargo, luego de las dificultades iniciales ha resultado ser un importante instrumento de inclusión financiera de cara a la cantidad de usuarios de billeteras activadas, su interconexión inmediata con el sistema financiero, así como de atracción de talento y de inversionistas entusiastas del bitcoin que se mantienen atentos a lo que sucede.

[14] https://registrobitcoin.bcr.gob.sv/web/proveedores-registrados

5. Chivo[15]

Chivo es la billetera oficial del Gobierno, que cuenta con una billetera digital en bitcoins y otra en dólares. Es operada por una sociedad anónima, con inversión pública, bajo la modalidad de proveedor de servicios registrado en el BCR. La regulación para su operación en bitcoins como en dólares es tan sucinta como el marco al que nos hemos referido previamente. Entendemos que para la billetera en dólares opera como un emisor de dinero electrónico, es decir, con una cuenta en el BCR en el que los dólares *digitales* están respaldados en un 100% por un depósito.

Chivo fue diseñada como una aplicación muy amigable -lo que identificamos nuevamente con las lecciones aprendidas de Bitcoin Beach- y cuenta con conectividad gratuita, de tal forma que los usuarios no utilizan sus datos al interactuar en Chivo. La vinculación se hace con el número del Documento Único de Identidad y un número de línea móvil. Aparecen de inmediato los saldos de la billetera digital en bitcoins y en dólares, permitiendo, entre otros, definir la conversión automática a una u otra moneda, o la no conversión, así como retiros de cuentas de bancos del usuario, recarga de la billetera en dólares desde cualquier tarjeta de crédito, recargas desde un cajero automático y transferencias en cualquiera de las monedas a través de generación de códigos QR.

Su funcionalidad y facilidad han permitido una efectiva inclusión financiera –se estima que 4.3 millones de salvadoreños de un total de 6.5 millones que viven en El Salvador tienen una billetera Chivo-, generando confianza, mitigando los riesgos de volatilidad y promoviendo que la población aprenda haciendo -otra lección asimilada de Bitcoin Beach: primero usar y luego profundizar en el aprendizaje; aprender haciendo y resolviendo una necesidad-.

6. Transfer 365

Mientras el Proyecto Bitcoin tomaba vida, el Banco Central trabajaba paralelamente en otro elemento del ecosistema: una cámara de compensación que permitiría la interoperabilidad y las transferencias en tiempo real de las entidades reguladas con cuenta en el Banco Central y eventualmente Chivo. Si bien ya existía una cámara de compensación privada por la que los bancos hacían este tipo de transferencias, la nueva normatividad obligó a la interconexión, llevando a los bancos a incluir, en sus opciones de transferencias a través de sus plataformas móviles y de banca en línea, el servicio Transfer 365[16] sin costo para los usuarios.

El proyecto ha representado retos tecnológicos y de aseguramiento de los estándares de prevención en materia de lavado de dinero; sin embargo, ha permitido que los usuarios de Chivo, desde su billetera en dólares, puedan hacer transferencia a sus cuentas en cualquier banco del sistema financiero local.

[15] Conforme a lo descrito por la escritora Jacinto Escudo, es una palabra característica de la cultura salvadoreña, utilizada con diversas intensidades. Chivo puede ser "Ok, está bien, bueno, me gusta, estoy de acuerdo, démosle; una expresión "de admiración y contento, de emoción". Columna de Opinión "Hablemos en salvadoreño", publicada en la versión digital de La Prensa Gráfica el 26 de septiembre de 2021.

[16]https://www.bcr.gob.sv/2021/06/07/bcr-pone-a-disposicion-de-los-usuarios-el-servicio-transfer365-para-realizar-operaciones-bancarias-24-7/

7. Funcionamiento de la Ley Bitcoin

Podemos calificar la Ley como una forma disruptiva de poner en marcha un proyecto jurídico, económico y de infraestructura tecnológica de gran envergadura.

Cabe destacar en su funcionamiento el rol del bono de US$30 en bitcoins que el Gobierno puso a disposición de los salvadoreños que activaran su billetera Chivo; este incentivo permitió que se superaran las barreras tecnológicas y la formación se asimilara a través de la práctica.

Chivo es una *wallet* custodial. El Gobierno entendió que la pérdida de la llave y consecuente pérdida de acceso al bitcoin era un riesgo que debía mitigarse para lograr confianza, y que también era necesario sumar a Transfer 365, un ecosistema que incluye quioscos a nivel nacional, cajeros automáticos, recargas con tarjeta de crédito y débito, y la necesidad de seguir ampliando un ecosistema que motive la adopción de *Chivo* y su uso. El proyecto sigue en una curva de aprendizaje continuo, y seguiremos escuchando de las evoluciones de Chivo y sus servicios.

El pasado 19 de enero de 2022, el presidente de la República anunció en su cuenta de Twitter que *Chivo* llegó a 4 millones de usuarios[17].

8. Lecciones aprendidas

Este proyecto nos llevó a comprender las diferencias entre operar en *Lightning* y operar *OnChain* –se llama *OnChain* a las operaciones en la blockchain de bitcoin-, con las consecuentes ventajas de costo y velocidad en comparación con los retos de trazabilidad y efectivo conocimiento de las transacciones; así mismo, nos condujo a desarrollos especializados y a profundizar en el conocimiento electrónico del cliente y de las transacciones. La red *Lightning* es una capa secundaria sobre la blockchain de bitcoin que permite a los usuarios crear canales de pago, donde las transacciones ocurren al margen de la capa principal, pero siempre beneficiándose de su seguridad y descentralización; son conocidas como operaciones *OffChain* o fuera de la red principal; ofrecen ahorro en costos y posibilidades de escalabilidad, así como velocidad para todo el esquema bitcoin.

Es también una lección aprendida desde el enfoque y rol del regulador y el supervisor; es válido decir que los proyectos de implementación también requirieron ser disruptivos. Por ello, destacamos el enfoque de nuestro regulador y supervisor y su compromiso por lograr que las cosas sucedieran con un espíritu 100% colaborativo, integrado y a disposición de los regulados para hacer efectiva la entrada en vigencia de la Ley, dispuestos a recibir recomendaciones y a construir de manera conjunta los habilitadores para su implementación. De su parte hubo equipos dedicados que nos acompañaron en el proceso de no objeción y autorización de nuestros servicios, lo que evidenció mucha claridad en el enfoque de producto mínimo viable, experiencia del cliente, alcance de objetivos y flexibilidad, así como transparencia para todos los grupos de interés.

[17] Se estima que a junio 2022 se cuenta con 4.3 millones de salvadoreños como usuarios de Chivo, de una población, que sólo en el territorio salvadoreño es de 6.5 millones.

9. Uso e impactos, conectividad, colaboración

En el corto plazo de experiencia con las transacciones en bitcoins, destacamos los siguientes aprendizajes:

9.1 El uso nos llevó a la rápida identificación de las necesidades de los usuarios, según la utilización del bitcoin como medio de pago o como medio de conservación de valor y, en consecuencia, a derivar diversos servicios. Como medio de pago, lo podemos identificar con el uso de las tarjetas de crédito y el sistema de adquirencia; un medio para llevar recursos de un extremo a otro de las relaciones, a través de un ecosistema que, interconectado, posibilita la movilización de recursos y pagos inmediatos; en este caso, el medio o vehículo de pago es la criptomoneda, y es así como advertimos su utilización para el pago de un crédito o la adquisición de un bien o servicio; incluso para el envío y recepción de remesas. Como medio de conservación de valor, vemos a los que mantienen sus posiciones en bitcoins en sus *wallets* e incluso transfieren dinero de sus cuentas hacia su cuenta en Chivo para adquirir bitcoins y mantener posiciones en esa criptomoneda; actualmente pueden adquirirse bitcoins sin cobro de comisión en la billetera oficial.

9.2 La efectividad que, de cara a mitigar la volatilidad, implica la utilización de mecanismos de convertibilidad a través de un proveedor especializado. El buen funcionamiento de estos proveedores de liquidez y convertibilidad incluso propone replantearse la necesidad o funcionalidad del Fideicomiso Bitcoin en el largo plazo, respecto a si este podría ser sustituido por un proveedor que no requiera un fondeo como el que originalmente dotó al Fidecomiso.

9.3 Se han encontrado proveedores especializados con altos estándares de gobierno corporativo, cumplimiento regulatorio y prevención de lavado de dinero.

9.4 El proyecto del Gobierno incluyó en sus justificaciones la de abaratar el costo de las remesas. Si bien este es un objetivo válido y existen ya soluciones para estos efectos y el número de operaciones va en ascenso, aún no se ha resuelto el problema del *cash in* –ingreso del dinero en efectivo al ecosistema-. En el exterior encontramos personas en muchos casos indocumentadas y con pocas posibilidades de bancarizarse, de modo que no pueden vincularse a una *wallet* y aún no encuentran cómo beneficiarse de esta posibilidad.

9.5 El *cash out*, o la posibilidad de retiro del dinero en efectivo, es un elemento necesario que ha logrado operarse a través de transferencias hacia cuentas bancarias y la posibilidad de retiro en cajeros automáticos bitcoin.

9.6 La necesaria gestión y prioridad de la ciberseguridad, considerando que en la actualidad la periferia de la ciberseguridad somos los individuos; es decir, que un proyecto de esta magnitud tecnológica, en el que los puntos de acceso son tan amplios como la cantidad de sus usuarios y dispositivos, requiere una importante capacidad de inversión y gestión de la ciberseguridad.

9.7 La necesidad de una ley de protección de datos que complemente el ecosistema y garantice los derechos fundamentales de los individuos, y que a la vez genere oportunidades de *Open Finance* y *Open Data*[18]. El Salvador no tiene aún una ley de protección de datos. Al

[18] Es la posibilidad que un cliente autorice la utilización de sus datos en entidades financieras o en un ecosistema específico, para interconectar servicios o que éstos le sean provistos alimentándose de esas fuentes de información.

ser el de bitcoin un ecosistema basado en la información y las bases de datos, es necesario contar también con los más altos estándares de protección de datos -los lineamientos del Reglamento General de Protección de Datos de la Unión Europea se están convirtiendo en el estándar adoptado por diversos países, incluso en Latinoamérica-.

9.8 La necesidad de encontrar una pronta solución para la incorporación al ecosistema de los menores de 18 años.

9.9 Las comunidades bitcoin y blockchain son verdaderas comunidades colaborativas, con amplia disposición para enseñar a todo el que esté dispuesto a aprender y a compartir abiertamente las experiencias y oportunidades.

9.10 Se requiere especialización de los equipos, y en ese esquema es también muy valioso el aprendizaje conjunto y colaborativo entre regulador, supervisor y entidades reguladas. Compartir el conocimiento y formar a otros debe ser parte del compromiso.

9.11 La conectividad no puede ser una barrera para el acceso y la inclusión.

10. Oficina de innovación BCR/SSF

Como un claro compromiso con este proyecto y con la ampliación del ecosistema, el Banco Central de Reserva y la Superintendencia del Sistema Financiero lanzaron una oficina conjunta de innovación financiera[19]. Esta iniciativa, acompañada también de la labor del Comité de Normas, entre otras, ha anunciado una ley del sistema de pagos y liquidación de valores, que incorpora lineamientos para instrumentos de pagos y empresas de transferencia de dinero; de igual manera, se discuten normas para corresponsales financieros móviles y corresponsales financieros digitales, que incluye las APIs como canal de corresponsalía financiera.

Este es el primer paso para contar con un arenero o *sandbox* en El Salvador que agilice la adopción de tecnologías y nuevos modelos de negocios en un ambiente controlado, que permita dimensionar su aplicación y necesidades regulatorias.

11. Bitcoin City

Llegamos así a la última estación de este recorrido: el proyecto Bitcoin City. Un proyecto anunciado por el presidente de la República en la BitConf celebrada en San Salvador en noviembre de 2021, que propone la construcción de una ciudad con muy favorable tratamiento tributario que atraiga la inversión del mundo cripto y de los ecosistemas vinculados. El Gobierno proporcionará el terreno para este desarrollo, así como la infraestructura pública que genere atracción de la inversión. Propone un círculo virtuoso que incluye un volcán y la generación de energía geotérmica que proveerá energía limpia a la ciudad, propiciando el desarrollo de minería cripto con esta fuente de energía, así como apoyo a la agricultura, la cultura y el deporte.

[19]https://www.bcr.gob.sv/2021/12/03/el-banco-central-de-reserva-y-la-superintendencia-del-sistema-financiero-lanzan-oficina-de-innovacion-financiera/

Complementariamente, se anunció una emisión de $1,000 millones de dólares, de los cuales $500 millones se invertirán en bitcoins. Al respecto, se han tenido noticias de que podría tratarse de la emisión de un bono tradicional en el mercado, que luego podría ser *tokenizado*[20] total o parcialmente en una plataforma Bitfinex[21] de infraestructura blockchain denominada Liquid[22]. Los fondos en bitcoins estarían bloqueados por 5 años para luego, en función del cambio de valor comparado con el valor de adquisición, pagar un dividendo adicional al rendimiento ordinario. Esta iniciativa busca democratizar la inversión, permitiendo el acceso desde los $100 dólares de inversión; una democratización a través de la *tokenización* y con miras a un posible mercado secundario descentralizado que facilite liquidez a los inversionistas.

Por el momento la emisión está retrasada. Las expectativas de los inversionistas, así como el actual nivel de deuda pública, la calificación país, la rentabilidad de los eurobonos El Salvador, el aún no concretado acuerdo con el Fondo Monetario Internacional y las condiciones internas que enfrentan un temporal régimen de excepción, no hacen prever que tal emisión pueda materializarse pronto. A pesar de ello, en el mes de mayo de 2022 la Asamblea Legislativa aprobó, a propuesta del Gobierno Central, las leyes de soporte para dos grandes proyectos vinculados a esta iniciativa: el Tren del Pacífico y un nuevo Aeropuerto Internacional en el departamento de la Unión y a las puertas de Bitcoin City[23].

Estamos ante la génesis de una emisión que podría llevarnos del mercado tradicionalmente conocido y regulado a un mercado que, por su característica de descentralizado, es no regulado; en el que desaparecen los terceros de confianza para ceder a la confianza en la plataforma, los protocolos tecnológicos, los contratos inteligentes y las operaciones de finanzas descentralizadas.

12. ¿Qué ha dicho al respecto el Fondo Monetario Internacional?

En este punto de la historia, consideramos importante abrir un espacio de reflexión respecto a la posición del FMI ante esta apuesta, sobre la que todos tenemos alguna opinión, por oídas o por lectura.

Inicialmente[24], con la aprobación de la Ley, el FMI indicó que la adopción de bitcoin como moneda de curso legal levanta temas macroeconómicos, financieros y legales, que requieren un muy cuidadoso análisis[25], y manifestó que continuarían su proceso de consulta con las autoridades. Este anuncio se dio en medio de un proceso de evaluación a El Salvador, muy relevante de cara a las fuentes y posibilidades de financiamiento necesario para el mediano plazo y el adecuado balance presupuestario.

---

[20] Proceso descentralizado por el cual puede proporcionarse a casi cualquier activo las propiedades de una criptomoneda, particularmente su posibilidad de partición y existencia digital a través de una plataforma.
[21] https://www.bitfinex.com/
[22] https://www.liquid.com/
[23] Con fecha 26 de abril de 2022, la Asamblea Legislativa de la República de El Salvador aprobó: la Ley de Régimen Especial para la Simplificación de Trámites y Actos Administrativos Relativos al Tren del Pacífico, y la Ley para la Construcción, Administración, Operación y Mantenimiento del Aeropuerto Internacional del Pacífico.
[24] IMF Press Briefing, June 10,2021
[25] "Adoption of Bitcoin al legal tender raises a number of macroeconomic, financial and legal issues that require very careful analysis so we are following developments closely and will continue our consultation with authorities".

Aún sin contar con un acuerdo con el Fondo, el pasado mes de febrero[26] el equipo a cargo de El Salvador comentó cuatro riesgos del uso del bitcoin como moneda de curso legal:

12.1 Estabilidad financiera en cuanto a la exposición de los bancos y otras entidades financieras a fluctuaciones masivas en el precio de los criptoactivos –necesidad de introducir reglas prudenciales de capital y liquidez, fortalecimiento de la regulación y supervisión de Chivo-;

12.2 Integridad financiera, en cuanto los criptoactivos puedan abrir la puerta a dinero ilícito, financiamiento al terrorismo y evasión de impuestos por el anonimato que estos proveen –cibercriminales pueden poner en riesgo la estabilidad del sistema afectando las relaciones con corresponsales-;

12.3 Protección al consumidor: familias y negocios tomando posiciones y ahorrando en bitcoins podrían perder riqueza ante grandes movimientos en su valor. Además, en un ambiente digital es siempre un riesgo el cibercrimen y el robo, más grave aún considerando los niveles de pobreza de la población, y

12.4 Contingencias de responsabilidad fiscal, dado que el fondeo para hacer el bitcoin moneda de curso legal ha sido realizado con fondos públicos a través de un fideicomiso, previendo la necesidad de futuros fondeos para garantizar la convertibilidad.

Consideramos que en estas posiciones encontramos un detallado análisis de identificación de riesgos, lo cual constituye el principal e inicial paso para poder diseñar su mitigación. Nuestra intención no es pronunciarnos al respecto de cada uno, pero sí proporcionar en esta lectura los elementos que permitan al interesado evaluar si esos riesgos ya están puestos sobre la mesa y si las mitigantes están implementadas o en proceso. Desde la visión de un administrador de riesgos, diremos que vamos con buen paso, que el Fondo confirma la ruta y que ojalá se llegue pronto a un entendimiento.

Volvamos luego de este recorrido a las tres preguntas inicialmente propuestas sobre la adopción del bitcoin.

13. ¿Por qué ahora?

No podemos desconocer importantes fenómenos que se aceleraron a raíz de la pandemia, que implicaron cambios en el comportamiento de las personas y se han convertido en factores de éxito de decisiones empresariales orientadas a la transformación de los procesos y modelos de negocio:

13.1 La relevancia de la generación de información, su uso y análisis; principalmente la capacidad de rentabilizarla o monetizarla, encontrando el valor agregado que aporta en la interacción con las personas y la efectiva satisfacción de sus necesidades. Un parámetro para estimar su relevancia es la cantidad de información generada: en el año 2018 se generaron 33 zettabytes de información equivalentes a la información que pueden almacenar 33 millones de cerebros humanos; cantidad y crecimiento que resultan abrumadores al compararlos con la generada en 2010 y 2015, correspondientes a 2 y 12 zettabytes, y que se estima llegará

[26] IMF NEWS, "El Salvador´s Comeback Constrained by Increased Risk" by the EL Salvador country team, IMF Western Hemisphere Department, February 16, 2022.

en el 2030 a 612[27]. Otro parámetro es la rentabilidad de las empresas que lo han entendido: para 2020, de las ocho empresas con la más alta capitalización de mercado, siete tienen a la base la gestión de la información[28]; estamos en el momento en el que los Gigantes de la Tecnología o BigTechs contabilizan su rentabilidad por minuto[29].

13.2 Los cambios en los comportamientos de los usuarios representan otro factor de interés. Mientras hace apenas unos años era difícil que un cliente autorizase el uso y tratamiento de sus datos personales, hoy en día el 78% está dispuesto a compartir sus datos y a realizar operaciones bancarias con empresas de tecnología. Este hecho repercute en un mejor conocimiento de los intereses de los clientes y les permite recibir ofertas relacionadas solo con aquello de su específico interés[30]. Son esas mismas personas, cuyos hábitos están siendo medidos por las interacciones en Internet, en las diferentes plataformas, quienes generan información sobre su comportamiento, gustos, elecciones, tiempos de uso de dispositivo, tipo de contenido que consumen, compras, etc.[31].

13.3 La Uberitización -también conocida como Uberización- del dinero: Mark Carney, ex Gobernador de los Bancos de Inglaterra y Canadá, ha denominado la Uberitización del dinero a este momento en el que se combinan dos grandes ecosistemas: el de las redes sociales y el de los sistemas de pagos[32]. En efecto, hoy en día tenemos acceso a cualquier video: YouTube; escuchamos cualquier canción: Apple music, Spotify; vemos cualquier película o serie: Netflix, Apple TV, Disney Channel; utilizamos cualquier vehículo: Uber; dormimos en cualquier cuarto: AirBnB. Entonces, quizás estemos también dispuestos a utilizar cualquier *moneda*.

13.4 De suma relevancia resulta el fenómeno Fintech, esa conjunción del mundo financiero y el tecnológico que está revolucionando los servicios financieros soportados en la transformación digital, generando más valor agregado que el de la mera suma de ambos mundos. Estudios del Centro para las Finanzas, la Tecnología y el Emprendedurismo -CFTE[33] muestran el rápido crecimiento y capitalización de mercado logrado por un grupo de 50 Fintech entre 2014 y 2019[34]; de estas, doce lograron una valuación que supera el billón de dólares; 33 a 2019 contaban ya con 319 millones de clientes, superando los 306 millones que a ese momento tenían de manera combinada Citi, Bank of America y HSBC. De este estudio destaco una frase de Tram Anh Nguyen, que refleja el espíritu de este fenómeno: *Algunas organizaciones se apalancarán en la tecnología y triunfarán. Otras no serán capaces de adaptarse, y se quedarán atrás. Lo mismo aplicará a las personas.* Este Grupo actualizó su estudio en el 2021[35] bajo el enfoque de que la *Tecnología se está comiendo a las Finanzas*; muestra un crecimiento de adopción Fintech del 16% en 2015 a 64% en 2019. En la misma tendencia, el valor de mercado de las 100 Fintech más importantes representa a 2021 el

[27] Buss, Sebastian et al "Digital Economy Compass 2019." Statista, 2019. https://www.statista.com
[28] Statista, "The Age of the Tech Giants." Statista, 2021. Sources: Financial Times, Yahoo! Finance. https://www.statista.com
[29] Statista, "Tech Giants Earn Fortunes by the Minute" Statista, 2021. Source: CNBC. https://www.statista.com
Rentabilidad por minuto entre los $55 Mil y $837 Mil.
[30] Kruger Innova y Open Vector. "Open Banking /Open Finance", Taller para Banco Agrícola, S.A., 2021
[31] Statista. "A Minute on the Internet in 2021." Statista, 2021. Source: Lori Lewis via AllAcces. https://www.statista.com
[32] Ledger Insights, Banking news. "Mark Carney: stable coins should have access to central bank balance sheet." Published: june 28, 2021.
[33] Nguyen Trieu, Huy et al "Fintech 59: 5 years in Fintech." CFTE Centre for Finance Technology and Entrepreneurship. CFTE 2019. https://blog.cfte.education/fintech-50-5-years-in-fintech/
[34] Heap, Ben. "The 50 Best Fintech Innovators Report 2014."KPMG/AWI/FSC, 2014. https://www.planet-fintech.com/file/163911/
[35] Nguyen Trieu, Huy et al "The Fintech Job Report – Technology is eating Finance." CFTE Centre for Finance Technology and Entrepeneurship. CFTE 2021. https://courses.cfte.education/wpcontent/uploads/2021/11Fintech_Job_Reports_2021_CFTE.pdf?

38% de la capitalización de mercado de los 100 mayores bancos[36]; igualmente, los tres principales rubros de inversión de las empresas para 2019 y 2020 corresponden a mejorar la experiencia digital de los consumidores, intensificar las capacidades analíticas de datos y reducir los costos operativos[37].

13.5 Como resultado de lo anterior, se percibe el rápido desarrollo de las Finanzas Descentralizadas -DeFi-, conjunción de la evolución y desarrollo de la plataforma blockchain, los activos digitales y los servicios financieros. Un mundo que, prescindiendo de los terceros de confianza o reemplazándolos por la confianza en las plataformas, con inversiones registradas a inicio de 2019 de US$275 millones, había atraído a febrero de 2021 inversiones en torno a US$1.2 billones[38], proporcionando al público en general desde servicios financieros específicos hasta lo que podríamos llamar verdaderos supermercados de servicios que integran servicios financieros de intermediación, seguros, sistema de pagos, inversiones bursátiles, inversiones en activos digitales y criptomonedas, así como casas de cambio tradicionales y exchanges para las operaciones con criptomonedas, y la integración del manejo de cuentas de servicios digitales como Amazon, Apple Pay, Spotify, etc. Un ejemplo de ello es Revolut, bajo su esquema One app, All Things Money[39].

A la base de estos fenómenos se encuentran nuevas tecnologías y aplicaciones que facilitan su adopción universal, el acceso sin fronteras, el uso sin restricción de arquitectura e infraestructura, adopción al margen de si existe legislación o si se entiende o no su funcionamiento. Destaco las siguientes:

- Blockchain, una base de registros descentralizada, compartida e inmutable que facilita el proceso de registro o resguardo de transacciones y la trazabilidad de los activos. Opera sobre los principios de un protocolo contenido en el White Paper[40] de Satoshi Nakamoto[41] -se cree que es un seudónimo-. Ha dado paso a gran cantidad de desarrollos, siendo el más destacado y su propósito original el bitcoin; así mismo, ha atraído a una entusiasta comunidad colaborativa que invita a sustituir a los terceros de confianza tradicionales[42] por la confianza en la robustez e inalterabilidad de la plataforma. Es el nuevo lienzo para el registro de transacciones seguras.

- Los contratos inteligentes o *smart contracts*, propuestos por *Nick Szabo*[43] en 1994, que se destacan por ser autoejecutables y que mitigan y prácticamente eliminan la posibilidad de incumplimiento de las prestaciones pactadas. Estos elementos plantean una nueva dimensión en el aseguramiento de las obligaciones, generando un entorno de confianza y quizás promoviendo un estándar aspiracional de pronta y cumplida justicia, esa aspiración de que los pactos deben ser cumplidos -*pacta sunt servanda*-.

- Las operaciones de finanzas descentralizadas y los servicios financieros prestados por las Fintech -pago de intereses, cobros de deuda, etc.-, cuya base de contraprestación

[36] Ibídem.
[37] Ibid.
[38] NFT Trending Crypto Art "DEFI Decentralized Finance, After Bitcoin & Ethereum." Cryptocurrency Investment Guides May 20, 2021. ISBN-10 1838365869
[39] https://www.revolut.com/
[40] Documento conciso de acceso público que con autoridad da guía sobre los principios esenciales sobre cómo enfrentar, decidir o resolver un asunto.
[41] https://bitcoin.org/bitcoin.pdf
[42] Estado, Banco Central, Supervisor, Regulador, Notarios, Bolsas de Valores, Bancos, registros contables, etc.
[43]https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

suelen ser las criptomonedas y los criptoactivos a los que se vinculan; es decir, son los vehículos que permiten prestar y recibir servicios, y asumir compromisos en este mundo intangible, con un importante componente de mitigación de riesgo. Constituye la nueva forma de relacionarse y generar confianza.

• Las APIs[44] que complementan, enriquecen y facilitan su operatividad; esos canales estándar que hacen la función de intermediario, posibilitando que diferentes programas puedan interactuar entre sí y compartir información, facilitando la conectividad, el consumo de soluciones prefabricadas y permitiendo acceso universal a los activos que escojamos compartir. Los desarrolladores pueden conectar -enchufar- sus aplicaciones y *data* para enriquecer la experiencia de los usuarios, apalancándose en los datos y servicios de otras aplicaciones. Esta modalidad impulsa el desarrollo de productos y servicios a la medida, que suman las capacidades del ecosistema para tocar de manera integral la cotidianeidad de las personas. Este elemento nos lleva a concluir cómo, en un mundo interconectado, el desarrollo de una idea de negocio no necesita partir de cero; basta el adecuado caso de uso de un servicio para que, sobre la plataforma de blockchain esa idea, sumada a contratos inteligentes con proveedores y receptores de servicios, más la conectividad que puedan dar algunas APIs, pueda tener repercusiones importantes al apalancarse en este ecosistema colaborativo. Por ello, es este uno de los mejores momentos para hacer crecer una idea que, sumada a un ecosistema inclusivo y colaborativo, no tiene fronteras. Representa los nuevos canales que conectan la información, los proveedores y las ideas transformadoras de negocios y servicios.

Estos desarrollos y los constantes cambios en el comportamiento, en la forma de interactuar con los demás y con proveedores de servicios son el contexto para responder la pregunta de: ¿Por qué ahora? Sin duda es el momento de evolucionar, de reinventarnos, de innovar.

14. ¿Por qué bitcoin?

A abril de 2021 la capitalización del mercado cripto alcanzaba US$2,200 billones, de los cuales el bitcoin representaba US$1,172 billones[45]. Para ese mismo año, el 7% del comercio mundial se tranzó en bitcoins[46], y al menos para el inversionista en Estados Unidos las criptomonedas ya representaban el 4% de sus preferencias de inversión para el largo plazo[47]. El 25 de julio de 2002, Binance compartió la noticia que el mercado cripto alcanzaba un valor de mercado de US$1.03 trillones, de conformidad con los datos de CoinMarketCap[48].

Si imaginamos un mapamundi, podríamos colorear en tres grupos los países que han regulado las criptomonedas: los que las han prohibido expresamente y aquellos en los que hay prohibiciones implícitas; muy pocos países quedarían sin color. Para El Salvador escogería un color diferente, pues no solo reguló, sino que adoptó el bitcoin como moneda de curso legal.

No resulta difícil comprender por qué a un país que desea incursionar en el mundo de los criptoactivos y específicamente adoptar una criptomoneda como moneda de curso legal, le

[44] An application-programming interface.
[45] Statista "Two Trillion Dollars Worth of Crypto." Statista 2021. Source CoinMarketCap.
[46] Statista "Qué tan comunes son las Criptomonedas en el mundo." Statista 2021. Fuente: Statista Global Consumer Survey.
[47] Statista "Stock Market is America´s Favorite Investment". Statista 2021. Source: Bankrate.
[48] https://coinmarketcap.com

resulta más eficiente optar por aquella moneda que representa los atributos de seguridad y confianza, sumándose a la plataforma y prestatarios de servicios ya existentes, así como a las tecnologías ya probadas y de acceso universal. Entre estos atributos es válido listar: (i) inmutabilidad y seguridad de la plataforma blockchain; (ii) el bitcoin como una moneda sin representación física, cuya posesión material no es posible, solo tener control sobre las claves o llaves que nos dan acceso a la misma y nos determinan como sus titulares; (iii) un sistema de emisión de bitcoins conocido como minería –mecanismo de acceso público que adjudica cada bitcoin creado y da la certeza de la cantidad y límite máximo de la moneda en circulación- controlado y definido por el protocolo de Satoshi Nakamoto; (iv) trazabilidad desde el minado hasta la última transacción, pasando por toda su historia de recorrido y transaccionalidad en la plataforma blockchain que impide su anonimato -a diferencia de lo que tradicionalmente se dice a propósito de la prevención de lavado de dinero-, y (v) principalmente la adopción del bitcoin por millones de personas que lo utilizan ya como medio de pago o como medio de acumulación de valor.

Podemos inferir que la decisión de adoptar el bitcoin conlleva eficiencias si la comparamos con lo que representaría desarrollar tecnología y/o plataformas propias, ser responsable de su emisión o minado, sus reglas de uso y transacción, los aspectos de ciberseguridad, su resguardo de valor ya sea como una *stablecoin* -respaldada por activos específicos- o una CBDC -*Central Bank Digital Currency*-, que es la representación digital de una moneda emitida por un banco central con respaldo soberano, en relación con la cual incluso los países más desarrollados, con capacidades y recursos para implementarlas con los más altos estándares, siguen dando pasos cautelosos, estudiando el tema, haciendo pruebas, desarrollando marcos regulatorios, midiendo impactos, etc.

15. ¿Por qué en El Salvador?

Entendiendo el contexto actual y tomando en cuenta el recorrido al que nos han acompañado en esta lectura, a la pregunta de: ¿Por qué en El Salvador? podríamos responder: ¿Por qué no? Pero como responder a una pregunta con otra puede percibirse de mal gusto, diremos que así como El Salvador ha experimentado desde el año 2001 los beneficios de haber dolarizado su economía, haciendo frente a las consecuencias de no contar con su propia moneda[49] y política monetaria[50], de similar manera, guardando las distancias conceptuales, económicas y regulatorias, ha propuesto a los salvadoreños adoptar como posibilidad para su sistema de pagos un activo intangible bajo la figura de criptomoneda y un protocolo específico, el bitcoin, como una alternativa para el comercio y sus transacciones, para el intercambio de bienes y servicios, para realizar pagos y acumular valor.

De otra parte, adoptar un cambio de esa magnitud en 90 días no era posible sino mediante una criptomoneda que contara con un amplio ecosistema de casos de uso, proveedores de servicios, posibilidad de transformar casi cualquier otra moneda a esa criptomoneda a través de un exchange, y que contara además con las tecnologías disponibles blockchain y *ligthning*; a pesar de los retos de desarrollos de conectividad e integración que implicaba, se encuentran soluciones de *plug & play* disponibles, y por ello resultó eficiente y segura la manera de proponer un cambio con este nivel de impacto.

[49] El colón.
[50] Aunque la ley estableció un sistema de bimonetarismo: colón y dólar, en la práctica circula únicamente el dólar.

Importante aclarar que el bitcoin no viene a sustituir al dólar, sino a sumarse como una opción adicional, con las facultades liberatorias de una moneda de curso legal. Además, no hay una sustitución del circulante desde una definición centralizada, sino que se deja a opción de las personas su adopción a través de la adquisición directa, salvo lo correspondiente al monto destinado por el Gobierno para promover la adopción, que es un aporte en bitcoins equivalente a US$30 para cada salvadoreño que active su billetera Chivo.

El Salvador pudo implementar la dolarización en 2001 porque sus reservas internacionales le permitían sustituir el dinero circulante en colones por dólares. Hoy nos encontramos ante un fenómeno que, sin desconocer sus riesgos, no requiere de la posibilidad que tenga un país para hacer esa adopción y transformación, sino de una decisión de apertura a un mundo de plataformas tecnológicas que desde una visión descentralizada y sin terceros de confianza -sin el respaldo de un emisor de moneda oficial y su tecnología, ni la confianza que puede generar un Estado o un banco central- genera confianza en sus usuarios desde el diseño de su protocolo y plataforma, reglas de uso e interacción. Por ello, su adopción en menor o mayor escala depende de las decisiones de cada persona sobre cuánto de su patrimonio invierte en criptoactivos o en criptomonedas. En este sentido, la adopción del bitcoin como moneda de curso legal viene a facilitar, a generar incentivos e incluso a promover el acceso a la tecnología y a la conectividad, para que los individuos tomen sus propias decisiones respecto de la criptomoneda; es un modelo de atracción de inversión, de generación de casos de uso y de inclusión financiera. Tal como señalé en nuestro viaje de Bitcoin Beach a Bitcoin City, más que una ley o una decisión de adopción del bitcoin, esta ruta abarca todo un ecosistema cuyos puntos de conexión incluyen, además de la Ley Bitcoin, proyectos hechos realidad en 90 días por los actores económicos, las normas emitidas por el BCR, la solución Chivo con billetera digital en bitcoins y dólares, un mecanismo automático de conversión, el servicio Transfer 365, una oficina de innovación, las lecciones aprendidas, conectividad y entorno colaborativo de los actores.

El Proyecto Bitcoin en El Salvador nos permite reflexionar sobre las oportunidades de negocios para integrar lo que parecerían ser dos mundos independientes: el mundo de las plataformas y el mundo tangible del sistema financiero, un mercado no *regulado* o sin terceros de confianza, con el mundo en el que el tercero de confianza es el garante del funcionamiento. El caso de El Salvador nos muestra que, cuando un Gobierno toma una posición en este ecosistema, el reto es el desarrollo institucional y de infraestructura para integrar esos dos mundos desde la perspectiva política y económica, manejo fiscal, de deuda, calificaciones de riesgo, etc.

Los retos y éxitos de este proyecto pueden analizarse desde diversas perspectivas. Con casi un año en operación y con mucho optimismo y camino por recorrer, podemos afirmar los siguientes beneficios:

- El Salvador dejó de ser el país de las *maras* o las *pandillas* para convertirse en el país del bitcoin. Tanto desde la perspectiva de la imagen país como de lo que representa para el colectivo de los salvadoreños, este es de suyo un importantísimo beneficio.

- Es el mayor proyecto de inclusión financiera que ha puesto a disposición de todos los salvadoreños poseedores de su Documento Único de Identidad[51] una *wallet* con

[51] Mayores de 18 años.

una billetera digital en bitcoins y dólares; 66.15%, de un total de 6.5 millones de salvadoreños en el territorio nacional, tienen ahora una billetera digital interconectada con el sistema financiero, que permite la integración de bancarizados y no bancarizados en un ecosistema que amplía la capacidad, tejido y efectividad del sistema de pagos. Ha llevado la bancarización al nivel de los países más desarrollados e inclusivos en Latinoamérica.

- Se ha constituido en una herramienta de empoderamiento financiero, al ser una oportunidad de bancarización que pone al servicio del comerciante, de todo nivel, un sistema de pagos para potenciar las ventas, ampliando las posibilidades para la recepción de pagos y su escalamiento, otorgando acceso a bajo costo a un amplio ecosistema de servicios, red de distribución y posibilidades de negocio.

- Ha puesto a El Salvador en los ojos de los proveedores de servicios y entusiastas del bitcoin. Los primeros efectos los podemos percibir en el crecimiento de registros de proveedores bitcoin en el Banco Central de Reserva y el turismo focalizado y especializado. Queda esperar la materialización en el corto y mediano plazo de las inversiones que puedan generarse en el sector real y el efecto que se pueda apuntalar desde Bitcoin City para la atracción de inversión sostenible.

El reto no radica en el éxito o no del Proyecto Bitcoin, ni siquiera en la efectiva medición de impactos de su volatilidad y cambios de valor, o sus efectos como moneda de curso legal. El reto requiere la visión integral como política pública, que propicie la concurrencia de un El Salvador que opera en el mercado internacional, los mercados regulados y la geopolítica tradicional, con un El Salvador de apertura al entorno digital, que opera en el mundo intangible de las plataformas y el bitcoin, de manera que de la suma de estos dos ecosistemas resulte un mejor El Salvador.

Bibliografía

Banco Central de Reserva de El Salvador. Circulares 615 y 616. Documentos publicados para consulta con fecha 17 de agosto de 2021.

Banco Central de Reserva de El Salvador. Lanzamiento de la Oficina de Innovación Financiera como iniciativa conjunta del Banco Central de Reserva y la Superintendencia del Sistema Financiero. https://www.bcr.gob.sv/2021/12/03/el-banco-central-de-reserva-y-la-superintendencia-del-sistema-financiero-lanzan-oficina-de-innovacion-financiera/

Banco Central de Reserva de El Salvador. Lanzamiento del servicio Transfer 365. https://www.bcr.gob.sv/2021/06/07/bcr-pone-a-disposicion-de-los-usuarios-el-servicio-transfer365-para-realizar-operaciones-bancarias-24-7/

Banco Central de Reserva de El Salvador. Norma NRP-29 aprobada por el Comité de Normas del BCR, CNBCR-12/2021 del 7 de septiembre de 2021.

Banco Central de Reserva de El Salvador. Registro de Proveedores Bitcoin. https://registrobitcoin.bcr.gob.sv/web/proveedores-registrados

Banco Central de Reserva de El Salvador. Resolución de Consejo Directivo 29/2021 "Lineamientos para la autorización del funcionamiento de la plataforma tecnológica de servicios con bitcoin y dólares", aprobada el 7 de septiembre de 2021.

Basel Committee on Banking Supervision - Consultative Document - Prudential treatment of crypto asset exposures. Issued for comments by September 10, 2021. June 2021. ISBN 978-92-9259-480-0 (online)

Binance. Your week in Crypto, 25th July 2022, Global crypto market cap hits $1T. https://binance.com
https://coinmarketcap.com

Bitcoin Beach. Entrevista a Michael Peterson sobre el Proyecto Bitcoin Beach. https://www.bitcoinbeach.com

Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin white paper. https://bitcoin.org/bitcoin.pdf

Bitfinex. Cryptocurrency Exchange. The home of digital asset trading. https://www.bitfinex.com/

Buss, Sebastian et al "Digital Economy Compass 2019." Statista, 2019. https://www.statista.com

Escudo, Jacinta. "Hablemos en salvadoreño". Columna de opinión publicada en la versión digital de La Prensa Gráfica el 26 de Septiembre de 2021.

Heap, Ben. “The 50 Best Fintech Innovators Report 2014.”KPMG/AWI/FSC, 2014. https://www.planet-fintech.com/file/163911/
IMF NEWS, “El Salvador´s Comeback Constrained by Increased Risk” by the EL Salvador country team, IMF Western Hemisphere Department, February 16, 2022.

IMF Press Briefing, June 10,2021 “Adoption of Bitcoin al legal tender raises a number of macroeconomic, financial and legal issues that require very careful analysis so we are following developments closely and will continue our consultation with authorities”.

Kruger, Innova y Open, Vector. “Open Banking /Open Finance”, Taller para Banco Agrícola, S.A., 2021.

Ledger Insights, Banking news. “Mark Carney: stable coins should have access to central bank balance sheet.” Published: june 28, 2021.

Ley Bitcoin. Decreto Legislativo No. 57 publicado en el Diario Oficial No. 110, Tomo No. 431 de fecha 9 de junio de 2021.

Ley de Creación del Fideicomiso Bitcoin, Decreto Legislativo No. 137 de la Asamblea Legislativa de la República de El Salvador, fechado 31 de agosto de 2021. Publicado en el Diario Oficial No. 165, Tomo No. 432, de fecha 31 de agosto de 2021.

Ley de Régimen Especial para la Simplificación de Trámites y Actos Administrativos Relativos al Tren del Pacífico. Aprobada por la Asamblea Legislativa de la República de El Salvador aprobó, con fecha 26 de abril de 2022.

Ley para facilitar la Inclusión Financiera. Decreto Legislativo No. 72 de la Asamblea Legislativa de la República de El Salvador, fechado 2 de septiembre de 2015. Publicado en el Diario Oficial No.160, Tomo No. 408 del 3 de septiembre de 2015.

Ley para la Construcción, Administración, Operación y Mantenimiento del Aeropuerto Internacional del Pacífico, aprobada por la Asamblea Legislativa de la República de El Salvador con fecha 26 de abril de 2022.

Liquid. Buy, Sale & Trade Crypto. https://www.liquid.com/

Missionsake. Missionary Community in El Salvador. https://missionsake.com

NFT Trending Crypto Art “DEFI Decentralized Finance, After Bitcoin & Ethereum.” Cryptocurrency Investment Guides May 20, 2021. ISBN-10 1838365869
https://www.revolut.com/

Nguyen Trieu, Huy et al “Fintech 59: 5 years in Fintech.” CFTE Centre for Finance Technology and Entrepreneurship. CFTE 2019. https://blog.cfte.education/fintech-50-5-years-in-fintech/

Nguyen Trieu, Huy et al “The Fintech Job Report – Technology is eating Finance.” CFTE Centre for Finance Technology and Entrepeneurship. CFTE 2021. https://courses.cfte.education/wpcontent/uploads/2021/11Fintech_Job_Reports_2021_CFTE.pdf?

Reglamento de la Ley para facilitar la Inclusión Financiera. Decreto Legislativo No. 27 de la Asamblea Legislativa de la República de El Salvador. Publicado en el Diario Oficial Tomo No 432 del 27 de agosto de 2021.

Statista "Qué tan comunes son las Criptomonedas en el mundo." Statista 2021. Fuente: Statista Global Consumer Survey. https://www.statista.com

Statista "Stock Market is America´s Favorite Investment". Statista 2021. Source: Bankrate. https://www.statista.com

Statista "Two Trillion Dollars Worth of Crypto." Statista 2021. Source CoinMarketCap. https://www.statista.com

Statista, "Tech Giants Earn Fortunes by the Minute" Statista, 2021. Source: CNBC. https://www.statista.com

Statista, "The Age of the Tech Giants." Statista, 2021. Sources: Financial Times, Yahoo! Finance. https://www.statista.com

Statista. "A Minute on the Internet in 2021." Statista, 2021. Source: Lori Lewis via AllAcces. https://www.statista.com

Szabo, Nick. Smart Contracts. https://www.fon.hum.uva.nl/rob/Cours.es/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

PARTE 2

EL NEGOCIO FINANCIERO BASADO EN DATOS

CAPÍTULO 4

Inteligencia artificial: la información como modelo de negocio

Juan Pablo García - Andrés Umaña[1]

Resumen

La Inteligencia Artificial -IA- promete cambiar radicalmente la forma de operar los negocios incluyendo el financiero a nivel mundial. De hecho, aunque en escala reducida, las implementaciones de esta tecnología ya permean áreas del negocio financiero desde la prevención del fraude financiero hasta la compra y venta de activos financieros -como las acciones transadas en bolsa-, con resultados inesperados en rapidez, confiabilidad y rentabilidad. Sin embargo, a pesar del gran interés que despierta la IA y los éxitos actuales, los líderes de negocio deben evaluar cómo se enfrentará la disminución en los estándares de privacidad, exactitud y capacidad de control de sus prácticas actuales, causadas por la implementación de herramientas de IA.

[1] Andrés Umaña es abogado corporativo de Microsoft Corporation en el grupo que presta soporte jurídico a los servicios de nube e inteligencia artificial de la compañía. Juan Pablo García es director de Transformación Digital e Inclusión Financiera en la Vicepresidencia Técnica de Asobancaria.

1. Introducción

La creciente popularidad de la Inteligencia Artificial -IA- y su inclusión en las agendas de innovación del sector privado reflejan sus potenciales beneficios[2]. Al mismo tiempo, han surgido preocupaciones sobre la gobernanza y ética de la IA que advierten sobre los riesgos de su implementación.

Estudios recientes muestran cómo se ha acelerado la utilización de IA en los negocios. Una encuesta realizada en 2021 a 1843 líderes empresariales de diversidad de sectores, tamaños y países muestra que 56% de las empresas están adoptando IA en alguna función central del negocio, un incremento de 12% respecto de los resultados del año anterior. La encuesta muestra además que la implementación de estrategias de IA está impactando positivamente las ganancias empresariales. El 27% de los líderes empresariales reportan que al menos un 5% de las ganancias antes de impuestos del 2021 se atribuye a la implementación de IA. Finalmente, la utilización de herramientas de IA es cada vez mayor en empresas de países emergentes y esta tendencia se acelera cada vez más[3]. Sin embargo, a pesar de los beneficios de la introducción de técnicas de IA en los negocios, existen riesgos en su implementación de estas técnicas, en particular, los relacionados con el uso inadecuado de datos personales sobre los que la regulación aún no se ha pronunciado.

Este documento busca informar a una audiencia amplia sobre qué es IA y cuáles son sus beneficios y potenciales riesgos, haciendo énfasis en los efectos sobre la industria de servicios financieros. La primera sección expone una introducción general a la IA y da algunos ejemplos de uso en la industria financiera. La segunda sección analiza los retos de gobernanza y éticos que surgen de la utilización de IA. La última sección concluye y propone las líneas de trabajo necesarias para impulsar la implementación ética de tecnologías de IA en el sector financiero colombiano.

2. IA: creación, desarrollo y estado actual

2.1 IA: desarrollo histórico y principales definiciones

La IA se define como la habilidad de una máquina de realizar funciones cognitivas típicamente asociadas con la inteligencia humana tales como percibir, razonar, aprender y resolver problemas. Los ejemplos más conocidos de la aplicación de IA en la solución de problemas de negocio son la robótica, los vehículos autónomos y el reconocimiento de imágenes y lenguaje[4]. Aunque el desarrollo de la IA inició en 1950, las últimas dos décadas han presenciado una expansión sin precedentes impulsada por progresos en el campo de la estadística, la rápida expansión en la capacidad de cómputo, los incrementos significativos en la cantidad y calidad de la información almacenada, y las fuertes inversiones en investigación y desarrollo en la materia.

En la historia de la IA se distinguen claramente dos paradigmas. En el primero, temporalmente ubicado entre 1950 y 1980, la IA se centró en traducir el conocimiento humano en programas

[2] FCA y Banco de Inglaterra, "Machine Learning in UK Financial Services", Research Note, 2019. Buchanan, B, "Artificial Intelligence in Finance", The Alan Turing Institute, 2019. Cambridge Centre for Alternative Finance y WEF, "Transforming Paradigms: A Global AI in Financial Services Survey", 2020.
[3] McKinsey & Co., "The State of AI in 2021", 2021.
[4] McKinsey & Co., "The State of AI in 2021", 2021.

con reglas explícitas del tipo: si hay una transferencia de más de $10 millones, entonces levante una alerta. En este caso, el conocimiento y la lógica de pensamiento humanos es *impresa* en la máquina mediante un conjunto de reglas explícitas que la máquina sigue al pie de la letra. Debido a que se traducen el conocimiento y lógica humanos en lenguaje de máquina, a esta etapa se le conoce como la IA simbólica. En el segundo paradigma del desarrollo de la IA implementado después de 1980, las capacidades de estos sistemas surgen del análisis estadístico de la información provista o generada de forma autónoma. Por su estrecha relación con la estadística y el manejo de grandes cantidades de información, a esta etapa se le conoce como IA estadística.

La diferencia entre los dos paradigmas de desarrollo de la IA se observa con mayor facilidad a través de los programas diseñados para jugar ajedrez. Del lado de la IA simbólica, los desarrolladores introducen las reglas del juego en el *software*, por ejemplo, *El alfil se mueve diagonalmente siempre en su color*, y adicionan una base de datos con partidas de Grandes Maestros. Desde el inicio, la máquina compara el estado de la partida con la base de datos de los Grandes Maestros y copia de esa base de datos la jugada más exitosa. En este sentido, la IA simbólica tiene una aproximación deductiva -de la teoría a la práctica- al ajedrez y basa su éxito en identificar en dicha base de datos las mejores jugadas para cada situación del juego.

En contraste, en la IA estadística, los desarrolladores le entregan a la máquina bases de datos con partidas y le indican qué debe entender por éxito en este contexto -en el caso del ajedrez, ganar la partida-. Previamente a la partida, la máquina mezcla esos dos elementos usando técnicas estadísticas, lo que le sirve para aprender las reglas del juego, jugar contra sí misma, aprender de sus éxitos y sus errores, y entregar como resultado un programa capaz de jugar ajedrez de forma autónoma. La IA estadística tiene en este sentido una aproximación inductiva -de la práctica a la teoría- al ajedrez y basa su éxito en la capacidad de aprender de forma rápida y autónoma.

La versatilidad, capacidad de aprendizaje y aproximación inductiva de la IA estadística, la han hecho capaz de enfrentar de forma eficiente un rango más amplio de problemas que la IA simbólica y por ello ahora es el paradigma dominante en el desarrollo de la IA. Las facetas más interesantes de la IA estadística han sido el resultado de la aplicación de técnicas de *Machine Learning* -ML- a grandes conjuntos de datos -tanto en bases de datos altamente estructuradas, como en información de difícil categorización tales como imágenes o texto-. En este entorno, las técnicas de ML detectan patrones y aprenden a predecir y recomendar al procesar información de forma inductiva -de los datos a la teoría-, lo que contrasta con el paradigma de la IA simbólica en la que la máquina seguía reglas programadas de forma explícita y razonaba de forma deductiva -de la teoría a los datos-. La IA estadística basada en ML también se diferencia del paradigma anterior en su capacidad de adaptarse de forma automática a nueva información.

Los tipos más comunes de ML son: aprendizaje supervisado, no supervisado y reforzado. En el aprendizaje supervisado, la técnica de ML usa información de entrenamiento sumada a la retroalimentación humana para identificar las relaciones de causalidad entre las variables de un mismo fenómeno -insumos y resultados-. Este tipo de desarrollo se usa cuando conocemos el resultado que queremos predecir y tenemos alguna idea de las variables que lo determinan. Un ejemplo es predecir la posibilidad de venta a un prospecto de cliente

dada la información demográfica y de contacto. En este caso sabemos con claridad qué queremos conocer -probabilidad de venta- y tenemos información de quién es el cliente, cuántas veces nos hemos contactado con él, durante cuánto tiempo, etc.

En el aprendizaje no supervisado la máquina explora la información dada con el objetivo de encontrar patrones. Esta metodología es usada cuando los desarrolladores desconocen cómo clasificar entre insumos y resultados las variables que componen un fenómeno dado; en ese caso se busca que la técnica de IA encuentre patrones y clasifique la información por nosotros. La segmentación de clientes para campañas de mercadeo basados en características demográficas y de relación con el producto o servicio es un ejemplo clásico de esta metodología de ML.

Finalmente, el aprendizaje reforzado usa técnicas que aprenden a maximizar una variable de interés del desarrollador mientras actúan con el medio que determina la variable a optimizar. Se usa en casos donde no existe gran cantidad de información para que la técnica aprenda del medio, no se puede definir claramente el resultado perseguido o la única forma de aprender es interactuando con el ambiente. El ejemplo más ilustrativo del uso de esta técnica es la compra y venta de acciones en el mercado de valores en donde la técnica de IA aprende del mercado y de la rentabilidad de la posición tomada, al comprar y vender títulos, observar el resultado de la acción en el retorno financiero y aprender de los resultados.

2.2 Algunos casos de implementación de la IA en la industria financiera

2.2.1 Inclusión financiera y empoderamiento del cliente

La implementación de técnicas de IA permite a la industria financiera, entre otras, mejorar la forma de operación del negocio y empoderar al cliente en su relación con la industria, lo que resulta en mayores niveles de inclusión financiera. En general, las barreras de inclusión financiera se deben a que el riesgo del potencial cliente es inaceptable para la institución financiera bajo las condiciones de servicio -estructura de costos del negocio- y mercado -tasas de interés- predominantes. En este contexto, la IA contribuye a aumentar los niveles de inclusión de tres formas: (i) reduciendo los costos operacionales; (ii) mejorando el análisis de riesgo, y (iii) generando ofertas personalizadas.

En el primer caso, negocios en donde la atención al cliente se maneje al menos en parte por herramientas de atención robótica -*robo advisors*- tienen costos de operación menores y amplían la capacidad de inclusión de poblaciones con bajo margen de utilidad. En el segundo, para productos financieros que dependen del perfil de riesgo del cliente -préstamos o seguros-, las técnicas de ML permiten generar perfiles de riesgo a clientes sin historial, lo que les abre las puertas del financiamiento y reduce la tasa de interés del crédito o de la prima de riesgo del seguro. En el tercer caso, la formulación de ofertas diferenciadas por tipo de cliente se beneficia por la implementación de técnicas de IA que permiten una segmentación más detallada de los clientes.

A pesar de estos avances, la materialización de estas ventajas en inclusión financiera y empoderamiento del cliente depende de la calidad y cantidad de información disponible. Las ganancias son exponenciales si el cliente crea huella digital de sus actividades a través

de pagos digitales que muestren su transaccionalidad o, en el caso de seguros médicos o de vida, se empodera al cliente de su perfil de riesgo a través del uso de equipos de salud personal que muestren su actividad física.

2.2.2 Falsas alarmas en la detección de crímenes financieros

Los mecanismos de monitoreo y supervisión para la prevención de lavado de activos y fraude pueden generar episodios en los que se declinan injustamente solicitudes de servicios financieros. Tanto en los procedimientos de conocimiento de clientes nuevos como en el monitoreo transaccional de clientes existentes pueden negarse servicios financieros si los modelos de monitoreo tienen altas tasas de falsas alarmas -rechazo de clientes u operaciones válidas-. Estimativos de industria indican que, a pesar de las grandes inversiones en la detección del crimen financiero -los bancos de Gran Bretaña gastan £5 billones al año-, los episodios de falsas alarmas alcanzan US$118 billones anuales y destruyen la relación con el cliente en uno de cada tres casos[5].

La implementación de técnicas de IA en los procesos de monitoreo, supervisión y detección reducen de un lado la posibilidad de falsas alarmas al incrementar la exactitud de la predicción del riesgo, y de otro, disminuyen los costos de la detección errónea al permitir, por ejemplo, el intercambio de mensajes de texto con el cliente que puede confirmar en tiempo real la legitimidad de la transacción que se está ejecutando.

2.2.3 Compra y venta de títulos valores en los mercados financieros

En el manejo de inversiones en el mercado financiero, el interés de los inversionistas puede verse afectado negativamente por conflictos de interés, cargos excesivos y ganancias subóptimas. La implementación de IA beneficia el manejo de las inversiones al mejorar los retornos, hacer el proceso menos costoso, o al ejecutar la estrategia de inversión de forma más eficiente -más rápida compra y venta de activos, menores costos o menor impacto en el mercado en operaciones de gran tamaño-[6] . La implementación de técnicas ML en datos no tradicionales, por ejemplo, disminuyen el impacto de sesgos de comportamiento del corredor en el proceso de toma de decisiones de inversión.

Investigaciones recientes encuentran que la compra y venta de activos por parte de programas creados con técnicas de IA es responsable del 50% de las transacciones de acciones, 60% de futuros y 50% de bonos del tesoro en el mercado de inversión en Estados Unidos[7]. Otros estimativos de industria muestran que el uso de sistemas de compra y venta de activos que usan IA tiene una participación en el mercado de inversiones cercano al 40%[8].

2.3 El potencial de disrupción de la IA en la industria financiera

La toma de decisiones de negocio difíciles está en el día a día de la operación. Ya sea aceptar como cliente a una empresa que opera en un sector usado por la delincuencia para lavar

[5] Javelin Strategy Report, "Future Proof Card Authorization", 2015.
[6] KIRILENKO y LO, "Moore's Law versus Murphy's Law: "Algoritmic Trading and Its Discontents", Journal of Economic Perspectives, 2013.
[7] BRUMER y YADAB, "Fintech Trilemma", Working Paper.
[8] ALDRIDGE y KRACWCIW, "Real-Time Risk: What Investors Should Know About Fintech, High-Frequency Trading, and Flash Crashes", Wiley, 2017.

dinero, aprobar un crédito a una persona con historial de incumplimiento de sus obligaciones financieras, o aprobar una transacción inusual, los negocios deben actuar rápidamente a partir de la información que tengan disponible, con las consecuencias evidentes sobre los resultados financieros de la compañía. En todos estos casos, la implementación de técnicas de IA ha mejorado significativamente las decisiones cuando se las compara con los procesos manuales, poco sistematizados y sobre todo altamente costosos usados previamente. En este sentido, el potencial de disrupción de la IA proviene de la disminución en el costo de hacer buenas predicciones sobre el resultado de una decisión de negocio como las descritas arriba.

Sin embargo, la predicción es solo un componente del proceso de toma de decisiones. Los otros componentes de la inteligencia humana requeridos para la toma de decisiones tales como el planteamiento de los problemas, el juzgamiento, la ejecución y la planeación de estrategias de control, seguimiento y aprendizaje son igualmente importantes. Si bien en la actualidad la IA tiene excelentes resultados en el componente de predicción del proceso de toma de decisiones, el resto de los componentes del proceso permanecen en control de los humanos.

Un ejemplo específico en el que las capacidades de juzgamiento y raciocinio humanas son superiores a las de la IA se encuentra en la aptitud para identificar la causalidad en un fenómeno. Mientras que la IA tiene capacidades superiores a las humanas para identificar correlaciones entre eventos, la inteligencia humana es superior para entender las relaciones de causalidad entre las variables que componen un fenómeno particular. En otras palabras, la IA es excelente a la hora de reconocer patrones, pero, a diferencia de la inteligencia humana, las técnicas usadas en la IA no pueden explicar cómo llegaron a las predicciones y tampoco pueden teorizar sobre las relaciones de causalidad entre las variables. Este último punto es de particular interés si tenemos en cuenta que en muchos casos de negocio es tan importante predecir la ocurrencia de dos eventos -reconocer patrones o ver correlaciones-, como entender su causalidad.

En este sentido, aunque la IA tiene la capacidad de transformar la operación de los servicios financieros en múltiples ámbitos, su efecto va a estar contenido por la necesidad de la inteligencia humana para plantear de forma adecuada los problemas, identificar causalidades y poner en marcha estrategias de negocio para la ejecución de planes de acción y seguimiento.

3. El marco jurídico de los proyectos de IA: privacidad, exactitud, control y otros elementos de análisis

Pese a sus remotos orígenes[9], los sistemas actuales de IA están todavía en una etapa inicial de desarrollo y subsisten muchas discusiones en torno al adecuado marco jurídico para su uso en contextos como el empresarial. A continuación, resumimos algunas de las preocupaciones más importantes:

[9] Los primeros desarrollos de sistemas de inteligencia artificial se remontan a las décadas de los 50 y 60 del siglo pasado. En las décadas de los 70 y 80 estas tecnologías tuvieron un primer periodo de apogeo, que termina hacia finales de los 80 en un periodo de estancamiento, llamado coloquialmente de "invierno", cuando las tecnologías predominantemente usadas en la época, los sistemas expertos basados en bases de datos de conocimiento y razonamiento simbólico, probaron ser demasiado complejas, entre otras dificultades. El apogeo reciente de estas tecnologías se debe en buena medida al crecimiento vertiginoso de las capacidades de procesamiento de información y el surgimiento de tecnologías de Grandes Datos (Big Data), que permiten la utilización de técnicas probabilísticas en el desarrollo de los sistemas de inteligencia artificial.

3.1 El uso masivo de datos, la privacidad y la protección de los datos

Las tecnologías de IA, y particularmente aquellas agrupadas bajo el concepto de ML, requieren de cantidades exorbitantes de datos para su funcionamiento[10], datos que en muchas oportunidades las empresas no recolectan en su giro ordinario, debiendo realizar esfuerzos adicionales para conseguirlos o acudir a terceros con ese fin[11]. Vale la pena revisar algunos de los riesgos jurídicos asociados a estos esfuerzos adicionales.

La primera y más importante consideración jurídica es que, en muchas oportunidades, los datos que se necesitan para entrenar modelos de IA son datos personales. Un sistema de reconocimiento facial exige para su entrenamiento procesar miles de imágenes de rostros humanos[12]. *Un sistema de aprendizaje reforzado* para generar predicciones y recomendaciones de productos financieros a los clientes de una entidad financiera requerirá entrenarse en el historial de compras o servicios adquiridos por muchos clientes, propios o de terceros, personas naturales y jurídicas. Esos datos, si están vinculados o asociados a personas naturales determinadas o determinables[13], o si están asociados al cálculo del riesgo crediticio en el caso de personas jurídicas[14], son datos personales bajo el ordenamiento jurídico colombiano.

Al ser datos personales, salvo excepción constitucional o de ley estatutaria, que no existe para el presente caso, su recolección y uso requiere del consentimiento previo, libre, expreso e informado del titular del dato[15]. Sobre este consentimiento conviene hacer dos precisiones: en primer lugar, el principio de autorización y el de finalidad exigen mencionar el propósito último del tratamiento -por ejemplo, ofrecer productos comerciales, hacer investigaciones de mercado, crear perfiles del titular, etc.-, pero esa exigencia no se extiende a los medios utilizados para lograrlo. Así, en tanto el uso de IA no sea el fin último sino apenas una herramienta para alcanzarlo no habría obligación de mencionarlo en la recolección del dato. No obstante, dada la sensibilidad que genera todo tratamiento de datos personales[16], es recomendable, o bien hacer una referencia expresa a ese uso, o cerciorarse de que, siguiendo el paradigma europeo, el entrenamiento es un uso que puede catalogarse como

[10] Algunos de los primeros sistemas de visión computacional de la pasada década utilizaron como base la base de datos ImageNet, que tiene alrededor de 14 millones de imágenes, y los sistemas actuales utilizan bases de datos mucho más grandes. El sistema de procesamiento de lenguaje natural más conocido en la actual, GPT-3, administrado por Open AI, tiene alrededor de 175 mil millones de parámetros, y es entrenado con información bajada masivamente de Internet y miles de libros, entre otras muchas fuentes de información: OpenAI debuts gigantic GPT-3 language model with 175 billion parameters | VentureBeat.

[11] Esto no significa desconocer que la masificación de estas tecnologías que vivimos en la actualidad se debe en gran medida a que los costos y el tiempo para entrenar sistemas de inteligencia artificial se han disminuido considerablemente. El costo de entrenamiento de los sistemas ha bajado 60% desde 2018. Descontando los costos de hardware, un sistema que costaba USD1.000 en ser entrenado o en día vale USD5, y si en 2018 tomaba 6 minutos entrenarlo hoy en día se puede hacer en menos de 14 segundos (Stanford AI Index).

[12] Las imágenes pueden ser de seres humanos, pero también existen sistemas que a su vez crean imágenes sintéticas de seres humanos para entrenar estos sistemas, pero esto todavía no es una práctica generalizada.

[13] Artículo 3 c de la ley 1581 de 2012.

[14] Artículo 3.e. de la ley 1266 de 2008 establece: "e) Dato personal. Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados";

[15] El artículo 4.c. de la ley 1581 de 2012 establece el principio de libertad, llamado también de Autorización: "c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento";

[16] Aunque muchos de ellos pueden generar más dudas que certidumbre, conviene en todo caso revisar las finalidades que soportarán el uso de datos personales para entrenamiento de sistemas de inteligencia artificial a la luz de los ejemplos de finalidades que se encuentran en la Guía de la Superintendencia de Industria y Comercio denominada "Formatos Modelo para el Cumplimiento de Obligaciones Establecidas en la Ley 1581 de 2012 y sus Decretos Reglamentarios", disponible en el siguiente enlace: https://perma.cc/75N6-8W9N.

compatible con las finalidades anunciadas al titular del dato[17].

La segunda práctica que conviene destacar desde la perspectiva jurídica es la conocida coloquialmente como Raspado de Datos -*Data Scraping*-, que consiste en extraer o bajar información de forma masiva en Internet sin el consentimiento expreso de los titulares de dicha información[18]. El Raspado de Datos se puede hacer sobre cualquier tipo de información: datos personales, imágenes, textos u otras obras protegidas por propiedad intelectual, o información que no ostenta ninguna categoría jurídica particular.

Los problemas jurídicos asociados a esta práctica son múltiples, por eso es una práctica que debe ser examinada detenidamente por los departamentos legales de las empresas. Por una parte, es técnicamente muy complejo determinar si la información que está siendo extraída de manera masiva y automatizada puede considerarse como un dato personal, pues el *dato personal* es una categoría jurídica ambigua, lo que genera un riesgo alto de errores en su clasificación y discusiones sobre su aplicación a casos concretos. El raspado de datos tiene entonces el grave riesgo de recolectar o usar información personal sin el cumplimiento de los principios de autorización y finalidad de la ley 1581. Ocurre algo similar con la información protegida por las normas de propiedad intelectual. Fotografías, videos, música y otros contenidos disponibles en Internet están en gran medida protegidos por el derecho de reproducción del titular del derecho de autor, por lo que su uso como datos de entrenamiento en IA podría eventualmente catalogarse como una violación de este derecho. Es conveniente aclarar que la práctica de raspado en sí misma no es ilegal, pero sí tiene estos importantes riesgos. Estas consideraciones dejaron de ser hipotéticas. En Estados Unidos, la Comisión Federal de Comercio -*Federal Trade Commission*- en mayo de 2021 ordenó a la compañía Everalbum borrar todos los modelos de IA de reconocimiento facial que había desarrollado a partir de datos personales obtenidos ilegítimamente[19]. En el caso de LinkedIn vs. HiQ, uno de los más importantes de los últimos años en estos temas en Estados Unidos, LinkedIn alegó que HiQ hizo raspado de datos ilegal de los perfiles profesionales de dicha red social, y si bien la práctica es considerada legal, de ese caso se desprenden importantes precauciones a tener en cuenta[20].

Finalmente, un último riesgo para la privacidad, que denominaremos de manera genérica como el riesgo de inferencia, tiene a su vez dos componentes. Nos referiremos por ahora al primero de ellos y dejaremos el segundo para el siguiente apartado. Si bien un modelo de IA no incorpora en sí mismo los datos de entrenamiento y, en esa medida, una vez utilizado un dato personal para entrenar dicho sistema ya no se requiere volver a utilizarlo -pues se puede, por ejemplo, reemplazar por otros nuevos-, ya existen técnicas que permiten extraer datos personales privados, usados como entrenamiento de sistemas de IA, a partir de los datos de salida del modelo de IA. Este problema se conoce como ataques de inferencia de membresía

[17] El artículo 5.1.b) del Reglamento General de Protección de Datos de la Unión Europea establece que los datos "…no serán tratados ulteriormente de manera incompatible con dichos fines…". Esta es la doctrina de los usos compatibles, que permite el tratamiento de los datos de manera no expresamente contemplados en la autorización siempre que se supere dicha prueba de compatibilidad.

[18] Cuando se recolecta o indexa toda la información de un sitio de Internet o de una sección utilizando programas o "motores", se suele hablar de Web Crawling a través de "motores", "web crawlers" o "spiders". Cuando se recolecta o indexa sólo parte de la información de un sitio o sección de Internet, se suele hablar de Web Scraping o Web Data Extraction. Cuando, adicionalmente, la información es transformada a otro formato para, por ejemplo, hacerla más fácilmente accesible, se habla adicionalmente de Parsing. En adelante nos referiremos al Raspado de Datos para referirnos de manera general a todos estos fenómenos.

[19] Véase la noticia en la Revista de Derecho y Tecnología de la Universidad de Harvard (https://perma.cc/J3LB-NNPQ) y los documentos del proceso y la decisión de la FTC aquí: https://perma.cc/SLL7-V7LN.

[20] Un resumen de los últimos acontecimientos del caso se encuentra aquí: https://www.forbes.com/sites/zacharysmith/2022/04/18/scraping-data-from-linkedin-profiles-is-legal-appeals-court-rules/?sh=36bc52de2a9c.

o de pertenencia[21]. Aunque no es todavía un problema frecuente en la implementación de sistemas de inteligencia artificial, conviene tenerlo presente porque evidencia la necesidad de tomar medidas por parte de las empresas para proteger la confidencialidad de los datos personales que se usan para entrenar un sistema o en general como insumo en el desarrollo de actividades comerciales, tal como explicamos más adelante.

3.2 La necesidad de exactitud y el problema de la alineación -equidad, transparencia y control-

La adecuada definición de sus objetivos y de los parámetros para predecir es tal vez el principal desafío que enfrenta actualmente el desarrollo de sistemas de IA. Los sistemas de inteligencia artificial cada vez más se están utilizando para tomar decisiones críticas en la vida de los seres humanos, decisiones que en muchas ocasiones son todavía tomadas con una fuerte intervención o control de un ser humano. El acceso a servicios comerciales y financieros, la calificación de nuestro comportamiento, la contratación de empleados, las asociadas con la libertad de los individuos en el sistema penal son decisiones que cada vez más se confían a sistemas de IA. Tradicionalmente, los seres humanos incorporamos valores como la igualdad de tratamiento y la libertad de elección en la manera que como sociedad tomamos decisiones. Pero si en estos sistemas solo se incluyen parámetros que busquen medir su eficiencia frente al cumplimiento de un objetivo, sin incorporar otros que reflejen dichos valores como parte de sus objetivos o como restricciones en el proceso de aprendizaje del sistema, las decisiones de estos sistemas pueden fácilmente generar resultados injustos o contrarios a nuestros valores como sociedad. Esto se ha denominado *Problema de la Alineación*[22].

El principal valor en el que se manifiesta el Problema de Alineación es la igualdad o equidad -*fairness*-. De manera general, se espera que un modelo de aprendizaje de máquinas: (i) obtenga los mismos resultados para datos con las mismas características, y (ii) no utilice otras características no deseadas para realizar diferencias entre estas personas. Si el modelo no arroja este tipo de resultados de manera sistemática, se suele decir que el modelo está sesgado[23]. El sesgo en los modelos de aprendizaje de máquinas es algo común, que hasta hace relativamente poco no había llamado la atención de los abogados. Pero, como vimos atrás, en los últimos años los sistemas de IA cada vez más se utilizan para tomar decisiones que afectan directamente a los seres humanos, especialmente decisiones de asignación de derechos o de recursos, y cuando ello ocurre el sesgo puede constituir jurídicamente una discriminación inconstitucional o ilegal por violar el derecho a la igualdad de las personas afectadas con dichas decisiones.

Este problema se ve exacerbado por la dificultad para definir lo que constituye tratamiento igual o equitativo en circunstancias concretas. La Corte Constitucional suele desprender cuatro mandatos de la igualdad, que aunque sirven de guía resultan todavía muy abstractos para una aplicación concreta: *(a) trato igual a personas en circunstancias idénticas; (b) trato paritario a personas que no están en circunstancias idénticas, pero cuyas similitudes son más relevantes que sus diferencias; (c) trato diferenciado a personas que no están en*

[21] Para una explicación no técnica de los ataques de inferencias de membresía se puede consultar la entrada al respecto del sitio TechTalks, disponible de manera permanente en este enlace: https://perma.cc/3W8R-3F3R.
[22] Véase Christian, Brian, "El problema de la alineación", página 67 y siguientes.
[23] La Organización Internacional para la Estandarización (ISO) define el sesgo como "El grado en el que un valor de referencia se desvía de la verdad", (véase NIST 1270, página 17).

circunstancias idénticas, pero cuyas diferencias son más relevantes; y (d) trato desigual a personas en circunstancias desiguales y disímiles[24]. Esta vaguedad y dificultad de aplicación práctica ha hecho que los equipos multidisciplinarios que desarrollan modelos de aprendizaje de máquinas utilicen definiciones distintas y a menudo contradictorias de igualdad. Un estudio de 2018 encontró que más de 20 definiciones distintas estaban siendo usadas para construir modelos de inteligencia artificial[25]. Así pues, una de las principales labores en la revisión jurídica de un proyecto de IA será asegurarse de que la definición de igualdad utilizada se enmarque en los parámetros establecidos por la Corte[26].

La posible discriminación antijurídica por parte de un modelo de IA se agrava por la dificultad para entender las razones por las cuales produce la discriminación, lo que se conoce como el problema de la transparencia. Como mencionamos atrás, muchos modelos de aprendizaje de máquinas[27] requieren regularmente decenas de millones de datos para lograr niveles de acierto razonables, y esos datos a su vez se procesan utilizando decenas de millones o incluso miles de millones de parámetros[28]. Esto hace que los sesgos sean muy difíciles de identificar, pues, por una parte, no surgen de un parámetro específico sino de la particular combinación de los pesos asignados a miles o incluso millones de los parámetros utilizados en el modelo, y, por otra, la asignación de los pesos de estos parámetros no se hace por el creador del modelo, sino que es el mismo modelo el que, usando algoritmos matemáticos, reasigna autónomamente los pesos en su proceso de aprendizaje.

Han sido muchas las soluciones que se han planteado a estos problemas. La Unión Europea, por ejemplo, ha decidido establecer restricciones al uso de sistemas automatizados que puedan afectar los derechos de una persona o afectarla *significativamente de modo similar* y ha creado un derecho para no verse sometido a dichas decisiones automatizadas[29], a la vez que está discutiendo un proyecto de regulación para establecer medidas específicas para evitar los sesgos de acuerdo con el nivel de riesgo que generan para la sociedad. Las medidas sugeridas para las empresas que pretendan sacar al mercado sistemas de IA que

[24] Sentencia C-050 de 2021, Corte Constitucional de Colombia, disponible en: https://perma.cc/266F-NUWY. A lo anterior se suma que la Igualdad es tratada por la Corte como principio, como valor y como derecho, generando consecuencias distintas en cada caso.
[25] Véase Verma (2018), página 3 y siguientes.
[26] El principal caso que suscitó la preocupación generalizada en torno a la discriminación jurídica que pueden producir los sistemas de inteligencia artificial fue el de la utilización del sistema Compas por parte de múltiples autoridades judiciales de EE.UU. para predecir la reincidencia de reclusos que estaban solicitando su libertad condicional. Un artículo de ProPublica denunció cómo el sistema Compas arrojaba predicciones de mayor riesgo de reincidencia en personas de raza negra vs. personas de raza blanca. Las denuncias llevaron a la suspensión del uso del sistema y a discusiones sobre la transparencia de los algoritmos que se usan en casos sensibles como este, discusión que sigue hasta hoy. El artículo original de ProPública se encuentra aquí: https://perma.cc/QC82-97UB.
[27] Recordemos que el modelo de aprendizaje de máquinas usa algoritmos para analizar estas cantidades gigantescas de datos usando parámetros con distintos "pesos" con los que se encuentran patrones que permiten a su vez hacer predicciones. Estas predicciones, conforme son verificadas, permiten a su vez ajustar progresivamente el "peso" que cada parámetro tiene en hacer predicción acertada, para hacer incrementar el nivel de precisión en nuevas iteraciones (esta progresividad es lo que hace que el modelo "aprenda" – con base en la precisión de sus predicciones ajusta el peso de los parámetros para hacer cada vez mejores predicciones en el futuro).
[28] Los sistemas de inteligencia artificial más desarrollados (llamados recientemente como "modelos fundacionales"), que sirven de base para desarrollar los modelos comerciales, utilizan incluso cantidades muy superiores. Por ejemplo, el sistema de procesamiento de lenguaje natural más conocido, denominado GPT-3, utiliza más de 175 mil millones de parámetros.
[29] El artículo 22 del Reglamento 2016/679 de la Unión Europea, el Reglamento General de Protección de Datos, establece: Artículo 22 *Decisiones individuales automatizadas, incluida la elaboración de perfiles 1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. 2. El apartado 1 no se aplicará si la decisión: a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del interesado. 3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. 4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.*

generen un riesgo alto incluyen análisis de riesgo y mitigación, obligaciones de información, obligaciones de calidad de los datos utilizados como insumo, información adecuada a los usuarios, entre muchas otras[30].

Se ha pensado incluso que la solución al problema de equidad sería tan simple como no usar parámetros sensibles en el modelo, por ejemplo, prohibiendo usar la raza o la condición socioeconómica. También se sugiere utilizar únicamente datos anónimos o seudónimos en el entrenamiento de los modelos, para proteger la privacidad de los titulares de esos datos, tal como explicamos atrás.

Si bien estas prohibiciones tienen sentido en ámbitos restringidos, lo cierto es que desconocen varias realidades de los sistemas de IA. En primer lugar, que los sesgos pueden surgir de múltiples fuentes y en cada una de las etapas de desarrollo de un modelo de inteligencia artificial. En ese sentido, la selección del objetivo del modelo puede contrariar un principio constitucional; los datos que se utilizan para entrenar el modelo pueden estar históricamente sesgados o no ser representativos, o haber sido medidos de manera incorrecta; los parámetros seleccionados pueden reflejar discriminaciones existentes en la sociedad o darles a ciertas características de los datos un peso mayor al que en realidad tienen; los algoritmos utilizados pueden generar un mayor peso a ciertos criterios sobre otros[31].

En segundo lugar, la solución planteada desconoce que en muchas ocasiones la discriminación no surge por la presencia de un parámetro explícito, sino a través de múltiples parámetros que actúan como sustitutos indirectos -*proxies*- del parámetro sensible. Así, eliminar el parámetro sensible no solamente no garantiza que no se genere la discriminación, sino que puede hacerla más difícil de detectar e incluso exacerbarla[32]. En Colombia, si bien no tenemos regulación específica sobre este tipo de problemas en el contexto de sistemas de inteligencia artificial, la ley 2157 de 2021, que modificó la ley estatutaria 1266 de 2008, ejemplifica en cierta medida la aproximación que venimos discutiendo, al establecer la obligación de eliminar la información para garantizar el *derecho al olvido* en el cálculo del riesgo crediticio. Si bien la ley tiene un propósito loable, carece de mecanismos que permitan monitorear el éxito de las medidas adoptadas en ese sentido, por lo que tendremos que esperar algunos meses a su aplicación para medir su verdadero impacto en favor de los deudores. Lo que sí parece claro es que necesitamos todavía regulación más precisa en esta materia.

Finalmente, las medidas técnicas para evitar los sesgos comportan un sacrificio en la exactitud del modelo y tienen, por lo tanto, un impacto negativo en su poder predictivo[33]. Por esto, la eliminación de los sesgos en un modelo de IA no es una labor unilateral o que deba mirarse desde esta única perspectiva, sino que requiere de un delicado balance entre la eficiencia del sistema y la alineación con nuestros valores como sociedad, buscando, en armonía con los pronunciamientos de la Corte Constitucional, evitar *discriminaciones injustificadas entre las personas* y tomar únicamente medidas que sean *proporcionales según las finalidades que*

[30] Un resumen y el proyecto se encuentran disponibles en este enlace: https://perma.cc/M34E-GJP2.
[31] Véase Surech y Guttag (2021).
[32] The Ethical Algorithm, página 67.
[33] Técnicamente se habla del sesgo-varianza, que en este contexto se suele denominar el compromiso "sesgo-varianza" que significa que la alteración de un algoritmo para reducir su sesgo aumenta su varianza, es decir aumenta el nivel de inconsistencia de las predicciones del modelo respecto de un sujeto particular si, hipotéticamente, el algoritmo fuera reentrenado muchas veces en diferentes sets de datos (Lehr y Ohm, 2017) página 697.

con ellas se busca[34].

A futuro, se discute incluso la necesidad de crear un derecho a *inferencias razonables* cuando se utilicen técnicas de *grandes datos* o de IA. Además de la tradicional protección en materia de privacidad, algunos autores argumentan que este nuevo derecho permitiría proteger a las personas de la utilización de sistemas de IA para obtener conclusiones sobre su vida o sus características que no sean acordes con la realidad, o que sean inexactas o impacten negativamente aspectos esenciales de las personas sin que estas tengan la posibilidad de controvertir dichas inferencias o el funcionamiento del sistema que toma la decisión[35].

Aunque Colombia no ha desarrollado regulación especial sobre el tema, la Presidencia de la República ha creado un *Marco Ético para la Inteligencia Artificial en Colombia*, que desarrolla esta problemática y ofrece algunos principios para la implementación de esta tecnología[36].

4. Reflexión final: una debida diligencia para aprovechar la oportunidad

Es indudable que la IA y su aplicación en los negocios, y en particular en la industria financiera, es desde hace algunos años una fuente positiva de disrupción. Por un lado, las empresas pueden ahora tomar mejores decisiones basándose en predicciones más precisas y costos eficientes, lo que mejora su rentabilidad. Por otro lado, los clientes ahora reciben ofertas menos costosas y más adecuadas a sus necesidades.

Sin embargo, existen riesgos de la implementación de técnicas de IA en los negocios, en particular las relacionadas con el uso inadecuado de datos personales sobre los que la regulación aún no se ha pronunciado. Ante un panorama regulatorio un tanto sombrío, conviene preguntarse por la manera cómo las empresas pueden aprovechar la oportunidad que representa la IA. Lo primero que debe destacarse es que ninguno de los riesgos que hemos presentado es un obstáculo para implementar esta tecnología en el sector financiero. Estos riesgos no son distintos o más prominentes que otros que las entidades financieras enfrentan rutinariamente cuando implementan nuevas tecnologías. Adicionalmente, todos los riesgos que hemos presentado pueden mitigarse, o bien creando un proceso interno que acompañe y evalúe todos los pasos de la creación del sistema de IA, o bien mediante medidas contractuales en las relaciones con terceros. Mientras la regulación se desarrolla, las empresas pueden implementar marcos éticos y procedimientos de cumplimiento que les permitan prevenir o mitigar estos riesgos.

Siguiendo la estructura del Marco Ético de la Presidencia de la República, podemos decir que estas medidas deben considerar la definición del objetivo y sus funciones del sistema, una aplicación estricta del principio de responsabilidad demostrada en el manejo de los datos para entrenarlo -ética de los datos-, una adecuada identificación y calibración de los parámetros y de los algoritmos usados -ética de los algoritmos- y un conjunto de prácticas que permitan identificar y corregir sesgos en el sistema y usarlos solamente en aquellas circunstancias en las que exista un adecuado balance entre exactitud y riesgo -ética en las prácticas-.

[34] En la sentencia T-1266 de 2008, la Corte Constitucional analiza la constitucionalidad de requisitos físicos en ciertos cargos públicos de las Fuerzas Armadas. La sentencia está disponible aquí: https://www.corteconstitucional.gov.co/relatoria/2008/T-1266-08.htm#_ftnref58.
[35] Véase Wachter (2019).
[36] El Marco Ético está disponible en la página https://inteligenciaartificial.gov.co, en la que se compendian los documentos y proyectos más importantes del Gobierno colombiano en esta materia.

Bibliografía

Aldridge y Kracwciw, “Real-Time Risk: What Investors Should Know About Fintech, High-Frequency Trading, and Flash Crashes”, Wiley, 2017.

Brumer y Yadab, “Fintech Trilemma”, Working Paper.

Buchanan, B, “Artificial Intelligence in Finance”, The Alan Turing Institute, 2019.
Cambridge Centre for Alternative Finance y WEF, “Transforming Paradigms: A Global AI in Financial Services Survey”.

Christian, Brian, “The Alignment Problem: Machine Learning and Human Values”, W.W. Norton & Company, Primera Edición, 2020. The Ethical Algorithm.

FCA y Banco de Inglaterra, “Machine Learning in UK Financial Services”, Research Note, 2019.

Javelin Strategy Report, “Future Proof Card Authorization”, 2015.
McKinsey & Co., “The State of AI in 2021”, 2021.

Kirilenko y Lo, “Moore’s Law versus Murphy’s Law: “Algoritmic Trading and Its Discontents”, Journal of Economic Perspectives, 2013.

Lehr, David y OHM, Paul, “Playing with the Data: What Legal Scholars Should Learn About Machine Learning”, UC Davis Law Review, Vol. 51 (2017-2018), disponible en: https://perma.cc/EC3B-QGF8.

NIST Special Publication 1270, “Towards a Standard for Identifying and Managing Bias in Artificial Intelligence”, Marzo de 2022, disponible en: https://perma.cc/ZG93-AHLZ.
Stanford AI Index Report 2022, disponible en AI Index 2022 | Stanford HAI.

Suresh, Harini y Guttag, John, “A Framework for Understanding Sources of Harm throughout the Machine Learning Life Cycle”, publicación de la ACM en la conferencia EAAMO ‘21, disponible en: https://perma.cc/8XY4-MTRH.

Verma, Sahil y Rubina, Julia, “Fairness Definitions Explained”, 2018 ACM/IEEE International Workshop on Software Fairness, 2018. Disponible en: https://perma.cc/RS5C-UHUC

Watcher, Sandra y Mittelstadt, Brent, “A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI” (October 5, 2018). Columbia Business Law Review, 2019(2), disponible en: https://ssrn.com/abstract=3248829

CAPÍTULO 5

Desafíos jurídicos del *score* de crédito

Natalia Tovar Ibagos[1]

La mémoire est l´avenir du passé, Paul Valéry

Resumen

Las nuevas regulaciones y la evolución del mercado crediticio ponen de presente la discusión en torno a la información que puede ser utilizada en los *scores* de crédito, no solo en términos de lo que es legal, sino desde la perspectiva de lo que es válido o aceptable, considerando el tratamiento justo y transparente de la información de los titulares de los datos. Implica poner en una balanza los diferentes principios que rigen el procesamiento de datos personales, como son los de libertad, finalidad, necesidad y pertinencia, entre otros, así como la valoración ética de su uso. Este ensayo presenta algunas consideraciones para encontrar un balance entre el resultado que se espera obtener con los *scores* y los fines propios del uso y tratamiento de la información que alimenta la medición, sin dejar de lado los derechos y libertades de los titulares.

[1] Vicepresidente Jurídico y de asuntos corporativos de Experian para la región Spanish Latam. Desde 1996 trabaja en el tema de tratamiento de datos personales.

1. Introducción

En la era digital, los datos, la automatización y la analítica son los motores que permiten avanzar en la inclusión financiera y en la democratización del crédito.

Se pone entonces de presente la discusión en torno a los datos que pueden ser utilizados para la evaluación del riesgo de crédito y, particularmente, para el cálculo de los *scores* de crédito. No solo en términos de lo que es legal, sino también desde la perspectiva de lo que es válido o aceptable, considerando el tratamiento justo y transparente de la información de los titulares, que son las personas a quienes se refieren los datos, incluidos aquellos datos de naturaleza financiera y crediticia. Esto implica poner en una balanza los diferentes principios que rigen el procesamiento de datos personales, como son los de libertad, finalidad, necesidad y pertinencia, entre otros, así como la valoración ética de su uso.

En este escrito presento algunas consideraciones con el propósito de encontrar un balance entre la finalidad del cálculo de los *scores* de crédito, el tratamiento razonable de la información que alimenta la medición y los derechos y libertades de los titulares de los datos.

Para estos efectos se abordan en un primer bloque las siguientes preguntas generales:

- ¿Qué es un *score* de crédito?
- ¿Cómo se calcula un *score* de crédito?
- ¿Cómo nació el *score* de crédito y cuál es su propósito?
- ¿Cuál es el propósito de tratar la información financiera y crediticia que se utiliza para el cálculo del *score* de crédito?
- ¿Cuáles son los principios de tratamiento de información aplicables al *score* de crédito?

En un segundo bloque se revisan los desafíos para lograr que, mediante el análisis de la información personal, se contribuya a consolidar un sistema de crédito equitativo, inclusivo y dinámico, sin incurrir en prácticas discriminatorias que excluyan a los titulares del crédito formal.

2. El *score* de crédito

2.1 ¿Qué es un *score* de crédito?

El *score* de crédito es el resultado numérico de un proceso matemático y sistémico, que parte de un análisis estadístico del comportamiento pasado para predecir el comportamiento futuro de manera fiable.

Para explicarlo, empezaremos con una analogía. Imaginemos un campeonato de fútbol, del que nos interesa saber qué equipo tiene mayor probabilidad de ganar.

¿Cómo se construye un *score* en este caso?

Primero, se define la población, que serán los equipos de primera categoría de ese campeonato.

Después se seleccionan las variables. Para este ejercicio se desestiman las variables subjetivas -como la pasión por la camiseta- y se seleccionan, con información histórica, las variables objetivas con más peso y de las que se cuente con información veraz y completa. En este caso, podrían ser el número de partidos ganados, perdidos y empatados, campeonatos de esa categoría ganados por el técnico, participación en partidos internacionales y nómina de jugadores, entre otros.

Una vez seleccionadas las variables, se definen las características de la muestra, es decir, se determina el periodo de observación y el tamaño de la muestra. Podría ser un análisis de los últimos cinco años de los equipos de primera categoría de las ciudades capitales.

Definidas la población, las variables y las características de la muestra, se analiza su comportamiento -por ejemplo, número de partidos ganados- en los equipos de primera categoría de las ciudades capitales durante los últimos cinco años. Con base en los resultados, se pondera estadísticamente cada variable para desarrollar un proceso matemático y sistémico.

A todos los equipos de la primera categoría se les aplica el proceso matemático y sistémico, y al final cada equipo va a tener un *score*, que es un resultado numérico; el equipo con mayor *score* tiene, estadísticamente, mayor probabilidad de ganar.

En materia de crédito, el *score* es también el resultado numérico de un proceso matemático y sistémico que mide la probabilidad de que una persona pague cumplidamente sus obligaciones o incurra en impago. El modelo que permite obtener el *score* se desarrolla mediante una metodología estadística, que consiste en analizar los datos de informes crediticios que reflejan el comportamiento de pago de un titular en el transcurso del tiempo. Esta metodología permite clasificar a un individuo tomando en cuenta a otras personas con atributos comunes que obtuvieron un resultado similar.

El *score* de crédito es diferente a la historia de crédito. La historia de crédito informa sobre el comportamiento pasado o actual del titular de la información. El *score* se expresa en un número, y entre más alto ese número se estima que hay menor posibilidad de incumplimiento.

Ahora bien, el *score* es una herramienta técnica para evaluar el riesgo, a disposición de los otorgantes de crédito, que son quienes ponderan su resultado con otra información relevante para el cálculo del riesgo crediticio. En otras palabras, el *score* es una herramienta más que pueden utilizar las entidades para tomar decisiones de crédito de forma autónoma e independiente.

2.2 ¿Cómo se calcula un *score* de crédito?

Igual que en nuestro ejemplo del fútbol, la construcción de los *scores* de crédito se basa en el supuesto de que el comportamiento pasado se puede utilizar para predecir el comportamiento futuro de manera fiable. La metodología consiste en identificar perfiles de solicitantes que, con base en información del pasado, estén asociados con el hecho que tratamos de predecir -esto es, que sea un cliente de mucho o poco riesgo-, y suponer que estos mismos perfiles conducirán al mismo acontecimiento en el futuro. De esta forma, es posible cuantificarlos y convertirlos en una probabilidad de que ese hecho ocurra.

2.2.1 Definir la población: lo primero que se hace es definir a la población que se va a analizar. Por ejemplo, personas naturales con historia de crédito.

2.2.2 Definir las variables: no todos los modelos son iguales, pero los *scores* genéricos de crédito, que son los construidos por los burós de crédito[2], utilizan variables similares que se pueden agrupar en las siguientes categorías:

- Las relativas al hábito de pago: el historial de pago de deudas a tiempo o en mora. Para estos efectos, el *score* solo toma la información que no hubiere caducado de acuerdo con los términos establecidos por las leyes 1266 de 2008 y 2157 de 2021.
- Las relativas a montos adeudados: cuánto debe en créditos y qué porcentaje de los cupos otorgados representan los saldos de las tarjetas de crédito.
- Las relativas a la duración del historial de crédito: la antigüedad de la historia de crédito y la antigüedad promedio de todos los créditos, conforme a lo previsto en la ley que regula a los burós de crédito. Es importante tener en cuenta que, en Colombia, la información positiva no caduca.
- Las relativas a la actividad reciente: cuántos créditos ha solicitado y le han aprobado recientemente.
- Las relativas a los tipos de crédito: si tiene experiencia con diferentes tipos de créditos.

2.2.3 Definir el periodo de observación y el tamaño de la muestra representativa en cada periodo: por ejemplo, cinco millones de registros que se analizan al corte del primer semestre de 2019, del primer semestre de 2020 y del primer semestre de 2021.

2.2.4 Desarrollo del proceso: como resultado de un análisis estadístico histórico, se ponderan las variables significativas y se crea un proceso matemático y sistémico, con base en el cual se calculan los *scores* de crédito.

Dichos *scores* varían de 150 a 990 para personas naturales y de 50 a 990 para personas jurídicas[3]. Un puntaje más alto indica que es menos probable que el titular de los datos se retrase en sus obligaciones. Sin embargo, el resultado de un *score* es relativo. Los bancos y demás otorgantes de crédito pueden determinar sus propios criterios o políticas de préstamo. Algunos solo buscan clientes con calificaciones crediticias excepcionalmente buenas y no incluyen a solicitantes de crédito que los demás aceptarían. Otros otorgantes de crédito se enfocan en clientes con una calificación de crédito menor, dado el contexto de su negocio. En cualquier caso, el *score* de crédito se recalcula automáticamente a medida que se actualizan los datos de los titulares.

2.3 ¿Cómo nació el *score* de crédito y cuál es su propósito?

En los años 50, con el desarrollo y expansión del uso de tarjetas de crédito bancarias en Estados Unidos, se iniciaron las primeras prácticas de evaluación del riesgo a través de los burós de crédito, quienes ponían a disposición de los bancos y comercios la historia de crédito de sus clientes actuales o potenciales, lo que les permitió a estos un mayor acceso al crédito.

[2] Los burós de crédito son empresas llamadas también centrales de riesgo o de información, que tienen bases de datos con información financiera y crediticia de diferentes Titulares. Esa información es entregada y circulada a entidades de diferentes sectores (financiero, real o cooperativo), conforme a los parámetros contenidos en la normativa que regula a los Burós de Crédito.
[3] Estos puntajes corresponden a los scores genéricos desarrollados por Experian en Colombia.

Con el tiempo y debido al incremento de los préstamos como herramienta para adquirir bienes y servicios, los burós de crédito tuvieron que adoptar procesos más automatizados, basados en modelos cuantitativos, con el fin de acelerar los procesos de entrega de información a sus clientes. No obstante, fue solo hasta inicios de los años 80, debido al aumento del mercado de tarjetas de crédito, que los burós de crédito introdujeron el uso del *score* en sus análisis de evaluación del riesgo de crédito.

Gracias a los avances tecnológicos, dicho *score* se convirtió en una herramienta para tomar decisiones automatizadas, lo que permitió que las entidades financieras pudieran ofrecer crédito a menores costos y expandirlo a segmentos más amplios de la economía, logrando así democratizar el crédito y el rápido crecimiento de los préstamos para consumo.

2.4 ¿Cuál es el propósito de tratar la información financiera y crediticia que se utiliza para el cálculo del *score* de crédito?

El tratamiento, es decir, la recolección, almacenamiento, uso, circulación o supresión de información financiera y crediticia relativa a una persona, por parte de los burós de crédito, es primordial para la democratización del crédito.

Según el Banco Mundial[4], la actividad de los burós de crédito es esencial para el éxito de los mercados de crédito. Ayudan a resolver un problema fundamental de los mercados financieros conocido como asimetría de la información, que significa que el prestatario -quien recibe el préstamo- tiene un conocimiento mucho mayor que el prestamista -quien otorga el préstamo- sobre sus posibilidades de pagar la deuda. Los prestamistas responden a este problema investigando la capacidad de pago del prestatario o exigiendo garantías para cubrir la pérdida en caso de incumplimiento[5]. Los burós de crédito son entonces la respuesta a esa asimetría de información, porque son el medio para que los titulares construyan su **garantía reputacional**.

Veámoslo con un ejemplo. Matilde tiene dos hijas y el sueño de darles un mejor futuro. Vivía en San Martín, Meta, y se trasladó a Villavicencio buscando oportunidades. Matilde sabe hacer las mejores paletas del mundo, dicen sus hijas, y quiere montar un negocio casero, pero no tiene una nevera.

Hay dos escenarios:

En el primer escenario, Matilde va a la entidad a pedir un préstamo para la nevera, pero desafortunadamente no tiene ninguna garantía real ni un codeudor que le dé a la entidad financiera la seguridad de que ella va a pagar su crédito. Por consiguiente, la entidad no se lo otorga.

En el segundo escenario, Matilde va a la entidad a pedir el préstamo para la nevera, y aunque no tiene una garantía real ni un codeudor, sí tiene una historia de crédito porque en San Martín obtuvo un préstamo para los uniformes de sus hijas y un servicio de telefonía móvil, y ambos los pagó cumplidamente. Matilde no tiene entonces una garantía real, pero tiene una

[4]Corporación Financiera Internacional. Grupo del Banco Mundial. Sistemas de Información crediticia. Guía Informativa. Washington. 2006, página 2.
[5]Ibidem.

garantía reputacional que le abre las puertas al crédito.

El de la nevera es un nuevo préstamo que registra en su historia de crédito, y después serán los préstamos para licuadoras industriales, la universidad de sus hijas, su casa propia, etc.

En Colombia, la actividad de administración de información financiera, crediticia, comercial y de servicios favorece una actividad de interés público, que es la actividad financiera, por cuanto contribuye a la democratización del crédito, promueve el desarrollo de la actividad de crédito, la protección de la confianza pública en el sistema financiero y su estabilidad, y genera otros beneficios para la economía nacional y en especial para la actividad financiera, crediticia, comercial y de servicios del país[6].

2.5 ¿Cuáles son los principios de tratamiento de información aplicables al *score* de crédito?

Para la construcción de los *scores* de crédito es preciso tener en cuenta los principios de libertad, finalidad, calidad y transparencia, como se explica a continuación.

2.5.1 Libertad que se manifiesta a través de la autorización

La recolección, almacenamiento, uso, circulación o supresión de información financiera y crediticia relativa a una persona implica el derecho del titular de *conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos*[7], esto es, el derecho al habeas data.

La libertad se manifiesta a través de la autorización que otorga el titular para que su información personal sea incluida en los archivos y bancos de datos. Así lo establece la ley mediante el principio de libertad[8]. Por esa razón, en el ordenamiento legal colombiano el sustento jurídico que legitima la administración de datos personales es el consentimiento o autorización otorgada por el titular de la información. Lo anterior supone que los datos utilizados para la construcción de *scores* deben estar autorizados. Existen excepciones a la regla mencionada[9], entre las que se encuentra el tratamiento de datos de naturaleza pública.

2.5.2 Finalidad de la recolección y uso de información personal

Según la ley, el principio de finalidad[10] se refiere al objeto o a los fines para los cuales se recolecta y utiliza la información personal. Conforme a este principio, los datos personales deben ser recolectados, utilizados y tratados solo para fines específicos y lícitos, que deben ser previamente conocidos por el titular.

Tratándose de información financiera y crediticia, la finalidad legítima se enmarca en el análisis de riesgo de crédito en todas sus etapas, esto es, en la iniciación, mantenimiento

[6] Artículo 10 de la Ley 1266 de 2008 modificado por el Artículo 5 de la Ley 2157 de 2021.
[7] Artículo 1, Ley 1266 de 2008.
[8] Literal c, Artículo 4, Ley 1581 de 2012.
[9] Artículo 10 de la Ley 1581 de 2012 aplicables a datos que no estén regulados por la Ley 1266 de 2008.
[10] Literal b), Artículo 4, Ley 1266 de 2008 y Literal b), Artículo 4, Ley 1581 de 2012.

y cobranza de una obligación dineraria. Si se trata de información distinta, la finalidad o finalidades deben ser específicas, es decir, plenamente identificadas y detalladas conforme al ordenamiento jurídico; no pueden ser genéricas o cobijar usos indefinidos con el objeto de utilizar la información recolectada para cualquier propósito -autorización sombrilla-.

Por lo tanto, es preciso delimitar los usos que tendrá la información antes de recolectarla y restringir su tratamiento a la consecución de los fines que se hayan determinado, así como darla a conocer a sus titulares en ejercicio del derecho al habeas data.

La finalidad o finalidades definidas delimitan la recolección y tratamiento de datos personales exclusivamente a aquellos que sean **pertinentes y adecuados**. Por esa razón, en la construcción del *score* es preciso considerar si los datos que se van a utilizar son **necesarios** para los propósitos que se persiguen y descartar el uso de aquellos que resultan excesivos y extraños a esos propósitos.

2.5.3 Veracidad o calidad de la información

De acuerdo con el principio de veracidad o calidad previsto en la ley[11], la información tratada debe ser veraz, completa, exacta, actualizada, comprobable y comprensible, de tal manera que se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan al error. Tampoco puede utilizarse información sobre incumplimiento de las obligaciones que, por el paso del tiempo, hayan caducado en los términos indicados por la ley[12].

En aplicación del principio de veracidad y calidad de los datos, la metodología utilizada para obtener el cálculo estadístico debe partir del hecho de que la información procesada sea: (i) veraz, y (ii) que permita predecir el comportamiento de pago del cliente y, de esa manera, medir el riesgo de incumplimiento en el futuro.

Los titulares tienen derecho a que su puntaje se actualice o se corrija, así como a conocerlo en todo momento en ejercicio de su derecho al habeas data. El *score* se actualizará de manera simultánea con modificaciones de la información financiera y crediticia utilizada en el modelo[13]. Lo anterior, teniendo en cuenta que existen múltiples variables que componen el *score* de crédito y que lo impactan.

En efecto, el *score* de crédito se compone de múltiples variables como las experiencias de crédito, la utilización de productos, tipos de créditos utilizados, etc. Y, además, obedece a las reglas de la estadística que involucran análisis de datos de otras personas que comparten determinadas características definidas en el modelo.

En este sentido, en cada caso particular será necesario analizar las diferentes variables que impactan la calificación del *score* de crédito para entender el resultado final que arroja el modelo.

[11] Literal a), Artículo 4, Ley 1266 de 2008 y literal d), Artículo 4, Ley 1581 de 2012.
[12] Ley 1266 de 2008 y Ley 2157 de 2021.
[13] Ley 2157 de 2021.

2.5.4 Transparencia

En términos de la ley[14], el principio de transparencia se refiere a que, en el tratamiento de datos personales, debe garantizarse el derecho del titular a obtener en cualquier momento y sin restricciones información acerca de la existencia de datos que le conciernan. En este sentido, la Corte Constitucional[15] ha resaltado que la ley estatutaria 1266 de 2008 establece garantías y herramientas eficaces para que la administración de datos personales de contenido comercial, financiero y crediticio sea un proceso transparente.

En el análisis puntual del principio de transparencia, la Corte Constitucional[16] precisó que *la información que debe ofrecerse al Titular de los datos debe ser cualificada y por tanto cuando procese datos personales, el Responsable o Encargado del Tratamiento de datos debe ofrecer, como mínimo, la siguiente información a la persona afectada: (i) información sobre la identidad del controlador de datos; (ii) el propósito del procesamiento de los datos personales; (iii) a quién se podrán revelar los datos; (iv) cómo la persona afectada puede ejercer cualquier derecho que le otorgue la legislación sobre protección de datos, y (v) toda otra información necesaria para el justo procesamiento de los datos.* (Subraya fuera de texto).

De acuerdo con lo anterior, debe ser claro para el titular el uso y tratamiento que se dará a los datos, los fines de este tratamiento, así como las consecuencias que se derivan del mismo cuando el suministro de esta información se considere necesaria para el justo procesamiento de los datos, lo que aplica al *score*. Los titulares tienen derecho a conocer el puntaje que se les asigna producto de esta metodología.

3. Los desafíos jurídicos del *score* de crédito

El *score* de crédito, como se indicó al comienzo de este artículo, es una herramienta que evalúa y procesa información financiera y crediticia con el fin de determinar de manera estadística el nivel de riesgo de una persona, en el sentido de señalar la probabilidad de que en el futuro cumpla sus obligaciones.

Vimos cómo la finalidad del *score* y, en general, de la gestión del riesgo crediticio mediante el tratamiento de información financiera y crediticia resulta en una actividad legítima incorporada en la ley 1266 de 2008, en la ley 2157 de 2021 y en la jurisprudencia de la Corte Constitucional.

Por consiguiente, el reto del score de crédito no consiste en probar que persigue fines constitucionalmente legítimos, sino en asegurar que, mediante el tratamiento adecuado de la información personal, se respeten los principios aplicables al tratamiento de información y se evite incurrir en discriminación de los titulares.

Sobre esto último, la Dirección de Investigación de Protección de Datos Personales de la Superintendencia de Industria y Comercio[17] analizó lo que implica *diferenciar* y *discriminar* en el tratamiento de la información:

[14] Literal e), Artículo 4, Ley 1581 de 2012.
[15] Sentencia de constitucionalidad C-1011 de 2008.
[16] Ibidem
[17] Resolución 27578 de 2020 emitida dentro del radicado número 16-460101, trajo a colación la sentencia C-530 de 1993.

> ***La distinción entre discriminación y diferenciación (…) es el elemento fundamental para calibrar el alcance del principio de igualdad. Dicho principio, en efecto, veta la discriminación, pero no excluye que el poder público otorgue tratamiento diverso a situaciones distintas -la diferenciación-.*** *El artículo 13 de la Constitución no prohíbe, pues, tratamientos diferentes a situaciones de hecho diferentes. La distinción entre discriminación y diferenciación viene, a su vez, determinada porque la primera es injustificada y no razonable. Discriminación es, por tanto, una diferencia de tratamiento no justificada ni razonable, o sea arbitraria, y solo esa conducta está constitucionalmente vetada. A contrario sensu, es dable realizar diferenciaciones cuando tengan una base objetiva y razonable. El punto consiste, entonces, en determinar cuáles son los elementos que permiten distinguir entre una diferencia de trato justificada y los que no lo permiten.*

En ese sentido, para cumplir con su propósito el *score* crediticio debe involucrar en la ecuación el trato justo y equitativo de la información, en el sentido de construir reglas que, además de aplicar los principios mencionados, impliquen la utilización ética de la información, a fin de que el resultado permita diferenciar a las personas sin discriminar, es decir, de manera legítima, proporcional y razonable.

3.1 Diferenciación de las personas dentro de un marco legal y ético

El *score* de crédito comporta una clasificación de las personas que resulta legítima frente al marco legal, en la medida que es el resultado de aplicar un método matemático de análisis a una situación futura, utilizando únicamente criterios objetivos y razonables.

Se observa entonces un riesgo asociado a: (i) el tipo de información o datos utilizados en el desarrollo del *score*, y (ii) los criterios utilizados para clasificar y diferenciar a las personas. Lo anterior, en la medida que la información y/o los criterios de segmentación utilizados no resulten apropiados o necesarios para el propósito perseguido y pueden dar lugar a un trato excluyente o diferenciador.

La Corte Constitucional se ha pronunciado en relación con los criterios a los que se debe enfrentar cualquier juicio de diferenciación para garantizar la prevalencia del derecho a la igualdad y el principio de no discriminación consagrados en el artículo 13 de la Carta Política, de acuerdo con el cual *(t)odas las personas nacen libres e iguales ante la ley, recibirán la misma protección y trato de las autoridades y gozarán de los mismos derechos, libertades y oportunidades sin ninguna discriminación por razones de sexo, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica (…)*[18].

Ha dicho la Corte que ***cualquier juicio de diferenciación, para que sea legítimo, debe ser compatible con los valores de la Carta y que, en todo caso, no puede ser contrario a los criterios del artículo 13 de la Constitución.***

La Corte definió la discriminación[19] así:

[18] Corte Constitucional, sentencia T-131 de 2006.
[19] Sentencia T- 098 de 1994.

> *un acto arbitrario dirigido a perjudicar a una persona o grupo de personas con base principalmente en estereotipos o prejuicios sociales, por lo general ajenos a la voluntad del individuo, como son el sexo, la raza, el origen nacional o familiar, o por razones irrelevantes para hacerse acreedor de un perjuicio o beneficio como la lengua, la religión o la opinión política o filosófica (...) El acto discriminatorio es la conducta, actitud o trato que pretende -consciente o inconscientemente- anular, dominar o ignorar a una persona o grupo de personas, con frecuencia apelando a preconcepciones o prejuicios sociales o personales, y que trae como resultado la violación de sus derechos fundamentales, también dijo que Constituye un acto discriminatorio, el trato desigual e injustificado que, por lo común, se presenta en el lenguaje de las normas o en las prácticas institucionales o sociales, de forma generalizada, hasta confundirse con la institucionalidad misma, o con el modo de vida de la comunidad, siendo contrario a los valores constitucionales de la dignidad humana y la igualdad, por imponer una carga, no exigible jurídica ni moralmente, a la persona.* ***La finalidad de su prohibición es impedir que se menoscabe el ejercicio de los derechos a una o varias personas ya sea negando un beneficio o privilegio, sin que exista justificación objetiva y razonable****. (…)*[20]*. (Negrilla fuera de texto).*

Asimismo, ha dicho la Corte que el principio de igualdad del artículo 13 de la Constitución Política

> *permite conferir un trato distinto a diferentes personas siempre que se den las siguientes condiciones:* ***que las personas se encuentren efectivamente en distinta situación de hecho; que el trato distinto que se les otorga tenga una finalidad; que dicha finalidad sea razonable, vale decir, admisible desde la perspectiva de los valores y principios constitucionales; que el supuesto de hecho -esto es, la diferencia de situación, la finalidad que se persigue y el trato desigual que se otorga- sean coherentes entre sí o, lo que es lo mismo, guarden una racionalidad interna; que esa racionalidad sea proporcionada, de suerte que la consecuencia jurídica que constituye el trato diferente no guarde una absoluta desproporción con las circunstancias de hecho y la finalidad que la justifican***[21]*. (Negrilla fuera de texto).*

Con ese fin, la Corte ha diseñado el test integrado de igualdad, que consta de tres etapas necesarias, para evidenciar si se está en presencia de una vulneración del derecho a la igualdad, así:

- Determinar los criterios de comparación, esto es, establecer si se trata de sujetos de la misma naturaleza;
- Definir si existe un trato desigual entre iguales o igual entre desiguales, y
- Concluir si la diferencia de trato está justificada constitucionalmente[22].

Ahora bien, la normativa internacional, en particular el Reglamento General de Protección de Datos -RGPD[23]-, adoptado por el Parlamento Europeo y el Consejo de la Unión Europea, establece reglas aplicables a la elaboración de perfiles, con el fin de que no se utilicen *de*

[20] Corte Constitucional, sentencia T-131 de 2006.
[21] Ibidem
[22] Este test ha sido acogido por el Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Segunda, Subsección A del Consejo de Estado, sentencia de tutela del 18 de noviembre de 2015, Consejero Ponente William Hernández Gómez.
[23] En inglés GDPR (General Data Protection Regulation).

forma que tengan un impacto no justificado en los derechos de las personas, tal como lo precisó el Grupo de Trabajo sobre Protección de Datos del Artículo 29 -GT29- en una de las últimas guías[24] aprobadas, relacionada con decisiones automatizadas y creación de perfiles[25]. El objetivo de tales guías es aclarar las disposiciones contenidas en el RGPD, en especial aquellas relativas a los principios de protección de datos personales, dentro de los que se encuentran los de licitud, lealtad y transparencia; tratamiento ulterior y limitación de la finalidad; minimización de datos; exactitud de los datos y limitación del plazo de conservación, que se asemejan en gran medida a los principios contenidos en la legislación colombiana y descritos en este ensayo.

De acuerdo con el pronunciamiento de la Corte mencionado, la segmentación o clasificación de las personas a partir de un *score* es legítima en la medida que permita establecer una diferenciación que esté justificada de forma objetiva y razonable. En este sentido, la segmentación no vulnera el derecho constitucional a la igualdad y no causa discriminación cuando concurren las siguientes situaciones, conforme el *test* integrado de igualdad a que se ha hecho referencia:

3.1.1 Determinación de los criterios de comparación, esto es, establecer que no se trata de sujetos de la misma naturaleza:

no se vulnera el derecho a la igualdad al conceder, de manera justificada, trato desigual a personas de diferente naturaleza o circunstancias distintas. A manera de ejemplo, si un titular del dato presenta características y circunstancias objetivas diferentes de las de otro titular, es posible realizar un trato diferenciado de esos dos individuos a partir de la asignación de un *score* o puntaje que los diferencia.

Lo anterior, bajo el entendido de que esas características tenidas en cuenta para realizar la diferenciación solo se fundamentan en hechos y circunstancias objetivas, **sin** incluir o **sin** tener en cuenta cualquier calificativo o adjetivo que, de forma subjetiva, discrimine y denigre la condición que tienen los titulares de los datos.

3.1.2 Verificar que no exista un trato desigual entre iguales o igual entre desiguales:

no es posible dar un tratamiento desigual a personas que presenten una situación igual o darle un tratamiento igual a personas o circunstancias distintas, sin justificación alguna.

Para el cálculo de los *scores* de crédito, se tienen en cuenta distintas variables y no un comportamiento aisladamente considerado. El *score* debe tener en cuenta la ubicación de un individuo en un grupo de personas que comparten características objetivas similares.

El tratamiento que se le asigne a un *score* no vulnerará el derecho a la igualdad en la medida que:

[24] "Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679" adoptadas el 3 de octubre de 2017 y revisadas por última vez y adoptadas el 6 de febrero de 2018.
[25] El Grupo de Trabajo del artículo 29 fue el órgano consultor de la Unión Europea en materia de protección de datos e intimidad, antes de que fuera creado el Comité Europeo de Protección de Datos.

- Se tengan en cuenta las diversas variables objetivas y modelos estadísticos que permitan anticipar el comportamiento futuro de una persona hipotética que reúne ciertas características;
- Con base en las diversas variables aludidas y en la información personal que resulte proporcionada, apropiada o necesaria para el fin perseguido de la base de datos, se pueda asignar o determinar un *score* de crédito a un sujeto particular.

Todo lo anterior bajo el entendido de que esa asignación se realiza de manera legítima, respetando y garantizando la efectividad de los derechos de los titulares de los datos y los principios de administración de información personal.

3.1.3 Concluir si la diferencia de trato está justificada constitucionalmente:

en la construcción del *score* de crédito el trato diferenciado no va a vulnerar el derecho a la igualdad en la medida que esté justificado conforme a la Constitución Política y la ley, incluyendo, sin limitarse, el cumplimiento de un fin constitucionalmente valioso como lo es la democratización del crédito.

Por consiguiente, conforme a lo explicado, la aplicación del *test* integrado de igualdad nos permite concluir que la metodología para el cálculo del *score* de crédito a partir de información financiera y crediticia evita incurrir en la discriminación de los titulares.

Ahora bien, en el mercado de crédito, a mayor información, aumenta la posibilidad de que las personas accedan al crédito y en mejores condiciones. Por lo tanto, es necesario incluir cada vez más información en el proceso de evaluación y administración del riesgo de crédito.

3.2 Retos frente al uso de información alternativa

Para el tema que nos ocupa, la información alternativa es aquella que no se trata tradicionalmente para adelantar estudios de riesgo de crédito; suele ser complementaria a la relacionada con el comportamiento crediticio de los titulares y permite tener una mejor visión del riesgo crediticio de un titular en particular. En el mundo, los datos alternativos han permitido impulsar el acceso al crédito.

El documento CONPES 4005 de 2020 de inclusión económica y financiera considera los datos alternativos como un aspecto estratégico en la inclusión financiera:

> *Para lograr que las personas y empresas puedan contar con un historial crediticio que facilite la gestión de riesgo cuando se busca un crédito formal, el Departamento Nacional de Planeación propondrá recomendaciones que permitan mejorar los modelos de calificación crediticia (scoring) para población vulnerable, jóvenes y mipymes utilizando información alternativa. El análisis tendrá en cuenta la inclusión de: (i) registros administrativos del sector público e información de sistemas de información que contengan datos de beneficiarios de subsidios del sector público; (ii) registros de naturaleza pública generados por el sector privado tales como la información transaccional de los servicios postales de pago y centrales de información empresarial*

> *como el Registro Único Empresarial y Social (RUES) y (iii) datos de economía comportamental y pruebas psicométricas. Esta acción iniciará en julio de 2021 y terminará en julio de 2022.* (Subraya fuera del texto).

Por lo tanto, el *score* de crédito tiene un nuevo desafío consistente en permitir que se diferencie a los titulares de datos, en cuanto a su probabilidad de pago, con base en información alternativa suministrada: (i) por el propio titular, o (ii) obtenida de fuentes no tradicionales, utilizando medios que en uno y otro caso se ajusten a lo establecido en la ley y que garanticen un trato justo y leal de la información.

Cuando entramos a un universo de datos no convencionales o alternativos debemos analizar con mucho juicio cada dato y las condiciones en las que fue recopilado, para salvaguardar el interés de los titulares, cumplir con el ordenamiento jurídico y garantizar igualdad de oportunidades en el acceso al crédito.

Para estos efectos aplican los principios de tratamiento de información que hemos mencionado, pero quisiéramos hacer énfasis en los principios de libertad, legitimidad, igualdad y calidad.

3.2.1 La autorización, legitimadora en el tratamiento de datos personales

El fundamento legal para el tratamiento de los datos personales en Colombia, tanto en la ley 1266 de 2008 como en la ley 1581 de 2012, es la autorización libre, previa, expresa e informada del titular de la información. Constitucionalmente se ha considerado que el principio de libertad de los colombianos en materia de administración de datos personales se surte mediante su consentimiento:

> *Este principio, pilar fundamental de la administración de datos,* ***permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos.*** *También impide que la información ya registrada de un usuario, la cual ha sido obtenida con su consentimiento, pueda pasar a otro organismo que la utilice con fines distintos para los que fue autorizado inicialmente.* (Negrilla fuera de texto)[26].

En la práctica, implica retos frente a la recolección y uso de la autorización para el tratamiento de *data* alternativa.

Al ser la autorización ejercicio del principio de libertad, es primordial entender las expectativas de privacidad de los titulares, quienes, dependiendo del contexto, asumen que sus datos personales serán tratados conforme a la autorización otorgada de manera expresa o a través de conductas inequívocas en los términos previstos en la ley[27]. Conductas inequívocas como las *imágenes captadas por sistemas de videovigilancia, en los que se comunica previamente a las personas que van a ingresar a un establecimiento que sus imágenes van a ser tomadas,*

[26] Sentencia C- 748 de 2011 de la Corte Constitucional.
[27] Artículo 7, Decreto 1377 de 2013 modificado por el Artículo 2.2.2.25.2.4. del Decreto 1074 de 2015.

conservadas o usadas de cierta manera y, conociendo tal situación, los titulares ingresan al establecimiento[28]. (Negrilla fuera de texto).

A lo anterior debe añadirse lo establecido en el principio de necesidad, en virtud del cual *los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos*[29].

Este principio obliga a quienes pretendan realizar el tratamiento de determinada información personal, no solo a recolectar los datos necesarios para las finalidades que persigue la base de datos, sino también a encontrar proporcionalidad entre esas finalidades y los datos que recopilan.

De acuerdo con la ley 1581 de 2012, no es necesario el consentimiento del titular de la información si los datos se requieren para el cumplimiento de un deber legal, por ejemplo, pago de prestaciones de seguridad social, o si se trata de un mandato judicial. En los demás casos, debe existir una autorización **expresa y voluntaria** otorgada por el titular.

Aplicadas estas consideraciones a la obtención de información alternativa para el cálculo del *score* de crédito, no se puede condicionar la prestación del servicio a la aceptación de la autorización del titular para tratar sus datos para la evaluación del riesgo crediticio; en virtud de lo anterior, el consentimiento otorgado por el titular de un dato alternativo para esas finalidades debe ser independiente de la autorización directamente asociada al producto o servicio que se desea adquirir.

Es claro, entonces, que al ser la autorización el fundamento legal para el tratamiento de datos personales en Colombia, el proceso para obtenerla debe ser transparente, pues será la llave de entrada para que los datos personales puedan tratarse con las finalidades que el titular haya consentido. Lo anterior también aplica cuando la ley exime la autorización, pues aún en tales casos el titular de la información tiene derecho a ser informado acerca del tratamiento de sus datos y sus fines.

Por lo tanto, las personas involucradas en el tratamiento de la información deben desplegar una serie de medidas para garantizar la transparencia frente al titular, por ejemplo, políticas de privacidad fáciles de entender, recursos como videos o un diseño de experiencia del usuario que le permita al titular entender los efectos de autorizar el tratamiento de sus datos personales. Esto aplica tanto en el uso de datos personales privados como de datos públicos; en relación con estos últimos, si bien no requieren autorización para su tratamiento, el titular debe conocer la finalidad para la cual se recolectan y tratan, de tal manera que sea transparente el uso que se dará a su información personal.

[28] Superintendencia de Industria y Comercio. Cartilla. Formatos modelo para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus Decretos Reglamentarios. Página 8.
[29] Corte Constitucional. Sentencias C-1011 de 2008 y C-748 de 2011.

3.2.2 Legitimidad e igualdad en el tratamiento de los datos personales alternativos

Además de la autorización, es indispensable asegurar la legitimidad e igualdad en el tratamiento de los datos personales alternativos.

Uno de los factores determinantes para afirmar que la información sobre el comportamiento crediticio es diferenciadora y no discriminadora, es que describa un hecho objetivo que evidencie el cumplimiento de una obligación dineraria. Se toma una decisión de crédito con base en el comportamiento crediticio pasado. Y si bien alrededor del cumplimiento de las obligaciones puede haber una cantidad de factores sociales y económicos, al final se calcula el riesgo de crédito basado en información crediticia parametrizada, tradicional y objetiva.

Este mismo ejercicio debe hacerse con la información alternativa, siendo lo primero determinar que, con el tratamiento de un dato personal, no se ponga en desventaja a una persona o grupo de personas. Adicionalmente, si de la inclusión de información en una base de datos se derivan situaciones ventajosas para el titular, la entidad administradora de datos debe incluirlos en sus registros. En ese sentido, aquella información alternativa que mejore las perspectivas de acceso al crédito debe incorporarse en los *scores* de crédito si el titular lo autoriza -habeas data aditivo-.

La Corte Constitucional[30] desarrolló el principio de incorporación así:

> ***Principio de incorporación: impone al responsable del tratamiento la obligación de registrar en la base de datos toda aquella información del sujeto concernido que involucre una consecuencia favorable para el titular.*** *En tal sentido, este debe guardar una relación estrecha con el principio de calidad y veracidad. Para efectos del presente análisis debe resaltarse que en aquellos eventos en que la inclusión de la información personal en la base de datos implica consecuencias desfavorables para su titular, el responsable y el encargado del tratamiento tienen la obligación de actualizar esa información con los datos que den cuenta de comportamientos que incidan en la aplicación de esas consecuencias. (…)*
>
> *Así las cosas, en la sentencia C-032 de 2021* ***esta corporación reiteró que los principios enunciados constituyen un referente de validez para las regulaciones sobre administración y transferencia de datos personales****, de tal forma que, al analizar la exequibilidad de las disposiciones de que se trate, estos parámetros constituyen un parámetro de control aplicable.* (Negrilla fuera de texto).

Según el habeas data aditivo -desarrollado por el principio de incorporación-, si de la inclusión de información en una base de datos se derivan situaciones ventajosas para el titular, la entidad administradora de datos debe incluirlos en sus registros. En ese sentido, aquella información alternativa que mejore las perspectivas de acceso al crédito debe incorporarse en los *scores* de crédito si el titular lo autoriza.

[30] Corte Constitucional. sentencia C-282 de 2021.

3.2.3 Calidad de los datos alternativos

El principio de calidad -según el cual la información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible- prohíbe el registro y la divulgación de datos parciales, incompletos, fraccionados o que induzcan al error[31], es fundamental en la creación de bases de datos con información alternativa, la cual tiene una caracterización particular. Por ejemplo, para el caso de los datos transaccionales debe determinarse cuál es la completitud que se requiere para no inducir a error en la toma de decisiones de crédito a través del acceso de datos fraccionados. Así mismo, debe analizarse cuándo deja de ser relevante por desactualización y, por ende, proceder a su eliminación.

4. Conclusiones

4.1 El tratamiento de información personal para la administración del riesgo de crédito, por parte de los burós de crédito, es la respuesta a la asimetría de información en los procesos de otorgamiento de préstamos y, por lo tanto, el camino para su democratización. Los burós de crédito son el medio para que los titulares de los datos construyan su historia de crédito y, así, su **garantía reputacional**.

4.2 El *score* de crédito es diferente a la historia de crédito. La historia de crédito informa sobre el comportamiento pasado o actual del titular de la información. El *score* de crédito es el resultado numérico de una fórmula matemática que mide la probabilidad de que una persona honre cumplidamente sus obligaciones o incurra en impago. El modelo que permite obtener el puntaje de crédito o *score* se desarrolla mediante una metodología estadística, que se basa en el análisis de datos obtenidos en un periodo. Esta metodología permite clasificar a un individuo tomando en cuenta a otras personas con atributos comunes que obtuvieron un resultado similar.

4.3 En los años 80 y gracias a los avances tecnológicos, el *score* de crédito se convirtió en una herramienta para obtener decisiones automatizadas y objetivas. Esto permitió que los prestamistas pudieran ofrecer crédito a menores costos y expandirlo a segmentos más amplios de la economía, logrando así la democratización del crédito y el rápido crecimiento de los préstamos de consumo.

4.4 El *score* de crédito se debe construir a partir de algoritmos que, además de aplicar, entre otros, los principios de libertad, finalidad, calidad y transparencia, utilicen de forma ética la información, de tal manera que el resultado permita diferenciar a los titulares sin discriminar, es decir, de una manera legítima, proporcional y razonable.

4.5 La Corte Constitucional ha precisado los criterios a los que se debe enfrentar cualquier juicio de diferenciación para garantizar la prevalencia del derecho a la igualdad y el principio de no discriminación consagrados en la Constitución Política. Para ello, ha diseñado el test integrado de igualdad, que consta de tres etapas para efectos de evidenciar si se está en presencia de una vulneración o no del derecho a la igualdad, así: (i) determinar los criterios de comparación, esto es, establecer si se trata de sujetos de la misma naturaleza; (ii) definir si existe un trato desigual entre iguales o igual entre desiguales, y (iii) concluir si la diferencia de trato está justificada constitucionalmente.

[31] Sentencia C-1011 de 2008 de la Corte Constitucional.

4.6 La segmentación o diferenciación de las personas a partir de un *score* calculado con la información financiera y crediticia es legítima en la medida que permita establecer una diferenciación que esté justificada de forma objetiva y razonable conforme a la constitución y la ley, acorde con las reglas que conforman el test integrado de igualdad a que se ha hecho referencia.

4.7 En el mundo, los datos alternativos han permitido mayor democratización del crédito. Por lo tanto, el nuevo desafío jurídico del *score* de crédito consiste en permitir que los titulares de datos puedan diferenciarse, en cuanto a su probabilidad de pago, con base en información alternativa suministrada por el propio titular u obtenida de fuentes no tradicionales.

4.8 El procesamiento de la información alternativa para el cálculo del *score* de crédito debe estar precedido de la autorización expresa e informada del titular, enmarcada en todos los principios de administración de datos personales, en especial, los de libertad y transparencia, de tal manera que el titular conozca y entienda el propósito que se persigue, cómo funciona y cómo lo puede mejorar. Adicionalmente, antes y durante el tratamiento de la información, se debe asegurar la legitimidad e igualdad en el tratamiento de los datos personales alternativos, para lo cual es conveniente aplicar el *test* de igualdad.

4.9 Aún en los casos en los que se utilicen datos públicos, debe aplicarse principalmente el principio de transparencia, porque, si bien no se requiere autorización del titular de la información para su tratamiento, se tiene el deber de informar y el correlativo derecho a ser informado. Así mismo, en estos casos es preciso analizar que los datos utilizados y la ponderación de las variables desarrolladas a partir de estos respondan al criterio de no discriminación.

Bibliografía

Corporación Financiera Internacional. Grupo del Banco Mundial, Washington (2006). Sistemas de Información crediticia. Guía Informativa. Página 2.

Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Segunda, Subsección A, sentencia de tutela del 18 de noviembre de 2015. Consejero Ponente William Hernández Gómez.

Decreto 1377 / 2013 modificado por el Decreto 1074 / 2015.

Grupo de Trabajo sobre Protección de Datos del Artículo 29 (GT29) de la Unión Europea. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 adoptadas el 3 de octubre de 2017 y revisadas por última vez y adoptadas el 6 de febrero de 2018.

Ley 1266 de 2008 "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones". Diario Oficial No. 47.219 de 31 de diciembre de 2008.

Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales.". Diario Oficial No. 48.587 de 18 de octubre de 2012.

Ley 2157 de 2021 "por medio de la cual se modifica y adiciona la Ley Estatutaria 1266 de 2008, y se dictan disposiciones generales del Hábeas Data con relación a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones" Diario Oficial No. 51.842 de 29 de octubre de 2021.

Reglamento general de protección de datos (RGPD). Parlamento Europeo y Consejo de la Unión Europea.

Sentencia C-1011 / 2008, Corte Constitucional.

Sentencia C-748 / 2011, Corte Constitucional.

Sentencia C-282/2021, Corte Constitucional.

Sentencia T-098 / 1994, Corte Constitucional.

Sentencia T-131 / 2006, Corte Constitucional.

Superintendencia de Industria y Comercio. Dirección de Investigación de Protección de Datos Personales. Resolución 27578 de 2020. Radicado número 16-460101.

Superintendencia de Industria y Comercio. Cartilla. Formatos modelo para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus Decretos Reglamentarios. Página 8.

CAPÍTULO 6

Finanzas abiertas: una mirada a los desafíos de protección de datos personales y la reserva bancaria

Álvaro Montero Agón[1]

Resumen

La circulación de los datos de los consumidores es el gran habilitador y uno de los retos más relevantes para todos los que participan en los diferentes ecosistemas. Por ello, los reguladores vienen implementando iniciativas que permitan una mayor apertura de los datos no solo de manera unidireccional, de los prestadores de servicios financieros a otras entidades financieras, aliados o terceros -finanzas abiertas u Open *Finance*-, sino también de otras actividades económicas -telecomunicaciones, servicios públicos, comercio, etc.- y del mismo Estado hacia las instituciones financieras y Fintech -*Open Data*, *Open Society* o, simplemente, apertura de datos-. Esas iniciativas tienen diversas aproximaciones: algunas de ellas hacen obligatoria la apertura de los datos y otras contemplan esquemas voluntarios, sea que vengan acompañadas o no de reglas o principios mínimos para su operatividad. La regla fundamental para que la información circule es la autorización de su titular; sin embargo, dada esa apertura de datos, surgen varios desafíos en cuanto a la responsabilidad de los diferentes actores en su tratamiento, el uso para fines no autorizados, la seguridad de la información y de las transacciones y otros retos que se abordan en el presente ensayo.

[1] Vicepresidente Jurídico del Banco Davivienda. Profesor de las universidades Externado de Colombia y Javeriana. Las opiniones expresadas son personales y no comprometen al Banco Davivienda.

1. Introducción

Hasta hace unos años, cuando se discutía al interior de las empresas cuál era su activo principal, muchas hacían referencia al recurso humano, su cultura, la estrategia, los productos, los clientes, los mercados en los que operaban, la innovación, etc. En ese momento eran pocas las compañías que mencionaban los datos, la analítica de datos y otros conceptos que hoy sin duda son esenciales para su éxito y supervivencia.

La información es la base de la cuarta revolución industrial o industria 4.0. Si bien la tercera revolución industrial -la de la informática, las comunicaciones, la biotecnología y la investigación- implicó enormes avances en el uso de los datos y su digitalización, no se basó en el uso, análisis y procesamiento de grandes cantidades, tipos y detalle de información, con el fin de conocer mucho más a los consumidores y sus preferencias.

Quién no conoce nombres tan relevantes como IBM, Unisys, Ericsson, etc., compañías líderes en tecnología en el siglo XX. Sin embargo, si bien algunas de ellas continúan siendo relevantes en sus mercados, ya no son las grandes firmas que se registran entre las más valoradas; han sido reemplazadas por las BigTech *(*Amazon, Facebook, Google, Apple, Microsoft, etc.*)*, que son las grandes compañías que manejan el mayor volumen de información y datos de los consumidores.

Pero ¿quién es el dueño de los datos: los Estados, las compañías que los recolectan, las grandes compañías que los administran y a partir de ellos deducen nuevos datos, o los clientes y usuarios, personas naturales o empresas?

Parece haber consenso mundial sobre la titularidad de los datos en las personas y muchas discusiones sobre el concepto de propiedad de los mismos en el sentido tradicional. Sin embargo, para efectos del presente escrito la discusión se centra en hasta dónde y de qué manera se deben proteger esos datos y los alcances y fines de su uso.

Los bancos y en general los sistemas financieros y de pagos no han sido ajenos a esta tendencia mundial de la relevancia de la información y por ello se han volcado a la digitalización de sus productos y procesos. Las entidades financieras cuentan con enormes y relevantes cantidades de datos de sus clientes y usuarios, y hoy son conscientes de la importancia que tiene extraerle el mayor valor posible a esa información, no solo para ofrecer sus propios servicios sino también para actuar como proveedores de información a terceros. Así mismo, se han abierto a otros ecosistemas, ya no como los actores preponderantes que eran en el pasado –cuando el mundo giraba alrededor de la entidad financiera-, sino como un actor más que presta sus servicios, en algunos casos de manera oculta. Finalmente, dada su experiencia en el desarrollo de tecnología para la gestión de sus procesos, esperan sacar provecho de dicha tecnología poniéndola al servicio de otros actores.

Esta relevancia en el uso de la data ha llevado al *Open* (*Banking, Finance* o *Data*), como desarrollo de la cuarta revolución industrial. Esta apertura de datos busca que la información, estructurada o no, de los clientes y usuarios pueda ser usada por los diferentes actores que intervienen o pueden intervenir en un ecosistema. En el *Open*, el cliente o usuario toma control de sus datos, lo que le permite escoger en un mayor espectro de servicios y proveedores. Existen diferentes modelos de finanzas abiertas en el mundo y de ahí la gran

discusión que se viene dando sobre cuál es la mejor manera de regularlo o, en algunos casos, de no regularlo para permitir su desarrollo.

En el presente ensayo, se busca dotar al lector de algunos ejemplos de cómo los usuarios compartimos datos de manera permanente, de casos de uso del *Open Finance* que existen en el mundo y en Colombia, y, especialmente, se busca explorar la tensión y desafíos que para el modelo *Open -Data*, *Finance* o *Banking-* representa la protección de datos personales -personas naturales- y la reserva de la información -personas jurídicas-.

Para el efecto, se propone abordar el tema en cinco capítulos: (i) la presente introducción; (ii) una aproximación práctica al *Open Banking*, *Open Finance* y *Open Data*. Análisis de la regulación en Colombia y otras iniciativas; (iii) la importancia de la protección de datos personales y la reserva bancaria; (iv) la tensión y desafíos entre acceso al dato -*Open*- y la privacidad del dato, y (v) principales conclusiones y desafíos regulatorios y de implementación.

2. *Open Banking*, *Open Finance* y *Open Data*. Ejemplos básicos de las finanzas abiertas

El *Open banking* tiene sus orígenes en el PSD1, una directiva de la Unión Europea -EU- de 2007, que estableció normas comunes en el Espacio Económico Europeo[2] a fin de regular los diferentes tipos de pagos electrónicos -sin uso de efectivo-. Su finalidad era generar mayor información de parte de los proveedores de servicios de pago a los consumidores, en especial sobre sus derechos y obligaciones, así como lograr mayor eficiencia en el sistema de pagos mediante la autorización de nuevos proveedores de servicios de pago -*Payment Service Providers*, PSP-[3]. Esta autorización de los nuevos PSP no bancarios llevó a una reducción de las tarifas de pagos y a una mayor competencia; en especial dio lugar al fortalecimiento de las Fintech[4].

En 2013, dada la alta digitalización de los pagos, se vio la necesidad de revisar la regulación, en particular para reforzar la protección al consumidor y los mecanismos de seguridad y para impulsar la competencia e innovación del sector, de manera que se establecieran las bases para el futuro desarrollo de un mercado integrado para pagos electrónicos en la Unión Europea. Esta nueva regulación se expidió en el 2015 y entró en vigencia en el 2018 -Directiva PSD2 de la Unión Europea-[5].

---

[2] Unión Europea, Islandia, Noruega y Liechtenstein.

[3] European Commission. Payment services. https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/payment-services

[4] Fernando Zunzunegui, La Digitalización de los Servicios de Pago. Página 194. En Fintech, Regtech y Legaltech: Fundamentos y desafíos regulatorios. Directores Aurelio Gurrea Martínez y Nydia Remolina. Ed. Tirant lo Blanch. Valencia, 2020.

[5] De manera paralela, en 2014 la Autoridad de Competencia y Mercados del Reino Unido (CMA por su sigla en inglés - Competition & Markets Authority) inició un análisis respecto del suministro de servicios de banca retail para clientes personas naturales de cuentas bancarias y pequeñas y medianas empresas (SMEs). Como parte de esa investigación, se publicó en el año 2016 un estudio sobre la competencia e innovación en la industria de la banca retail en el cual concluyó que los grandes bancos dominaban el mercado y los clientes y pequeños negocios podrían beneficiarse de un incremento en la competencia.
Como consecuencia de esta investigación la CMA y el Gobierno del Reino Unido emitieron la Retail Bank Market Investigation Order 2017 que, entre otros aspectos, obligó a los nueve bancos más grandes que operaban en el Reino Unido a implementar estándares uniformes para el Open Banking. Esta orden aseguraba que existieran estándares de mecanismos de interconexión (APIs por la sigla en inglés de Application Programming Interface) que permitieran a los clientes a compartir de manera segura su información financiera o permitir de manera segura la iniciación de pagos. Así mismo, se dispuso la creación de la Open Banking Implementation Entity (OBIE) que es la entidad encargada de crear estándares de software, seguridad y mensajería y administrar el Directorio de Banca Abierta que permite a los participantes inscribirse en el ecosistema de Open Banking del Reino Unido.
Así mismo, en el 2017 se emitió en el Reino Unido The Payment Services Regulation 2017 que corresponde a la incorporación y adaptación del PSD2 a la Legislación del Reino Unido, la cual entró en vigor en 2018. Tomado de https://www.openbanking.org.uk/regulatory/

Entre los aspectos más relevantes de la regulación PSD2 se destaca la promoción de la competencia a través de autorizar la entrada de nuevos actores al mercado de pagos -PSP- que cuentan con reglas claras de licenciamiento y actuación, lo que en teoría les permite competir en igualdad de condiciones[6].

Las directivas antes mencionadas tienen como finalidad que terceros no bancarios -PSP- puedan tener acceso a la información de los clientes y usuarios en las entidades financieras a fin de ofrecerles servicios directamente. Estos nuevos servicios están relacionados con: (i) proveer información de cuentas -agregación de cuentas-[7], esto es, permitirle al cliente una visión general y global de su situación financiera en todas las entidades donde tiene productos financieros, y (ii) proveer servicios de iniciación de pagos[8] para permitir que los clientes y usuarios, a través de un tercero, originen una orden de pago contra una cuenta abierta en una entidad bancaria -gestor de cuenta-.

Estas dos actividades dan origen al *Open Banking*. La Directiva PSD2 responde a la necesidad de regular estas actividades que ya se venían desarrollando, a fin de brindar claridad y protección a los clientes y usuarios y un marco unificado para la prestación de estos servicios[9].

Así mismo, el PSD2 estableció la obligación para los gestores de las cuentas de los clientes -entidades bancarias-[10] de no establecer trabas a las actividades de los PSP, tanto de iniciación de pagos como de agregación de cuentas[11]. Los PSP fueron, igualmente, autorizados para tratar los datos de los clientes y usuarios, previa aprobación de los titulares[12].

Respecto a la forma como se accede a la información, ya sea para la agregación de las cuentas o para la iniciación de pagos, las reglas técnicas emitidas por la EBA -Autoridad Bancaria Europea, por sus siglas en inglés European Banking Authority- dieron lugar a la consolidación de las APIs -Interfaz de programación de aplicaciones, por sus siglas en inglés, *Application Programming Interface*- que son los programas de software que les permiten a los PSP conectarse a los sistemas de los bancos para acceder a la información que los clientes y usuarios les han autorizad[13].

Las APIs son los mecanismos que los mercados y las diferentes regulaciones -sin que algunas se refieran específicamente a ellas o las consideren como estándares obligatorios[14]- han establecido para garantizar la interoperabilidad de los sistemas y, por ende, garantizar

[6] https://eur-lex.europa.eu/legal-content
[7] Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de la Unión Europea de 25 de noviembre de 2015. PDS2. Artículo 4. Definiciones. Numeral 16. «servicio de información sobre cuentas»: servicio en línea cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago bien en otro proveedor de servicios de pago, bien en varios proveedores de servicios de pago.
[8] Ídem. Directiva PSD2. Artículo 4. Definiciones. Numeral 15. «servicio de iniciación del pago»: servicio que permite iniciar una orden de pago, a petición del usuario del servicio de pago, respecto de una cuenta de pago abierta con otro proveedor de servicios de pago.
[9] Ídem. Directiva PDS2, considerandos (28) y (29).
[10] Entendidos como las entidades incumbentes que manejan las cuentas de los clientes.
[11] Ídem, Directiva PSD2, artículos 66 y 67.
[12] Ídem, Directiva PSD2, artículo 94.
[13] El PSD2 no exige la creación de estándares comunes de conectividad a través de APIs. Por el contrario, la Autoridad Bancaria Europea expidió las Normas Técnicas Regulatorias (RTS), que disponen que los bancos deben garantizar el acceso a proveedores externos, ya sea a través de la creación de un API o de la modificación de la interfaz existente, este último se ha denominado "raspado de pantalla" –conocido en inglés como screen scraping. La no definición de estándares de desarrollo de las APIs dificulta la interconexión, ya que al permitir que cada entidad financiera construya y maneje sus APIs bajo sus propios términos y condiciones hace que cada Third-Party Provider (TPP) debe llevar a cabo desarrollos para conectarse a cada tipo de API y a los sistemas de las entidades financieras que las expongan.
[14] Remolina, Nydia. Open Banking: Regulatory challenges for a new form of financial intermediation in a data-driven world (2019). Centre for AI & Data Governance, pág. 11.

la estandarización de los mecanismos de intercambio de información. Mediante una API, el banco o la entidad en la cual el cliente tiene su cuenta y sus recursos expone a los proveedores de servicios de pago -PSP- la información que se requiere para la respectiva operación -agregación de cuentas, iniciación de pagos, etc.-. Esto facilita que los incumbentes -las entidades financieras- no requieran hacer grandes ajustes a sus sistemas para permitir a los terceros acceder a la información y que los terceros proveedores de servicios de pago -PSP- no requieran tampoco incurrir en grandes costos de desarrollo para ajustar sus sistemas con ese fin.

Esta interconexión entre sistemas es más común de lo que pensamos. Veamos algunos ejemplos sencillos del uso de APIs. El primero está relacionado con las redes sociales. Al acceder por primera vez a la página web o aplicación de un proveedor -hoteles, compra en línea, etc.-, es usual que para registrarse aparezca una ventana emergente -*pop up*- que pida aceptar que el registro se haga con el usuario de, por ejemplo, Facebook, Instagram u otra red social. Detrás de este sencillo *pop up* se encuentra una API que conecta el software del proveedor al que se quiere acceder con el de la red social. Esta API permite que tanto proveedor como la red social compartan los datos y el usuario pueda autenticarse en la página del proveedor de manera automática. Así, cada vez que se adquiere un bien o servicio en ese proveedor, el gestor de la red social lo sabrá y le ofrecerá al cliente o usuario publicidad de productos o contenido relacionado con sus preferencias.

Las APIs también están presentes en el sistema financiero. En ciertos comercios existe la opción de pagar las compras con un QR que se puede generar directamente desde la página o app del comercio. Este QR permite proveerle al comercio información detallada de los pagos que ha recibido, le facilita las conciliaciones bancarias y, lo más importante, los recursos se acreditan directamente a la cuenta del comercio en el banco -en muchos casos evitando el uso de una red de pagos de bajo valor-.

Además de las APIs, existen otros modelos que permiten acceder a la información. Entre estos se destaca el *Screen Scraping* mediante el cual el cliente le otorga las credenciales -usuario y claves- a su PSP para que acceda a toda la información que tiene con el banco. Si bien el cliente puede autorizar que el acceso solo sea a cierta información, el cumplimiento de dichas limitaciones depende de la voluntad y ética del proveedor de servicios de pago. Dado que se ha utilizado de manera ilícita -para obtener información no autorizada-, este modelo tiene muchos detractores y en algunos países, como Colombia, no es una práctica aceptada[15].

2.1. Modelos *Open Banking*

Las entidades financieras poseen una gran cantidad de datos; algunos corresponden a *data* estructurada, tales como pagos, retiros, saldos de cuenta; otros a información semiestructurada, como la incluida en los *emails* cruzados con las entidades financieras o el historial de navegación en las páginas de dichas entidades, y, finalmente, data no estructurada como la que se obtiene a partir de interacciones presenciales -oficinas- o a

[15] El numeral 4 del Artículo 2.17.4.1.3 del Decreto Único 2555 de 2010 (modificado por el Decreto 1297 de 2022) señala que los iniciadores de pago "En ningún caso podrán tener acceso a las claves, contraseñas o mecanismos de autenticación del ordenante con su entidad emisora."

través de canales análogos como *Call Centers*[16].

De igual manera, la cantidad de datos puede corresponder a información personal, como identificación, nombre, nacionalidad, lugar y fecha de nacimiento, edad, género, estado civil, detalles de contacto -teléfono, dirección, correo electrónico, geolocalización, etc.-, historial de navegación en las páginas web del banco, dirección IP, propiedades, activos, pasivos, ingresos, gastos, educación, profesión, datos de empleo, etc.[17] Todos estos datos son usualmente suministrados por los clientes y usuarios al momento de vincularse con una entidad financiera.

Además de la información personal, los bancos cuentan con datos relativos a la relación puramente financiera con sus clientes. Estos incluyen cuentas bancarias, saldos, créditos, inversiones, comportamiento crediticio, perfiles de cliente, solvencia, comportamiento de pago, transferencias, medios de pago, etc. Así mismo, como lo mencionamos respecto del uso de la analítica, pueden establecerse comportamientos específicos del cliente, preferencias de compras o de proveedores, etc.

Toda esta información es, sin duda, un activo muy relevante de las entidades financieras, y no solo ellas sino también los terceros desean tener acceso a la misma a fin de brindar a sus clientes y usuarios productos acorde con sus preferencias y necesidades.

Dentro del *Open Banking* se destacan dos formas de participación o de apertura de datos. El primero, conocido como el *Banking as a Service –BaaS-*, reconoce que en un mundo de ecosistemas los servicios bancarios son un medio y no un fin. Significa, por ejemplo, que el crédito hipotecario que otorga una entidad financiera no es el fin o propósito que persigue un cliente; el fin es adquirir vivienda, que la familia tenga un hogar; de modo que el crédito solo es un medio para alcanzarlo.

En este modelo, el servicio bancario pasa a un segundo plano y en algunos casos ni siquiera el consumidor conoce que está haciendo uso de un servicio de una entidad financiera. Así, por ejemplo, es posible que el cliente o usuario al hacer una transacción crea que el comercio al cual accede le está otorgando un crédito para financiar el producto que está adquiriendo -*buy now pay later*-. Sin embargo, lo cierto es que detrás del comercio se encuentra una entidad financiera que no aparece[18], pero que es la que otorga la financiación de ese producto.

El éxito de los modelos *BaaS* radica en que el cliente o usuario no tiene que abandonar la página o app del comercio para acceder a los servicios financieros, sino que a través de APIs los servicios financieros están subsumidos en el comercio.

Hay muchos ejemplos de *BaaS*, algunos en el mundo digital y otros en el mundo análogo. Así, en el modelo tradicional se encuentran las tarjetas de crédito personalizadas por parte de los grandes comercios que comparten las marcas con las entidades bancarias. En este caso, los comercios cuentan con toda la información de los clientes y usuarios, lo que les

[16] Tomado de European Banking Authority (Autoridad Bancaria Europea). Discussion Paper on innovative uses of consumer data by financial institutions. Mayo 2016
[17] Ídem.
[18] Este modelo se denomina "marca blanca", en el cual el proveedor de bienes o servicios los promociona u ofrece a su propio nombre cuando en realidad son producidos u ofrecidos por un tercero que no es visible para el cliente.

permite optimizar la oferta de bienes o servicios de acuerdo con sus preferencias. Los bancos, por su parte, pueden acceder al detalle de los bienes o servicios que adquieren sus clientes y usuarios.

En el mundo digital, podemos citar el caso de los grandes comercios que usan métodos de pago que son servicios prestados por entidades financieras -cuentas de depósito, billeteras electrónicas, etc.-, pero que se encuentran disponibles en las páginas de los comercios, en algunos casos como marcas blancas, pero en todos privilegiando la experiencia del cliente con la facilidad de no tener que salirse de la página del comercio en la que se hace todo el proceso de autenticación y aprobación del pago.

El decreto 1297 de 2022 –decreto de *Open Banking*- reconoce el modelo *BaaS* como parte relevante de los ecosistemas digitales en los que interactúan las entidades financieras bajo dos figuras. En la primera, el servicio financiero es ofrecido y prestado a través de la plataforma digital o electrónica del tercero no vigilado, caso en el cual ese tercero se considera un corresponsal digital del banco[19].

La característica fundamental de esta figura es que las transacciones se llevan a cabo en la plataforma del tercero no vigilado, por lo que el citado decreto establece que los corresponsales deberán indicar a los clientes y usuarios la entidad financiera que ofrece y presta los servicios financieros, exponiendo de forma visible la marca de aquélla -al parecer proscribiendo el uso del modelo de marca blanca-, así como informar los canales de atención establecidos por la entidad financiera. En todo caso, el corresponsal, al ser el dueño de la plataforma en que se accede a los servicios financieros, debe disponer de las medidas de seguridad necesarias para garantizar el debido tratamiento de los datos personales del consumidor financiero, sin que la regulación establezca claramente su responsabilidad en dicho tratamiento.

En la otra figura regulada, el tercero no vigilado sirve como un canal de acceso a las plataformas o sistemas de la entidad financiera. En este caso, el corresponsal ofrece el servicio, pero el mismo es prestado directamente por la entidad financiera. Las entidades financieras deberán aplicar las reglas establecidas por la Superintendencia Financiera para la seguridad de las operaciones a través de este canal, usualmente canal de Internet[20]. A este modelo no se le aplican las reglas y restricciones que mencionamos para los corresponsales digitales, por lo que resulta más atractivo para la entidad financiera que lo puede ofrecer en los mismos términos en que lo hace directamente.

El otro modelo en el que están incursionando las entidades financieras es el *Bank as a Channel -BaaC-*. En este, las entidades financieras ofrecen *Market Places* o supermercados en línea, que son espacios a través de los cuales varios terceros, por ejemplo, en la app de la entidad financiera, ofrecen bienes y servicios a los clientes y usuarios de dicha entidad y a sus propios clientes.

Uno de los primeros desarrollos de un *BaaC* son los contratos de uso de red entre entidades aseguradoras y bancos. En este modelo las aseguradoras ofrecen sus productos a los

[19] Esta figura se encuentra limitada por las condiciones establecidas por el Gobierno Nacional en el Decreto Único 2555 de 2010, Título Noveno, Libro 36, Parte 2.
[20] Superintendencia Financiera de Colombia. Circular Básica Jurídica. Parte I, Título II, capítulo I. numeral 2.3.4.9.

clientes y usuarios de los bancos utilizando la red, física o digital, de estos[21].

Pero el mundo de los ecosistemas va más allá. Como los servicios financieros son un medio y no un fin, al final los diferentes proveedores de bienes o servicios -conocidos como TPP por sus siglas en inglés, *Third-Party Providers*- pueden acceder a los canales dispuestos por las entidades financieras para ofrecer sus productos y servicios a todos los clientes de dichas entidades.

En estos canales se les facilita a los proveedores de bienes y servicios -TPPs- el acceso a botones de pago, medios de pago -tarjetas de crédito y tarjetas débito- y a créditos para sus clientes -*buy now pay later*-. La información de pagos y preferencias de consumo se comparten entre las entidades bancarias y los TPPs, lo que facilita la profundización de sus clientes.

Este modelo fue igualmente regulado por el decreto de *Open Finance* en el cual se señala que, en desarrollo del principio de conexidad de las operaciones, las entidades financieras pueden ofrecer para su comercialización, en sus canales no presenciales, productos o servicios de terceros no vigilados por la Superintendencia Financiera de Colombia y cobrar contraprestaciones a tales terceros[22].

El principio de conexidad significa el ofrecimiento de productos de terceros siempre que con ello se promueva el uso de los productos o servicios de las entidades financieras, tales como sus medios de pago -tarjetas débito o crédito, depósitos de bajo monto u operaciones de crédito-.

El mencionado decreto establece que bajo esta modalidad las entidades financieras deberán dar cumplimiento al Estatuto de Protección del Consumidor[23] en la modalidad de comercio electrónico, efecto para el cual se consideran portales de contacto[24]. Las entidades financieras no se consideran productor, proveedor o expendedor de los bienes o servicios, pero sí tienen la obligación de contar con un registro de los oferentes en sus plataformas, de tal manera que tanto consumidores como autoridades puedan ponerse en contacto con el proveedor o productor de los bienes o servicios.

La citada regulación de *Open Finance* reconoce que la realidad va más allá del modelo de *Open Banking* que surgió en el entorno de la iniciación de pagos y agregación de cuentas, ampliando su espectro a otros servicios e información de las entidades financieras, con nuevos actores tales como las compañías de seguros, las administradoras de recursos de terceros -fondos de pensiones, fondos de inversión colectiva, APT y patrimonios autónomos-, así como a otros actores tales como las comisionistas de bolsa y los proveedores de

[21] El Decreto 1297 de 2022, artículos 5, 6 y 7, modificó las normas de uso de red de entidades financieras eliminando la obligatoriedad de que los mismos fueran remunerados.
[22] Decreto 1297 de 2022, Título primero, Capítulo noveno.
[23] Ley 1430 de 2011.
[24] Ley 1430 de 2011, Artículo 53. PORTALES DE CONTACTO. Quien ponga a disposición una plataforma electrónica en la que personas naturales o jurídicas puedan ofrecer productos para su comercialización y a su vez los consumidores puedan contactarlos por ese mismo mecanismo, deberá exigir a todos los oferentes información que permita su identificación, para lo cual deberán contar con un registro en el que conste, como mínimo, el nombre o razón social, documento de identificación, dirección física de notificaciones y teléfonos. Esta información podrá ser consultada por quien haya comprado un producto con el fin de presentar una queja o reclamo y deberá ser suministrada a la autoridad competente cuando esta lo solicite.

infraestructura[25].

Así mismo, a medida que avanza el modelo y se ven sus beneficios, se empiezan a abrir datos no financieros de los clientes y usuarios, ya sea de otros sectores como el de las telecomunicaciones o del sector público, en especial datos relacionados con comportamientos en el pago de impuestos, servicios públicos, etc.[26].

Este modelo de *Open Data* tiene como su principal exponente a Australia, donde las autoridades regularon la necesidad de compartir datos no solo desde el sector financiero sino también en otros como energía y telecomunicaciones, con la mirada puesta en ampliar a más sectores y tener un modelo *Open Society,* en el que el ciudadano tiene el control completo de sus datos -en todos los ámbitos- y los gestiona y administra para facilitar a través de la tecnología todas sus actividades diarias[27].

En nuestro país, previo a la reciente expedición del decreto de *Open Finance*, muchas entidades financieras y terceros han avanzado voluntariamente en la adopción de modelos *Open*.

Esta implementación voluntaria tiene su fundamento, principalmente, en la autorización de tratamiento de datos que los clientes y usuarios de las entidades financieras otorgan al momento de su vinculación a sus bienes o servicios de compartir la información con aliados para fines comerciales.

Así, las entidades financieras han puesto a disposición de estos aliados un mercado de APIs para que tales terceros puedan acceder a cierta información de los clientes y usuarios y poder ofrecerles servicios como la iniciación de pagos, incluir botones de pago en sus páginas web, facilitar pagos con códigos QR en los activos digitales de los aliados -apps o páginas web-, transferencias instantáneas a sus cuentas, etc.

Como señalamos, el Gobierno Nacional emitió recientemente la regulación base que permitirá ordenadamente el desarrollo y adopción de este modelo. Con el apoyo del Banco Mundial, durante el 2021 se llevaron a cabo varias mesas de trabajo que finalizaron en la expedición del citado decreto que (i) precisa las reglas aplicables al intercambio de datos del consumidor; (ii) enmarca la administración de plataformas digitales y la prestación de servicios por parte de las entidades; (iii) reglamenta la iniciación de pagos, y (iv) fortalece los estándares de protección al consumidor en la era digital[28].

Si bien la citada regulación no es explícita en señalar que el modelo adoptado de *Open Finance* es voluntario, eso es lo que se deduce de los documentos técnicos previos que son su sustento y de algunos apartes de la misma[29]. Además, es claro que el Gobierno, a

[25] Los proveedores de infraestructura del mercado de valores son, entre otros, las bolsas de valores y de bienes y productos agropecuarios y agroindustriales y de otros commodities, las cámaras de riesgo central de contraparte, las sociedades administradoras de sistemas de negociación y de registro de operaciones y los depósitos centrales de valores. Estos agentes facilitan la operación del mercado. AMV Colombia. https://www.amvcolombia.org.co/glosario/proveedor-de-infraestructura/

[26] Unidad de Regulación Financiera del Ministerio de Hacienda y Crédito Público – URF. Documento técnico. Modelo de finanzas abiertas en Colombia. Octubre de 2021.

[27] Asobancaria. Openbanking: Experiencias de implementación en el ámbito internacional.

[28] Unidad de Regulación Financiera del Ministerio de Hacienda y Crédito Público – URF. Documento técnico. Modelo de finanzas abiertas en Colombia. Octubre de 2021. En este proyecto como se indica, se le autorizaba a las entidades vigiladas para ofrecer plataformas digitales a terceros y prestar servicios no bancarios como el suministro de tecnología.

[29] Ídem. URF Documento Técnico y Documento de política pública 2020-2025 del Ministerio de Hacienda y Crédito Público Para un mayor desarrollo del sistema financiero.

través de la Superintendencia Financiera, es el encargado de señalar las reglas y principios generales de su operación -estándares-, sin perjuicio de la facultad de la Superintendencia de Industria y Comercio de emitir reglas en materia de seguridad de la información y protección de datos.

Este modelo ha sido adoptado en países como Singapur, Nueva Zelanda y Hong Kong, en contraposición a modelos obligatorios como los adoptados en la Unión Europea -PSD2-, Reino Unido, Brasil y México, o modelos voluntarios sin reglas o principios generales como el de Estados Unidos.

En paralelo a la discusión del citado proyecto de decreto, en marzo de 2022 el Gobierno, en sustitución del proyecto de Ley 413 de 2021[30], presentó, con mensaje de urgencia, el proyecto de Ley 337 de 2022[31], en el que se establecía un modelo de *Open Finance* obligatorio, en contra de los análisis previamente efectuados, y se buscaba avanzar en un modelo *Open Data*[32] que involucrara información de otros sectores económicos diferentes al sector financiero[33].

Pese al mensaje de urgencia del Gobierno, este proyecto de ley no fue discutido por el Congreso en la Legislatura 2021-2022 y, en consecuencia, fue archivado. Si es de interés del nuevo Gobierno avanzar hacia un modelo de Open Data, tendría que presentarse otro proyecto de ley en tal sentido.

Por ahora se debe esperar la reglamentación de los estándares que debe emitir la Superintendencia Financiera, sin perjuicio de que continúe, ya con una base mucho más sólida, la implementación voluntaria y regulada por alianzas bilaterales entre las entidades financieras y los TPPs.

Ahora bien, para que los diferentes modelos de *Open* tengan éxito, los clientes y usuarios deben otorgar las autorizaciones necesarias para compartir su información. Por eso, en el siguiente capítulo nos referiremos a la importancia de la protección de datos personales y de la reserva bancaria.

3. Protección de datos y reserva bancaria

Como lo mencionamos, la cuarta revolución industrial se basa en el uso, análisis y procesamiento de la información. Los datos se han vuelto uno de los principales activos en todas las industrias.

---

[30] Proyecto de ley "Por la cual se dictan normas relacionadas con el sistema de pagos, el mercado de capitales y se dictan otras disposiciones".

[31] "Por la Cual se Dictan Normas Relacionadas con el acceso y el Financiamiento para la Construcción de Equidad, y se dictan otras disposiciones".

[32] En el Documento Técnico: Modelo de finanzas abiertas en Colombia publicado por la URF en octubre de 2021, se precisó que "[e]n paralelo al trámite de expedición del esquema de Open Finance, se buscará avanzar conjuntamente con otras autoridades en un segundo frente denominado Open Data con el fin de promover el intercambio de información de otros sectores de manera que se fortalezca el ecosistema y se potencien sus beneficios" y "Como complemento, y en forma paralela al trámite de expedición normativo, se propone avanzar conjuntamente con otras autoridades en un segundo frente denominado Open Data, el cual busca escalar las reglas y principios relativos al intercambio de información a entidades no financieras".

[33] El artículo 33 del citado proyecto de ley establecía "Acceso a la información. Con el propósito de promover la competencia, la inclusión y la eficiencia en la prestación de servicios financieros, aquellos que traten información deberán permitir el acceso a ésta, siempre que haya sido autorizado previamente por el titular en los términos señalados en las leyes 1266 de 2008 y 1581 de 2012." (negrilla ajena al texto original).

La información de las personas está directamente ligada a su derecho a la intimidad, que ha sido reiteradamente definida por la Corte Constitucional como *el derecho que garantiza en los asociados, el poder contar con una esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas*[34]. Este derecho a la intimidad tiene dos dimensiones: la negativa, que consiste en la posibilidad de negarse a cualquier injerencia arbitraria en la esfera íntima de las personas, y la positiva, que es el derecho a la libertad en el ejercicio de su vida privada.

En relación con la primera, el derecho a oponerse a la intromisión en su ámbito privado implica también la posibilidad exclusiva del individuo de permitir el acceso a la información de su intimidad -Corte Constitucional, sentencia C-094 de 2020-. Para ello, se han definido diferentes tipos de datos como lo veremos más adelante. Sin embargo, es sobre este aspecto de intimidad que se construyen las diferentes regulaciones relativas a la protección de los datos.

3.1 La titularidad de los datos

En la introducción hicimos referencia a que las diferentes regulaciones han tratado ampliamente el concepto de titularidad de la información y que aún existen discusiones sobre la propiedad de los datos en el sentido tradicional. Iniciando la vigencia de la Constitución de 1991 ya se discutía sobre la diferencia de estos dos conceptos.

En efecto, la Corte Constitucional señaló que, dada la complejidad del dato y la forma como se construye la información, el concepto clásico de la propiedad no se puede aplicar de manera estricta. Principalmente, porque en el tratamiento de los datos confluyen diferentes relaciones y actores. Por ello, concluyó la Corte que …*los diversos sujetos son apenas titulares de algunas facultades que no les confieren necesariamente la calidad de propietarios*,…, de tal manera que no pueda hablarse de la existencia de un propietario del dato en estricto sentido, pues no por el hecho de permitir su tratamiento, uso y en algunos casos su comercialización, el titular pierde el control del mismo y los derechos que sobre tal dato puede ejercer[35]. Si bien en sentencias posteriores pareciera que la Corte Constitucional ha señalado que el titular del dato es su propietario, tales citas hacen referencia a la noción antes expuesta, esto es, que la titularidad no puede enmarcarse en el concepto clásico de propiedad. Esta misma visión se recoge en el documento técnico elaborado por la Unidad de Regulación Financiera del Ministerio de Hacienda y Crédito Público que soporta el decreto de *Open Finance* -decreto 1297 de 2022-.

Lo anterior se hace evidente cuando se analiza el tratamiento de ciertos datos indispensables para iniciar o mantener una relación comercial o de servicios -por ejemplo, datos públicos como nombre e identidad, o datos personales privados como correo electrónico o teléfono-. En el caso de una cuenta bancaria, si bien el titular de los datos sigue siendo el cliente, por lo menos uno de los atributos de la propiedad, el uso -*jus utendi*-[36] se le concede a la

[34] Corte Constitucional. Colombia. Sentencia C-094 del 3 de marzo de 2020. Sala Plena. M.P. Dr. Alejandro Linares Cantillo. Num. 65.
[35] Corte Constitucional. Colombia. Sentencia T-414 del 16 de junio de 1992. Sala Primera de Revisión. M.P. Dr. Ciro Angarita Mejía.
[36] Hasta ahora, hemos visto que, para buena parte de los libros de derecho civil colombiano, los juristas romanos entendían que el derecho de propiedad estaba compuesto de tres elementos: el jus utendi, el jus fruendi, y el jus abutendi. Inclusive, un autor le atribuyó al derecho romano la siguiente definición: "dominium est ius utendi atque abutendi re sua quatenus iuris ratio patitur (dominio es el derecho de usar y disponer de su propia cosa, en cuanto respaldado por una razón jurídica)" (Barragán 1971: 57). No obstante, vimos dos voces en contra de la tendencia: una, la de Rodríguez Piñeres, advirtiendo que las denominaciones de jus utendi, fruendi, y abutendi, "no son romanas" (1990: 81); y otra, la de Rodríguez Fonnegra, señalando que la idea de jus fruendi proviene de "los comentadores del Derecho Romano, que no propiamente los textos en que éste se contiene" (1960: 192). EL DERECHO ROMANO DE LA PROPIEDAD EN LA DOCTRINA CIVIL COLOMBIANA. Federico Escobar Córdoba. Página 315 (Este texto forma parte de una investigación sobre el derecho de propiedad en el derecho romano y en las codificaciones modernas, que el autor realiza en la Universidad Icesi.)

entidad financiera, mientras subsista la relación y aún después de terminada si consideramos la obligación legal de conservar los documentos soporte de sus operaciones[37].

Sin embargo, para los propósitos de este escrito haremos referencia al concepto de titularidad del dato, noción que utilizan las diferentes regulaciones en el mundo.

Empecemos por definir algunos conceptos básicos como el *dato*. La RAE lo define como la *información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho*. El dato permite contar con información de algo concreto o tener conocimiento de una situación. Puede estar referido a una persona, compañía, situación, etc.

Los datos personales, es decir, aquellos que hacen referencia a las personas naturales, han sido objeto de una especial regulación y protección.

Así, el Reglamento -UE- 2016/679 del Parlamento Europeo y del Consejo de la UE del 27 de abril de 2016[38] define el dato personal como *toda información sobre una persona física identificada o identificable* (*«el interesado»*); *se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*[39].

Similar definición ha sido adoptada por nuestra regulación en la cual se define el dato personal como *(c)ualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables*[40].

Obsérvese que las definiciones citadas no están referidas únicamente a los datos puros y duros de una persona, tales como su nombre, edad, identificación o ubicación, sino a toda o cualquier información que pueda asociarse a una persona natural, lo que abre un espectro enorme de lo que puede entenderse como dato personal.

En ese mundo de posibilidades surge la denominada Big Data, es decir, el manejo y procesamiento de grandes cantidades de datos personales y de las compañías a través de la analítica, cuyo objetivo es conocer mejor a los clientes y usuarios o potenciales clientes y ofrecer productos o servicios que se adecuan a sus preferencias y necesidades.

En cuanto a la clasificación de los datos, las regulaciones internacionales -GDPR- y locales -ley 1581 de 2012- hacen referencia exclusiva a los datos sensibles y los datos de menores. Sin embargo, en Colombia otras regulaciones -ley 1266 de 2008 y decreto 1377 de 2013-, así como la jurisprudencia de la Corte Constitucional, han venido creando una clasificación que resulta importante para los efectos de este ensayo.

---

[37] Estatuto Orgánico del Sistema Financiero. Decreto 663 de 1993. Artículo 96.
[38] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos - GDPR por sus siglas en ingles). https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504.
[39] Idem.
[40] Ley 1581 de 2012, artículo 3, literal c).

En efecto, la ley 1266 de 2008 establece tres tipos de datos: públicos, semiprivados y privados o sensibles.

Se define como público el dato que no sea semiprivado, privado o sensible. Son considerados públicos, entre otros, los relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros y documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva[41].

Los datos privados o sensibles son … *aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos*[42].

Los datos semiprivados, son *…aquellos que no tienen naturaleza íntima, reservada, ni pública y que, por ende, su conocimiento puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general. Ejemplo de esta categoría es el dato financiero y crediticio de actividad comercial o de servicios*[43].

Esta clasificación resulta relevante para el tratamiento de datos por parte de las entidades financieras, por cuanto los datos pueden ser luego compartidos con terceros en virtud del *Open Banking*, *Open Finance* u *Open Data*. Allí se pueden incluir datos públicos, cuyo tratamiento y uso no tiene mayor complejidad; datos semiprivados, como son los datos financieros de los usuarios de los bancos, que requieren autorización previa del titular para su tratamiento, pero también se puede llegar a compartir datos sensibles, tales como los capturados -biométricos- o los que a través de la analítica y otros mecanismos permiten inferir información relacionada con comportamientos y preferencias y generar perfiles que de una u otra manera puedan involucrar datos privados.

Así, por ejemplo, mediante la captura biométrica de la cara de una persona para permitirle el acceso a sus servicios financieros y autenticarlo se puede determinar su raza. Estos datos, al ser sensibles, requieren de autorizaciones expresas y tratamiento especial, y si se va a compartir por virtud de la apertura de datos, resulta de la mayor relevancia la calidad de las autorizaciones otorgadas por su titular.

Ahora vale la pena preguntarse cómo se autoriza el manejo de datos y la captura o creación de perfiles o preferencias. La respuesta es: de manera fácil, cotidiana y, muchas veces, inconsciente.

Las personas, al acceder a las redes sociales o a cualquier servicio por Internet, suelen suministrar a los proveedores cierta información básica como nombre, dirección, teléfono, correo electrónico, edad, domicilio/ubicación, etc. Al acceder a estos servicios de Internet -de consulta de información o transaccionales- están autorizando a los proveedores o terceros

[41] Decreto 1377 del 27 de junio de 2013, artículo 3º, numeral 2.
[42] Corte Constitucional. Sentencia C-1011 del 16 de octubre de 2008. M.P. Jaime Córdoba Triviño.
[43] Idem.

para que capturen toda la información relacionada con sus comportamientos, preferencias, páginas visitadas, direcciones IP, apps utilizadas, tiempos de permanencia, etc.

Estos mecanismos de captura, desde el punto de vista tecnológico, son muy variados. El más conocido son las *cookies*, especialmente por la obligación que impuso el GDPR a los proveedores de servicios de obtener expresa autorización de los usuarios para su uso.

Las *cookies* son archivos de texto que son colocados en los dispositivos -computadores, móviles, tabletas, etc.- cada vez que se visita un sitio web o una app. En principio, las *cookies* son necesarias para permitir la navegabilidad en la web o app; usualmente, las necesarias para tal propósito se eliminan del dispositivo una vez se abandona la página respectiva[44].

Sin embargo, existen diferentes tipos de *cookies*[45]; algunas son utilizadas para capturar información y el comportamiento de los usuarios en la respectiva web. De acuerdo con la regulación del GDPR, dada la cantidad de datos que se puede capturar y el hecho de que es posible asociar esos datos a una persona, las *cookies* están sujetas a dicha regulación y, por ende, es necesario que el usuario acepte expresamente su uso.

Similares a las *cookies*, existen los identificadores de anunciantes. Son un número que identifica al propietario de un móvil, tableta o computador. Estos identificadores les permiten a las empresas de tecnología móvil -sistemas IOS o Android- rastrear el comportamiento de los usuarios y elaborar perfiles de preferencias de consumo para hacer publicidad relevante.

Dado este sinnúmero de mecanismos que permiten capturar la información -datos duros y otros datos como comportamientos, ubicación geográfica, permanencia en apps, webs, preferencias de compras, etc., así como otros datos que se logran inferir mediante analítica y que pueden además generar perfiles de las personas-, se hace necesario establecer mecanismos idóneos de información y de autorización clara y específica para su tratamiento; en particular, para el caso del *Open Finance*, contar con las autorizaciones respectivas para compartir la información con terceros y establecer las responsabilidades que de ello se derivan.

3.2 Reserva bancaria

La actividad bancaria o financiera es una actividad basada en la confianza. El usuario confía en que el profesional bancario hará un adecuado manejo de sus depósitos y que obtendrá

[44] Tomado de https://gdpr.eu/cookies/

[45] En general, hay tres diferentes formas de clasificar las cookies, (i) según su propósito, (ii) el tiempo que duran (temporales o permanentes) y (iii) la procedencia (incluidas por el proveedor o por un tercero).
Las más relevantes resultan ser las del propósito que persiguen. Estas a su vez se clasifican en las (i) necesarias (las que permiten acceder al sitio web y utilizar sus funcionalidades, incluidas las de seguridad del sitio), (ii) cookies de preferencias, que permiten recordar las preferencias del usuario (idioma, ubicación, usuario, etc) que permiten una mejor experiencia del usuario; (iii) de estadística o de desempeño, que permiten capturar información sobre cómo se usa el sitio web, qué páginas visitó, así como los enlaces a los cuales accedió, y (iv) finalmente, las cookies de mercadeo que rastrean la actividad en línea y permiten conocer las preferencias de tal manera que los anunciantes puedan enviar publicidad o información relevante para al usuario. Usualmente, permiten compartir información con terceros y no son del proveedor sino de terceros. Estas cookies pueden compartir esa información con otras organizaciones o anunciantes. Se trata de cookies persistentes y casi siempre de procedencia de terceros. Tomado de https://gdpr.eu/cookies/
También existen otras cookies como las de redes sociales o de interacción, también llamadas plugins sociales (como “Me gusta” de Facebook), estas permiten al usuario mostrar su interés por una página o recomendarla, y pueden recolectar información aún si el usuario no las utiliza. (Tomado de Documentos Dejusticia 48. RENDICIÓN DE CUENTAS DE GOOGLE Y OTROS NEGOCIOS EN COLOMBIA: la protección de datos personales en la era digital).

su reintegro en las condiciones pactadas -a la vista o a plazo-. Así mismo, dado el carácter de profesional, espera que el manejo de los recursos se haga con la mayor diligencia posible y, adicionalmente, que la información suministrada a este profesional se manejará de manera apropiada.

De esa relación de confianza surge la reserva bancaria como una expresión del secreto profesional y, de paso, del derecho a la intimidad.

La reserva bancaria fue definida en su época por la entonces Superintendencia Bancaria como *el deber de los establecimientos bancarios y demás entidades financieras de guardar reserva y discreción sobre los datos de su cliente, la que conozcan en desarrollo de su profesión u oficio, por cuanto para el cliente pueden derivarse inmensos perjuicios con la divulgación de ciertos aspectos que por razones comerciales y personales no deben ser de libre acceso al público*[46].

Más recientemente, la Superintendencia Financiera de Colombia, en concordancia con el artículo 7, literal i, de la Ley 1328 de 2009, definió la reserva bancaria como … *el deber que tienen las entidades y sus funcionarios de guardar reserva y discreción sobre los datos de los consumidores financieros o sobre aquellos relacionados con la situación propia de la compañía, que conozcan en desarrollo de su profesión u oficio, so pena de asumir las consecuencias penales, laborales y administrativas que el incumplimiento a dicho precepto podría acarrear al infractor*[47].

Respecto del origen del derecho/deber a la reserva bancaria, la Corte Constitucional[48] señaló:

> *En Colombia, la reserva bancaria, ha sido definida por la Corte como "el deber jurídico que tienen las instituciones de crédito y las organizaciones auxiliares y sus empleados, de no revelar los datos que lleguen directamente a su conocimiento, por razón o motivo de la actividad a la que están dedicados.*
>
> *La razón por la cual la entidad bancaria entra en contacto con información personal de sus usuarios y el deber mismo de proteger dichos datos, están estrechamente ligados con su condición de profesional de las actividades bancarias. Por ello, desde el punto de vista conceptual, la reserva bancaria es en Colombia una especie del secreto profesional, y la protección de los datos en manos del banquero encuentra como una de sus fuentes constitucionales al artículo 74 de la Carta.*
>
> *Por su parte, el secreto bancario cumple funciones esenciales en la realización de intereses públicos en el ámbito económico. La confianza en el sistema bancario y financiero, uno de los pilares no solo de su funcionamiento sino de su existencia misma, depende en gran medida de la seguridad con que sean manejados los datos proporcionados por los usuarios. Los agentes económicos se verían desincentivados a adelantar transacciones por medio de los sistemas financiero y bancario si la reserva mencionada no fuere respetada de forma debida.*

[46] Superintendencia Bancaria de Colombia. Conceptos OJ-050 de 8 de marzo de 1982 y OJ-288 de 12 de agosto de 1976. Tomado de la sentencia T-440 de 2003 de la Corte Constitucional, num. 4.2.2., nota a pie de página [37].
[47] Superintendencia Financiera de Colombia, Circular Básica Jurídica, Parte primera, Título IV, Capitulo Primero, numeral 6.
[48] Corte Constitucional, Sala Tercera de Revisión, M.P. Dr. Manuel José Cepeda Espinosa. Sentencia T- 440 del 29 de mayo de 2003.

> *(…) Adicionalmente, con sustento en el artículo 15 de la Constitución, la Corte ha establecido que la reserva bancaria, se fundamenta en el derecho a la intimidad.*

Así, resulta que la reserva bancaria en Colombia tiene su origen y protección en dos preceptos constitucionales: el artículo 15 de la Carta Política, referente al derecho a la intimidad, y el artículo 74 de la misma Carta que hace referencia a la inviolabilidad del secreto profesional.

Obsérvese cómo, desde esa perspectiva, el concepto de reserva bancaria, si bien hace parte del derecho a la intimidad, contempla dos aspectos fundamentales: la protección de los datos personales, referidos a una persona natural, pero también la protección de la información de los clientes y usuarios que no tienen la calidad de persona natural, por ejemplo, las personas jurídicas o cualquier otra estructura jurídica sin personería jurídica -patrimonios autónomos, fondos de pensiones y cesantías, fondos de inversión colectiva, etc.-. La Corte Constitucional ha reconocido igualmente que las personas jurídicas -y por extensión las estructuras jurídicas sin personería jurídica- son titulares del derecho fundamental al habeas data y a la intimidad[49].

En tal sentido, la reserva bancaria se erige como un elemento relevante a considerar en una apertura de datos de los clientes y usuarios de las entidades financieras a terceros con el propósito de prestarles servicios adicionales, pues la misma solo se puede levantar con la expresa autorización del titular -persona natural o jurídica-.

El decreto de *Open Finance* expresamente señala que la regulación emitida en momento alguno implica una modificación a las obligaciones que tienen las entidades financieras de proteger la reserva bancaria. Así, cualquier información de clientes y usuarios que la entidad financiera quiera compartir con terceros deberá contar con la previa autorización del levantamiento de la reserva.

4. La tensión y los desafíos entre acceso al dato -*Open*- y la privacidad

Como vimos, el *Open Banking*, *Open Finance* y *Open Data* se basan en que el titular de los datos adquiere el control de los mismos y, en esa medida, les permite a terceros el acceso a su información, a fin de que puedan prestarle nuevos o mejores servicios. En el caso del *Open Finance*, la información a compartir desde el lado de la entidad financiera corresponde a la que ha recibido o ha sido generada en desarrollo de la relación con sus clientes y usuarios -titulares de la información-.

Dado que compartir información implica entrar en la órbita de protección al derecho a la intimidad de las personas y de la reserva bancaria, los principales desafíos del *Open Finance* están referidos a la protección de los clientes y usuarios en relación con el uso de sus datos y la seguridad, así como a la responsabilidad de los diferentes actores por las afectaciones que puedan generar en caso de vulneración o uso indebido de los datos.

En tal sentido, existen varios desafíos o retos relativos al *Open Finance* en relación con las autorizaciones para el tratamiento de datos, los cuales se resumen así: (i) las autorizaciones obtenidas por las entidades financieras y las que otorguen los clientes y usuarios a los TPPs

[49] Corte Constitucional. Sentencia T-462 del 24 de septiembre de 1997. Sala Novena de Revisión. M.P. Vladimiro Naranjo.

deben ser claras en cuanto a las finalidades -legítimas, determinadas y explicitas- para las cuales aprueban compartir sus datos; (ii) las autorizaciones deben ir más allá de compartir datos puros y duros -información base del cliente y/o usuario-; deben además ser claras y expresas en cuanto a poder compartir datos inferidos y perfiles de los clientes y usuarios obtenidos mediante procesos de analítica u otros procesos; (iii) las autorizaciones deben tener claridad respecto de su temporalidad. Dada la naturaleza de los datos que se comparten y las finalidades para los cuales se tratan, se deben evitar autorizaciones indefinidas en el tiempo; (iv) los clientes y usuarios deben autorizar, debidamente informados, el uso de mecanismos tales como *cookies* o identificadores de anunciantes que permiten capturar información sobre sus preferencias, y (v) en el caso de datos sensibles o de menores, las autorizaciones no solo deben ser expresas sino explícitas respecto de los datos sensibles que se tratarán. Así mismo, algunos países exigen que las autorizaciones para compartir ciertos datos sean otorgadas dejando claridad expresa del TPP que puede acceder a la información.

Las diferentes regulaciones se han aproximado de disímil manera a estos retos. El GDPR, como referente internacional, y la regulación local de tratamiento de datos -ley 1581 de 2012- son precisos en determinar que la autorización o el consentimiento -manifestación de voluntad- para el tratamiento de los datos debe ser libre, específica, informada e inequívoca[50]. En términos del GDPR, mediante una declaración o una clara acción afirmativa. En el caso colombiano, las normas de protección de datos incluyen un elemento adicional y es que el consentimiento debe ser expreso[51].

En el mismo sentido, el decreto de *Open Finance*, al referirse al tratamiento de la información por parte de las entidades financieras, señaló que se podrá llevar a cabo respecto de los consumidores -clientes y usuarios- que lo autoricen de manera previa, expresa e informada[52]. De manera más específica señala que, en desarrollo de las normas de protección de datos personales, las entidades financieras deben adoptar medidas de responsabilidad demostrada[53], las cuales deben ser apropiadas, efectivas, útiles, eficientes, demostrables y garantizar la seguridad, la confidencialidad, la veracidad, la calidad, el uso y la circulación restringida de esa información.

Respecto de las autorizaciones indefinidas en el tiempo, algunas jurisdicciones no regulan el tema, otras establecen la obligación de obtener una refrendación, de tiempo en tiempo y ante la entidad financiera, de la autorización de compartir información con un TPP determinado. En nuestro país, el decreto de *Open Finance* establece que los iniciadores de pago no podrán iniciar órdenes de pago sin haber sido autorizados previamente por el ordenante y cada orden de pago o transferencia iniciada debe ser autorizada por el ordenante. Esto se traduce en que, para cada transferencia o pago, el iniciador de pagos debe contactar al cliente o usuario y obtener su autorización para llevar a cabo la transacción. Es posible que para otros casos de uso del *Open Finance* -tales como agregación de cuentas-, la Superintendencia Financiera establezca algunos estándares diferentes dada la operatividad de estos servicios, pero en todo caso, en nuestra opinión, es esencial que se establezca una periodicidad de las autorizaciones y/o su refrendación periódica.

[50] Artículo 4, numeral 11. GDPR y articulo 3, literal a) de la ley 1581 de 2012.
[51] Ley 1581 de 2012, artículo 4, literal c) "Principio de libertad".
[52] Artículo 2.35.8.1.1. del Decreto Único 2555 de 2010 adicionado por el Decreto 1297 de 2022.
[53] Según este principio las entidades que recogen y hacen tratamiento de datos personales deben ser responsables del cumplimiento efectivo de las medidas que implementen los principios de privacidad y protección de datos. Superintendencia de Industria y Comercio. Guía para la implementación del principio de responsabilidad demostrada (Accountability).

En adición a los aspectos antes mencionados, el decreto de *Open Finance* establece la prohibición para los iniciadores de pago de tener acceso a las claves, contraseñas o mecanismos de autenticación del usuario con la entidad emisora. Esta protección resulta esencial tanto en materia de seguridad de las transacciones como de la restricción que ello implica de acceder de manera ilimitada a la información de los consumidores bajo mecanismos como el explicado del *Screen Scraping*.

De los otros aspectos antes mencionados, tales como el tratamiento de datos sensibles, la autorización para el uso de *cookies* o identificadores de anunciantes y la claridad sobre los datos que serán tratados, el mencionado decreto no se ocupa, con lo que reitera la cláusula de competencia general de la Superintendencia de Industria y Comercio de emitir ordenes en materia de seguridad de la información[54] y de supervisar el cumplimiento de las normas en materia de protección de datos.

El otro gran desafío relacionado con las autorizaciones es la responsabilidad por el tratamiento de los datos y las obligaciones de las entidades financieras y de los TPPs o terceros que acceden a la información.

Así, la directiva de la Unión Europea PSD2 estableció que *[e]l proveedor de servicios de iniciación de pagos y el proveedor de servicios de información sobre cuentas, por una parte, y el proveedor de servicios de pago gestor de cuenta [entidad financiera], por otra, deben cumplir las disposiciones sobre la necesaria protección y seguridad de los datos que se establecen o a las que se alude en la presente Directiva, o que figuren en normas técnicas de regulación*. (Texto aclaratorio entre corchetes es ajeno al texto original)[55]. Así mismo, estableció como uno de sus presupuestos para el tratamiento de datos por parte de todos los actores en los sistemas de pago la aplicación estricta de las reglas de protección de datos -GDPR- y de los principios de la protección de datos desde el diseño y por defecto[56].

De igual manera, la regulación de la Unión Europea establece la obligación para las entidades de pago de obtener una previa autorización de la entidad competente del respectivo Estado, para lo cual deben acreditar de manera previa que cuentan con los mecanismos de seguridad y los procesos adecuados para la protección de los datos[57].

En Colombia, se cuenta con una regulación robusta en materia de protección de datos. Por su parte, el decreto de *Open Finance* reiteró el deber de las entidades financieras de dar cumplimiento a las normas en materia de tratamiento de datos personales[58] y de la reserva bancaria[59], incluido el principio del tratamiento de la información por defecto, esto es, que los iniciadores de pago no podrán solicitar a los ordenantes más información de la estrictamente

[54] Artículo 2.35.10.1.1 del Decreto Único 2555 de 2010 adicionado por el Decreto 1297 de 2022.
[55] Directiva PSD2. Consideración (93).
[56] GDPR. Artículo 25. Numerales 1 y 2. "1.Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. 2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.
[57] GDPR. Artículo 5, numeral 1.
[58] Artículo 2.35.8.1.1. del Decreto Único 2555 de 2010 adicionado por el Decreto 1297 de 2022.
[59] Ídem. Parágrafo 2.

necesaria para iniciar la orden de pago o transferencia de fondos, aunque no fue explícito en cuanto a regular la responsabilidad de los diferentes actores en los modelos *Open Finance*.

Esperemos que esta materia sea objeto de análisis y regulación por parte de la Superintendencia Financiera al momento de definir los estándares tecnológicos, de seguridad y otros que considere necesarios para el desarrollo de la arquitectura financiera abierta en Colombia[60], así como por parte de la Superintendencia de Industria y Comercio como autoridad en materia de protección de datos del país[61].

No obstante, se echa de menos que el Gobierno no haya acogido algunas recomendaciones y comentarios efectuados en la discusión del proyecto de decreto, tales como establecer, al igual que en otras jurisdicciones: PSD2 o Reino Unido, requisitos y estándares de seguridad a los TPPs que tendrán acceso a la información de los consumidores y que se construyera un registro centralizado de TPPs que cumplan con requisitos mínimos de capital, funcionamiento y garantías adecuadas, así como reglas claras que permitieran identificar el responsable de cara al consumidor cuando sea el TPP quien esté manejando la información.

Contrario a esta aproximación, el decreto de *Open Finance* determina que los iniciadores de pagos serán participantes en los sistemas de pago de bajo valor y, por ende, que deben cumplir las reglas que fijen los administradores de dichos sistemas. El Gobierno Nacional optó por una supervisión indirecta de los iniciadores de pago[62] por intermedio de las entidades administradoras de sistemas de pago de bajo valor.

Así mismo, no se hace claridad alguna respecto de la condición en que actúan los TPPs, esto es, como responsables o encargados de la información[63], dejando tal responsabilidad en cabeza de las entidades financieras y en las entidades administradoras de sistemas de pago de bajo valor, que deberán exigir a los iniciadores de pago el cumplimiento de ciertos estándares mínimos. Si actúan como responsables del tratamiento de datos, deberán responder en toda la extensión posible por la existencia de las autorizaciones y el alcance de las mismas, así como por cualquier incumplimiento en dicho tratamiento y en la seguridad de la información. Por el contrario, si el modelo con el que se comparte la información trata a los TPPs como simples encargados, si bien tienen responsabilidades, las más relevantes seguirán bajo el control y en cabeza de las entidades financieras, en especial las relativas a la autorización, la debida información al titular del dato y las finalidades de su tratamiento.

De otra parte, en cuanto a la necesidad de tener certeza de que la persona con la que se interactúa, ya sea desde la entidad financiera o del tercero proveedor -TPP-, es en efecto el cliente o usuario que dice ser -titular de los datos-, el decreto de *Open Finance* resuelve tal desafío dejando en cabeza de las entidades emisoras -entidades financieras- la responsabilidad de autenticar, en todos los casos, al ordenante de acuerdo con las reglas que para el efecto dicte la Superintendencia Financiera de Colombia. Si bien este modelo

[60] Artículo 2.35.10.1.1. del Decreto Único 2555 de 2010 adicionado por el Decreto 1297 de 2022.
[61] Ídem. Parágrafo.
[62] Numeral 4 del artículo 2.17.4.1.2. del Decreto Único 2555 de 2010 adicionado por el Decreto 1297 de 2022. *"Los iniciadores de pago deberán cumplir con las reglas y estándares operativos, técnicos y de seguridad que establezca la entidad administradora del sistema de pagos de bajo valor, que permitan el desarrollo de sus operaciones en condiciones de seguridad, transparencia y eficiencia, conforme a lo dispuesto en el artículo 2.17.2.1.5. del presente Decreto".*
[63] Ley 1581 de 2012. Artículo 3o. "DEFINICIONES. Para los efectos de la presente ley, se entiende por: (…)
d) Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;
e) Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos".

permite una mayor seguridad de las transacciones de los clientes y usuarios, aumenta las responsabilidades de las entidades financieras y sus riesgos al conectarse con los TPPs.

Respecto de la seguridad de las transacciones -contrario al modelo adoptado en Colombia, en donde, reiteramos, se optó por una supervisión delegada y se difirió el establecimiento de estándares en cabeza de la Superintendencia Financiera-, el PSD2 establece algunos parámetros que tienen una doble mirada. La primera referida a la seguridad de las transacciones del cliente o usuario y la integridad y confidencialidad de la información que se suministra a los TPPs, y la segunda relativa a los niveles de seguridad que emplean los TPPs para vincularse a los sistemas de las entidades financieras a través de las APIs.

Respecto de la primera mirada, existen a su vez varios riesgos. El primero referido a una violación de la confidencialidad e intimidad de los clientes y usuarios de las entidades financieras. En efecto, una vez el TPP ha accedido a la información que el cliente o usuario le ha autorizado, el riesgo de pérdida o vulneración de la seguridad de dicha información debería ser responsabilidad del TPP. Sin embargo, este tipo de vulneraciones, además de afectar a los clientes y usuarios, afecta al TPP y también las entidades financieras tendrán un alto riesgo reputacional por la pérdida o divulgación indebida de información de sus clientes y usuarios.

Por su parte, el riesgo de fraude se puede materializar por brechas de seguridad de los TPPs en sus propios sistemas. Así, si un TPP ve comprometida su seguridad informática -por no contar con los mecanismos suficientes que garanticen la no vulnerabilidad de la información de sus clientes y usuarios-, es posible que la entidad financiera, a pesar de efectuar la autenticación de los clientes, no pueda reconocer que las transacciones llevadas a cabo desde las aplicaciones del TPP que se conecta mediante APIs al banco son fraudulentas, como ocurriría en caso de que se vulneren los mecanismos adicionales de autenticación, tales como OTPs u otros, con los consecuentes riesgos de responsabilidad y reputacional, o en los casos en que los TPPs tratan información de los clientes que permiten la vulneración de los diferentes mecanismos de seguridad.

En tal sentido, las regulaciones en el mundo exigen a los TPPs ciertos niveles de seguridad en sus sistemas y operaciones. Así, por ejemplo, la resolución PSD2 es clara en señalar que los proveedores de servicios de pago autorizados deben contar con mecanismos de control y medidas para gestionar los riesgos operativos y de seguridad, así como mecanismos y procesos para la gestión de incidentes. Estos mecanismos deben ser evaluados permanentemente y por lo menos una vez al año se debe reportar a la autoridad competente la suficiencia de tales medidas de control[64].

Tales medidas implican que los TPPs deben establecer perfiles transaccionales, adicionales a los de las entidades financieras, para determinar, por ejemplo, mediante seguimientos al perfil transaccional de los clientes y usuarios, si una operación puede considerarse sospechosa de fraude.

Finalmente, en cuanto a la posibilidad de que las entidades financieras puedan monetizar o comercializar información de sus clientes y usuarios -estructurada, semiestructurada o no estructurada-, dado que esta información resulta del mayor interés para todos los terceros que quieran prestar servicios a los clientes y usuarios de las entidades financieras, el decreto

[64] Directiva PSD2. Artículo 95.

de *Open Finance* recoge lo previamente establecido en el documento técnico soporte del mismo[65], en cuanto a que no existe disposición en el ordenamiento legal colombiano que proscriba la venta de datos cuando se cuenta con la debida autorización para ello[66], y en ese sentido señala que, salvo expresa prohibición legal, las entidades vigiladas por la Superintendencia Financiera podrán comercializar el uso, almacenamiento y circulación de los datos personales objeto de tratamiento, siempre que cuenten con la autorización expresa del titular de los datos y se dé estricto cumplimiento a las normas relacionadas con protección de datos y habeas data de las que tratan las leyes 1266 de 2008 y 1581 de 2012[67].

Consideramos que esta autorización debe ser contemplada como una de las finalidades del tratamiento de la información, y en caso de que la información a comercializar sea privada o sensible, es necesario que la autorización sea explícita al respecto y se garantice que el uso de la información sensible en momento alguno llevará a prácticas discriminatorias respecto de su titular.

Este tema no fue objeto de regulación expresa en la directiva europea PSD2, toda vez que el modelo de *Open Banking* allí establecido es obligatorio. Sin embargo, la comercialización de datos ya se ha implementado en otras latitudes con el fin de hacer eficiente el acceso a las APIs que facilitan la interconexión con las entidades bancarias.

Así, por ejemplo, en México, al establecer la obligación, entre otras, a las entidades financieras, las transmisoras de dinero y las sociedades de información crediticia de compartir sus datos[68], se dispuso que la entidad de supervisión respectiva o el Banco de México deben … *autorizar las contraprestaciones que cobren las entidades mencionadas en el primer párrafo de este artículo con motivo del intercambio de datos e información, las cuales deberán ser equitativas y transparentes a todos los individuos involucrados a fin de que en ningún caso constituyan barreras de entrada, formales, regulatorias, económicas o prácticas.*

En desarrollo de la citada ley, el Banco de México -Banxico- estableció que los proveedores de datos[69] deben publicar de manera *…clara, precisa y en idioma español, en su página de Internet o cualquier otro medio de comunicación electrónica, aplicaciones informáticas o digitales, el proceso que deberán seguir los Solicitantes de Datos para acceder a los Datos a través de APIs y* ***las contraprestaciones que, en su caso, deberán pagar por el intercambio de Datos****.* (Negrilla ajena al texto original).

Esta posibilidad establecida en el decreto de *Open Finance* resulta adecuada ya que

[65] URF. Documento técnico. Modelo de finanzas abiertas en Colombia. Octubre de 2021.
[66] Es importante precisar que el Código Penal Colombiano (artículo 269F) establece como un delito la violación de datos personales, siendo necesario para que se tipifique tal conducta que no se cuente autorización para la realización de cualquiera de los verbos rectores que la norma establece. (URF. Documento técnico. Modelo de finanzas abiertas en Colombia. Octubre de 2021).
[67] Artículo 2.35.8.1.2 del Decreto Único 2555 de 2010 adicionado por el Decreto 1297 de 2022.
[68] Ley para Regular las Instituciones de Tecnología Financiera 2018. Estados Unidos Mexicanos. Artículo 76 "Las Entidades Financieras, los transmisores de dinero, las sociedades de información crediticia, las cámaras de compensación a que se refiere la Ley para la Transparencia y Ordenamiento de los Servicios LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN Secretaría General Secretaría de Servicios Parlamentarios Nueva Ley DOF 09-03-2018 31 de 53 Financieros, las ITF y las sociedades autorizadas para operar con Modelos Novedosos estarán obligadas a establecer interfaces de programación de aplicaciones informáticas estandarizadas que posibiliten la conectividad y acceso de otras interfaces desarrolladas o administradas por los mismos sujetos a que se refiere este artículo y terceros especializados en tecnologías de la información, con el fin de compartir los datos e información siguiente: (…)".
[69] Banco de México. Disposiciones de Carácter General Relativas a las Interfaces de Programación de Aplicaciones Informáticas Estandarizadas a que hace referencia la Ley para Regular las Instituciones de Tecnología Financiera. Artículo 1, numeral VIII. Proveedores de datos, a las Entidades Financieras, ITF, sociedades autorizadas por la CNBV para operar con Modelos Novedosos y transmisores de dinero, que conforme al primer párrafo del artículo 76 de la Ley, estén obligados a establecer APIs con el fin de compartir Datos".

permitirá, bajo reglas objetivas, incentivar los modelos de apertura de datos reconociendo los costos asociados a la disponibilidad de las APIs para su consulta por los terceros, así como los propios del procesamiento de datos y los relativos a la analítica y estructuración de los mismos.

5. Principales conclusiones y desafíos regulatorios

Las entidades financieras se han venido transformando para ofrecer sus servicios en ambientes no tradicionales o a través de terceros. Así mismo, se vienen preparando para brindar a los clientes y usuarios, a través de sus propios canales, el acceso a bienes y servicios ofrecidos por terceros que complementan su oferta financiera. Hoy las entidades financieras han tomado consciencia de que sus servicios y productos son un medio y no el fin mismo de las relaciones de los clientes y usuarios en la satisfacción de sus necesidades.

Los terceros proveedores de servicios y las Fintech vienen ganando terreno en la prestación de servicios ágiles, en un solo canal y con la menor fricción posible para sus clientes y usuarios. El acceso a la información financiera de los clientes y usuarios del sector financiero resulta relevante para que estos nuevos actores puedan competir adecuadamente. No obstante, esta competencia, como cualquier otra, no puede darse en condiciones desiguales o tomando ventaja, sin contraprestación alguna, de los negocios y activos que las entidades financieras han construido en desarrollo de su actividad.

Por su parte, los clientes y usuarios esperan tener el control de su información con el fin de tener acceso a la mejor oferta posible de bienes y servicios, pero, igualmente, esperan una mayor protección del Estado y una mayor responsabilidad de los proveedores de bienes o servicios con los que interactúan.

Como se ha visto, la protección de datos y la reserva bancaria son elementos esenciales en la implementación de un modelo de finanzas abiertas en nuestro país -*Open Banking* y *Open Data*-. Todos los actores involucrados -entidades financieras, TPPs y clientes y usuarios- deben tener claridad de sus derechos y obligaciones. La implementación del *Open Finance* trae muchos desafíos desde el punto de vista regulatorio. La reciente regulación expedida en Colombia, así como las prácticas implementadas voluntariamente por las entidades financieras, buscan resolver muchos de ellos y otros se han diferido a los estándares que debe fijar la Superintendencia Financiera o a la supervisión de la autoridad de tratamiento de datos.

La aproximación de supervisión delegada de algunos TPPs en cabeza de las entidades vigiladas puede llevar a que el desarrollo del *Open Finance* tome más tiempo del esperado. Una regulación más clara en cuanto a requisitos y supervisión del Estado sobre estos nuevos actores con seguridad contribuiría a una mayor apertura de las entidades financieras y a una mayor confianza de los clientes y usuarios en el modelo.

Sin duda, la regulación secundaria que deberá emitir la Superintendencia Financiera tendrá que resolver temas tales como interoperabilidad entre actores, riesgos en materia de protección a los titulares de la información -protección al consumidor-, seguridad en el manejo de la información y de las transacciones, así como una definición de la responsabilidad de los diferentes actores ante eventos de vulneración de la integridad y acceso a la información y fraudes.

Bibliografía

AMV Colombia. https://www.amvcolombia.org.co/glosario/proveedor-de-infraestructura/

Asobancaria. Open banking: Experiencias de implementación en el ámbito internacional.

Banco de México. Disposiciones de Carácter General Relativas a las Interfaces de Programación de Aplicaciones Informáticas Estandarizadas a que hace referencia la Ley para Regular las Instituciones de Tecnología Financiera. Artículo 1, numeral VIII.

Corte Constitucional. Colombia. Sentencia T-414 del 16 de junio de 1992. Sala Primera de Revisión. M.P. Dr. Ciro Angarita Mejía.

Corte Constitucional. Colombia. Sentencia T-462 del 24 de septiembre de 1997. Sala Novena de Revisión, M.P. Vladimiro Naranjo.

Corte Constitucional. Colombia. Sentencia T- 440 del 29 de mayo de 2003, Sala Tercera de Revisión, M.P. Dr. Manuel José Cepeda Espinosa.

Corte Constitucional. Colombia. Sentencia C-1011 del 16 de octubre de 2008. M.P. Jaime Córdoba Triviño.

Corte Constitucional. Colombia. Sentencia C-094 del 3 de marzo de 2020. Sala Plena. M.P. Dr. Alejandro Linares Cantillo

Decreto 1297 del 25 de julio de 2022.

Decreto 1377 del 27 de junio de 2013, artículo 3º, numeral 2.

Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de la Unión Europea de 25 de noviembre de 2015. PDS2.

Escobar Córdoba, Federico. (1960: 192). EL DERECHO ROMANO DE LA PROPIEDAD EN LA DOCTRINA CIVIL COLOMBIANA. Página 315

European Banking Authority (Autoridad Bancaria Europea). Discussion Paper on innovative uses of consumer data by financial institutions. Mayo 2016.

European Commission. Payment services. https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/payment-services

Estatuto Orgánico del Sistema Financiero. Decreto 663 de 1993.

https://eur-lex.europa.eu/legal-content

https://gdpr.eu/cookies/

Ley 1430 de 2011.

Ley 1581 de 2012.

Ley para Regular las Instituciones de Tecnología Financiera 2018. Estados Unidos Mexicanos. Artículo 76.

Proyecto de ley 413 de 2021. "Por la cual se dictan normas relacionadas con el sistema de pagos, el mercado de capitales y se dictan otras disposiciones". Congreso de la República.

Proyecto de Ley 337 de 2022. "Por la Cual se Dictan Normas Relacionadas con el acceso y el Financiamiento para la Construcción de Equidad, y se dictan otras disposiciones". Congreso de la República.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos - GDPR por sus siglas en inglés).

Remolina, Nydia. Open Banking: Regulatory challenges for a new form of financial intermediation in a data-driven world (2019). Centre for AI & Data Governance, pág. 11.

Rendición de cuentas de Google y otros negocios en Colombia: La protección de datos personales en la era digital. Tomado de Documentos Dejusticia 48.

Superintendencia Financiera de Colombia. Circular Básica Jurídica. Parte I, Título II, capítulo I. numeral 2.3.4.9.

Superintendencia Financiera de Colombia, Circular Básica Jurídica, Parte primera, Título IV, Capitulo Primero, numeral 6.

Superintendencia Bancaria de Colombia. Conceptos OJ-050 de 8 de marzo de 1982 y OJ-288 de 12 de agosto de 1976. Tomado de la sentencia T-440 de 2003 de la Corte Constitucional, num. 4.2.2., nota a pie de página [37]

The Payment Services Regulation 2017 que corresponde a la incorporación y adaptación del PSD2 a la Legislación del Reino Unido, la cual entró en vigor en 2018. Tomado de https://www.openbanking.org.uk/regulatory/

Unidad de Regulación Financiera del Ministerio de Hacienda y Crédito Público – URF. Documento técnico. Modelo de finanzas abiertas en Colombia. Octubre de 2021.

Zunzunegui, Fernando. La Digitalización de los Servicios de Pago. Página 194. En Fintech, Regtech y Legaltech: Fundamentos y desafíos regulatorios. Directores Aurelio Gurrea Martínez y Nydia Remolina. Ed. Tirant lo Blanch. Valencia, 2020.

CAPÍTULO 7

Identidad Digital

Felipe Noval Acevedo[1]

Resumen

La identidad digital -entendida como la recolección de datos y atributos asociados con la identificación de un individuo en un entorno digital, que le permitan validar su identidad con fines transaccionales, interacciones o representaciones digitales- ofrece a las organizaciones un sistema robusto que integra diferentes tecnologías por medio de las cuales se puede verificar la identidad de los usuarios de manera ágil y sencilla, pero garantizando la privacidad, seguridad e integridad de la información. La identidad digital permite a las entidades optimizar recursos, facilitar procesos de autenticación de identidad de clientes y disminuir el riesgo de fraude y ciberataques, al tiempo que mejora la experiencia de los clientes y reemplaza los procesos tradicionales por los digitales, teniendo como pilares fundamentales la seguridad y la privacidad de los datos de cada parte. Se mencionan casos de éxito en Bélgica y Canadá, así como el desarrollo que estas soluciones de identidad digital están teniendo en Colombia.

1 Vicepresidente Jurídico y de Cumplimiento de SoyYo – Servicios de Identidad Digital, y profesor de cátedra en materia de Fintech, Banca y Transformación Digital de la Pontificia Universidad Javeriana, Universidad de los Andes y CESA.

1. Introducción

Con la revolución de las tecnologías emergentes y su impacto en el desenvolvimiento de la economía, la banca tradicional ha comenzado un proceso de transformación digital desarrollando nuevos modelos de negocio en los que la ingeniería de productos y servicios financieros se centra en las necesidades del consumidor, que demanda propuestas de valor personalizadas, flexibles y ágiles. La democratización de Internet y la adopción de canales digitales han permitido la entrada de nuevos jugadores en el mercado financiero como Fintech, BigTech y neobancos, que han llegado con modelos de negocio netamente digitales, habilitando transacciones a bajo costo, inmediatas y seguras. Por lo anterior, la transformación digital apoyada en las tecnologías emergentes se ha convertido en un objetivo estratégico de la banca tradicional, a fin de adaptar sus procesos internos y soluciones financieras a las necesidades del consumidor.

Para la mayoría de empresas con canales digitales transaccionales, y especialmente para las entidades financieras, es necesario contar con un sistema de verificación de identidad y mecanismos fuertes de autenticación, como la biometría, certificados digitales, OTPs -por su sigla en inglés *One Time Password*-, entre otros. Este proceso es ineludible para que las organizaciones se aseguren de que una persona es quien dice ser, cuando hace uso de canales no presenciales.

La identidad digital ofrece a las organizaciones un sistema robusto que integra diferentes tecnologías por medio de las cuales se puede verificar la identidad de los usuarios de una manera ágil y sencilla, garantizando la privacidad, seguridad e integridad de su información.

Además, la identidad digital permite a las entidades optimizar recursos, facilitar la autenticación de identidad de clientes y disminuir el riesgo de fraude por suplantación en procesos de vinculación, autenticación y consultas. Así, soluciones de identidad digital en el sector financiero permiten la disminución de ciberataques, mejoran la experiencia de los clientes y reemplazan los procesos tradicionales por los digitales, teniendo como pilares la seguridad y la privacidad de los datos de los usuarios.

2. ¿A qué nos referimos cuando hablamos de identidad?

Identificar a una persona significa determinar que es esta y no otra. Para ello solemos utilizar atributos únicos de una persona que nos permitan diferenciarla de las demás. El ejemplo más claro de estos atributos es el nombre, puesto que, cuando nos referimos a alguien por su nombre, lo estamos individualizando y singularizando: así, cuando usamos Pedro para referirnos a una persona y no a otra, lo identificamos.

En este sentido, podríamos decir que identificarse es responder a la pregunta de "¿quién es usted?". Sin embargo, el grupo de atributos que utilicemos para responder esta pregunta dependerá directamente del ámbito en el que estemos identificando a la persona. Por ejemplo, dentro del ámbito universitario, usualmente se toman en consideración el nombre, sexo y fecha de nacimiento registrados en el documento de identidad nacional. Con esta información, la universidad asigna un código de identificación especialmente creado para el alumno que identifica. Sin embargo, para la identificación de esa misma persona en el

ámbito de las amistades, puede que baste únicamente con el apodo con el que se refieren a él o ella[2].

Ahora bien, de acuerdo con el Foro Económico Mundial[3], los atributos que utilizamos para identificar a las personas pueden ser clasificados en 3 categorías: inherentes, desarrollados y asignados. Los primeros son aquellos propios de la persona identificada, que no dependen de ninguna entidad externa; por ejemplo, la edad, estatura, fecha de nacimiento y huellas dactilares. Los segundos hacen referencia a datos sobre una persona que son generados o recolectados a través del tiempo; en esta categoría encontramos los hábitos de consumo. Finalmente, los atributos asignados están atados a la persona que identifican, pero no le son intrínsecos; por ejemplo, el número de teléfono, el número de identificación nacional o la dirección de correo. Dependiendo del ámbito en que nos encontremos, una mezcla diferente de estos atributos nos permite identificarnos. Retomando el ejemplo del ámbito universitario, la identidad de Pedro, por ejemplo, es conformada por una mezcla de atributos inherentes -su fecha de nacimiento o su sexo-, atributos asignados -su código universitario- e inclusive atributos desarrollados -su registro de materias y calificaciones-.

Siguiendo el ejemplo de Pedro, identificarse ante su universidad le permite acceder a los servicios que ella le ofrece. Las materias que curse, las notas que reciba, los libros que alquile, todos estarán condicionados y ligados a su identificación ante la universidad. Si Pedro fuera indistinguible de los demás estudiantes de la misma institución, no sería posible garantizarle el acceso a las clases de su carrera, registrar las notas que den cuenta de su progreso ni conocer qué libros ha retirado de la biblioteca. La evidente importancia de la identificación se extiende a otros ámbitos de la vida con igual impacto. En la vida personal, por ejemplo, establecemos relaciones de amistad y confianza con otros de manera selectiva y singular. La información que se comparte con los amigos no es la misma que se compartiría con un desconocido, de manera que para determinar si se comparte una ocurrencia personal o un pensamiento privado primero se identifica a quién se le está comunicando.

En este último ejemplo la identificación es un proceso sencillo. Si buscamos identificar a una persona con quien tenemos una amistad, nuestra frecuente interacción con ella hace que su identidad nos sea evidente. Bien porque reconocemos su rostro, su voz o su forma de escribir. Identificamos a las personas más cercanas a nosotros sin advertir que lo estamos haciendo de manera prácticamente automática. No obstante, nuestro día a día está lleno de interacciones con otros que no necesariamente reconoceríamos de manera automática, pero de quienes necesitamos saber quiénes son. Por ejemplo, si quiero comprar una casa, es esencial saber que la persona a quien se la estoy comprando es efectivamente la dueña -o que sea la persona designada por el dueño para venderla-. Es muy probable que no reconozca al dueño de la casa por su rostro, pero con ayuda de instrumentos públicos de registro, puedo saber quién es efectivamente el propietario de la casa. Supongamos que reviso el registro correspondiente y descubro que la dueña de la casa que quiero comprar se llama Ana. El día del negocio, una mujer se presenta diciendo que se llama Ana. Aunque confío en la buena fe de otras personas, vale la pena que me cerciore de que la persona que se identifica como Ana sea efectivamente quien dice ser, la dueña de la casa. A este proceso lo llamamos autenticación.

[2] Cuno, A., Aldoradín, Y., Ganz, H., Veliz, F. y Papa, E. (2021). Un modelo de gestión de la Identidad Digital para el Estado Peruano. Revista Ibérica de Sistemas e Tecnologiuas de informação, 166-182.
[3] World Economic Forum. (2016). A blueprint for digital identity. Recuperado de: https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

2.1 Identificarse vs. autenticarse

Como vimos, identificarse responde a la pregunta ¿Quién es usted?, y el contenido de esta respuesta dependerá del ámbito en que la pregunta haya sido formulada. En esta época, para muchos de los ámbitos de la vida cotidiana resulta indispensable contar con una identificación legal, como prueba de que un Estado u organización política ha registrado los datos de cada persona en sus archivos oficiales. Sin embargo, según el último estudio realizado por el Banco Mundial, a 2018 había cerca de mil millones de personas en el mundo sin ningún tipo de identificación legal. Esto significa que cerca de mil millones de personas contaban con graves obstáculos para su participación en la vida política, social y económica de sus naciones. En efecto, sin una manera segura de identificarse, una persona puede no lograr abrir una cuenta bancaria, votar en las elecciones, acceder a servicios de educación o salud, recibir una pensión o acceder al sistema de justicia[4]. Además, la ausencia de identificación de estas personas también significa que los Estados a los que pertenecen tendrán dificultades para recolectar impuestos, direccionar programas sociales y garantizar seguridad[5].

Ahora bien, si identificarse responde la pregunta de ¿Quién es usted?, autenticarse responde a *¿Es usted quien dice ser?*. La autenticación es un proceso posterior a la identificación, y requiere de esta última para existir. Podríamos decir que autenticarse es un proceso compuesto, que consta en primera instancia de identificarse, y luego de permitir la verificación de dicha identificación. En el ejemplo de la casa de Ana, lo más probable es que usted le pida a Ana su número de identificación y verifique que sea el mismo número de identificación que aparece vinculado a su nombre en el registro de propiedad de la casa. Si la respuesta de su vendedora y los datos que reposan en el registro de propiedad coinciden, podemos decir que usted y ella hablan de la misma Ana. Sin embargo, esto no resuelve aún la pregunta de *¿Es Ana quién dice ser?*. Podría suceder que esta persona se identifique como Ana, dueña de la casa, y sea capaz de dar el número de identificación correspondiente y aun así no sea Ana, la propietaria de la casa.

Dependiendo del riesgo que quiera correr, puede dar por verificada la identidad de Ana al preguntarle su número de identificación y confirmar que sea el mismo del registro de propiedad, o puede pedirle que le muestre su documento de identidad. Si opta por la segunda opción, está haciendo una autenticación de credenciales. Este proceso consiste en verificar una base de datos de identidad para confirmar que hay coincidencia con las credenciales presentadas[6]. Una credencial puede ser un documento verificable expedido por una tercera parte que especifica atributos de identidad, como un documento de identificación expedido por el Estado[7]. Como normalmente los documentos de identificación cuentan con una foto de su titular, su estatura, nombre y fecha de nacimiento, observará a Ana y confirmará que los datos que aparecen en su documento coinciden con la persona que tiene en frente y a la vez con los datos consignados en el registro de propiedad. Si los datos coinciden y logra identificar a Ana en la foto de su documento, sabrá que Ana es quien dice ser.

---

[4] Banco Mundial. (2018). Identification For Development (ID4D) Global Dataset. Recuperado de: https://datacatalog.worldbank.org/search/dataset/0040787

[5] GMSA. (2016). Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. Recuperado de: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf

[6] Asobancaria. (2018). Recomendaciones a la política pública sobre la identificación/autenticación digital en Colombia. Bogotá, Colombia: Autor.

[7] Sedlmeir, J. y otros. (2021). Digital Identities and Verifiable Credentials. Catchword, 36(5), 603-613, doi:10.1007/s12599-021-00722-y

3. Identidad en la era digital

Hemos visto para qué y cómo identificarnos en el plano físico; sin embargo, teniendo en cuenta que nuestras interacciones con los demás miembros de la sociedad cada vez más toman lugar en el entorno digital, resulta de primordial importancia analizar las posibilidades y retos que los procesos de identificación y autenticación representan en dicho entorno.

Según estadísticas de la Cámara Colombiana de Comercio Electrónico, los pagos digitales en Colombia han tenido un crecimiento acelerado. Entre 2016 y 2017 crecieron 16%, pero entre 2018 y 2019 el crecimiento se aceleró a 30%[8]. La tendencia general parece indicar que la transformación digital es inevitable. En el mismo sentido, según la firma alemana Statista[9], entre 2017 y 2022 el número de usuarios de teléfonos inteligentes aumentó 49.89%. El 83.72% de la población mundial tiene un teléfono inteligente y el 91.54% tiene teléfonos móviles. Esta tendencia hacia interacciones humanas a través de canales digitales obliga a repensar las formas en que nos identificamos ante otros y en cómo se verifica dicha identidad.

La transformación digital trae consigo retos técnicos considerables. Entre ellos, la suplantación de identidad personal. En la medida en que un mayor número de transacciones tienen lugar en canales digitales, la suplantación de identidad también se incrementa. Así, entre el 1º de enero y el 26 de julio de 2019, la Superintendencia de Industria y Comercio de Colombia recibió 122% más quejas por suplantación de identidad que en el mismo periodo del año anterior[10]. Cuando la mencionada Superintendencia advirtió esta tendencia, envió una carta a los gremios más afectados -telecomunicaciones y ventas por catálogo- instándolos a fortalecer las medidas de autenticación de la identidad real de las personas en los procesos de contratación, de manera que se compruebe la veracidad de la información y se eviten suplantaciones de identidad[11]. Un ecosistema robusto de identidad digital deberá poder afrontar estos retos de manera satisfactoria, garantizando seguridad de la información y confianza para las entidades y para los usuarios identificados.

3.1 Pero, entonces, ¿qué entendemos por identidad digital?

La identidad digital es una colección de atributos de identidad electrónicamente capturados y almacenados que describen a una persona dentro de un contexto particular y son usados para transacciones electrónicas[12]. Podemos decir también que *la identidad digital es una representación digital de la información que se conoce sobre un individuo específico, grupo u organización*[13]. En otras palabras, la identidad digital es la recolección de datos y atributos asociados con la identificación de un individuo en un entorno digital, que le permitan validar su identidad con fines transaccionales, interacciones o representaciones digitales. Imagine

[8] Cámara Colombiana de Comercio Electrónico. (2019). Informe de transacciones digitales en Colombia 016-2019. Recuperado de: https://www.ccce.org.co/wp-content/uploads/2017/06/informe-transacciones-colombia-2016-2019.pdf
[9] Statista. (2022). Global smartphone penetration rate as share of population from 2016 to 2020. Recuperado de: https://www.statista.com/statistics/203734/global-smartphone-penetration-per-capita-since-2005/
[10] Superintendencia de Industria y Comercio. (2019). Quejas por suplantación de identidad ante la Superintendencia crecieron 122%. Recuperado de: https://www.sic.gov.co/Quejas-por-suplantacion-de-identidad-ante-la-Superindustria-crecieron-122.
[11] Ibidem
[12] Asociación GSM y otros. (2016). Digital identity: towards shared principles for public and private sector cooperation. Recuperado de: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf
[13] World Economic Forum. (2018). Digital Identity: On the threshold of a Digital Identity Revolution. Recuperado de: https://www3.weforum.org/docs/White_Paper_Digital_Identity_Threshold_Digital_Identity_Revolution_report_2018.pdf

que en lugar de cargar con un documento que acredita su identidad -una credencial como el documento de identidad nacional, carnet universitario o carnet de vacunación-, usted pueda autenticarse digitalmente y acceder, de forma segura, a su información personal, tal como su historia clínica, declaración de renta, extractos bancarios, productos financieros, entre otros, a través de un dispositivo vinculado a Internet. Imagine además que usted pueda utilizar su identidad digital para autenticarse y probar que efectivamente usted es quien dice ser en el entorno digital. De esta manera, cuando requiera, por ejemplo, solicitar un crédito a un banco, el banco no le pedirá que responda preguntas reto o que vaya presencialmente a una de sus oficinas para saber que usted es quien dice ser, sino que podrá autenticarse a través de un canal digital. O digamos que usted califica para un subsidio de vivienda del gobierno, cuando vaya a comprar su vivienda o aplicar al subsidio, puede permitir al gobierno revisar los datos asociados a su identidad a través de un canal digital seguro sin necesidad de reunir certificados y presentarlos en una oficina.

El uso de tecnologías cada vez mejor adaptadas a nuestras necesidades, como los mecanismos de autenticación biométrica facial -o reconocimiento facial- como atributo de la identidad digital, hacen posible que usted pruebe que es quien dice ser con tan solo tomarse una *selfie*, sin necesidad de recordar un alias o nombre de usuario -como el código universitario-, una clave de acceso, cargar con un *token* de clave dinámica o presentarse presencialmente en una oficina de la entidad ante la que se busca autenticar.

3.2 ¿Qué debe tener una solución de identidad digital?

El objetivo ulterior es que las personas puedan identificarse y autenticarse de manera segura y confiable en el entorno digital. Pero ¿qué es necesario para que un sistema permita alcanzar estos objetivos? Para responder esta pregunta, el Banco Mundial[14], el Foro Económico Mundial[15] y la Asociación GSM[16] han recopilado ciertos principios que deben guiar la implementación de una solución de identidad digital efectiva. Destacamos los siguientes:

3.2.1 El sistema de identificación y autenticación digital debe estar disponible para todos los usuarios, debe permitir acceso universal y estar libre de discriminación en sus políticas y prácticas por diseño. Los sistemas de identificación y datos nunca deben ser usados como una herramienta para la discriminación o para negarle derechos individuales o colectivos a nadie. Como parte de esto, es también necesario asegurar que se eliminen las barreras de acceso y uso del sistema. En este sentido, las brechas tecnológicas, la asimetría de información y los costos directos e indirectos que representa para el usuario participar del sistema de identificación deben ser reducidos si no totalmente eliminados.

3.2.2 La solución debe establecer una identidad confiable. Esto significa, por un lado, que cada identidad debe ser única, no debe haber una persona con dos identidades digitales. Por otro lado, también significa garantizar estándares de seguridad que impidan el acceso no autorizado de terceros. Los datos que construyen el sistema de identidad deben estar

[14] Banco Mundial. (2021). Principles on identification for sustainable development: Toward the digital age. Recuperado de: https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf

[15] World Economic Forum. (2016). A blueprint for digital identity. Recuperado de: https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

[16] Asociación GSM y otros. (2016). Digital identity: towards shared principles for public and private sector cooperation. Recuperado de: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf

protegidos durante su almacenamiento y también durante su tránsito, y las medidas de seguridad correspondientes deben incluir sistemas que generen consciencia sobre el uso seguro de la plataforma. Además, los usuarios deben ser notificados en caso de que se den pérdidas de datos, al igual que sobre las identidades que sean suplantadas o vulneradas y cuyas credenciales necesitan ser expedidas de nuevo. Finalmente, los datos con que cuente el sistema de identidad deben ser exactos y actualizados.

3.2.3 También es importante que el sistema de identidad digital esté centrado en el usuario. En este sentido, es esencial que los usuarios tengan control sobre su información y determinen quién tiene acceso a ella. En esta misma línea, el sistema debe ser diseñado de forma que pueda adaptarse a las necesidades de identificación y autenticación de sus usuarios. Uno de los retos más importantes en este sentido es garantizar la interoperabilidad de las tecnologías asociadas al sistema. Esto significa que usted pueda usar su identidad digital independientemente del sistema operativo o dispositivo desde el que acceda a ella. También significa que las entidades ante las que se identifica o autentica deben poder interactuar con el sistema de identidad digital independientemente de la arquitectura tecnológica en la que operen sus respectivos sistemas de datos.

3.2.4 Siguiendo esta idea, otro principio guía para una solución de identidad digital es que esté construida sobre la base de estándares abiertos, es decir, que los estándares de seguridad y desarrollo tecnológico sean transparentes para todas las partes interesadas. Esto aporta a la interoperabilidad de la que hablamos anteriormente, pero además asegura que no se atente contra la libre competencia de proveedores, pues una solución estandarizada permite a los usuarios elegir entre diferentes alternativas y promueve el mejoramiento de estas. La construcción de la solución sobre la base de estándares abiertos permite también su escalamiento y desarrollo de manera que, en un futuro, pueda soportar mayor tráfico de datos, bien sea por un mayor número de usuarios o por el desarrollo de nuevas funcionalidades.

3.2.5 También es esencial para el desarrollo de una solución digital de identidad que esté basada en la privacidad y seguridad como principios. Para esto suele hablarse de la privacidad y seguridad por diseño, lo que refiere a que la protección y privacidad de la información sean priorizadas e integradas como una configuración predeterminada. El compromiso con la privacidad de la información debe extenderse a las prácticas organizacionales, marcos legales y procedimientos establecidos y aplicados durante el almacenamiento y tratamiento de los datos de identidad de los usuarios.

3.2.6 Finalmente, el último principio guía para el desarrollo de la solución es que debe ser económicamente sostenible. La infraestructura necesaria para el desarrollo de un sistema de identidad digital guiado por estos principios requiere de un músculo financiero que le permita sobrellevar diferentes adversidades, como por ejemplo un panorama de prioridades políticas cambiantes.

4. Identificación en Colombia

Podríamos decir que la identificación de las personas en Colombia se establece en dos sistemas paralelos, teniendo en cuenta los dos tipos de personas que contempla el ordenamiento jurídico colombiano. Tal y como en otros ordenamientos jurídicos sucede,

en Colombia se reconoce la existencia de personas naturales y personas jurídicas[17]. Las personas naturales son todos los individuos de la especie humana, mientras que las personas jurídicas son personas ficticias a quienes les atribuimos la posibilidad de tener derechos y obligarse.

Para el caso de las personas jurídicas, existen diversos registros que les permiten identificarse dependiendo del ámbito para el que sea necesario hacerlo. Las cámaras de comercio administran los registros Mercantil, Único de Proponentes -que permite contratar con el Estado-, de Entidades sin Ánimo de Lucro, Registro Nacional Público de Vendedores de Juegos de Suerte y Azar, Registro Público de Veedurías Ciudadanas, Registro Nacional de Turismo, Registro de Entidades Extranjeras de Derecho Privado sin Ánimo de Lucro y Registro de la Economía Solidaria. Todos estos registros permiten la identificación y autenticación de la identidad de las personas jurídicas en Colombia, y desde el año 2000 se encuentran integrados en el Registro Único Empresarial –RUES- de Confecámaras, la red de Cámaras de Comercio de Colombia. El RUES cuenta con una plataforma de consulta web que permite a cualquier persona revisar los datos de identificación de una persona jurídica en línea, mostrando además detalles sobre la representación legal y posibles multas o sanciones.

Por otro lado, la identificación de las personas naturales en Colombia es conducida oficialmente por la Organización Electoral, que a su vez está compuesta por el Consejo Nacional Electoral y la Registraduría Nacional del Estado Civil[18]. Su tarea contribuye a la materialización del derecho fundamental a la personalidad jurídica, consagrado en el artículo 14 de la Constitución Política. En términos generales, por personalidad jurídica entendemos la capacidad de una persona de tener derechos y contraer obligaciones. En efecto, como ha sido ampliamente aclarado por la Corte Constitucional, la personalidad jurídica es un derecho fundamental y presupuesto esencial para garantizar la efectividad de los demás derechos de los colombianos[19]. La Registraduría lleva el registro de identidad de los colombianos mediante la expedición de tres documentos distintos: el registro civil, la tarjeta de identidad y la cédula de ciudadanía. El primero de estos documentos cuenta con 3 modalidades: de nacimiento, de matrimonio y de defunción. El segundo sirve para identificar a los colombianos mayores de 7 años. El tercero, para los mayores de 18 años.

Los dos primeros documentos de identidad mencionados son regulados por el Estatuto Registral[20], donde se establece que el estado civil de una persona *es su situación jurídica en la familia y la sociedad, determina su capacidad para ejercer ciertos derechos y contraer ciertas obligaciones (…). Bajo esta lógica, los hechos y actos relativos al estado civil de las personas deben estar inscritos en el competente registro civil*[21]. La necesidad de llevar el registro de los nacimientos, matrimonios, adopciones, legitimaciones y reconocimiento de hijos naturales fue por primera vez establecida como ley en 1850. En su momento, este registro estaba a cargo de los notarios. No obstante, dada la fuerte presencia de la iglesia católica en el país, en 1887 se reconoció que las partidas de bautismo, matrimonio o defunción expedidas por los sacerdotes servían como prueba del estado civil. No fue hasta 1938 que el registro del estado civil se reconoció como una competencia exclusiva del

[17] Código Civil [Código] (2021). Recuperado de: https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1827111
[18] Constitución Política de Colombia [Const.]. (1991). Legis
[19] Corte Constitucional de Colombia, Sala Sexta de Revisión de Tutelas. (26 de junio de 2018) Sentencia T-241. [MP Gloria Stella Ortiz Delgado]
[20] Decreto 1260 de 1970
[21] Ibidem

Estado. Luego, en 1970, una reforma a la ley 92 de 1938 le asignó a la Superintendencia de Notariado y Registro la responsabilidad de ser la oficina central de registro, adonde debía ser enviada una copia de toda inscripción hecha en el registro. Finalmente, con la Constitución Política de 1991 se asignó la función de dirigir y organizar el registro y la identificación de las personas al Registrador Nacional del Estado Civil[22].

Hoy en día, con la inscripción del nacimiento, reconocimiento de hijos naturales, legitimaciones, adopciones, matrimonios, divorcios, cambios de nombre y la muerte de las personas, entre otros, la Registraduría lleva varias bases de datos que dan cuenta de la identificación de los colombianos. La información que se recolecta en el registro civil es complementada con la recolectada al momento de expedición de la cédula de ciudadanía y es consolidada en el Sistema Nacional de Identificación. Este se compone de diversas bases de datos como el censo electoral, el sistema de información de registro civil, el sistema automático de identificación biométrica, entre otras. La base de datos primigenia del sistema es el Archivo Nacional de Identificación, que contiene información de nombres, apellidos, fecha, vigencia y lugar de expedición de la cédula de ciudadanía, fecha de nacimiento, grupo sanguíneo, género y estatura, entre otros, de las personas identificadas por el Estado colombiano[23]. El Archivo Nacional de Identificación es una base de datos dinámica, puesto que se actualiza teniendo en cuenta las modificaciones que las personas que identifica hacen a sus datos biográficos.

El modelo de identificación colombiano permite la centralización de los registros de identidad y su consulta, de manera que la autenticación de la identidad de una persona natural pueda hacerse mediante la verificación de los datos contenidos en las credenciales que expide la Registraduría -los documentos de identidad- y la base de datos del Archivo Nacional de Identificación. De este archivo se nutren el censo electoral, el sistema general de salud, el sistema financiero y el sistema educativo. Para garantizar la inalterabilidad de los datos consignados en los documentos de identidad, tanto la cédula de ciudadanía como la tarjeta de identidad cuentan con medidas de seguridad físicas como hologramas tridimensionales, la huella dactilar de la persona identificada y un código de barras. Además, desde el año 2004 el número único de identificación asignado a cada colombiano -NUIP- es el mismo desde el nacimiento hasta la expedición de la cédula de ciudadanía. Podemos decir que la identificación de las personas en Colombia funciona en un sistema coherente y unificado a cargo del Estado.

Como podemos ver, el Estado colombiano ha hecho un esfuerzo constante en el mantenimiento y actualización de su modelo de identificación de las personas. Como parte de este esfuerzo, la Registraduría Nacional del Estado Civil dispone de una herramienta web para la consulta de datos e identificación de los colombianos denominada Web Service ANI. El procedimiento necesario para consultar el Archivo Nacional de Identidad fue regulado a través de la resolución 5633 de 2016. En ella se establece que para poder acceder a la información no sujeta a reserva legal se necesita suscribir un contrato con la Registraduría, un compromiso de confidencialidad y el cumplimiento de los estándares internacionales de políticas de seguridad de la información ISO 27001. Actualmente, la Registraduría cuenta

[22] Registraduría Nacional del Estado Civil. (s.f.) Historia de la Identificación. Recuperado de: https://registraduria.gov.co/-Historia-de-la-identificacion-.html

[23] Romero Mondragón NS. (2020). Generación de identidad digital para el acceso a los servicios ciudadanos digitales en Colombia. Recuperado el 6 de mayo de 2022 de: https://search.ebscohost.com/login.aspx?direct=true&db=ir01494a&AN=seneca.1992.48441&lang=es&site=eds-live&scope=site

con convenios para este fin con 78 entidades públicas -y privadas que ejercen funciones públicas- y 28 entidades privadas, quienes pueden acceder a la información que reposa en la base de datos primigenia de identificación de los colombianos.

En este sentido, el compromiso de la Registraduría con la constante actualización del sistema de identificación de los colombianos pone a Colombia en una posición ventajosa para la adopción de un ecosistema de identidad digital robusto. El registro de los datos personales de identificación de los colombianos es llevado por el Estado a través de una institución que genera confianza en la verificación de identidad y que, además, permite a los particulares consultar sus registros bajo estándares de seguridad claros, previa autorización de los titulares de datos personales. En todo caso, la verificación de identidad necesaria para los trámites de la vida cotidiana resulta, en la práctica, un proceso dispendioso y muy limitado a la presencialidad. Es allí donde una solución de identidad digital podría sacar provecho del actualizado sistema de identificación colombiano para permitir procesos de autenticación no presencial seguros y confiables, por lo que es imperativo que los ciudadanos puedan conocer sus datos personales que reposan en los archivos de la Registraduría y autorizar el acceso a terceros particulares con fines de verificación.

5. Fraude y ciberseguridad

Día a día, el mundo se sigue introduciendo en una mecánica de constante cambio, y esto ha provocado que la forma de vida de las personas esté cada vez más en función de lo digital, a medida que las actividades y transacciones por Internet sean más rápidas, más fáciles, más accesibles y, por ende, más cómodas. Esta tendencia va a seguir creciendo, como lo menciona la Cámara Colombiana de Informática y Telecomunicaciones en su informe *El comercio electrónico en 2021* y perspectivas 2022, de acuerdo con el cual en el 2021 las ventas en línea crecieron 40,2% respecto al 2020 y se espera que para el 2022 las ventas no presentes crezcan un 19% respecto a lo observado en 2021[24]. Algunos factores importantes que ayudaron a impulsar el crecimiento de las compras a través del comercio electrónico durante los últimos dos años fueron los días sin IVA establecidos por el gobierno colombiano, el *cyberlunes* y *black friday*; tan sólo en la primera jornada, llevada a cabo el 28 de octubre de 2021, se hicieron ventas por $9,8 billones de pesos, un crecimiento del 130% respecto del último día sin IVA del 2020[25]. Esta dinámica obliga a que los comercios y entidades bancarias respalden este crecimiento y, de una u otra forma, lo aprovechen, mejorando significativamente la experiencia de su cliente digital, y brinden tranquilidad y seguridad en sus operaciones y transacciones.

No obstante, en esta evolución del mundo físico al digital, donde los usuarios se sienten más cómodos, asimismo se sienten los ciberdelincuentes, que se adaptan e implementan nuevas formas y estrategias para cometer fraude. En el mundo digital, el delincuente no tiene que exponerse físicamente, ubicarlo es más complejo y para obtener las herramientas con las que lograría hacerse a sumas de dinero significativas necesita una inversión relativamente baja. En esta medida, la migración a entornos digitales resulta también atractiva para personas inescrupulosas: les es más rentable delinquir en ataques cibernéticos y pueden llegar a una gran población con un par de clics. Así lo evidencian las cifras de ciberdelitos del

[24] CCIT. (2021). Cámara Colombiana de Informática y Telecomunicaciones. Comportamiento del Ciberdelito durante el 2021. Obtenido de: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf
[25] Ibidem

mencionado informe: al finalizar noviembre de 2021, se presentaron 46.527 en el país, un crecimiento de 21% comparado con 2020. Del mismo modo, el famoso malware de secuestro de información *ramsomware* ha afectado de manera importante al sector empresarial, en especial a las pymes, con más de 500 casos durante los primeros 9 meses del año[26].

5.1 Fraude e Identidad Digital

Lo que las personas o empresas publican en Internet, su forma de interactuar, lo que comunican por correo electrónico o publican en redes sociales son piezas que van armando un rompecabezas llamado perfil en la red, que también se puede definir como traza digital. Por eso los esfuerzos deben ir enfocados a proteger, mantener y preservar la identidad, ya que el fraude en sus distintas expresiones y la suplantación de identidad son riesgos que no se deben desatender. Según el portal de Paycomet, el fraude *online* consiste en el uso de dispositivos digitales con el fin de cometer actividades delincuenciales como suplantación de identidad, robos de contraseñas y datos, estafas, secuestros digitales, entre otros[27].

Dada la anterior definición, nadie está exento de ser víctima de estafas y engaños que causen graves perjuicios económicos y considerables daños a la imagen, con consecuencias como la divulgación de información confidencial y la pérdida o robo de datos personales.

Según el portal de seguridad español Incibe, hoy en día el fraude *online* es una de las ciberamenazas que más preocupa a las empresas. A través de metodologías que utilizan la ingeniería social y las herramientas tecnológicas, los ciberdelincuentes juegan sus cartas para engañar tanto a empresarios como a empleados. Este tipo de engaños normalmente se realizan a través del correo electrónico y tienen una motivación económica importante para el ciberdelincuente, que se lucra a través del engaño, la estafa y la extorsión[28].

Entre los casos más habituales de fraude se encuentra el *email spoofing* o suplantación de identidad por correo electrónico. Mediante esta técnica, los ciberdelincuentes envían correos con remitente falso para difundir *spam, malware* o llevar a cabo ataques de *phishing* suplantando la identidad de perfiles con capacidad de toma de decisiones en la empresa, proveedores, clientes, etc.[29].

La ingeniería social suele ser la aliada perfecta para que las víctimas no sospechen del engaño. Entre los principales casos de fraude y con mayor crecimiento se encuentran la violación de datos personales, acceso abusivo a sistemas informáticos y el hurto por medios informáticos, de los cuales hablaremos a continuación.

[26] Ibidem
[27] Paycomet. (2020) Fraude. Obtenido de: https://www.paycomet.com/news/glosario/que-es-fraude/
[28] Incibe. (2021). fraude y gestión de la identidad digital. Obtenido de: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_fraude_y_gestion_de_la_identidad_online.pdf
[29] Incibe. (2021). Fraudes online: aprende a identificarlos. Obtenido de: https://www.incibe.es/protege-tu-empresa/blog/fraudes-online-aprende-identificarlos

5.2 Delitos con mayor crecimiento durante el 2021 en Colombia

Según el informe de CCIT sobre las tendencias del cibercrimen 2021-2022[30], la violación de datos personales, con 13.458 casos, es el delito de mayor crecimiento en el país durante el 2021, con un 45% de variación respecto a los casos registrados durante el 2020. Lo anterior se explica por las campañas de *phishing*, mediante las cuales los cibercriminales consiguen enviar enlaces que redireccionan hacia sitios web con formularios utilizados para robar información personal, principalmente datos de cuentas bancarias, datos de identificación personal, número de documento de identidad, lugar de nacimiento y demás información necesaria para preparar y adelantar campañas y generar procesos fraudulentos vinculados a solicitudes de crédito, trámites de tarjetas de crédito, fraudes en seguros o venta de datos en la Internet profunda para suplantación de identidad.

La segunda modalidad de mayor crecimiento es el acceso abusivo a sistemas informáticos que presenta un total de 9.926 denuncias, y un incremento del 18% respecto a las cifras reportadas durante el 2020, mencionado en el mismo informe. El acceso abusivo a sistemas informáticos tiene la característica de ser uno de los pasos iniciales de un ciberataque, especialmente cuando el intruso, luego de analizar por donde puede ingresar, consigue acceder al sistema para así escalar privilegios o realizar modificaciones a las configuraciones principalmente en los sistemas de defensa como antivirus y herramientas de seguridad disponibles en la infraestructura del sistema comprometido.

En tercer lugar se encuentra el hurto por medios informáticos, que tuvo un incremento de 3%. Se instauraron 17.608 denuncias entre enero y noviembre de 2021, siendo el delito de mayor frecuencia en el país, lo que señala claramente que la motivación de los ciberataques guarda la tendencia recurrente de los últimos años. En efecto, parece que en su interés económico los cibercriminales afectan y comprometen las cuentas bancarias de las personas y empresas sin consideración al capital o tamaño de estas.

5.3 Cifras del ciberdelito en Colombia

En un análisis que hace CCIT, da a conocer el comportamiento del cibercrimen en Colombia reflejado en el número de denuncias instauradas ante el ecosistema de la Fiscalía General de la Nación, las policías judiciales del CTI y la Policía Nacional -DIJIN-SIJIN- a través del aplicativo *A denunciar*[31]. Al finalizar noviembre del 2021, se habían registrado 46.527 denuncias por distintos delitos, lo que equivale a un incremento de 21% respecto al 2020. Si se tienen en cuenta comparativamente los años 2019 y 2021, es decir, sin contabilizar el año de pandemia, el incremento alcanzó 107% acumulado entre el 2020 y el 2021.

Continuando con las estadísticas, otras cifras interesantes hablando de fraude digital son las presentadas por la empresa TransUnion sobre las tendencias mundiales de fraude en línea[32], que encontró cómo, desde el comienzo del Covid 19, los defraudadores en Colombia están aumentando sus ataques contra las empresas y en ese sentido pudo establecer en un

[30] CCIT. (2021). Cámara Colombiana de Informática y Telecomunicaciones. Tendencias del Cibercrimen 2021-2022. Obtenido de: https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf
[31] CCIT. (2021). Cámara Colombiana de Informática y Telecomunicaciones. Comportamiento del Ciberdelito durante el 2021. Obtenido de: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf
[32] TransUnion. (2021). 206% aumentaron intentos de fraude digital originados desde Colombia. Obtenido de: https://noticias.transunion.co/206-aumentaron-intentos-de-fraude-digital-originados-desde-colombia/

estudio complementario, llamado Pulso del Consumidor, que el 30% de los consumidores colombianos han sido blanco de fraude digital.

5.4 ¿Cómo funciona la suplantación de identidad?

Los ciberdelincuentes son muy hábiles y en su quehacer han desarrollado varias técnicas para lograr persuadir a sus víctimas. Una de sus herramientas más importantes es atacar directamente su cerebro emocional, ya que los seres humanos estamos expuestos por nuestras emociones y por aquello que nuestro subconsciente percibe; desde allí, el ciberdelincuente diseña y define sus tipos de ataque dependiendo de sus objetivos.

La suplantación de identidad puede comenzar con un correo electrónico u otro tipo de comunicación que esté destinada a atraer a una víctima, el mensaje se crea para que parezca como si procediera de un remitente de confianza. Si engaña a la víctima, se le persuade para que proporcione información confidencial, a menudo en un sitio web de estafa. En algunas ocasiones los correos también tienen adjuntos maliciosos que se pueden descargar en el dispositivo de la víctima.

Los siguientes ejemplos de ataques de suplantación de identidad son proporcionados por el artículo de CISCO: *¿Qué es la suplantación de identidad?*[33]

5.4.1 Ataque de suplantación de identidad dirigido

El ataque de suplantación de identidad dirigido se orienta a personas específicas en vez de a un amplio grupo de personas. Los atacantes a menudo investigan a sus víctimas en las redes sociales y en otros sitios. De esa manera, pueden personalizar sus comunicaciones y parecer más auténticas. El ataque de suplantación de identidad dirigido, en algunas ocasiones, es el primer paso que se utiliza para penetrar las defensas de una empresa y llevar a cabo un ataque dirigido. Según el Instituto SANS, el 95% de todos los ataques a las redes de grandes empresas son el resultado del ataque de suplantación de identidad dirigido[34].

5.4.2 Suplantación de identidad engañosa

La suplantación de identidad engañosa es el tipo más común de suplantación de identidad. En este caso, un atacante intenta obtener información confidencial de las víctimas. Los atacantes utilizan la información para robar dinero o para lanzar otros ataques. Un correo electrónico falso de un banco que le pide hacer clic en un enlace y verificar los detalles de su cuenta es un ejemplo de suplantación de identidad engañosa.

5.4.3 Whaling

Cuando los atacantes van tras un *pez gordo*, como un CEO, se llama *whaling*. Estos atacantes a menudo dedican un tiempo considerable a definir el perfil del objetivo para encontrar el momento y los medios oportunos de robar las credenciales de inicio de sesión. El *whaling* es de particular preocupación porque los ejecutivos de alto nivel pueden acceder a una gran cantidad de información de la empresa.

[33] Cisco. (2021). ¿Qué es la suplantación de identidad? Obtenido de: https://www.cisco.com/c/es_es/products/security/email-security/what-is-phishing.html
[34] Ibidem.

5.4.4 Pharming

De manera similar a la suplantación de identidad, el *pharming* envía a los usuarios a un sitio web fraudulento que parece legítimo. Sin embargo, en este caso, las víctimas ni siquiera tienen que hacer clic en un enlace malicioso para terminar en un sitio falso. Los atacantes pueden infectar el dispositivo del usuario o el servidor DNS del sitio web y redirigir al usuario a un sitio falso, incluso si la URL correcta está escrita.

5.4.5 Suplantación de identidad de Office 365

Estos sofisticados ataques están dirigidos a ejecutivos de alto nivel, asistentes y departamentos financieros. Tienen la capacidad de evitar la seguridad del correo electrónico y las defensas de Office 365. Las investigaciones señalan que la mayoría de los ataques que interceptaron intentaron violar los departamentos financieros.

Según el informe de *Area 1 Security*, los atacantes podrían potencialmente obtener acceso a datos confidenciales de terceros a través de facturas y facturación, comúnmente conocido como ataque BEC -*Business Email Compromise*-. Esto permite a los atacantes enviar facturas falsificadas desde direcciones de correo electrónico legítimas a los proveedores, lo que resulta en pagos a cuentas del atacante.

Estos ciberatacantes buscan también nuevos CEO durante sus períodos de transición. En este punto son más vulnerables, por trámites como el proceso de incorporación a la nómina y otros sistemas internos[35].

5.4.6 Recomendaciones para la prevención del fraude digital

En términos generales, para obtener un nivel mínimo de protección en ciberseguridad, es necesario: (i) utilizar contraseñas robustas, que contengan números, letras, símbolos, mayúsculas y minúsculas, y no sean palabras que puedan estar en un diccionario o combinaciones de letras demasiado simples; (ii) instalar programas antivirus y *antimalware* con protección en tiempo real, actualizados permanentemente y de fabricantes reconocidos; (iii) mantener el *software* de los dispositivos permanentemente actualizado. Un programa no actualizado puede presentar vulnerabilidades que los ciberdelincuentes podrían aprovechar para colarse en los sistemas y robar información; (iv) cifrar la información sensible de la empresa, tales como fotos, documentos, bases de datos, etc. Deberían estar cifrados con contraseñas seguras, ya que, en caso de que un sistema se vea comprometido, será más difícil para el ciberatacante hacer uso de la información confidencial, (v) emplear redes seguras o VPN -*Virtual Private Networks*- en el teletrabajo o para navegar por Internet, para evitar que la información pueda ser vista directamente por terceros, y al mismo tiempo[36], y (vi) implementar modelos de inteligencia artificial que permitan correlacionar eventos que conlleve a identificar sesiones sospechosas.

Dado lo anterior, en esta era digital en la que nos encontramos más expuestos a estos tipos de ataques cibernéticos de suplantación, la identidad digital juega un papel importante

[35] Bafing. (2021). Ataques de suplantación de identidad de Office 365 se dirige a ejecutivos financieros. Obtenido de: https://www.bafing.com/ataques-de-suplantacion-de-identidad-de-office-365-se-dirige-a-ejecutivos-financieros/
[36] Incibe. (2021). fraude y gestión de la identidad digital. Obtenido de: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_fraude_y_gestion_de_la_identidad_online.pdf

como agente diferenciador, beneficioso tanto para las personas como para las empresas, pues no solo brinda tranquilidad y confianza, sino que reduce significativamente el fraude por suplantación de identidad, uno de los delitos con mayor crecimiento, y las consiguientes pérdidas económicas que genera. Este efecto positivo se debe a que el proceso para corroborar la identidad de una persona se basa en un ecosistema que no solo se apoya en mecanismos tradicionales de autenticación sino que va más allá, pues integra distintos modelos de inteligencia basados en datos, lo que genera como resultado, por un lado, un usuario confiado en la protección de su identidad, que incluso puede adoptar esquemas de autenticación *passwordless*, y, por el otro, una empresa segura de no ser víctima de personas o ciberdelincuentes.

6. Marco regulatorio en factores fuertes de autenticación para operaciones no presenciales

Como se mencionó al inicio de este capítulo, para la mayoría de empresas con canales digitales transaccionales, y especialmente para las entidades financieras, es necesario contar con un sistema de verificación de identidad y mecanismos fuertes de autenticación que les permita mitigar el riesgo de fraude por suplantación en el uso de los mismos.

Según cifras de la Superintendencia Financiera de Colombia, al cierre del año 2021 se realizaron aproximadamente 11000 millones de operaciones -monetarias y no monetarias- en el sistema financiero colombiano, de las cuales 8000 millones se efectuaron a través de canales digitales, lo cual significó un crecimiento de 9% en comparación con el año anterior.

La banca móvil fue el canal mediante el cual se realizó el mayor número de operaciones financieras con una participación de 54% del total de las operaciones del sistema financiero, representando aproximadamente 6000 millones de operaciones, seguido por la banca por Internet, como segundo canal con mayor participación en el número de operaciones financieras realizadas, con un aproximado de 2000 millones de operaciones, equivalente a 17% del total de las operaciones del sistema financiero.

Es así como los canales digitales tienen cada vez más una mayor participación sobre el número de operaciones realizadas en el sistema financiero, representando 71% del total de operaciones. Esto va en línea con las nuevas preferencias del consumidor financiero y el valor agregado que encuentran en los productos y servicios ofrecidos mediante los canales digitales.

En consideración a lo anterior, la Superintendencia Financiera de Colombia, inspirada en la *Payment Service Directive* 2 -PSD2- de la Unión Europea, expidió la Circular Externa 029 de 2019 en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones y acceso e información al consumidor financiero y uso de factores biométricos.

De manera general, la Circular denota la consciencia de la Superintendencia Financiera respecto a la transformación de los sistemas financieros como producto y en respuesta al uso de canales digitales para la prestación de servicios financieros. Acorde con esto, y en aras de fortalecer, facilitar y fomentar el uso de nuevas tecnologías que promuevan la eficiencia en la prestación de los servicios financieros, y a la vez garantizar condiciones de

seguridad y con apego a estándares internacionales en la materia, definió instrucciones en materia de seguridad, autenticación y factores fuertes de autenticación en operaciones no presentes.

En relación con la seguridad, impartió instrucciones en materia de confidencialidad, integridad y disponibilidad de la información, remitiendo a estándares de ISO 27000, sistemas de gestión de seguridad de la información, vulnerabilidades informáticas, cifrados fuertes, entre otros, con el fin de dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad.

En materia de autenticación, estableció los parámetros y conjunto de técnicas para verificar la identidad de un cliente, entidad o usuario. Señaló que los factores de autenticación son: (i) algo que se sabe; (ii) algo que se tiene, y (iii) algo que se es. En cuanto a este tercer factor, *algo que se es*, definió como factor biométrico aquel atributo biológico o comportamental de un individuo del cual se pueden extraer propiedades distintivas y repetibles para su reconocimiento, estableciendo que las muestras biométricas son aquellas representaciones que se obtienen de una característica biométrica capturada mediante un dispositivo vinculado a un sistema biométrico, como una imagen facial, una grabación de voz o una imagen de huella digital.

Por último, con relación a la implementación de factores fuertes de autenticación, la Superintendencia Financiera estableció la obligación de contar con los mismos para aquellas operaciones que, de acuerdo con el análisis de riesgo de cada entidad financiera, generen mayor exposición al riesgo de fraude o suplantación. Este análisis debe tener en cuenta aspectos como el perfil transaccional del cliente, monto de operaciones, tipo de producto, canal, entre otros. Sin embargo, estableció que, independientemente del análisis de riesgo de la entidad financiera, se debe contar con mecanismos fuertes de autenticación para: (i) la realización de operaciones monetarias que impliquen el retiro de efectivo, transferencias de fondos, recepción de giros y desembolsos; (ii) transacciones realizadas mediante pago con o sin contacto; (iii) la actualización de datos del cliente para la notificación de operaciones monetarias o generación de alertas, y (iv) las operaciones realizadas con tarjeta débito y crédito, en el territorio nacional, en ambiente presente, cuando el emisor sea colombiano y se superen los parámetros de seguridad asociados a esas tecnologías.

De conformidad con lo anterior, la Circular Externa 029 de 2019 definió como uno de los mecanismos fuertes de autenticación el uso de la biometría en combinación con un segundo factor de autenticación para operaciones no presenciales, y señaló que en la implementación de factores biométricos se deben contemplar mecanismos de prueba de vida para fortalecer la confiabilidad y seguridad del sistema tales como: (i) medición de propiedades fisiológicas del individuo; (ii) identificación de respuestas de comportamiento humano, donde la biometría comportamental permite analizar, en el momento de una transacción, tanto la forma en que las personas interactúan con un dispositivo móvil, como la forma en que escriben y sostienen el mismo, comparándolo con patrones de comportamiento registrados previamente, o (iii) protocolos de desafío-respuesta.

7. Ecosistemas de identidad digital en el mundo

En la actualidad, existen diversos ejemplos de ecosistemas de identidad digital exitosos. Todos ellos permiten a sus usuarios realizar trámites con entidades públicas, bancos u otras personas a través de medios no presenciales, de manera segura y generando confianza en la autenticidad de quienes se autentican. Los siguientes son algunos ejemplos.

7.1 Itsme® – Bélgica

7.1.1 Descripción

La aplicación móvil de identidad digital Itsme® fue creada en 2017 por el consorcio Belgian Mobile ID, compuesto por cuatro de los más grandes bancos belgas -Belfius, BNP Paribas Fortis, ING y KBC- y tres operadores móviles -Orange Belgium, Proximus y Telenet-. La aplicación permite a los usuarios verificar su identidad ante el gobierno, bancos, aseguradoras y otras empresas privadas en canales digitales. Según cifras de 2022, 6.5 millones de belgas usan Itsme®[37].

7.1.2 Casos de uso

En 2017, antes de ser reconocidos por el gobierno belga, Itsme® lanzó su primer caso de uso de la mano de Bolero, una plataforma que permite a sus usuarios acceder al mercado de valores de Bélgica. Antes de esta alianza, los clientes de Bolero debían cargar consigo una tarjeta de acceso conocida como *digipass* y un lector de tarjetas para poder acceder seguramente a la plataforma desde un computador de escritorio. De la mano con Itsme®, Bolero permite ahora a sus clientes acceder desde cualquier dispositivo al mercado de valores luego de haberse identificado a través de su identidad digital. Los usuarios deben dirigirse a su cuenta de Bolero y configurar en ella el acceso con Itsme® -configuración que luego es inmodificable-. Posteriormente, cuando deseen acceder al mercado de valores mediante Bolero, usarán su nombre de usuario y el pin de cinco dígitos o biometría dactilar para confirmar que son quienes dicen ser.

Un año después, Itsme® fue reconocida por el gobierno de Bélgica. Los ciudadanos de ese país acceden a una variedad de servicios del Estado a través de un canal oficial del gobierno, el CSAM -portal de acceso a servicios gubernamentales en línea-. Desde su alianza, los usuarios de Itsme® pueden acceder a esta plataforma sin necesidad de un lector de tarjetas y su e-ID -el documento oficial de identificación que, en Bélgica, cuenta con un sistema de seguridad verificable a través del lector de tarjetas conectado a un computador-. Esto significa que, a través de su identidad digital, los ciudadanos belgas pueden acceder de manera fácil y segura a declarar y pagar impuestos, a su sistema de pensión o a su sistema de trabajo estudiantil permitido. Durante el mismo año, también la aseguradora AXA Bélgica decidió seguir los pasos del gobierno y permitirles a sus clientes acceder a sus contratos de seguros, diligenciar reclamaciones de siniestro y seguir dichas reclamaciones a través de su página web, luego de haberlos identificado a través de Itsme®.

[37] Quoistiaux, G., (2 de junio de 2022). 6,5 millions de Belges utilisent l'appi Itsme. L'Echo. Recuperado de: https://www.lecho.be/entreprises/general/6-5-millions-de-belges-utilisent-l-appli-itsme/10392843

En 2019, el gobierno federal belga expandió su alianza con Itsme® al sector de salud. Las historias clínicas de los ciudadanos son información personal de extrema sensibilidad, y por esta razón era tradicionalmente resguardada por los prestadores de salud. Sin embargo, el gobierno reconoció que, al tener el ciudadano que interactuar con múltiples especialistas, hospitales y farmacias, lo más lógico era que esta información siguiera al paciente independientemente de quién lo atendiera. Para alcanzar este objetivo, el gobierno ha permitido que los pacientes tengan acceso a su información médica a través de canales digitales oficiales. Luego de verificar su identidad con Itsme®, los usuarios pueden descargar a un solo lugar sus resultados de exámenes médicos, recetas farmacéuticas, certificados de vacunación y otros documentos relevantes. Además, el funcionamiento del ecosistema también permite restringir el acceso a la totalidad de la historia clínica de un paciente. De esta manera, es imposible para un proveedor de servicios de salud acceder al historial de su paciente a menos que se logre establecer un vínculo entre el tratamiento particular y los registros médicos específicos, o bien que el paciente autorice el acceso a su información.

En 2020, Itsme® expandió sus casos de uso a un sector más amplio del mercado con las funcionalidades de firma electrónica calificada y *chatbot* con verificación de identidad. La primera de estas funcionalidades permite a los usuarios verificar su identidad en Adobe Sign®, para así firmar electrónicamente documentos PDF. La segunda permite a las empresas que utilizan programas informáticos de atención al cliente automatizados por inteligencia artificial -*chatbots*- integrar en sus soluciones un paso automático de verificación de identidad del cliente: la solución de identidad digital de Itsme®.

En 2021, la compañía belga de identidad digital se alió con Twikley, una solución empresarial diseñada para automatizar los débitos y registros de órdenes de servicio a través de la figura de mandato. Así, es posible autorizar los débitos de las cuentas por cobrar o pagar luego de utilizar el servicio de confirmación de Itsme® para firmar los mandatos de dichos débitos. Actualmente, la mayoría de los proveedores de tarjetas de combustible, compañías de leasing y compañías de empleos temporales que trabajan con Twikley utilizan Itsme®.

7.2 Verified.Me de SecureKey Technologies – Canadá

7.2.1 Descripción

El ecosistema de identidad digital canadiense, Verified.Me, fue desarrollado por SecureKey Technologies Inc. en cooperación con siete de las instituciones financieras más grandes de Canadá: BMO, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank y TD en 2019. Los usuarios utilizan la aplicación Verified.Me para vincular sus datos personales con distintas instituciones en el país. En 2021 fue adquirida por Interac Corp., organización dedicada a la prestación de servicios financieros transaccionales.

7.2.2 Casos de uso

Dentro de este modelo de identidad digital existen casos de uso en los ámbitos de atención al consumidor -*Call Center*- para trámites con aseguradoras, así como en materia de videojuegos y prestación de servicios gubernamentales, entre otros.

El primero de los casos mencionados permite a las compañías integrar a sus páginas web o piezas publicitarias un código QR con fines de servicio al cliente. Cuando el usuario lee el código a través de su dispositivo móvil, este lo redirecciona a la aplicación de Verified. Me, donde puede autorizar que se compartan su número de teléfono celular y otros datos relevantes dependiendo de la atención requerida para la operación particular de servicio al cliente. Al autorizar dicho tratamiento de sus datos, el usuario será añadido a una lista de espera y luego contactado por un agente de servicio al cliente que podrá brindarle una atención personalizada desde antes de atender el teléfono.

El sector asegurador también se ha visto beneficiado por la solución de identidad digital canadiense. Tradicionalmente, las compañías de seguros recolectan numerosa documentación personal de sus asegurados para identificar el riesgo que están asegurando con un grado satisfactorio de confianza. Verified.Me incorpora la verificación de identidad del asegurado con herramientas de conocimiento de cliente -como la consulta de coincidencias en listas restrictivas- diseñadas para el sector asegurador, permitiéndole a todas las partes involucradas una experiencia más sencilla, segura y ágil.

Otra industria beneficiada por la identidad digital en Canadá es la de los videojuegos. Para muchas compañías de videojuegos la creación de *identidades sintéticas* o cuentas falsas en sus plataformas se estaba tornando en un problema de escala, pues prácticas como el aprovechamiento masivo de bonos por registro o la inflación artificial de apuestas requerían una solución de verificación de identidad. Verified.Me sirvió como solución para esta problemática, permitiéndoles a los jugadores compartir su información de usuario, progreso y recompensas en sus juegos, verificación de edad y métodos de pago a través de distintas plataformas y videojuegos.

Finalmente, los ciudadanos canadienses también se ven beneficiados por Verified.Me al poder acceder a la plataforma oficial de la agencia canadiense de empleo y desarrollo social –ESDC- a través de su identidad digital. En dicha plataforma, los canadienses pueden acceder a beneficios de seguridad social como el sistema público de pensión, bolsas de empleo, licencias de maternidad o paternidad, subsidios de vivienda y educación, entre otros. Para permitir una interacción personalizada entre el gobierno y los beneficiarios de estos programas, Verified.Me permite al usuario compartir información personal desde las bases de datos de las seis principales instituciones financieras del país con la agencia gubernamental que lo necesite.

8. Estado del arte en Colombia

8.1 Descripción

Al igual que en los anteriores ecosistemas, a mediados de 2018 el sector bancario comenzó a generar alianzas para trabajar en un proyecto que le permitiera al país romper los paradigmas actuales y avanzar en la transformación digital desde la identidad como el epicentro de las interacciones. Las iniciativas producidas nacieron pensando en contribuir no solo a los bancos, sino también a otros sectores de la economía con soluciones de identidad digital que permitieran dar confianza a las transacciones que se realizan en entornos digitales y de esta manera apalancar el crecimiento del país.

Luego de un proceso minucioso de investigación, análisis, diseño y prototipado de soluciones, los bancos vieron la necesidad de crear una solución de identidad digital nueva, que abordara la necesidad de todos los sectores económicos, desarrollando una propuesta de valor innovadora que contribuyera a la construcción de confianza y progreso del país. Ya para 2019 algunos proyectos empezaron a tomar forma, con la misión de proveer confianza en las transacciones y servicios digitales cotidianos, incorporando tecnologías que permiten manejar la identidad digital de forma segura y fácil.

8.2 Casos de uso

La solución de identidad digital que se encuentra en desarrollo en Colombia contaría con un proceso inicial de registro riguroso en el cual se valida la identidad de los usuarios a partir de: (i) la captura de datos básicos iniciales; (ii) la captura biométrica y prueba de vida a través de la toma de una *selfie* para validar que los usuarios sean personas vivas y que no se trata de videos o fotos; dicha *selfie* se contrasta con bases de datos biométricas; (iii) la consulta al Archivo Nacional de Identificación de la Registraduría Nacional del Estado Civil; (iv) la validación de los documentos de identidad de los usuarios, y (v) el análisis de la traza digital, con el ánimo de verificar la confiabilidad y reputación de los atributos asociados a la conectividad de los usuarios, así como elementos que den confianza a su identidad.

Una vez culmine el proceso de registro de manera exitosa y se cree la identidad digital de un usuario, la solución planteada le permitiría contar con un mecanismo de autenticación de su identidad, facilitando y agilizando sus trámites de manera segura y confiable, con entidades públicas y privadas.

En otras palabras, el ecosistema de identidad digital en desarrollo en Colombia ofrecería un modelo descentralizado que pone al ciudadano en el centro de todo y le permite controlar sus datos personales en el marco de diversos mecanismos de autenticación. Así, el ciudadano figura como único titular de sus datos personales sin importar cuántas transacciones realice o el número de entidades con las que interactúe en línea, y es quien decide cómo y cuándo utilizar su información personal para asegurar el acceso a bienes y servicios digitales, con los mayores estándares de seguridad y privacidad de la información, y manteniendo el control de su información personal.

De esta manera, bajo un ecosistema de identidad digital centrado en el usuario, los ciudadanos no estarán forzados a realizar múltiples procesos de registros, vinculación y autenticación con diferentes tipos de entidades en sus interacciones digitales, debiendo entregar sus datos personales una y otra vez, superar preguntas reto de seguridad y memorizar múltiples nombres de usuario, alias y contraseñas cuando interactúan con los diferentes agentes de manera digital -por ejemplo, Gobierno, bancos, *retail*, educación, seguros, salud, etc.-.

Así, la construcción de una única identidad digital que pueda reutilizarse en múltiples ocasiones para hacer trámites con distintas empresas es la esencia de la solución que se adelanta en Colombia desde el sector financiero. Por consiguiente, el usuario es quien decide con quién quiere compartir su información personal y en qué trámites o servicios quiere autenticarse a través de su identidad digital.

De tal suerte, tanto las entidades públicas como las privadas podrán verificar la identidad de sus usuarios potenciales para realizar su vinculación, o de usuarios actuales cuando estos soliciten nuevos productos. También podrán autenticar digitalmente a sus usuarios al momento de realizar un pago u otro trámite de alto riesgo que requiera un segundo factor de autenticación, e incluso controlar el acceso de colaboradores a las sedes físicas de la organización sin necesidad de carnetización, o a los portales digitales privados sin usuarios ni contraseñas.

9. Conclusiones

Los procesos de transformación avanzan a pasos agigantados y la digitalización es cada vez más una realidad para las diferentes industrias. Si bien la tecnología se entiende como un habilitador de nuevos canales, productos y servicios digitales, la velocidad de estas disrupciones no es proporcional a los tiempos de adopción de hábitos y conductas que brinden seguridad a los ciudadanos en el mundo digital.

Así, en la creación de nuevos productos o servicios digitales es imperativo priorizar la seguridad y privacidad de los ciudadanos como elementos fundamentales para construir relaciones de confianza, y para esto es esencial que los usuarios tengan control sobre su información y determinen quién tiene acceso a ella en un plano digital.

En esta tarea, es fundamental contar con mecanismos de autenticación robustos y asegurar que estén bajo el control del ciudadano. La identificación es tan solo el primero de varios pasos requeridos para autorizar el acceso a bienes o servicios digitales, e incluso desarrollar iniciativas de *Open Finance*, que permitan la transferencia o portabilidad de datos del consumidor entre entidades financieras, fomentando el acceso a dicha información en favor del desarrollo de nuevos productos y servicios a través de plataformas electrónicas en beneficio del ciudadano.

Por lo tanto, los procesos de autenticación deben ser absolutamente respetuosos de las normas de privacidad: si no se brindan controles de seguridad y procesos que ubiquen al ciudadano como único dueño de su información personal, cualquier tercero podría hacer uso de estos elementos de autenticación y tener acceso no autorizado a servicios o bienes digitales.

Así, la identidad digital permite romper los paradigmas actuales y avanzar en la transformación digital desde la identidad como el epicentro de las interacciones. Las soluciones de identidad digital contribuyen no solo a los bancos, sino también a otros sectores de la economía que utilicen canales digitales y requieran dar confianza a las transacciones que en ellos se realizan, al tiempo que les permite a los usuarios mantener control sobre su información personal en el mundo digital.

Bibliografía

Area 1. (2021) Stopping Business Email Compromise (BEC). Obtenido de: https://www.area1security.com/resources/stopping-business-email-compromise-bec/

Asobancaria. (2018). Recomendaciones a la política pública sobre la identificación/autenticación digital en Colombia. Bogotá, Colombia: Autor.
Asociación GSM y otros. (2016). Digital identity: towards shared principles for public and private sector cooperation. Recuperado de: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf

Bafing. (2021). Ataques de suplantación de identidad de Office 365 se dirige a ejecutivos financieros. Obtenido de: https://www.bafing.com/ataques-de-suplantacion-de-identidad-de-office-365-se-dirige-a-ejecutivos-financieros/
Banco Mundial. (2018). Identification For Development (ID4D) Global Dataset.

Recuperado de: https://datacatalog.worldbank.org/search/dataset/0040787

Banco Mundial. (2021). *Principles on identification for sustainable development: Toward the digital age. Recuperado de:* https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf

Cámara Colombiana de Comercio Electrónico. (2019). *Informe de transacciones digitales en Colombia 2016-2019.* Recuperado de: https://www.ccce.org.co/wp-content/uploads/2017/06/informe-transacciones-colombia-2016-2019.pdf

CCIT. (2021). Cámara Colombiana de Informática y Telecomunicaciones. Comportamiento del Ciberdelito durante el 2021. Obtenido de: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe- evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

CCIT. (2021). Cámara Colombiana de Informática y Telecomunicaciones. Tendencias del Cibercrimen 2021-2022. Obtenido de: https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

CCIT. (2022). Cámara Colombiana de Informática y Telecomunicaciones. El comercio electrónico en 2021 y perspectivas 2022. Obtenido de: https://www.ccce.org.co/gestion-gremial/

Cisco. (2021). ¿Qué es la suplantación de identidad? Obtenido de: https://www.cisco.com/c/es_es/products/security/email-security/what-is-phishing.html
Código Civil [Código] (2021). Recuperado de: https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1827111

Constitución Política de Colombia [Const.]. (1991). Legis
Corte Constitucional de Colombia, Sala Sexta de Revisión de Tutelas. (26 de junio de 2018)

Sentencia T-241. [MP Gloria Stella Ortiz Delgado]

Cuno, A., Aldoradín, Y., Ganz, H., Veliz, F. y Papa, E. (2021). Un modelo de gestión de la Identidad Digital para el Estado Peruano. Revista Ibérica de Sistemas e Tecnologiuas de informação, 166-182.

GMSA. (2016). *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*. Recuperado de: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf

Incibe. (2021). fraude y gestión de la identidad digital. Obtenido de: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_fraude_y_gestion_de_la_identidad_online.pdf

Incibe. (2021). Fraudes online: aprende a identificarlos. Obtenido de: https://www.incibe.es/protege-tu-empresa/blog/fraudes-online-aprende-identificarlos

Paycomet. (2020) Fraude. Obtenido de: https://www.paycomet.com/news/glosario/que-es-fraude/

Quoistiaux, G., (2 de junio de 2022). 6,5 millions de Belges utilisent l'appi Itsme.

L'Echo. Recuperado de: https://www.lecho.be/entreprises/general/6-5-millions-de-belges-utilisent-l-appli-itsme/10392843

Registraduría Nacional del Estado Civil. (s.f.) *Historia de la Identificación. Recuperado de: https://registraduria.gov.co/-Historia-de-la-identificacion-.html*

Romero Mondragón NS. (2020). *Generación de identidad digital para el acceso a los servicios ciudadanos digitales en Colombia.* Accessed May 6, 2022. https://search.ebscohost.com/login.aspx?direct=true&db=ir01494a&AN=seneca.1992.48441&lang=es&site=eds-live&scope=site

Sedlmeir, J. y otros. (2021). Digital Identities and Verifiable Credentials. Catchword, 36(5), 603-613, doi:10.1007/s12599-021-00722-y
Statista. (2022). *Global smartphone penetration rate as share of population from 2016 to 2020*. Recuperado de: https://www.statista.com/statistics/203734/global-smartphone-penetration-per-capita-since-2005/

Superintendencia de Industria y Comercio. (2019). Q*uejas por suplantación de identidad ante la Superintendencia crecieron 122%*. Recuperado de: https://www.sic.gov.co/Quejas-por-suplantacion-de-identidad-ante-la-Superindustria-crecieron-122

TransUnion. (2021). 206% aumentaron intentos de fraude digital originados desde Colombia. Obtenido de: https://noticias.transunion.co/206-aumentaron-intentos-de-fraude-digital-originados-desde-colombia/
World Economic Forum. (2016). *A blueprint for digital identity.* Recuperado de: https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

World Economic Forum. (2018). Digital Identity: On the threshold of a Digital Identity Revolution. Recuperado de: https://www3.weforum.org/docs/White_Paper_Digital_Identity_Threshold_Digital_Identity_Revolution_report_2018.pdf

PARTE 3

DIGITALIZACIÓN EN EL SECTOR BANCARIO

CAPÍTULO 8

Fintech, riesgo sistémico y desafíos de supervisión y regulación prudenciales

Mauricio Rosillo Rojas[1]

Resumen

La industria de la tecnología financiera, Fintech por sus siglas en inglés, es una realidad que tocó las puertas del mundo sin distinción en los niveles de desarrollo de las sociedades y las regulaciones. En sus inicios se percibió como una forma de competencia con el sector financiero tradicional, pero con el tiempo, no solo los desarrolladores de esa industria sino las entidades constituidas bajo modelos de negocio tradicionales, han tomado provecho para construir sinergias y generar oportunidades para modernizar los negocios financieros. En este documento se identifican los principales frentes donde la industria Fintech hace presencia en Colombia, su aporte a los objetivos del Estado y a la profundización financiera impulsada por el Covid-19. En paralelo, se recogen los principales retos y con ellos los riesgos que deberían ser considerados por los reguladores y supervisores al definir la normativa para los nuevos jugadores Fintech, y de su extensión hacia las BigTech que cada vez se vuelven más relevantes en la oferta de servicios financieros pudiendo representar un riesgo sistémico que afecte la estabilidad financiera.

[1] Vicepresidente Corporativo del Grupo Bancolombia. Director de la Especialización en Derecho Financiero y de Mercado de Valores de la Universidad de Javeriana y profesor de postgrados en las universidades Javeriana y de los Andes.

1. Introducción

Con el auge de la denominada industria Fintech, entendida como la innovación aplicada a los servicios financieros a través de la tecnología con el propósito de generar un efecto significativo en nuevos modelos de negocio, aplicaciones, procesos o productos[2], han sido muchas las predicciones sobre el aporte de estos desarrollos a los ecosistemas[3], agentes[4] y consumidores financieros[5]. La evidencia ha mostrado un crecimiento exponencial de partícipes y con ello la potencial mayor competencia y eficiencia de los subsectores impactados, como el relacionado con medios de pagos y de consecución de recursos por fuera del mercado de valores y de los mismos bancos. Sin embargo, también se ha convertido en un mecanismo de fortalecimiento y profundización de los agentes y mercados ya existentes, como el sector bancario y del mercado de valores, que se han transformado a ofrecer productos y servicios cada vez más centrados en el perfil de los clientes, con experiencias que están más cerca de sus necesidades, preferencias y objetivos individuales, por ejemplo, la creación de productos propios para los emprendedores, créditos / tarjetas débito y otros puramente transaccionales para personas que inician su vida estudiantil o laboral, oferta de inversiones en el exterior, en fondos apropiados para el consumo masivo más conservador, microseguros o seguros como los previsionales o de salud, adecuados para determinados grupos de clientes, etc.

En los países en desarrollo, el acceso a Internet, la transformación digital y el uso de la tecnología fueron potenciados por la pandemia del Covid-19, convirtiendo estas herramientas en palancas para el cumplimiento de políticas públicas, principalmente aquellas enfocadas en la inclusión financiera. Colombia no ha sido la excepción: desde el año 2014 se observa una evolución constante en la agenda regulatoria que promueve nuevos modelos de negocio con el uso de tecnologías, así como la aparición de prestadores de servicios que, estimulados por la digitalidad, han desarrollado diferentes modelos de negocios financieros innovadores.

Es el caso de las Sociedades Especializadas en Depósitos Electrónicos -SEDPE-, promovidas por la regulación local, con el fin de llevar sus servicios a sectores no atendidos por la banca tradicional y que para finales del 2021 ya sumaban al menos seis entidades autorizadas por la Superintendencia Financiera de Colombia -SFC-, lo que es un factor relevante para generar confianza y ampliar la oferta de productos[6].

En paralelo, ha sido preponderante el desarrollo de los productos puramente transaccionales, cuyo objetivo es incrementar y facilitar el acceso a medios de pago digitales como las billeteras electrónicas -*wallets*- y las cuentas de trámite simplificado, depósitos de bajo monto y cuentas de ahorro electrónico, productos que pueden abrirse con menos requisitos, lo que los hace más accesibles en cuanto a experiencia y costos para el usuario.

Desde el 2017 han aparecido iniciativas de esquemas colaborativos que permiten conseguir recursos, enmarcados en regulación como la que viabilizó el *Crowdfunding* como actividad

[2] Financial Stability Board. Financial Stability Implications from Fintech. Junio de 2017.
[3] Ambientes formados por un conjunto de tecnologías de la información que se encuentran interconectadas entre sí.
[4] Conjunto de actores que hacen parte de un ecosistema.
[5] Es todo cliente, usuario o cliente potencial de las entidades vigiladas por la Superintendencia Financiera de Colombia (Ley 1328 de 2009).
[6] En palabras del Superintendente Financiero, Jorge Castaño, en el Foro LR 'Fintech-Microfinanzas' (2021) expresó que *"los nuevos actores disruptivos, como los neobancos o los crowdfunding, llegaron a complementar la metodología tradicional de acompañamiento al microempresario, de la mano de la tecnología."*

supervisada -en la medida que fue autorizada a las vigiladas-, consistente en que, a partir de una infraestructura electrónica y a través de plataformas, páginas de internet u otro medio de comunicación electrónica, se ponen en contacto un número plural de aportantes con receptores que solicitan financiación en nombre propio para destinarlo a un proyecto productivo de inversión[7], por ejemplo, A2censo-bvc, Inverti, entre otros[8].

Tal vez por su gran popularidad en el mundo, desde 2018 han tomado mucha fuerza los habilitadores de pagos digitales, entre ellos las numerosas pasarelas de pago en línea -PSE, PayU, Mercado Pago, Wompi, entre otras-. Además, como un paso más adelante y más reciente, el uso de la analítica de datos en los nuevos desarrollos que buscan profundizar los modelos de negocio basados en ofrecer servicios de asesoramiento para la transformación de los negocios -plataformas tipo *marketplace* ampliado[9]- y la administración patrimonial utilizando *bots*[10] y otros servicios de Inteligencia Artificial -IA- y *Customer Relationship Management* -CRM[11]-. Así, alrededor de los productos Fintech se vuelve una constante la mayor personalización y facilidad de acceso, incrementando la satisfacción de los consumidores.

A su lado, se tienen infraestructuras superiores como la computación en la nube o los servicios en la nube que, a través del uso de una red de servidores remotos conectados a Internet, permiten almacenar, administrar y procesar datos, servidores, bases de datos, redes y software, facilitando que las empresas no tengan que encargarse de aprovisionar, configurar o gestionar los recursos y permitiendo que paguen únicamente por los que usen[12].

Desde el lado de los oferentes, un número importante de compañías ha conquistado sus espacios propios, sobre todo de nicho, operando principalmente el negocio de las tarjetas débito y crédito como lo evidencia el crecimiento de licencias de compañías de financiamiento, aun cuando también se han autorizado neobancos o bancos cien por ciento digitales, con las flexibilidades propias de esas estructuras -básicamente sin los costos que implica la apertura de oficinas o agencias y en general la logística y costos de la infraestructura física-; pero, en todo caso, bajo la figura de la licencia de un establecimiento de crédito. En paralelo, se tiene otro grupo de emprendedores que ofrecen servicios que no son netamente financieros -o que no requieren autorización o licenciamiento-, pero que sí están estrechamente relacionados con servicios financieros; esto genera importantes riesgos para toda la industria por cuenta de la interconexión de los sistemas en los que comparten todo tipo de información transaccional-financiera, como es el caso de plataformas que en adición a servicios comerciales -adquisición de bienes y servicios- ofrecen esquemas de financiamiento y, en algunos casos, operaciones de *cash in* y *cash out* -depósitos y retiros- operando con recursos propios.

Sin embargo, los anteriores esquemas no son los únicos. La realidad muestra, además, que alrededor del auge de las Fintech se han construido alianzas poderosas que buscan promover la interacción de industrias de distinta naturaleza entre las nuevas compañías Fintech y las entidades financieras tradicionales, como es el caso de algunos bancos que han entrado

[7] Decreto 1357 de 2018
[8] Según datos de la SFC las sumas de los proyectos en estos vehículos ascienden a la suma de $45.288 millones financiados / 104 campañas exitosas y cuentan con 8.159 inversionistas.
[9] En redes interconectadas de ofertas de servicios, que permite a sus usuarios satisfacer gran variedad de necesidades, en una experiencia integral.
[10] Programas de computadora que simulan respuestas humanas para atender agentes de la plataforma.
[11] Procesos en los que una compañía administra sus interacciones con los clientes aprovechando tecnologías de la información.
[12] https://cloud.google.com › learn › what-is-cloud-computing

como socios de compañías -*startup*- que tienen como propósito la compra de productos *online* y el cumplimiento de entrega a los clientes a domicilio. Dichas alianzas pueden darse, en cierta medida, por la dificultad para obtener las licencias necesarias para ofrecer servicios financieros, pero también como resultado de decisiones estratégicas en el propósito de llegar a los clientes con soluciones simples y cercanas, que, al convenir estructuras disruptivas con las entidades financieras tradicionales, les permiten potencializarse sobre lo ya existente, apalancándose legalmente en sus licencias y creciendo de manera más segura y rápida.

La tecnología aplicada a los servicios financieros, en lo que se ha denominado la cuarta revolución industrial, implica el reconocimiento de varias cosas. La primera, relacionada con los resultados favorables en determinados frentes como la inclusión[13] y profundización financiera[14], con productos a los que se accede con menos requisitos, a través de herramientas propias de la cotidianidad de las personas como los celulares y otros instrumentos cuyo fácil manejo mejora la usabilidad de los productos financieros. Lo propio sucede con el desarrollo de nuevas capacidades a partir, por ejemplo, de análisis de datos o de la desaparición de fronteras hasta hace poco infranqueables, tanto a nivel geográfico como en la oferta de valor que pueden brindarse entre sectores, empresas o entre productos y servicios, incluso ahora en la creación de espacios paralelos al mundo físico, como lo plantea el nuevo ámbito conocido como *metaverso*[15].

Lo anterior sin considerar otros frentes, como podría ser la incorporación de monedas digitales o autorización de operaciones en activos con subyacentes no tradicionales, como es el caso de las criptomonedas o los bitcoins[16].

El fenómeno Fintech ha crecido a tal punto que las grandes empresas tecnológicas -BigTech- han venido adquiriendo mayor apetito por participar en el sistema financiero. Se destaca el interés de las llamadas FAANGs -Facebook-Meta, Amazon, Apple, Netflix y Google-Alphabet- desde Estados Unidos y de las BATs -Baidu, Alibaba y Tencent- desde China, que han ingresado al sistema financiero mediante diversos esquemas por cuenta de las diferencias regulatorias que existen entre los dos países. Las BigTech tienen importantes ventajas comparativas frente a las compañías Fintech y a las entidades financieras tradicionales para convertirse en habilitadores y prestadores directos de servicios financieros: (i) cuentan con acceso a información masiva de los clientes; (ii) desde hace años poseen mecanismos de vinculación directa mediante sus plataformas; (iii) tienen una posición de liderazgo en

[13] Dr. Claudio González Vega, Academia de Centroamérica, 2019. La "inclusión financiera" es un concepto aún en evolución, en la actualidad se habla de tres pilares base para alcanzarlo: el acceso, el uso y la calidad. El acceso se refiere a la importancia de llevar a la población de un país, una amplia gama de servicios financieros e institucionales que permitan incorporar a personas excluidas del sistema, dando facilidades como la diversidad de canales de acceso físico y digital, proximidad, reducción de los costos de transacción y minimización de las barreras de entrada.
El uso, se enfoca en dirigir las oportunidades productivas, impulsar mecanismos de protección como los seguros para reducir los riesgos, sistemas de información transparentes como en el caso de puntos de atención, tipos de productos, costos y educación para mayores capacidades financieras.
Por último, el pilar de la calidad implica que los productos deban adaptarse a las circunstancias y requerimientos de los usuarios, ya que no se puede asumir que todas las personas tengan las mismas necesidades, por lo que es sustancial ofrecer un amplio menú de opciones.
[14] Profundización financiera, entendida como la capacidad del sistema financiero de trasmitir los recursos hacia el sector real y es medida como la relación entre la cartera y el PIB.
[15] https://www.xataka.com/basics/ El término metaverso viene de una novela de 1992 llamada 'Snow Crash', y es un término que se ha asentado para describir visiones de espacios de trabajo tridimensionales o virtuales. Este metaverso, por lo tanto, significa un mundo virtual en el que podemos interactuar, y que ha sido creado para parecerse a una realidad externa. Como generalidad se entiende que El Metaverso es un mundo virtual, uno al que nos conectaremos utilizando una serie de dispositivos que nos harán pensar que realmente estamos dentro de él, interactuando con todos sus elementos.
[16] Son considerados instrumentos financieros digitales ya que no tiene representación física y se transfieren en medios digitales replicando como subyacente un activo criptográfico. El producto utiliza el precio de bitcoin, por poner un ejemplo, como punto de referencia o benchmark y lo emula en su propio mercado para que los comerciantes puedan beneficiarse de la volatilidad del activo. (Glosario de Bitcoin y blockchains).

innovación y desarrollo de tecnología y de modelos avanzados de analítica de datos e inteligencia artificial, y (iv) tienen acceso a capital y/o financiamiento a costos relativamente más bajos que sus posibles competidores por cuenta de su gran tamaño y la presencia de años atrás en los mercados de capitales más importantes.

Vale la pena resaltar que el ingreso de las BigTech al sistema financiero se ha dado de manera gradual con diversos modelos de negocio. En efecto, las primeras iniciativas fueron esquemas transaccionales de billeteras virtuales -Apple Pay, Google Pay, Facebook Pay, Amazon Pay, entre otros- en los que, a pesar de ciertas diferencias específicas -relaciones comerciales, características de las apps, términos y condiciones-, se ofrece un servicio gratuito de agregación de distintos medios de pago emitidos por entidades tradicionales. En dicho esquema las BigTech no generaban cobros, pero sí accedían a la información transaccional de los clientes.

Más recientemente, las BigTech se han interesado en participar de la intermediación financiera directa -sin asociaciones con entidades tradicionales-; sin embargo, los crecientes costos regulatorios -exigencias de capital y de liquidez para el sector financiero-, tasas de interés globales que comprimen los márgenes de ganancia del negocio bancario y los numerosos trámites para adquirir licencias de funcionamiento- han derivado en que estas compañías / plataformas busquen alianzas con entidades financieras tradicionales, similar a sus contrapartes Fintech. En efecto, la oferta de productos financieros como tarjetas de crédito o apertura de cuentas corrientes por parte de las BigTech, así como la iniciación de pagos de las entidades financieras en las plataformas de las grandes de las tecnologías, solo se ha presentado mediante asociaciones con bancos tradicionales que se encargan de absorber la pesada carga regulatoria que ello implica.

Aparece entonces un potencial riesgo y es que, de manera indirecta, sean las BigTech quienes tomen el control de la relación con el consumidor financiero, convirtiendo a las entidades financieras tradicionales en prestadoras de servicio sin poder de mercado, es decir, dejándolas como meros canales de transferencia, pero trasladando los márgenes de intermediación y tarifas a una industria que no tiene interés ni función de servir como transmisor de los recursos de la economía vía operaciones activas o crédito, como sí los tiene el sector financiero.

Mientras esta ha sido la tendencia en Estados Unidos y Europa, en China las BigTech han jugado un papel mucho más relevante, al ser las promotoras de la formalización financiera en ese país. Dicha incidencia se ha dado por cuenta de: (i) un contexto macrofinanciero *más anticuado* que el del resto de países desarrollados, con una economía altamente dependiente del efectivo y sin infraestructura bancaria para soportar el uso de tarjetas/datáfonos, lo que favorece la difusión de esquemas de pago vía apps-QR-smartphones; (ii) una regulación más flexible, y (iii) ciertos intereses del gobierno chino en mantener la información centralizada en algunos grandes jugadores más fáciles de vigilar.

De esta manera, la innovación tecnológica se ha abierto paso al interior del sistema financiero mediante cuatro canales: (i) la creación de nuevas empresas -*startups*- sin experiencia financiera previa[17]; (ii) las innovaciones al interior de instituciones financieras -vigiladas- ya

[17] Esta es la ruta más comúnmente asociada con fintech. Aunque estas empresas suelen estar fuera del sistema financiero regulado, sus productos podrían ser indistinguibles de los ofrecidos por las instituciones financieras reguladas. Además, estas empresas pueden ser reguladas, vender su producto innovador a una institución financiera o ser adquiridas por una empresa regulada

existentes[18]; (iii) la incursión en el sistema financiero de grandes compañías que ya cuentan con una gran base de clientes y ventajas en desarrollo tecnológico y financiamiento -las denominadas BigTech-[19], y iv) las compañías ubicadas fuera de la jurisdicción, que ofrecen productos financieros de forma remota a los clientes locales[20] . Estos caminos no necesariamente son excluyentes; de hecho, pueden verse combinaciones de estos canales, como el caso de las instituciones financieras tradicionales que establecen asociaciones o alianzas con empresas Fintech -HSBC-Tradeshift para automatización de procesos operativos de terceros y Deutsche Bank-Traxpay para ofrecer productos de *factoring* a clientes específicos- o grandes empresas extranjeras no financieras que ofrecen productos Fintech de forma remota -Apple pay, Samsung pay, entre otras[21]-.

Con este panorama, enmarcado en entornos cada vez de mayor penetración y globalización, la invitación es a reconocer que, antes que competidores, las compañías Fintech son aliadas fundamentales de la industria financiera y de su evolución al punto que, según algunos analistas de riesgos[22], para el año 2027 el 82% de las empresas de servicios financieros habrán establecido modelos de alianzas con este tipo de compañías.

2. Evolución de la visión regulatoria y de supervisión

El contexto hasta aquí recogido supone muchos retos para los reguladores y supervisores financieros y, sin duda, cambios en los fundamentos prudenciales que han operado hasta el momento, aspectos que serán abordados más adelante, pero sobre los cuales hoy es impensable que se vaya a retroceder.

La pretensión de proteger antiguos espacios que se consideraban como propios del sector financiero, o de que sean las entidades tradicionales las originadoras de desarrollos independientes e internos, está cada vez más lejos. Por el contrario, el éxito estará en generar valor con nuevos socios o aliados expertos, que buscan la mayor interconectividad posible de mercados y prestadores de servicios, en sus distintas escalas, desde el acceso hasta el cierre de operaciones, en los que intervienen diferentes entidades. Esta aptitud no es sólo de los participantes de los mercados, sino que se ha convertido incluso en una competencia de países que cada vez buscan más un reconocimiento como centros Fintech o *Fintech-hubs*[23], entendiendo estos últimos como centros que ofrecen marcos regulatorios flexibles y otros factores que los hacen atractivos Así, en relación con la innovación financiera, los reguladores están llamados en la era Fintech a encontrar el balance adecuado entre la protección de la estabilidad del sistema y la promoción de la innovación[24].

[18] Esta es la ruta tradicional. Cabe señalar que en esta modalidad la innovación puede introducirse sin conocimiento previo del regulador, especialmente cuando se trata de un proceso interno o un modelo de negocio ya adoptado por una empresa matriz en otro país.
[19] En este caso, una empresa tecnológica, de telecomunicaciones u otro tipo de empresa no financiera, introduce un producto fintech, aprovechando su actual base de clientes, para alcanzar rápidamente una masa crítica. Eso caracteriza a este modo de funcionamiento en comparación con el modelo de introducción a través de una start-up.
[20] Muchos productos de Fintech, por su naturaleza, no requieren la presencia física de un proveedor para entrar en un mercado. Esto permite a estas empresas competir, en efecto, en el mismo mercado con instituciones financieras reguladas. Esta modalidad incluye las tres mencionadas anteriormente, pero ofrecidas a distancia.
[21] ASBA y BID Lab. *Consideraciones de Regulación y Prácticas de Supervisión para las Innovaciones Tecnológicas Financieras.* Junio, 2020.
[22] Real Risk, 2022.
[23] Aurelio Gurrea Martínez, Nydia Remolida. Fintech, Regtech y Legaltech: Fundamentos y desafíos regulatorios. 2020.
[24] Ídem. Pie de página No.12 (pág. 144).

La literatura internacional, especialmente aquella basada en la European Banking Authority, ha generado un enfoque regulatorio y de supervisión soportado en tres frentes[25]:

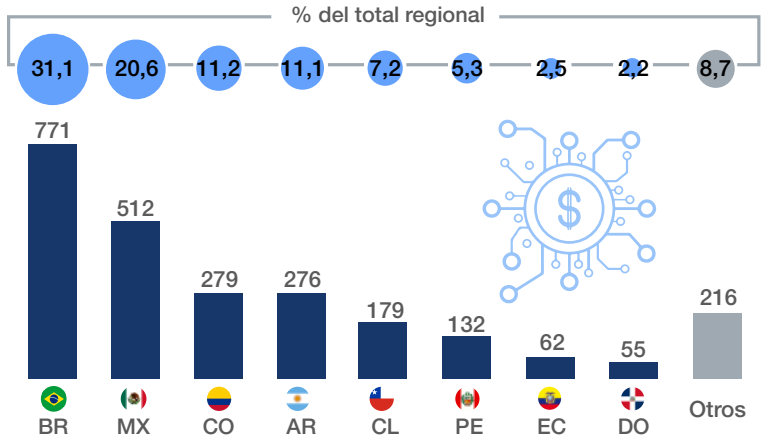
- Establecimiento de una regulación que permita determinar con claridad qué cabe dentro del marco regulatorio tradicional y qué podría ser objeto de algunos ajustes -por ejemplo, banca digital-, qué requiere de nueva regulación -por ejemplo, Crowdfunding- y qué posiblemente deba ser prohibido o amerite un mayor estudio -por ejemplo, criptoactivos-.
- La definición de un modelo de licencias o autorizaciones acorde con los nuevos modelos de negocio -por ejemplo, licencias modulares de mercado de capitales, es decir por actividad, de manera que las exigencias son equivalentes a los riesgos y responsabilidades que asumen y no a toda la gama de actividades que se predican bajo el esquema de licenciamiento por sujeto-, que mantengan la seguridad y confianza en los mercados, y
- La creación de espacios en los que se puedan hacer desarrollos innovadores en ambientes controlados con el acompañamiento de las autoridades -*sandbox*-, al tiempo que se avanza en el desarrollo del marco regulatorio adecuado -por ejemplo, decreto 1234 de 2020-.

Algunas jurisdicciones, con distintos grados de avance -Bras[26], México, Colombia, Perú y Chile-, desde hace unos años vienen impulsando normativas que regulan a las Fintech[27], facilitando e incentivando el desarrollo de esos modelos de negocio como ha sucedido en otras partes del mundo y como ha sido enunciado por instancias como el mismo Comité de Basilea[28] o el Fondo Monetario Internacional -FMI-[29].

De acuerdo con información de Finnovista y el BID, al corte de 2021 en América Latina había más de 2.400 startups financieras, de las cuales cerca del 63% estaban ubicadas en: Brasil (31%), México (21%) y Colombia (11%). Ver gráfico 1.

[25] Las autoridades en Colombia se han movido en los 3 frentes.
[26] https://pmi-americas.com/es/el-boom-de-los-neobancos-en-latinoamerica-una-oportunidad-historica-para-crecer-es/ En el caso de Brasil, ya no caben dudas que hoy es el indiscutido hub del Neobanking en Latinoamérica, con 19 Neobancos y varios jugadores integrándose en los próximos años.
[27] M. Lavalleja, "Panorama de las Fintech: principales desafíos y oportunidades para el Uruguay", serie Estudios y Perspectivas-Oficina de la CEPAL en Montevideo, N° 48 (LC/TS.2020/53; LC/MVD/TS.2020/3), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.
[28] BIS. Sound Practices: implications of fintech developments for banks and bank supervisors. Febrero 2018. El Banco Internacional de Pagos (BIS por sus siglas en inglés) es una organización internacional que fomenta la cooperación monetaria y financiera internacional y actúa como banco para los bancos centrales, y fue el creador del Comité de Basilea en 1974.
[29] La finalidad primordial del FMI es garantizar la estabilidad del sistema monetario internacional, es decir el sistema de pagos internacionales y tipos de cambio que permite a los países y a sus ciudadanos efectuar transacciones entre sí.

Gráfico 1. Número de compañías Fintech identificadas a finales de 2021



Fuente: Elaboración Statista con base en Finnovista y BID.

Ahora bien, mientras México tiene una Ley Fintech que regula diversos frentes de la prestación de servicios financieros como billeteras, instituciones de financiamiento colectivo -*Crowdfunding*- y agentes de los ecosistemas de pago digitales[30], Brasil se caracteriza por la normativa en materia de *Open Banking*[31] como pionero en América Latina. Entre tanto, en Colombia, además de los avances dados en los propios mercados de productos, la regulación ha buscado cubrir dos frentes fundamentalmente. En primer lugar, se emitió regulación relativa a la actividad de financiación colaborativa -*Crowdfunding*-, esperando ampliar los esquemas de financiamiento, se hicieron ajustes al sistema de pago de bajo valor y, más recientemente, se ha buscado autorizar la iniciación de pagos como una actividad nueva dentro de los servicios de pago[32], e incorporar el concepto de *Open Finance* y comercialización de la data en esquemas de prestación mutua de servicios entre entidades financieras tradicionales y terceros[33]. En segundo lugar, el Gobierno 2018-2022 presentó un proyecto de ley que buscaba una regulación funcional o por actividades para el mercado de capitales con la adopción de la figura de las licencias modulares, lo cual es un avance para

[30] Colombia debe seguir avanzando en la construcción de un ecosistema de pagos digitales, entendiendo el ecosistema como un relacionamiento efectivo entre actores, medios e instrumentos de pago. En un ecosistema un actor puede interactuar con otro de manera fluida, rápida, compatible y efectiva, lo que se traduce en menores costos asociados al pago, como ha venido propiciándose en varias sociedades referentes, de allí que eliminar las barreras que impiden esa comunicación fluida entre agentes al momento de realizar un pago digital resulte imperativo en este proceso. (Asobancaria, Semana Económica 2018, Edición 1122).

[31] El open banking o banca abierta es un sistema en línea en el que los clientes de las instituciones financieras (desde bancos hasta empresas fintech, pasando por casas de bolsa, sociedades financieras populares y sociedades de ahorro y préstamo) autorizan compartir su información con otras entidades. (https://www2.deloitte.com/mx/es/pages/dnoticias/articles/open-banking-y-sus-beneficios.html)

[32] Entendiendo por iniciación de pagos la actividad consistente en el envío de una orden de pago o transferencia electrónica por parte de un tercero distinto al usuario, al beneficiario, a la entidad emisora y a la entidad receptora; a la entidad emisora, a través de la infraestructura del sistema de pagos de bajo valor. (Definición contenida en el proyecto de decreto "Por medio del cual se modifica el Decreto 2555 de 2010 en lo relacionado con la regulación de las finanzas abiertas en Colombia y se dictan otras disposiciones".

[33] Las entidades vigiladas por la Superintendencia Financiera de Colombia podrán comercializar el uso, almacenamiento y circulación de los datos personales objeto de tratamiento, siempre que cuenten con la autorización expresa del titular de los datos y se dé estricto cumplimiento a las normas relacionadas con protección de datos y habeas data de las que tratan las leyes 1266 de 2008 y 1581 de 2012 (Idem).

esa industria, pero que podría quedarse corto en otros frentes de la prestación de servicios[34], como la de intermediación financiera. No obstante, este proyecto de ley fue archivado en el Congreso y es poco probable que surta su trámite en la nueva legislatura con nuevos Gobierno y Congreso a bordo.

La regulación y la supervisión, por lo tanto, son ejes fundamentales de análisis y no pueden ni deben ser excluidos de discusiones como las que se han dado en torno a responsabilidades y riesgos sistémicos. Es entonces pertinente señalar que, con miras a preservar dicha estabilidad y confianza necesarias para proteger el sistema financiero y los recursos que este administra, los focos que deben ser tenidos en cuenta por las autoridades responsables de esos temas son: (i) las posibles afectaciones sobre el sistema financiero y especialmente en su estabilidad por cuenta de los nuevos riesgos derivados de la implementación de tecnologías en la prestación de servicios financieros -afectando no solo a las nuevas compañías Fintech sino a los jugadores tradicionales-, y (ii) los posibles arbitrajes regulatorios que les den ventajas a ciertos competidores, tanto en lo que hace a requerimientos prudenciales -capital, modelos integrales de riesgo, etc.- como de cara a la responsabilidad frente a las normas de protección al consumidor -canales de atención PQR, defensor del consumidor, reportería a la SFC- y al riesgo de ciberseguridad -fugas o mal uso de la *data*-, poniendo en riesgo la competencia y la confianza en determinados servicios financieros.

En efecto, la disrupción que han causado las Fintech ha llevado a que se modifiquen las normas, pasando de un modelo pensado para la banca en su esquema tradicional a un nuevo modelo que aún no termina de inventarse y que debe admitir la participación de diversos jugadores, fomentando la innovación tecnológica, la disminución de los costos asociados a los servicios financieros y la cercanía con todos los consumidores. Esta nueva visión de la regulación tiene su efecto en la supervisión -y viceversa- como se ha observado en Colombia, donde incluso el impulso se ha dado más desde la órbita de la Superintendencia Financiera. Contener los riesgos propios de las nuevas tecnologías aplicadas a un sector híper regulado como lo es el financiero, requiere de un balance que permita seguir aprovechando los beneficios de estos productos y servicios, al tiempo que atrape los peligros que pueden representar, especialmente cuando estos escapan de la esfera de supervisión de la industria financiera. Aquí se requerirá un nuevo enfoque que tenga en cuenta las características únicas no solo de las pequeñas compañías Fintech sino de las BigTech -que, además de las ventajas antes mencionadas, se caracterizan por desarrollar múltiples negocios no financieros, lo que las convierte en actores muy heterogéneos a los ojos de las autoridades- y será necesario extender la visión prudencial a los efectos de la interconexión entre diferentes entidades, grupos de interés en los que se mueven todos los agentes relacionados y el sistema financiero en general[35]. Así mismo, hay que prepararse desde la perspectiva regulatoria y de supervisión cuando alguna de estas compañías Fintech tenga una escala cuya dimensión pueda generar riesgo sistémico o riesgo de desconexión.

3. Desafíos desde la regulación y supervisión prudenciales

Sin detenerse en el detalle de las corrientes que buscan definir el mejor modelo de regulación y supervisión a regir el mundo Fintech, en este aparte se busca identificar, primero desde

[34] PL- S337 de 2022.
[35] FSI Briefs No 12 Big techs in finance: regulatory approaches and policy options. Juan Carlos Crisanto, Johannes Ehrentraud and Marcos Fabian. March 2021.

lo macro y luego a un nivel más preciso, aquellos retos que enfrentan los supervisores y los riesgos propios o de contagio que están llamados a ser reconocidos en un régimen prudencial en el desarrollo de esta industria y su conexión con otras.

Tal vez el primer desafío para la regulación y supervisión local y transnacional está representado en la desaparición de las fronteras entre actividades financieras y no financieras por cuenta de las innovaciones tecnológicas y los nuevos modelos de negocio que han surgido del fenómeno Fintech. Si bien estas actividades se encuentran estrechamente relacionadas con el sector financiero, muchas veces se salen del límite regulatorio generando dudas acerca de quién debe ser vigilado y regulado, además de sobre quién cae la responsabilidad y la gestión de los riesgos que estas actividades implican. Esto se puede evidenciar en materia de pasarelas de pago, donde si bien los comercios y los mismos agregadores no están llevando a cabo ninguna actividad financiera, sí están generando unos riesgos en la medida que no cuenten con los estándares mínimos de ciberseguridad para proteger la información transaccional y de pagos.

Esta preocupación necesariamente lleva al siguiente desafío y es la contención del riesgo sistémico[36], tema sobre el cual ya no sólo existen voces que piden un reconocimiento expreso en el ámbito de la actividad financiera sino que con fuerza se empiezan a considerar como posibles focos de contagio global, tal como sucede en la actualidad con la proliferación de los criptoactivos[37] y los ecosistemas en los que se desarrollan, que claramente no tienen una localización geográfica ni un modelo de supervisión que se pueda señalar como el más adecuado.

De otro lado, confluyen una diversidad de autoridades alrededor de lo que mueve la industria Fintech aplicada o no a los servicios financieros, y en tal sentido resulta indispensable que trabajen de manera colaborativa en aras de sacar el mejor provecho de la innovación para los destinatarios finales. En la misma línea, surge la necesidad de que las autoridades incorporen el componente ético a los desarrollos digitales como un todo y de psicología comportamental, entendida esta como la forma de modelar el comportamiento de las personas a través de condicionamientos impuestos en los ambientes para conseguir unos resultados determinados, respetando la individualidad y la capacidad de toma de decisiones de los consumidores de estos desarrollos.

La coalición de competencias de distintas autoridades alrededor de un solo frente -en la era de la tecnología e innovación financiera- impone la necesidad de articulación y determinación de límites en los ámbitos gubernamentales; solo con un trabajo coordinado desde el Estado es posible identificar las dificultades a las que se enfrentan las autoridades para diseñar las normas en torno a estas nuevas formas de negocio -requiriendo coordinación entre todos los niveles del gobierno y los diferentes actores privados-, así como los esfuerzos para lograr que todos los actores del sector financiero y no financiero puedan innovar, garantizando la robustez que requiere el manejo de los recursos del público.

Ejemplo de ello es la creación de los *sandboxes* en distintos sectores que pueden o no estar interrelacionados, como es el caso del espacio controlado de pruebas de servicios

[36] El riesgo sistémico es el riesgo de contagio que se produce en una crisis financiera como consecuencia de su concentración en un determinado sector de la economía, pudiendo afectar directamente al resto de sectores productivos comprendidos en ésta. (https://economipedia.com/definiciones/riesgo-sistemico.html)
[37] Ver definición nota 12 de pie de página.

financieros[38], que inició y se mantiene en cabeza de la Superintendencia Financiera, en el que agentes no licenciados[39] fueron autorizados a montar pilotos de prestación de servicios propios de los vigilados al amparo del mismo supervisor financiero y con un régimen de constitución y otorgamiento de certificado de funcionamiento temporal, pero que podrían haber acudido a otro espacio como el que ha creado el Ministerio de Telecomunicaciones.

La Superintendencia Financiera ha venido implementando estrategias y herramientas para fomentar la innovación en la industria. En tal sentido, además de la definición de las reglas del sandbox, ha basado su gestión en: (i) fortalecer esquemas de transparencia en la supervisión, revelando abiertamente las expectativas que tiene sobre diferentes temas desde el principio; (ii) supervisión conductual[40] y Smartsupervision[41], protegiendo los derechos de los consumidores y permitiendo la movilidad entre productos-entidades; (iii) consolidación del esquema de supervisor único, construyendo una regulación homogénea y minimizando arbitrajes regulatorios; (iv) mayor eficiencia en el proceso de licenciamiento; (v) mayor y más eficiente revelación de datos, y (vi) cursos de educación financiera digital para una toma de decisiones óptima por parte de los diferentes actores[42].

4. Riesgos derivados del fenómeno Fintech

La expansión de las compañías Fintech se ha dado mediante desarrollos o pequeñas empresas enfocadas en prestar de manera especializada un servicio financiero específico -muchas veces de la mano de una entidad financiera tradicional que absorbe la carga regulatoria y los costos que implican las licencias correspondientes-. Este fenómeno se ha denominado el *unbundling* del sistema financiero -que consiste en separar las licencias para permitir el acceso no discriminatorio de competidores al mercado-, donde el concepto de multibanca, como el modelo a partir del cual se permite a unas entidades robustas -generalmente bancos- ofrecer, bajo el mismo techo, todos los servicios financieros, ha venido cambiando por el de pequeños negocios que ejecutan distintas operaciones financieras.

Si bien las compañías Fintech se han caracterizado por especializarse en un negocio financiero específico, no son ajenas a los distintos riesgos que deben enfrentar a la hora de realizar su negocio. El cuadro 1 resume brevemente qué tan expuestas se encuentran las compañías a los diferentes riesgos financieros considerando las actividades que realizan. Nótese cómo sobresale el riesgo operacional-cibernético que se muestra alto -en rojo- para todas las actividades por cuenta de la estrecha relación que tienen estas compañías con la innovación tecnológica.

[38] Mediante el Decreto 1234 de 2020, que reglamenta los objetivos, requisitos y etapas de funcionamiento del espacio controlado de prueba, se presenta por el Gobierno Nacional como una herramienta para promover la innovación en la prestación de los servicios financieros y para facilitar a las autoridades de supervisión y regulación la identificación de nuevos desarrollos financieros.

[39] Valga señalar que en Colombia las actividades financiera, bursátil, aseguradora y cualquier otra relacionada con el manejo, aprovechamiento e inversión de los recursos de captación a las que se refiere el literal d) del numeral 19 del artículo 150 son de interés público y sólo pueden ser ejercidas previa autorización del Estado.

[40] La manera en que las instituciones financieras protegen los intereses de los clientes, inversionistas y participantes del mercado en general en la equidad transaccional, el acceso a la información razonablemente simétrica y el mantenimiento de la confianza en la integridad del mercado. (Toronto center 2016).

[41] Software que permite la administración y gestión de PQRs que se radican por parte de los usuarios en las entidades del sector Financiero vigiladas por la Superintendencia Financiera de Colombia y que cumple con la normatividad vigente, Circular Externa 023 de 2021

[42] Jorge Castaño Gutiérrez, 2022, "La innovación como eje de crecimiento del sistema financiero". Superintendencia Financiera de Colombia.

Cuadro 1. Riesgos financieros para las actividades financieras de las Fintech

		Riesgos Financieros				
		Operacional cibernético	Reputacional	Modelo	Mercado	Crédito
Tipo de actividad financiera	Asesoramiento y gestión patrimonial	Alto	Medio	Medio	Alto	Bajo
	Finanzas personales	Alto	Alto	Alto	Bajo	Alto
	Lending	Alto	Medio	Medio	Bajo	Bajo
	Crowlending	Alto	Alto	Alto	Bajo	Bajo
	Equity Crowdfunding	Alto	Alto	Alto	Medio	Bajo
	Crowlending/crowdfunding sobre activos o bienes tangibles	Alto	Medio	Medio	Bajo	Bajo
	Servicios transaccionales o Divisas	Alto	Alto	Medio	Alto	Bajo
	Medios de pago	Alto	Medio	Medio	Bajo	Bajo

Fuente: Elaboración Bancolombia con base en "Los Riesgos Financieros de las Fintech" de Antonio Martín Holgado (2017).

En el presente capítulo se detallará de manera general por qué las compañías Fintech son vulnerables a los distintos tipos de riesgo, considerando la manera en la que operan; con ello se busca que sean claros los ajustes que se requieren desde la regulación, la supervisión y el control interno sobre este tipo de compañías, seguramente atendiendo el nivel de participación de cada agente en los ecosistemas que se van creando.

5. Riesgo operacional

El riesgo operacional es entendido como la posibilidad de que una entidad tenga pérdidas por deficiencias o fallas relacionadas con los recursos humanos, los procesos internos, la infraestructura tecnológica o incluso afectaciones externas como fallas de energía, conectividad, accidentes, entre otros. Como ya se indicó, en esta categoría se encuentran los riesgos cibernéticos relacionados con la estabilidad de las plataformas tecnológicas-digitales, la seguridad y manejo de la información y la operatividad de los sistemas internos. Por la importancia que estos riesgos cibernéticos representan para las compañías Fintech, en el presente documento las analizaremos en un capítulo independiente.

De otro lado, las compañías Fintech enfrentan riesgos operacionales similares a las entidades financieras tradicionales, entre los que vale la pena destacar:

• **Riesgo del modelo de negocio:** considerando la velocidad de la innovación digital en el negocio Fintech, muchas de estas compañías han desarrollado esquemas de negocio novedosos que, si bien parecen atractivos a primera vista, pueden no lograr los estándares mínimos de servicio -revelación de información a los clientes, calidad de los productos-, de cumplimiento regulatorio -violación de normas de tarifas o tasas de interés- o de revelación de información para los inversionistas.
• **Riesgos de prestación de servicio:** las compañías Fintech se han visto favorecidas por acelerados crecimientos derivados del éxito que han tenido en ofrecer productos y servicios financieros no tradicionales y con menores exigencias regulatorias y de supervisión. Sin embargo, dicho éxito ha implicado un rápido crecimiento de su base de clientes involucrando potenciales riesgos de que la compañía no tenga o no pueda consolidar rápidamente la infraestructura necesaria para proveer sus servicios de manera eficiente y segura. Esta situación se une de manera indisoluble con la capacidad económica, que es la mayor causa de fracaso de los emprendimientos que no logran conseguir el capital estable y recurrente que requieren para sostener el crecimiento de la operación. Estos detrimentos pueden no solo derivar en pérdidas económicas coyunturales o permanentes sino en pérdidas reputacionales donde los consumidores pierden confianza y, finalmente, con riesgo de posible pérdida de sus recursos en productos o servicios que pueden no favorecerlos en el largo plazo.
• **Riesgo de incumplimiento regulatorio:** las actividades realizadas por las compañías Fintech usualmente están reguladas de manera marginal y no están sujetas a una supervisión plena, por lo que requieren reforzar sus procesos de *Compliance -cumplimiento-*. El desarrollo de cualquier actividad debería involucrar no solo el envío de información marginal de su actividad a los reguladores sino la obligación de tener diferentes sistemas de gestión de riesgos, especialmente el relacionado con incumplimiento regulatorio cuando empiezan a entrar en terrenos que ameritan una supervisión estatal por comprometer los más altos objetivos del Estado, tales como la protección al consumidor, el uso de los recursos involucrados del público, cuando hay lugar a ello, etc. De ahí que sea necesario recoger la experiencia del pasado y exigir a estas empresas, como mínimo, modelos de reportería y de gestión de riesgos que cumplan con los estándares regulatorios de las entidades vigiladas.
• **Competencia-regulación global:** muchas compañías Fintech operan a través de las fronteras de múltiples países. Esto ha derivado en que deban enfrentarse tanto a riesgos de competencia con compañías existentes dentro de un país como a los desafíos regulatorios de operar en diferentes jurisdicciones.

6. Riesgos cibernéticos y de ciberseguridad

Como se indicó, los riesgos cibernéticos y de ciberseguridad hacen parte de los riesgos operacionales a los que se enfrentan todas las empresas, y de manera específica, tanto las entidades financieras tradicionales como las compañías Fintech. Sin embargo, este tipo de riesgos tiene particular importancia para las empresas de tecnología financiera por su estrecha relación con los procesos de innovación tecnológica para ofrecer servicios financieros -modelos avanzados de analítica de datos, apps, servicios de transferencias instantáneas, agregadores de datos[43], etc.-. Más aún, estos riesgos que inicialmente

[43] Los agregadores de datos son agentes cuya función consiste en recopilar información de cuentas u otra información de sitios web designados mediante el uso de los números de identificación personal de los titulares de la cuenta y, luego, poner la información de la cuenta de los usuarios a su disposición en un solo sitio web operado por el agregador a solicitud del titular de la cuenta.

se vinculan con temas de fraude o fuga de información merecen toda la atención, en la medida que pueden afectar las operaciones de las compañías Fintech; también tienen un efecto importante cuando se enfrentan a posibles vulneraciones a la privacidad y bienestar de los consumidores financieros, sobre todo si se tiene en cuenta que la prestación de estos servicios financieros está soportada principalmente en el uso masivo de datos[44], con consecuencias en materia de riesgos reputacionales para el sistema financiero en general.

Los principales riesgos cibernéticos y de ciberseguridad a los que se enfrentan las compañías Fintech son:

- **Seguridad informática:** considerando que muchas compañías Fintech ofrecen servicios de conectividad entre diferentes proveedores de productos y servicios financieros, son más vulnerables a brechas dentro de la cadena digital que pongan en riesgo sus operaciones, la información que manejan y los posibles recursos que administren.
- **Manejo de la información:** el uso de herramientas avanzadas de analítica de datos -*big data, machine learning*, IA, entre otras- se ha popularizado en el ecosistema Fintech usando información masiva para producir *scoring*[45], *matching*[46], asesoramiento de portafolios, Bots-CRM, entre otros. Sin embargo, dichas aproximaciones estadísticas pueden resultar discriminatorias para ciertos grupos poblacionales -raza, género, religión, entre otras- y generar afectaciones de tipo legal -posibles demandas por discriminación- y reputacional.
- **Fraude:** debido a la masificación de los servicios financieros digitales, las compañías Fintech deben enfrentar riesgos de suplantación de identidad, falsificación de documentos o esquemas de estafa organizados, que imponen la necesidad de mantener robustos esquemas de ciberseguridad y uso adecuado de las herramientas tecnológicas para prevenir la criminalidad financiera[47].
- **Manipulación del consumidor:** considerando la gran cantidad de información que manejan, muchas compañías Fintech podrían tener la capacidad de inducir a los consumidores a tomar decisiones financieras que no son óptimas como sobreendeudamiento, sobregastos o productos que no les generen valor. Todo esto puede derivar en riesgos legales y reputacionales para las compañías Fintech, así como efectos negativos en los consumidores financieros.

7. Riesgo de Lavado de Activos y Financiación del Terrorismo -LAFT-

Es la posibilidad de que una compañía sea utilizada para dar apariencia de legalidad a activos provenientes de actividades delictivas o para la canalización de recursos para actividades terroristas. Si bien las compañías Fintech han contribuido a la profundización financiera -especialmente en países en desarrollo-, por cuenta de la facilidad que ofrecen para acceder a los productos y servicios financieros, su masificación puede permitir que dichas infraestructuras sean aprovechadas como canales por quienes quieran ingresar dineros ilícitos al sistema financiero y a la economía de los países en general.

[44] Aurelio Gurrea, Nydia Remolina. Una aproximación regulatoria y conceptual a la innovación financiera y la industria Fintech. Pag. 164 Fintech, Regtech y Legaltech: Fundamentos y Desafíos regulatorios.
[45] Producción de puntajes crediticios mediante análisis estadísticos.
[46] Mecanismo de emparejamiento para reunir a diferentes actores para realizar alguna actividad juntos.
[47] Aurelio Gurrea, Nydia Remolina. Una aproximación regulatoria y conceptual a la innovación financiera y la industria Fintech. Pag. 164 Fintech, Regtech y Legaltech: Fundamentos y Desafíos regulatorios Pag. 367 y sgtes.

Esto, en países como Colombia, representa un reto de la mayor importancia, pues aun cuando los estándares internacionales se han aplicado rigurosamente a las entidades financieras tradicionales, lo que no podría pasar es que se abran espacios de conexión delincuencial so pretexto de generar mayor acceso e inclusión financiera.

8. Riesgo de crédito

Es la posibilidad de que una entidad incurra en pérdidas como consecuencia de que un deudor o contraparte incumpla sus obligaciones. Si bien el riesgo crediticio al que se enfrentan las compañías Fintech no dista mucho del que enfrenta el sector financiero tradicional, sí hay diferencias significativas en los mecanismos para mitigarlo. En efecto, dado que las compañías Fintech no pueden captar recursos de fondeo sin una licencia bancaria, tampoco deben cumplir con los requerimientos propios de la actividad financiera[48], con lo cual no es comparable la carga regulatoria y de supervisión a la que están sometidas frente a las entidades vigiladas y, por lo tanto, la exposición a las contrapartes tiene dimensiones diferentes.

La gestión del riesgo crediticio de este tipo de compañías debe basarse en: (i) esquemas de colocación organizados y estructurados para solo otorgar préstamos a personas con un perfil de riesgo que se ajuste a los estándares de la entidad, lo que no es tan claro en la actualidad, y (ii) un seguimiento y control a los créditos otorgados para poder cuantificar las posibles pérdidas y evitar situaciones de insolvencia o quiebra de las entidades y las consecuencias para los clientes. Ahora bien, la parametrización de las metodologías de asignación de crédito en esta industria podría terminar causando otros problemas, como la falta de personalización del producto. En efecto, si bien por cuenta de los análisis de riesgo automatizados se logra abaratar los modelos de oferta de productos, también puede llevar a desconocer la individualidad de cada persona y con ello generar discriminación o exclusión de alguna población.

9. Riesgo de mercado

Igual que para el sector tradicional, este riesgo consiste en la probabilidad de obtener una rentabilidad inferior de la esperada e incluso de pérdidas de capital como consecuencia de incidentes que cambian el valor de los productos que se administran, afectados por temas como el comportamiento de las tasas de interés, tipo de cambio, volatilidad, valoración de los instrumentos financieros, etc.

10. Riesgo reputacional

Es la posibilidad de pérdida o afectación de la reputación de una organización, de forma que afecte de manera negativa la percepción de ella en el entorno social. Este daño reputacional puede producir una pérdida directa o indirecta del valor de una compañía.

Debido a la juventud relativa del universo Fintech, estas compañías son particularmente susceptibles a este riesgo. De hecho, cualquiera de los diferentes riesgos que hemos analizado podría derivar en pérdidas generalizadas de confianza en las compañías. Además,

[48] Tales como, la obligación de constituir provisiones que soporten los riesgos de las operaciones activas, las cargas de capital y ponderaciones atendiendo los rubros en los que se mantengan los recursos del público (activos ponderados por nivel de riesgo) o los requerimientos de mayor solvencia asociados a tamaño de la entidad o importancia sistémica.

un episodio de riesgo reputacional puede conllevar un riesgo de contagio a otros actores y al sistema en el que actúen.

11. Riesgo sistémico

Es la posibilidad de que la falla de una entidad o grupo de entidades pueda causar un efecto en cascada, que impacte al sistema o mercado en su totalidad. Si bien por el momento no existe una compañía Fintech que se considere que pueda causar un daño masivo del mercado, el ecosistema Fintech en su totalidad sí representa una serie de riesgos que puede afectar a todo el sistema financiero.

En primer lugar, si bien las Fintech se desarrollaron rápidamente durante la década posterior a la crisis financiera de 2007-2008, este crecimiento se vio favorecido por un contexto de indicadores generales de las economías de los países de elevada liquidez y posturas de política monetaria expansivas[49]. Sin embargo, las condiciones en el mundo han cambiado, y ahora deben enfrentar contextos menos favorables como las políticas monetarias globales, las presiones inflacionarias derivadas de la guerra Ucrania-Rusia, la crisis global de logística y los bloqueos en la cadena de suministros de China producto de la pandemia del COVID-19.

El comportamiento de las compañías Fintech en este período de desaceleración económica global resulta incierto. Por lo tanto, se deberán probar: (i) los sistemas de gestión de riesgo de estas compañías, con escenarios de pérdidas de demanda, mayor morosidad y volatilidad en los instrumentos financieros; (ii) la capacidad de continuar generando utilidades ante mayores presiones regulatorias, consecuencia de posibles eventos en la parte descendente del ciclo económico, y (iii) la susceptibilidad de estas compañías al efecto contagio del sector financiero tradicional, es decir, a verse afectadas por otros actores o industrias en las que se mueven y la posible pérdida de valor o de atractivo de sus productos y servicios, que en otros momentos podrían resultar optimistas o pesimistas de manera excesiva, generando consecuencias exageradas.

Adicionalmente, los esquemas de negocio de algunas Fintech pueden resultar en mayor riesgo sistémico. Por un lado, los negocios estructurados alrededor del *Open Banking*[50] podrían derivar en una mayor volatilidad en el comportamiento de los clientes, incluso con riesgos de corridas bancarias. Asimismo, los modelos de negocio de robo-advisoring[51] podrían incrementar los riesgos de contagio en periodos de estrés financiero[52].

12. Riesgos derivados de las BigTech

Dada la capacidad de penetración de los grandes de la tecnología, es relevante dedicar un espacio a este tipo de compañías, pues aunque en la actualidad los servicios financieros siguen siendo marginales dentro del desarrollo del objeto social de los negocios que ofrecen

[49] También conocida como fase de recuperación, en referencia a una economía y el ciclo económico, es el fenómeno que experimenta una economía determinada, mediante el que la economía comienza a crecer en base a determinados factores (https://economipedia.com/definiciones/expansion-economica.html).
[50] Mirar nota 27 de pie de página.
[51] Modelo de gestión y administración de inversiones automatizado. Un Robo Advisor es un tipo de asesor financiero que ofrece un servicio de gestión online de carteras de inversión mediante algoritmos, automatización y, normalmente, la supervisión de un equipo de expertos inversores. Los robo advisors hacen más fácil crear carteras de inversiones personalizadas para cada persona y adaptadas a sus posibilidades.
[52] Pagnottoni P. y Polinesi G. (2019), "Network models to reduce robo advisory market risk", Working Paper, 2019.

las BigTech, el potencial para incrementar su participación en el sistema financiero de manera acelerada es un riesgo advertido, en la medida en que su posicionamiento se soporta en las autorizaciones de uso de los datos de sus usuarios y, a partir de ello, de los demás agentes que vía la apertura de datos[53] pueden expandir servicios de pago, crédito y otros, todos ellos puntos de partida que pueden llegar a dificultar todavía más la labor de regulación y supervisión financiera.

En efecto, las BigTech tienen múltiples frentes de negocio -la mayoría con alcance transnacional-, conocen muy bien cómo funciona la psicología comportamental y son tal vez los más expertos en analítica de datos e inteligencia artificial. Eso impone a los reguladores el desafío de empezar por comprender su modelo de negocio, cómo se interconecta en todos sus frentes con múltiples agentes de distintas jurisdicciones y la manera en la que las diferentes líneas de negocio pueden derivar en riesgos que podrían contagiar sectores y que merecen ser gestionados. De ahí que lo primero sea entender (i) el efecto de estas compañías de cara a los riesgos específicos del sector financiero ya mencionados -crédito, liquidez, apalancamiento, operacional etc.-, que seguramente podrían ser gestionados con la misma regulación del sector financiero tradicional, que se relacionará más adelante; (ii) la interconectividad de las BigTech con pequeñas compañías, dado que un choque a las primeras podría llegar a tener efectos sobre las segundas, y (iii) el riesgo sistémico, si se considera que muchas de las grandes tecnológicas prestan su infraestructura al sector financiero, de modo que una falla en sus operaciones podría implicar un colapso de estas entidades tradicionales. Además, la heterogeneidad de las compañías BigTech genera dificultades que no se miden cuando se piensa en los objetivos de política pública y tampoco se tienen en cuenta para poder definir un esquema regulatorio específico.

Con miras a lograr una normatividad efectiva de este sector se han propuesto diferentes enfoques[54]:

- **Generar una mezcla de regulación por actividad y por entidad:** si bien tradicionalmente las entidades que realizan una misma actividad se enfrentan al mismo tipo de riesgos, para el caso de las BigTech esto puede no resultar cierto por sus múltiples líneas de negocio y su importancia como proveedor de infraestructura. Con eso en mente, si bien las licencias por actividad darían una primera guía de los requerimientos para estas entidades, es necesario complementarlas con reglamentos específicos para que cada entidad pueda gestionar adecuadamente los riesgos financieros a los que se enfrenta.
- **Generar un enfoque de política específico para las Fintech:** dada su creciente participación no solo en los negocios financieros sino en todas las actividades económicas, hay quienes consideran prudente diseñar esquemas de política que regulen tanto la participación BigTech en el sector financiero como en otros sectores económicos -teniendo en cuenta su creciente importancia sistémica-. Esta propuesta no es excluyente con la de regulación por actividad y por entidad, pero permite que comience a construirse a partir de las reglas planteadas para los conglomerados financieros u otras que busquen medir los riesgos de partes relacionadas o conectadas, atendiendo el nivel de penetración individual.
- **Mejorar la cooperación local e internacional:** dado el alcance internacional de

[53] Mirar nota 27 de pie de página.
[54] Crisanto Juan Carlos, Ehrentraud Johannes y Fabian Marcos (2021), Big-Tech in finance: regulatory approaches and policy options, FSI Briefs.

las operaciones de las BigTech, se vuelve fundamental trabajar en esquemas regulatorios y de información que reúnan múltiples jurisdicciones y países para vigilar conjuntamente estas entidades.

13. En resumen

Hemos visto cómo el ecosistema financiero como un todo está atravesando por significativos cambios debido a la potencialización de las nuevas tecnologías en la prestación de servicios financieros, bajo el denominado fenómeno Fintech. La primera etapa de este fenómeno fue el surgimiento de pequeñas compañías tecnológicas -*startups*- que mediante diversas innovaciones tecnológicas comenzaron a prestar servicios financieros especializados con mayor atractivo para los clientes.

Si bien en principio se creía que las Fintech iban a ser competidoras del sector financiero tradicional, los elevados requisitos y costos regulatorios para poder ofrecer los servicios financieros llevaron a que estas compañías se volvieran aliadas de los incumbentes. Estas alianzas han permitido que las entidades tradicionales adquieran una nueva línea de ingresos por medio de habilitar canales para que las Fintech presten servicios financieros sin necesidad de adquirir una licencia propia.

Posterior al surgimiento de las *startups*, se ha evidenciado cómo, en lo que se podría denominar una segunda etapa del fenómeno Fintech, las grandes compañías tecnológicas -las denominadas BigTech- se han interesado en prestar servicios financieros. Estas compañías parecerían representar mayores riesgos para las entidades tradicionales por cuenta de sus ventajas comparativas en materia de disposición de datos masivos, desarrollos tecnológicos, alcance comercial y capitalización de bajo costo; sin embargo, nuevamente las elevadas cargas regulatorias que ha implicado la implementación de Basilea-III han llevado a que estas compañías busquen alianzas con los incumbentes -similar a las compañías Fintech de menor tamaño-.

Si bien las entidades tradicionales continuarán jugando un papel importante en el sector financiero, la proliferación de las compañías Fintech y BigTech no deja de representar importantes desafíos para el sistema y, por lo tanto, para los responsables de las políticas públicas y de la supervisión de estas actividades. En efecto, estas compañías que tienen como fin incursionar en los negocios financieros siguen construyendo los esquemas de gestión de riesgos necesarios -especialmente en materia de ciberseguridad, donde los modelos innovadores continúan evolucionando tanto en su operación como en la manera de gestionar los riesgos correspondientes- para prevenir pérdidas en sus operaciones y, más aún, preservar la confianza y estabilidad del sistema financiero como un todo.

La participación en el sistema financiero de las compañías Fintech y BigTech todavía no resulta significativa frente a las entidades tradicionales; no obstante, el balance del sistema financiero sí puede verse afectado por cuenta de una pérdida generalizada de confianza que provenga del ecosistema Fintech. Justamente, la rápida proliferación de estos nuevos esquemas de negocio, que ha logrado incrementar la profundización financiera, también puede ser un arma de doble filo en caso de tener fallas que puedan dañar la percepción de los consumidores, con efectos negativos que también afecten a los jugadores tradicionales y potencialmente generando efectos sistémicos.

Todo esto se vuelve más preocupante si se considera que las Fintech existen recientemente y que han tenido más de diez años de un favorable ambiente macrofinanciero con reducidas tasas de interés, abundante liquidez y favorable crecimiento económico y financiero. Todo esto ha generado inquietudes sobre cuál será el comportamiento de las Fintech en esta nueva etapa del ciclo económico, en la que los bancos centrales del mundo comienzan a elevar sus tasas de interés para enfrentar la creciente inflación global con cada vez mayores señales de una recesión global.

Por todo esto la regulación alrededor del ecosistema Fintech no puede ser desatendida ni delegada sólo en las entidades tradicionales. Son muchos los riesgos que ya se han mapeado en torno a lo que puede implicar el descalabro de entidades tipo Fintech, bien sea por el daño directo que producen a sus clientes o usuarios, o por la posibilidad de contagiar a otras entidades y con ello afectar la estabilidad financiera y la eficiencia del propio sector financiero y de los recursos del público que puedan verse involucrados.

Bibliografía

ASBA y BID Lab. Consideraciones de Regulación y Prácticas de Supervisión para las Innovaciones Tecnológicas Financieras. Junio, 2020.

Asobancaria, Semana Económica 2018, Edición 1122.

BIS. Sound Practices: implications of fintech developments for banks and bank supervisors. Febrero 2018.

Castaño Gutiérrez, Jorge. Intervención Foro LR 'Fintech-Microfinanzas' (2021).

Castaño Gutiérrez, Jorge, 2022, "La innovación como eje de crecimiento del sistema financiero". Superintendencia Financiera de Colombia.

Crisanto, Juan Carlos; Ehrentraud, Johannes y Marcos, Fabián (2021), Big-Tech in finance: regulatory approaches and policy options, FSI Briefs.

Decreto 1234 de 2020.

Decreto 1357 de 2018.

Dr. González Vega, Claudio. Academia de Centroamérica, 2019.

Gurrea Martínez, Aurelio; Remolina, Nydia. Fintech, Regtech y Legaltech: Fundamentos y desafíos regulatorios. 2020.

Gurrea Martínez, Aurelio; Remolina, Nydia. Una aproximación regulatoria y conceptual a la innovación financiera y la industria Fintech. Pg. 164 Fintech, Regtech y Legaltech: Fundamentos y Desafíos regulatorios.

Gurrea Martínez, Aurelio; Remolina, Nydia. Una aproximación regulatoria y conceptual a la innovación financiera y la industria Fintech. Pg. 164 Fintech, Regtech y Legaltech: Fundamentos y Desafíos regulatorios Pg. 367 y sgtes.

Financial Stability Board. Financial Stability Implications from Fintech. Junio de 2017.

FSI Briefs No 12 Big techs in finance: regulatory approaches and policy options. Juan Carlos Crisanto, Johannes Ehrentraud and Marcos Fabian. March 2021.

https://cloud.google.com › learn › what-is-cloud-computing. https://economipedia.com/definiciones/expansion-economica.html

https://economipedia.com/definiciones/expansion-economica.html

https://economipedia.com/definiciones/riesgo-sistemico.html

https://pmi-americas.com/es/el-boom-de-los-neobancos-en-latinoamerica-una-oportunidad-historica-para-crecer-es/

https://www.2.deloitte.com/mx/es/pages/dnoticias/articles/open-banking-y-sus-beneficios.html

https://www.xataka.com/basics

Leyes 1266 de 2008 y 1581 de 2012.

Lavalleja, M., "Panorama de las Fintech: principales desafíos y oportunidades para el Uruguay", serie Estudios y Perspectivas-Oficina de la CEPAL en Montevideo, N° 48 (LC/TS.2020/53; LC/MVD/TS.2020/3), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.

Pagnottoni P. y Polinesi G. (2019), "Network models to reduce robo advisory market risk", *Working Paper*, 2019.

PL- S337 de 2022.

Real Risk, 2022.

Toronto Center 2016.

CAPÍTULO 9

La protección al consumidor financiero en la era digital

Eduardo Arce Caicedo[1]

Resumen

La digitalidad, ajena al contacto físico y personal en que se dictaron inicialmente las normas de protección al consumidor financiero, fomenta decisiones que deben tomarse en segundos. La comodidad para tomar las decisiones y el menor tiempo que se destina a ejecutarlas son elementos determinantes en el mundo digital y en la experiencia del consumidor. Pero al mismo tiempo incrementan los riesgos y retos, como que el producto para el ahorrador no sea el adecuado o que se efectúen inversiones ajenas al perfil de riesgo. Se aumenta la vulnerabilidad frente a la delincuencia informática y la probabilidad de ser víctima de sofisticados esquemas en los que se manipula al consumidor para obtener su información y hacerlo víctima de fraudes. Hay avances importantes en la cultura y la regulación, pero debe permitirse a ciertos consumidores financieros –los más vulnerables- el acceso a mecanismos que hagan realidad sus derechos, sin poner en riesgo la estabilidad del sistema.

[1] Vicepresidente Jurídico del Banco Agrario. Candidato a Doctor de la facultad de Ciencias Jurídicas de la Pontificia Universidad Javeriana. Profesor de pregrado de esa universidad y de postgrado de la Universidad del Rosario y de la Universidad de la Sabana.

1. Introducción

El discurso del presidente John F. Kennedy en 1962, en el que pronunció la célebre frase *Consumidores somos todos*, impulsó la adopción de medidas legislativas integrales dirigidas a la protección de consumidor y, por lo tanto, la elaboración de un conjunto de principios y reglas con ese propósito[2]. Sin embargo, las conductas y prioridades del consumidor de 1962 no son las mismas que las del consumidor de 2022. Las diferencias en los hábitos e intereses del consumidor imponen modificar las normas que lo protegen.

Las primeras normas se expidieron en entornos de presencialidad física e interrelación directa entre seres humanos, con mensajes diseñados y elaborados para ese ambiente. La virtualidad es ajena a ese contacto físico y personal. El entorno virtual fomenta decisiones rápidas, tomadas en segundos, que excluyen desplazamientos físicos y comunicaciones por medios tradicionales. La comodidad para ejecutar las decisiones y el menor tiempo que se destina a hacerlas efectivas son elementos determinantes para el consumidor actual.

Otro elemento introducido por la virtualidad es la participación de nuevos actores no vigilados por la Superintendencia Financiera que ofrecen servicios de pagos, transferencia, negociación de divisas, obtención de préstamos y hasta financiación a inversionistas particulares, entre otros. Las similitudes, afinidad y complemento con servicios prestados por la banca tradicional imponen el examen de la regulación y nuevos retos para la protección del consumidor financiero en esos ámbitos.

A la par de esas realidades, la categoría inicial de consumidor ya no es única. Dependiendo de sectores y mercados, las reglas generales se complementan y adicionan con disposiciones especiales. Ese es el caso del sector financiero donde el consumidor se relaciona con profesionales a quienes confía sus recursos excedentarios y acude a ellos cuando se encuentra en situación deficitaria. Parafraseando a Rengifo cuando dice que *(e)l propósito del derecho del consumo es hacer que los mercados sean confiables para aquellas personas que no son profesionales en el ejercicio del comercio*[3], afirmamos que el propósito del derecho del consumo financiero es hacer confiable el sistema financiero para aquellos que no son actores profesionales en él.

Con base en los anteriores supuestos, se describirá en primer lugar la regulación vigente de protección al consumidor financiero[4]. Posteriormente se presentarán los riesgos que traen consigo las nuevas tecnologías. Riesgos que, desde la perspectiva jurídica, deben ser considerados no solo por la regulación sino por todas las entidades que participen en alguna transacción en la que intervenga un consumidor financiero. A partir del énfasis que se hace en dos de esos riesgos se soportan las reflexiones y conclusiones que constituyen la parte final de este ensayo.

El objetivo primero es, entonces, reflexionar en torno a la conveniencia y necesidad de

[2] El discurso pronunciado ante el Congreso de los Estados Unidos formuló cuatro derechos de los consumidores: el derecho a la seguridad, a la información, a elegir y a ser oído. Allí se propusieron al Congreso y luego fueron adoptadas medidas de protección en la alimentación y la medicación, transporte y protección financiera.

[3] RENGIFO G, Mauricio, "Derecho del Consum: Problemas y Conceptos fundamentales". En VARON P., Juan Carlos, RENGIFO G, Mauricio, PEÑA B, Fernando, Derecho del Consumo. Tomo I. Introducción al Derecho del Consumo" Universidad de los Andes, 2022, p. 16. http://dx.doi.org/10.15425/2017.529.

[4] El literal d) del artículo 2º de la ley 1328 define al consumidor financiero como todo cliente, usuario o cliente potencial de las entidades vigiladas.

ampliar el concepto legal de consumidor financiero y la posibilidad de que se extiendan a esos nuevos actores no vigilados las reglas de protección y la jurisdicción a las que están sometidas las entidades vigiladas por la Superintendencia Financiera. En el mismo sentido, también se propone examinar la conveniencia, tanto para los incumbentes como para las entidades no vigiladas, de nuevas reglas y conductas acorde con su nivel de participación en las transacciones de los consumidores.

Una acotación previa es necesaria. El texto versa sobre aspectos puntuales de la protección del consumidor financiero –ahorrador, deudor, inversionista– en el sistema financiero, pero por su extensión y propósito no se pretende describir cada una de las manifestaciones y operaciones del mercado intermediado[5] y desintermediado[6] que se pueden desarrollar en entornos virtuales. Presentar las particularidades, describir las posibles innovaciones tecnológicas y proponer medidas de protección para cada una de ellas exigiría una extensión y un detalle que exceden el objetivo planteado. En ese orden de ideas, solo se hará referencia a la protección del consumidor financiero en el marco de algunas operaciones y a partir de ellas se formularán los comentarios y reflexiones que se proponen al lector.

2. Marco normativo de la protección al consumidor financiero

El primer marco de protección integral al consumidor se promulgó en el año 1981 mediante una ley[7] que fijaba los parámetros de la intervención estatal en la distribución de bienes y servicios para la defensa del consumidor. Posteriormente, en ejercicio de facultades extraordinarias se dictaron normas[8] relativas a la idoneidad, la calidad, las garantías, las marcas, las leyendas, las propagandas y la fijación pública de precios de bienes y servicios, así como a la responsabilidad de sus productores, expendedores y proveedores. En esas disposiciones el énfasis estaba puesto en las transacciones de compraventa de bienes y no había referencias al mercado o la contratación financiera.

Reglas específicas de protección al consumidor financiero se encuentran en el Estatuto Orgánico del Sistema Financiero[9], dirigidas a garantizar decisiones informadas tanto en la elección de la entidad financiera como en las transacciones, productos o servicios ofrecidos, lo que pretende corregir la asimetría de información entre el profesional -la entidad financiera- y el consumidor, que termina por afectar el correcto funcionamiento del mercado.

Posteriormente, en julio de 2009 se dictó la ley[10] que, entre otros aspectos, consagra el régimen de protección al consumidor financiero. No es el objeto de este trabajo describirlo, pero sí enfatizar algunos de sus elementos más relevantes, así: (i) la noción amplia de consumidor financiero, que incluye personas jurídicas y abarca no solo a los clientes sino también a los usuarios y clientes potenciales de las entidades vigiladas; (ii) la extensa y

[5] Mercado intermediado es aquel en el que instituciones captan los excedentes de liquidez de los ahorradores, para luego trasladarlos a los sujetos que los requieren -deficitarios– mediante contratos de mutuo o préstamo.
[6] Mercado desintermediado es aquel donde los sujetos deficitarios – los que requieren recursos- los obtienen directamente de los sujetos superavitarios- inversionistas-.
[7] Ley 73 de 1981.
[8] Decreto 3466 de 1982.
[9] Artículo 72 sobre información al público y obligaciones en la materia, Numeral 1 del artículo 97 sobre información de servicios prestados, Los numerales 1 a 3 del artículo 98 sobre reglas generales de competencia, los numerales 4.2 a 4.4. del mismo artículo sobre Defensor del Consumidor Financiero, Artículo 99 relativo a la publicidad y promoción al consumidor mediante incentivos.
[10] Ley 1328 de 2009.

detallada relación de derechos de los consumidores y de obligaciones concretas de los profesionales. Entre los derechos de los consumidores se encuentra el de exigir la debida diligencia y recepción de los servicios y productos que adquiere, y entre las obligaciones de los profesionales la de prestar los servicios y entregar los productos en las condiciones ofrecidas, y (iii) otros elementos destacables como la existencia de un sistema de atención al consumidor financiero, reglas relativas al defensor del consumidor financiero y la descripción de prácticas y condiciones abusivas y requerimientos puntuales sobre cumplimiento del deber de información.

En el año 2011 se dictó el Estatuto del Consumidor[11] que estableció derechos y deberes, así como definiciones relevantes y disposiciones sobre responsabilidad, garantías e información que modificaron totalmente el entendimiento de la relación de consumo. De hecho, y para efectos de este ensayo, el capítulo VI resulta relevante porque establece preceptos puntuales para la protección del consumidor en el ámbito del comercio electrónico. Uno de los aportes más importantes fue la atribución de facultades jurisdiccionales a la Superintendencia Financiera, que en la práctica ha representado significativos avances tanto en la celeridad de los procesos iniciados por los consumidores contra las entidades como en la protección efectiva de sus derechos.

Resulta llamativo que la norma especial de protección al consumidor financiero sea anterior a la norma general de protección al consumidor. Sin embargo, esta situación no es problemática, pues el mismo Estatuto del Consumidor indica que si existe regulación especial, como es el caso de la actividad financiera, se aplicará esta.

A este conjunto de normas legales se unen las instrucciones de la Superintendencia Financiera en la Circular Básica Jurídica. La Superintendencia ha desarrollado las reglas generales y establecido condiciones puntuales en materia de Sistema de Atención al Consumidor, de Defensoría del Consumidor y de presentación de quejas. De igual manera, ha dictado instrucciones en materia de programas publicitarios, información que se debe suministrar al consumidor, condiciones de gestión de cobranza y conductas que configuran cláusulas y prácticas abusivas. También ha establecido instrumentos de supervisión como Smartsupervision y el White Paper sobre supervisión del riesgo de conductas. El primero ha sido concebido como un desarrollo tecnológico que permite a la Superintendencia contar con información oportuna y actualizada sobre la gestión de las quejas o reclamaciones interpuestas por los consumidores financieros ante las entidades vigiladas, el Defensor del Consumidor Financiero y esa misma entidad[12]. El segundo introduce el análisis de riesgos de conducta de las entidades vigiladas en materia de protección del consumidor financiero. Es decir, que se revisarán las acciones u omisiones en orden a garantizar un trato justo de los consumidores financieros.

Todo este conjunto de normas corresponde a técnicas que particularizan el derecho financiero[13]. Las normas de carácter legal son generales y amplias y permiten la concreción y adaptación por parte del regulador y del supervisor a las cambiantes preocupaciones

[11] Ley 1480 de 2011.
[12] Circular Externa 021 de 2021.
[13] "El sistema financiero está gobernado por un sistema de normas que se ha clasificado como Derecho regulativo, cuyas características son: es un derecho flexible que responde relativamente más rápido a los cambios en el contexto, producto por ejemplo, de las innovaciones tecnológicas; es un derecho "administrativizado" en tanto es dictado por el Gobierno en la delimitación y marco que le otorga el Congreso como instrumento para responder a la dinámica del sector financiero. BLANCO-BARÓN, Constanza. La protección del consumidor financiero en la era digital: retos para los reguladores. (en línea). Bogotá. Universidad Externado de Colombia, 202133 páginas ISBN 9789587905847. P 657 (Fecha consulta: 22 de julio 2022).

sociales y económicas[14]. En ese orden de ideas, la relación de disposiciones que hemos presentado refleja la casi inexistente preocupación por el consumidor financiero a finales del siglo pasado y el creciente interés e importancia que el tema desarrolló desde esa época hasta ahora.

La realidad de hoy es que el consumidor financiero se ha convertido en factor relevante para las autoridades que desarrollan la intervención estatal en el sistema financiero. Relevancia que ha adquirido como sujeto fundamental de las economías de libre mercado y también por el impacto mediático y político que tienen las situaciones y acciones que vulneran sus derechos.

3. Los riesgos de los entornos virtuales

La normatividad citada estaba lejos de concebir un mundo de apps, Fintech y *startups* tecnológicos. Es decir, que no estaban en el perímetro de sus preocupaciones los recién aparecidos servicios financieros digitales -DFS, por sus siglas en inglés- y mucho menos los desarrollos de los *smartphones*. Lo que sí fue considerado ayer por el legislador y hoy debe seguir siéndolo es la existencia de elementos que modifican e influencian la voluntad del consumidor.

Dicho de otra forma, con independencia de que sea entorno presencial o virtual, el derecho del consumo tiene en cuenta el proceso a través del cual el consumidor toma decisiones. La teoría económica clásica parte del supuesto de que las decisiones del consumidor son racionales pues se producen en un *marco de acción racional –rational action framework–* también llamado marco de elección racional *–rational choice framework–*. El supuesto es que los seres actúan libremente, determinados solo por sus intereses y deseos sin ningún tipo de influencia o presión ajenas a su propia voluntad[15]. En ese escenario la persona toma, siempre que esté bien informada, las decisiones que más le convienen, es decir, las que le producen el mayor beneficio económico. Sin embargo, estudios posteriores[16] han demostrado que en ciertas circunstancias el consumidor toma su decisión con base en sesgos cognitivos. Los sesgos son impulsos o motivaciones inconscientes que alteran el entendimiento de

[14] La intervención del estado en el sistema financiero se da mediante lo que la Corte Constitucional ha denominado "reparto competencial". Al Congreso, le corresponde dictar leyes que fijan pautas u objetivos generales – Leyes marco -. El Gobierno Nacional de una parte ejecuta "de manera permanente la necesaria intervención sobre tales actividades, adoptando, con cierta regularidad, las medidas que considere apropiadas para dar cabal desarrollo a los contenidos legales". A eso llamamos regulación. Finalmente a la misma rama ejecutiva, a través de la Superintendencia Financiera, le corresponde ejercer la inspección y vigilancia sobre los actores del sistema financiero. Ver Sentencia C-909 de 2012. Magistrado ponente Nilson Pinilla.

[15] "El marco de referencia para el análisis del comportamiento económico como comportamiento racional suele denominarse "marco de acción racional" (MAR, en inglés rational action framework) o "marco de elección racional" (MER, en inglés rational choice framework"). Este marco supone la existencia de sujetos libres, es decir capaces de tomar decisiones sin estar bajo coerción, racionales (en el sentido de poseer preferencias coherentes, dotadas de irreflexibilidad y transitividad) y que, actúan en función de sus preferencias, es decir en función de sus propios deseos o intereses y no en función de otras consideraciones" (Maleta, 2010)" Citado por HERNÁNDEZ RECHE, Vicente. El sesgo de decisión en la inversión financiera. 2017., https://www.tesisenred.net/handle/10803/457889#page=1 (last visited May 25, 2022).

[16] El hito en la materia lo marca el *paper* de Kahneman y Tverski (1974) Judgement under uncertainty: Heuristic and Biases. Sobre ese texto comentan Cortada y Macbeth "El núcleo de las ideas del programa de heurística y sesgos es que el juicio bajo incertidumbre se basa a menudo en una cantidad limitada de conceptos heurísticos simplificadores, más bien que en un procesamiento algorítmico más formal y extensivo. Véase con algún detalle esto. Los procedimientos utilizados en la resolución de un problema pueden ser por algoritmos o por heurísticos. Los algoritmos (viene de guarismo = cantidad y es una alteración por influjo del griego arithmós) son estrategias que garantizan la solución. Por ejemplo, un algoritmo son las reglas para realizar una división cualquiera de dos números, es decir lo que haríamos para dividir 240/30. Está garantizado que estas reglas nos darán un resultado indefectiblemente correcto. Los procedimientos heurísticos en cambio, (de heuriskó, yo hallo, descubro, en griego) (Corominas, 1973) son procedimientos que proveen ayuda en la solución de un problema, pero no de manera justificada: son juicios intuitivos, que se basan en el conocimiento parcial, en la experiencia o en suposiciones que a veces son correctas y a veces erradas, no existe una seguridad absoluta y lógica, sobre los mismos" CORTADA DE KOHAN, Nuria; MACBETH, Guillermo. Los sesgos cognitivos en la toma de decisiones. [en línea]. Revista de Psicología, 2(3). Disponible en: http://bibliotecadigital.uca.edu.ar/repositorio/revistas/sesgos-cognitivos-toma-de-decisiones-kohan.pdf.

la información de la que dispone el consumidor[17]. Estos sesgos producen decisiones que resultan inconvenientes -no racionales para el consumidor- y pueden ser aprovechados e incluso generados por los oferentes de productos o servicios.

Ahora bien, estos sesgos que se habían identificado en la presencialidad física también se presentan en el entorno digital. De hecho, en este último su ocurrencia podría ser más probable por factores tales como la imposibilidad del consumidor de procesar toda la información que se suministra digitalmente, lo visualmente atractivas que resultan ciertas opciones y la celeridad que concreta la operación con un simple clic. Lo dicho significa que en el entorno digital el consumidor podría tomar decisiones que no le resulten provechosas y que, por el contrario, terminen por afectarlo.

Sin mencionar expresamente el concepto de sesgo cognitivo, un documento del año 2020 elaborado por la Asociación de Supervisores Bancarios de América -ASBA- y el Banco Interamericano de Desarrollo -BID- relaciona una serie de situaciones que pueden afectar al consumidor financiero en el entorno digital, tales como la dificultad de acceso a productos y servicios financieros por parte de quienes no tienen los medios tecnológicos o la formación para usarlos, el riesgo de malas decisiones por la inmediatez y celeridad que impone la digitalidad y la dificultad de identificar e interactuar con la población vulnerable. Otras situaciones que según el documento podrían afectar al consumidor son la información equívoca o insuficiente, la presentación poco clara de los costos de los servicios, el uso de términos técnicos complejos y el desconocimiento del funcionamiento de la tecnología. Además de ellas, entre otras situaciones vinculadas con la idoneidad de productos y servicios se menciona el ofrecimiento de productos que no corresponden a las necesidades de los consumidores, o que les resultan excesivamente costosos o innecesarios, así como las asociadas a la ciberseguridad, el fraude y el robo de datos del consumidor financiero.

Un método diferente para identificar los riesgos relacionados con la protección del consumidor en el entorno virtual es el empleado por Tsany Ratna Dewi[18]. Para esta autora, los temas centrales de la protección del consumidor financiero se relacionan con la asimetría de información, el analfabetismo financiero, el comportamiento y las prácticas abusivas de las empresas, el lenguaje de los contratos de adhesión, los riesgos de los avances tecnológicos y la estructura de gobierno de los proveedores de servicios financieros digitales.

Las diferencias entre los listados no esconden las coincidencias en los aspectos esenciales y el hecho de que hay una variedad de situaciones que en el entorno digital podrían afectar al

[17] García- Tejeda Enrique (2020) trae una síntesis tanto de los postulados de la decisión económica racional como de los elementos de la racionalidad limitada: "El surgimiento de la economía conductual en el campo de la economía modificó la concepción del comportamiento racional. La aplicación de estos nuevos fundamentos de la economía conductual al derecho provino de la investigación de Jolls, Thaler y Sunstein. Estas investigaciones han mostrado que, en determinadas circunstancias, las personas observan una conducta diferente a la postulada por el modelo de racionalidad clásica en el derecho y la economía. Las principales características son: a) Racionalidad limitada: en lugar de utilizar una capacidad ilimitada de razonamiento sobre la información que poseen, las personas utilizan atajos heurísticos para tomar decisiones. b) Fuerza de voluntad limitada: las personas toman decisiones en que los costos son mayores a los beneficios, en el largo plazo. c) Interés propio limitado: las personas son más amables, menos competitivas y se comportan de forma altruista y cooperativa más allá de la predicción del modelo de racionalidad clásica". GARCÍA-TEJEDA, Enrique. ¿Alguien quiere una rebanada de pizza? Los sesgos cognitivos en la contratación de servicios digitales: el punto ciego de la regulación en México. Latin American Law Review, 2021, no 6, p. 175-194.

[18] DEWI, Tsany Ratna. The Promise and Perils of Digital Finance: Toward Financial Inclusion and Smart Consumer Protection. *University of Luxembourg Law Research Paper*, 2022, no 2022-002, Available at SSRN: https://ssrn.com/abstract=4095330 or http://dx.doi.org/10.2139/ssrn.4095330

consumidor de diversas formas[19]. Es decir, que el consumidor puede tomar decisiones que económicamente resulten contrarias a sus intereses, impulsadas por los sesgos cognitivos estimulados o aprovechados por un entorno virtual. Decisiones, en fin, que no le resultan convenientes y que además terminan por alterar el funcionamiento del mercado pues benefician a agentes que no son los más eficientes.

Sin embargo, la existencia de estos riesgos o situaciones que pueden afectar al consumidor financiero no deben llevar a prohibir o asfixiar a través de un excesivo intervencionismo las innovaciones y emprendimientos de servicios financieros digitales. Por el contrario, las ventajas de la innovación en términos de inclusión financiera, disminución de costos, accesibilidad a los productos y competencia, entre otros, exigen hallar un justo equilibrio entre la ausencia de regulación y la regulación excesiva.

En orden a cumplir el objetivo propuesto, se destacan dos de los riesgos enunciados: (i) el de ausencia o insuficiencia de información y comunicación en el uso de herramientas digitales, y (ii) el de seguridad, fraudes o ciberdelitos que afectan a los consumidores financieros. Estos dos riesgos agrupan varios de los fenómenos mencionados y afectan tanto al consumidor individual como a la confianza en el sistema financiero y el mercado. Adicionalmente, con la perspectiva de estos riesgos podemos abordar dos momentos diferentes de la relación del consumidor con los prestadores de servicios financieros digitales: la etapa precontractual, que termina en la celebración del contrato, y la ejecución del mismo.

3.1 Riesgo de ausencia o insuficiencia de información y comunicación

La falta e insuficiencia de información afectan la interacción del consumidor financiero en el mundo digital, en tanto permiten la adquisición de productos que difieren o no encajan con sus expectativas, necesidades o posibilidades.

Información y comunicación están íntimamente unidas en un Estado social de derecho fundamentado en la solidaridad. La información es un mecanismo unidireccional que supone un consumidor que entiende todos los mensajes que le son emitidos, de modo que, una vez el profesional emite la información, el consumidor debería tener la aptitud para tomar la decisión económica que más convenga a sus intereses. De hecho, la regulación que se ha mencionado, aplicable a las entidades vigiladas, establece los datos mínimos que deben suministrarse al interesado en los servicios financieros, incluidos costos, tasas de interés y plazos. En relación con los servicios ofrecidos por entidades no vigiladas, a ellos se aplican las normas generales –ley 1480– que también prevén estándares en la materia.

La información que se suele suministrar a través de plataformas y apps sería entonces suficiente para que el consumidor adopte una decisión racional. Sin embargo, la realidad económica y social y los ya mencionados sesgos contradicen esta premisa y demuestran que el simple cumplimiento formal de suministrar información no es suficiente.

[19] "It is important to identify potential threats to consumers that relate to the use of artificial intelligence in the provision of financial services. In the case of financial services, one can indicate, for example, such risks for consumers resulting from the use of artificial intelligence: protection of their privacy on the Internet, exposure to cyber-attacks, issues of liability for crimes committed with the use of artificial intelligence" NIZIOŁ, Krystyna. The challenges of consumer protection law connected with the development of artificial intelligence on the example of financial services (chosen legal aspects). Procedia Computer Science, 2021, vol. 192, p. 4103-4111. https://www.sciencedirect.com/science/article/pii/S1877050921019244

La extensión de la información, el empleo de términos técnicos y su ubicación[20] afectan su lectura y comprensión, de manera que no producen necesariamente el efecto deseado. La celeridad que se impone en las transacciones y los sesgos son enemigos de la comprensión y asimilación de la información. Más aún, si desplazarse físicamente a una oficina es una molestia para la mayoría de los consumidores, también lo son los problemas de funcionalidad que afectan las aplicaciones.

De otra parte, en ocasiones la lectura de las condiciones e informaciones que trasmiten los profesionales exige formación y, la mayoría de las veces, tiempo que el consumidor no tiene o no está en disposición de dedicar. Esto, que podría verse como una omisión del deber de diligencia, es la conducta del consumidor promedio y en ocasiones es aprovechada por quienes manejan los medios y la publicidad. Al ser esta la conducta del consumidor promedio de la segunda década del siglo XXI, es la que debe ser considerada por los profesionales que, en consecuencia, no solo deben acreditar que han informado, sino hacer todo lo que esté a su alcance para facilitar el entendimiento de la información.

Sin embargo, no basta con informar, es necesario comunicar para acreditar la toma de una decisión responsable y a consciencia del consumidor. Si hay comunicación entre profesional y consumidor, este último no puede excusarse en la asimetría de la relación para negarse a cumplir sus compromisos. La razón es simple: la comunicación suprime esa asimetría porque el acto de comunicar pone en igualdad de condiciones a las partes y le garantiza al consumidor el ejercicio reflexivo de su libertad. Por lo tanto, el consumidor debe asumir las consecuencias de sus decisiones -incluyendo las pérdidas económicas que pueden implicar- cuando los profesionales han informado y se han esforzado por comunicar.

¿Qué es entonces comunicar? La comunicación es el intercambio de informaciones. Se decía que informar es unidireccional, comunicar por el contrario es bidireccional. El receptor del mensaje se vuelve, a su vez, emisor. Informa al profesional sus expectativas, inquietudes y situación real. El profesional, que es el emisor inicial, acoge ese mensaje y formula uno nuevo que tiene en cuenta lo informado por el consumidor. En términos coloquiales es *ponerse en los zapatos del interlocutor*[21]. Entendida así la comunicación, surgen preguntas sobre su aplicación en el mundo digital. Las apps, plataformas y *chatbots* suponen la ausencia de relación con otro ser humano y, por lo tanto, excluyen el concepto de comunicación como se ha delineado. La contratación de productos y servicios financieros se efectúa sin intervención o participación de seres humanos por parte de la entidad financiera. Con base en una serie de preguntas y opciones, el consumidor contrata el producto sin mayor interacción, pues los sistemas que integran las plataformas tecnológicas utilizan la información que entrega el consumidor financiero para proveer el servicio. Alguien podría afirmar entonces que no hay comunicación en el mundo digital y, por lo tanto, que no hay contratación que se haga en forma libre y consciente.

Esa afirmación desconoce que los avances tecnológicos también pueden contribuir a tomar decisiones más informadas, libres y conscientes. En otras palabras, la tecnología

[20] El texto de los contratos requiere acceder a pestañas u opciones adicionales que se encuentran al margen del circuito de vinculación o están en archivos adjuntos de gran tamaño.

[21] En palabras de Woltion (2010) "La comunicación es la cuestión del otro. Ello supone una diferencia casi ontológica respecto de la información. Por supuesto, no hay mensaje sin destinatario, pero la información existe, sin embargo, en sí misma. Nada parecido ocurre, por el contrario, con la comunicación. Esta solo tiene sentido a través de la existencia del otro y el reconocimiento mutuo. Desde siempre ha existido el destinatario, pero la ruptura democrática consiste en reconocer la libertad y la igualdad de los protagonistas y, por lo tanto, la igualdad del receptor, que puede aceptar, rechazar, negociar la información" WOLTON, Dominique. Informar no es comunicar: contra la ideología tecnológica. *Informar no es comunicar*, 2010, p. 1-144.

puede contribuir a establecer nuevas formas de comunicación que tengan más en cuenta los intereses y necesidades del consumidor. Su existencia no es per se amenaza a la comunicación, pues ella puede facilitar el intercambio de informaciones de forma más eficiente que muchas conversaciones que establecen dos seres humanos. Lo importante es que al momento de diseñarse, programarse y ponerse en funcionamiento se tenga en cuenta esa necesidad.

De hecho, la ausencia de interacción física ya no es relevante en productos simples, carentes de riesgos para el consumidor promedio como cuentas de ahorros, depósitos de bajo monto o certificados de depósito a término. Productos que, por implicar la captación de recursos del público, solo pueden ser ofrecidos y contratados por entidades autorizadas y vigiladas por la Superintendencia Financiera. En esos productos el deber de información es relevante, pues garantiza el conocimiento del consumidor de datos esenciales como costos y rentabilidades. Esta información debe darse en la forma más sencilla de manera que el consumidor pueda comparar con la oferta de otras entidades y escoger aquella que le resulte más conveniente.

En el caso de la apertura de estos productos, lo que se ha demostrado es que la interacción física no es necesaria, pero ello no significa que en esas vinculaciones se prescinda de la comunicación. Por el contrario, en todos los casos debe considerarse la necesidad del cliente y hacer énfasis en los costos de los productos y servicios. En ese orden de ideas, la apertura digital de dichos productos debería permitir la posibilidad de entablar diálogos con la entidad –físicos o a través de otras herramientas– que le permitan al consumidor plantear dudas y obtener respuestas a sus inquietudes. El canal de comunicación podría ser o no empleado por él, pero debería estar a su disposición al momento de celebrar el contrato.

En el caso de los créditos, la comercialización a través de herramientas tecnológicas tiene otras connotaciones. El riesgo de la falta de información y comunicación es que se otorgue crédito a consumidores que no cuenten con la capacidad de pago. Este evento, conocido como sobreendeudamiento[22], pone en riesgo los recursos de los ahorradores cuando los otorgantes son entidades financieras que captan recursos del público. Vale recordar que los establecimientos de crédito prestan los recursos captados; por lo tanto, el incumplimiento de los pagos por los deudores podría terminar afectando la capacidad del establecimiento de crédito para devolver los dineros a los depositantes. Por esa razón, las entidades financieras están obligadas a elaborar y aplicar modelos robustos dirigidos a controlar el riesgo de crédito, es decir, el riesgo de incumplimiento de las obligaciones, lo que implica un examen riguroso de la capacidad de pago. En dicho examen se fundamentan muchas de las negativas de acceso al crédito para vastos sectores de la población que se dedican a actividades informales y no tienen cómo acreditar ingresos permanentes y/o suficientes para honrar los créditos que requieren.

[22] Aunque aquí se describe con sencillez el término vale mencionar que hay clases de sobreendeudamiento: "por un lado hay sobreendeudamiento activo y pasivo…. El primero es el que se asocia como tema de exceso en el importe de las deudas, que hace referencia a un consumidor que no atiende su nivel de renta, ni posibilidad de pago y que se vincula a su adicción de consumo o al menos, a un consumo irreflexivo estimulado por publicidad inmediata de financiación a través de un medio de pago: la tarjeta de crédito. El sobreendeudamiento pasivo se caracteriza porque no se debe a un comportamiento irresponsable del deudor, si no que en cambio, es la incapacidad para hacer frente a los créditos y se debe a circunstancias sobrevenidas y en gran parte, imprevisibles (muerte, enfermedad, grave, separación o divorcios, partos múltiples o pérdida de empleo) que generan aumento y disminuciones de ingresos propios" OBRIEN, Esteban Carbonell. El consumidor sobreendeudado: Hacia una respuesta eficiente desde el derecho de la insolvencia. https://www.institutoiberoamericanoderechoconcursal.org/images/eventos/congreso_peru/memorias/ARTICULO.%20El%20consumidor%20sobre%20endeudado.pdf

En el caso de los prestadores de servicios financieros digitales no vigilados, podría pensarse que, como los préstamos no se otorgan con dineros captados del público sino con recursos propios, es decir, bajo su propio riesgo, es innecesaria cualquier medida regulatoria. Sin embargo, esta visión fundada en el individualismo absoluto desconoce que en un Estado solidario esta práctica afecta y vulnera los derechos del consumidor financiero. La razón es que se le estaría permitiendo a una persona endeudarse sin razón y sin respaldo. Ese endeudamiento probablemente se convertirá en factor futuro de estrés y afectación de su salud mental y física cuando tenga que pagar y no pueda hacerlo[23]. Aunque no se ponga en riesgo la estabilidad del sistema financiero, el sobreendeudamiento genera malestar en los consumidores y, por lo tanto, debe ser evitado por quienes otorgan los créditos.

Ahora bien, en principio se dice que no se pone en riesgo la estabilidad del sistema financiero, pero si esta práctica es masiva y generalizada, tanto por los volúmenes monetarios transados como por la sensación de insatisfacción y abandono, las consecuencias económicas y sociales podrían generalizarse. En ese orden de ideas, que sean entidades no vigiladas que no reportan información a la Superintendencia Financiera impide un monitoreo permanente, y quienes se relacionan con ellas no tienen los mecanismos de protección con los que cuentan los consumidores de las entidades vigiladas; por ejemplo, en caso de controversia con el acreedor, al deudor no le es posible acudir a la acción de protección del consumidor financiero que permite a la Delegada con funciones jurisdiccionales de la Superintendencia Financiera conocer de estos asuntos; acción que ha demostrado sus bondades para todos los involucrados con decisiones ponderadas y oportunas.

La diferencia regulatoria en materia de sobreendeudamiento es clara, porque las entidades vigiladas por la Superintendencia Financiera tienen la responsabilidad de impedirlo. Se les impone una serie de reglas en materia de administración del riesgo de crédito que implican un monitoreo constante de la situación de los deudores y la constitución, entre otras, de provisiones en caso de mora. No se trata de que esas mismas reglas se impongan a los actores no vigilados, pero sí que asuman ciertas conductas para impedir el sobreendeudamiento.

En ese sentido, el Center for Financial Inclusion publicó los Estándares de Protección para Crédito Digitales[24], entre los cuales incluyó expresamente *Prevención del Sobreendeudamiento*. De las 28 acciones recomendadas, vale citar, para efectos ilustrativos, las siguientes:

> *2110 El proveedor dispone de una definición práctica de sobreendeudamiento de clientes que utiliza cuando se suscriben préstamos. La definición incluye el estrés financiero del cliente.*
> *2120 Para los préstamos por debajo del 10% del PIB per cápita mensual,[25] el proveedor puede demostrar que la capacidad de pago se toma en cuenta bien sea al momento de la suscripción, o a través de una supervisión robusta de clientes y cartera.*
> *2130 Para los préstamos entre el 10% y 6 veces el PIB per cápita mensual, los datos utilizados en la suscripción del crédito deben incluir variables tales como el ingreso*

[23] Aunque elaborado en un contexto diferente, los relatos que trae Sabatel Muriel (2019) en su escrito reflejan la situación de angustia y los efectos que traen para los deudores de buena fe, el no pago de las obligaciones. MURIEL, Irene Sabaté. Sobrendeudamiento, ejecuciones hipotecarias y cuestionamiento de la legitimidad de las deudas. Arbor, 2019, vol. 195, no 793, p. a516-a516. https://doi.org/10.3989/arbor.2019.793n3004

[24] Center for Financial Inclusion. Prevención del sobreendeudamiento. https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2019/06/Digital-Credit-Standards_ES_August-2021-update.pdf

[25] El PIB per cápita anual de 2021 en Colombia fue de US$6.132,2, según el Banco Mundial. En ese orden de ideas el PIB per cápita mensual seria de US$511,01

disponible, o alternativas que indiquen la capacidad de pago del cliente como por ejemplo datos transaccionales, saldo de ahorros, historial crediticio o relación ingresos/ gastos del cliente, de su hogar o negocio, etc. Igualmente se debe incluir el servicio de la deuda con otros prestamistas, verificado o informado por el propio cliente. Si el proceso de suscripción no incluye indicadores directos o indirectos de la capacidad de pago del cliente, el proveedor monitorea regularmente los resultados del cliente, es decir que examina anualmente su estrés de deuda o sobreendeudamiento, y lleva a cabo ajustes en función de ello. Las garantías, los ingresos del garante y/o la cobertura de seguros no son los elementos principales para aprobar un préstamo.
2140 Si se automatiza el análisis de la capacidad de pago (por ejemplo, mediante el uso de un algoritmo), la lógica del algoritmo se documenta, lo que incluye los factores/los tipos de variables utilizados y la justificación para confiar en esos factores. El documento está disponible para la gerencia superior, independiente del equipo de desarrollo de algoritmos.
2150 Si se utiliza algún algoritmo, los insumos del sistema, así como la eficacia del mismo para predecir la capacidad de pago del cliente es revisada por una unidad de la organización, independiente del equipo del desarrollo de algoritmos; por ejemplo, auditoría interna, la gerencia superior u otro departamento. La revisión incluye la coherencia entre la lógica, el algoritmo y sus salidas; por ejemplo, la calidad de la cartera y los segmentos mal predichos. La documentación acerca de las revisiones y las pruebas realizadas, así como de las recomendaciones de mejora, y de la puesta en práctica de las acciones de mejora, debe estar disponible.

Nótese cómo la guía pretende armonizar las eficiencias de la automatización con el necesario análisis y supervisión permanente que tiene por objeto prevenir el sobreendeudamiento. Aunque no pueda hablarse de comunicación humana, a través de las herramientas tecnológicas se logran los objetivos de la comunicación. Se conoce el cliente y sus conductas para tomar decisiones que lo protegen. Protección que puede consistir en la negación del crédito si el solicitante carece de capacidad de pago.

Sin embargo, la contribución de estas herramientas no debe excluir la posibilidad de un ejercicio de comunicación directa y personal. Como se ha indicado, a los futuros deudores se les debería permitir y poner a disposición medios para absolver sus inquietudes y preguntas, medios con capacidad de emitir recomendaciones y eventualmente sugerirle al solicitante no endeudarse.

Finalmente, los estándares elaborados con base en criterios técnicos son solo lineamientos para servicios financieros digitales -DFS, por sus siglas en inglés-. No hay norma que obligue su implementación ni ente que vigile su aplicación. La ausencia de estos dos elementos puede traducirse en un déficit de protección al consumidor cuando se trate de entidades no vigiladas.

Una última referencia sobre el déficit de información y comunicación se relaciona con el mercado de valores. Allí la regulación ha impuesto una expresión técnica de la comunicación, que es el deber de asesoría. Existen normas y reglas que detallan la forma de cumplir tanto con el deber de informar como con el de asesorar. De igual manera, la labor del Autorregulador del Mercado de Valores también ha sido determinante para hacer efectivo el cumplimiento de esas obligaciones y establecer buenas prácticas para su aplicación.

Resulta conveniente profundizar en estos desarrollos, pues los agentes no vigilados no están en el perímetro de regulación ni autorregulación, y de otra parte porque es necesario, aún para los actores vigilados, profundizar la comunicación en épocas de coyunturas desfavorables y volatilidades. En este sector es fundamental que la información no se limite a aspectos formales en el momento de vinculación de los inversionistas. Es necesario fortalecer los canales de comunicación que le permitan al consumidor tomar decisiones cuando sus inversiones se están afectando por coyunturas del mercado. La inclinación natural de la mayoría es a liquidar la inversión y materializar una pérdida. Pero, con independencia de ello, los administradores de fondos de inversión colectiva, comisionistas o plataformas deberían poner a disposición de los inversionistas en forma sencilla y accesible elementos que les permitan tomar la decisión que mejor convenga a su perfil. El concepto de perfil del cliente es uno de los que mejor reflejan la necesidad de comunicación, pues supone que el profesional examina la situación financiera, intereses y necesidades del cliente para determinar los productos que más le convengan[26]. Cumplido ese deber de informar y comunicar con base en su perfil, la decisión de permanecer en la inversión o liquidarla será responsabilidad exclusiva del inversionista. Las herramientas y desarrollos que permitan esa actualización permanente de los inversionistas y ayuden a formar su juicio son esenciales para profundizar la confianza en el mercado. En esa comunicación, la precisión en los datos y el objetivo de permitir una decisión consciente deben ser los criterios que motiven la actuación del profesional.

Ahora bien, al igual que la definición de perfil del cliente hay otros términos que se han venido introduciendo y que exigen el cumplimiento de informar y comunicar. Es el caso del concepto de trato justo[27], al que se le ha dado la naturaleza de principio en diferentes documentos internacionales y en el White Paper Supervision de riesgos de conducta de la Superintendencia Financiera de Colombia.

3.1.1 Principio de trato justo

En desarrollo de este principio, las ES[28] deben garantizar en el diseño, ofrecimiento y prestación de productos y servicios:

- Que se atienden las necesidades y expectativas de los consumidores financieros.
- Que se brinda acceso e información clara, transparente y oportuna, acorde con las necesidades y perfil del consumidor financiero, en todo el ciclo de vida del producto.
- Que no existen barreras para movilizarse entre diferentes productos, servicios y entidades financieras.
- Que el proceso para interponer quejas o reclamos permite a los consumidores el ejercicio oportuno de sus derechos[29].

[26] Artículo 2.40.1.1.5. del decreto 2555 de 2010.
[27] El concepto de trato justo tiene menciones en diferentes documentos como el documento del G20 "G20 High-level principles on financial consumer protection". Disponible en https://www.oecd.org/daf/fin/financial-markets/48892010.pdf "All financial consumers should be treated equitably, honestly and fairly at all stages of their relationship with financial service providers. Treating consumers fairly should be an integral part of the good governance and corporate culture of all financial services providers and authorised agents. Special attention should be dedicated to the needs of vulnerable groups".
[28] Entidades supervisadas.
[29] Consultadas diferentes fuentes lo más cercano a una definición de trato justo se encontró en el documento de política de la CMF de Chile "Desarrollo de estándares y principios generales en materia de Conducta de Mercado referidos a Protección al Cliente Financiera" (2021) https://www.cmfchile.cl/portal/principal/613/articles-47839_doc_pdf.pdf "Este principio es fundamental en las prácticas de CdM enfocadas en PCF e implica que las entidades consideren los intereses de sus clientes en la realización de sus negocios, velando siempre porque éstos reciban un producto o servicio apropiado a sus necesidades, y se les proporcione en todas las etapas de su relación con ellos, una correcta y transparente atención y/o asesoría".

A pesar de llamarse principio, el trato justo no es un principio de derecho[30], pues no es base y fundamento de todo el ordenamiento jurídico y, por lo tanto, no debe soportar el pronunciamiento y actuación de autoridades y ciudadanos. Se trata de una regla, es decir, de una norma para situaciones puntuales, en este caso la relación consumidor-institución financiera. En ese sentido, el trato justo es un parámetro de conducta que permite valorar y examinar el comportamiento de las entidades y de su personal en todas las interacciones que tenga con el consumidor financiero.

El trato justo, entonces, no modifica los deberes de informar y comunicar que hemos presentado como necesarios en los entornos digitales. Por el contrario, hay trato justo cuando se informa y comunica –lo que incluye asesorar en el mercado de valores– en debida forma al consumidor financiero. Informar y comunicar permiten construir una relación que no se fundamente en los intereses inmediatos del profesional, sino en el beneficio e interés del consumidor financiero y, en particular, de aquel que se encuentra en una situación de protección especial constitucional.

Puede concluirse entonces que la comunicación y la información, como fundamento de ella, son esenciales en la protección del consumidor financiero en la era digital. Comunicación e información que ya son de recibo en nuestro ordenamiento por conceptos como perfil del cliente y el trato justo. Pero su carácter fundamental, en un Estado de derecho solidario, exige la aplicación y extensión a cualquier tipo de servicio financiero digital y sobre todo que no se limite al cumplimiento formal, para que pueda desarrollarse como actividad inherente a la de cualquiera que preste servicios financieros.

3.2 Fraudes, protección de la información y datos del consumidor

Como es sabido, los confinamientos debidos a la pandemia del Covid-19 incrementaron el volumen de operaciones realizadas por canales virtuales. Ese resultado benéfico tuvo como efecto colateral el incremento en los fraudes a los consumidores financieros. Estructuras criminales completas han sido desmanteladas, pero, pese a los esfuerzos de autoridades e instituciones, continúan las prácticas delincuenciales. Se confirmó lo que la literatura en la materia[31] había advertido sobre los riesgos de fraude y brechas en la protección y privacidad de los datos en el uso de nuevas tecnologías. A pesar del retorno a la *normalidad*, las cifras de ciberdelitos siguen en aumento. A manera de ejemplo, al 23 de junio de 2002 el observatorio de Cibercrimen de la Policía Nacional reportó 1168 delitos cometidos en la modalidad de *phishing*, es decir, mediante el uso del correo electrónico para robar datos como claves de tarjeta o acceso a portales; 637 delitos por *malware*[32] o *software* malicioso que se instala en los equipos de los usuarios con diversos fines, entre los cuales puede estar el robo de datos o la usurpación de identidad, y 515 por *smishing*, valerse de mensajes de texto para obtener

[30] Sobre los principios de derecho hay abundante literatura pues es un tema que ha ocupado a los grandes estudiosos del derecho. Para ampliar el tema puede verse Dworkin, Rober Alexi (Tres escritos sobre los derechos fundamentales y la teoría de los principios) y Zagrebelsky (El derecho dúctil. Ley, derechos, justicia), entre otros. Este autor pone de presente las diferencias entre reglas y principios. Entre las varias que menciona indica: "..los principios desempeñan un papel propiamente constitucional, es decir "constitutivo" del orden jurídico…las reglas, en efecto se agotan en sí mismas, es decir, que no tienen ninguna fuerza constitutiva fuera de los que ellos mismos significan" (p.110)

[31] "Fraud types that have potential negative effects on customers, such as SIM swaps and card skimming • Breaches of data privacy and protection, as inadequate data handling can trigger other risks, such as identity theft, misuse by government, sale of one's data without knowledge or consent, etc." BUCKLEY, Ross P.; MALADY, Louise. Building consumer demand for digital financial services–the new regulatory frontier. *Journal of Financial Perspectives*, 2015, vol. 3, no 3., Available at SSRN: https://ssrn.com/abstract=3084037

[32] Son tipos de software malicioso los troyanos, los gusanos, el spyware, el adware y el ransomware.

los datos del cliente. De esos delitos, 829 fueron denunciados por instituciones financieras.

Así las cosas, la protección al consumidor en esta materia demanda el trabajo en dos frentes: la prevención y la responsabilidad. En cuanto a la prevención, requiere decisiones y acciones concertadas de actores que son ajenos al sistema financiero como la Registraduría Nacional del Estado Civil o la Fiscalía General de la Nación. Una gestión eficiente en el marco de sus competencias contribuye a mitigar los riesgos asociados a estos fenómenos. Es decir, dicha problemática no es responsabilidad exclusiva de las instituciones financieras, sino del esfuerzo conjunto y coordinado de autoridades, entidades y los mismos consumidores. Si todos ellos contribuyen en el marco que les corresponde, las cifras deberán disminuir y minimizarse el impacto de los cibercrímenes.

Ahora bien, en lo que les corresponde, las entidades financieras han venido desarrollando herramientas que permiten identificar hábitos transaccionales de los consumidores en los diferentes canales y, por lo tanto, mejorar las señales de advertencia. En el mismo sentido, los cruces de bases de datos y la identificación de patrones de los grupos delictivos son de gran utilidad. En otras palabras, se crean nuevas formas de operación y aplicaciones que tienen como propósito pasar de modelar datos y grupos de riesgo en forma separada a una evaluación inteligente. Con ello se implementan *capacidades para permitir el análisis de datos agregados y las correlaciones entre los datos cibernéticos y los datos de fraude*[33], es decir, que se usa la inteligencia de datos para identificar situaciones o amenazas de fraude.

Los esfuerzos de la industria y las instrucciones del supervisor reflejan la preocupación por el cumplimiento de los deberes y obligaciones frente al consumidor financiero a quien corresponde educar en la materia. Las campañas sobre conductas riesgosas y buenas prácticas deben ser permanentes y efectivas. Por todos los medios posibles y en cualquier oportunidad, especialmente mediante herramientas digitales, debe advertirse al consumidor financiero sobre las conductas que facilitan las acciones criminales.

Sin embargo, y a pesar de la destinación de recursos humanos, financieros y técnicos, los fraudes continúan, y teniendo en cuenta la existencia de complejas redes delincuenciales, seguirán ocurriendo. En ese sentido, adquiere relevancia la responsabilidad de las entidades financieras cuando se cometen ciberdelitos. Es decir, el comportamiento que deben asumir cuando el fraude ha ocurrido y los recursos han sido sustraídos o la persona ha sido suplantada y a su nombre se han desembolsado créditos.

Las decisiones judiciales han radicado la responsabilidad en los profesionales por cuanto ellos han creado la situación de riesgo y se benefician de ella[34]. En otras palabras, los avances tecnológicos permiten a los profesionales optimizar sus costos, mejorar su competitividad y aumentar sus ingresos, entre otros beneficios que les reportan. Los riesgos que crean esas innovaciones, y en particular el fraude electrónico, deben ser asumidos por quien en su condición de profesional los pone a disposición del consumidor. Lo anterior porque la institución, en su condición de profesional, cuenta -o debería contar- con las herramientas y recursos para prevenir la defraudación de sus clientes.

[33] PALMER, Adam, MARTINS de A, Gilberto, Tendencia del Fraude Cibernético y Mejores Prácticas en el Sector Finaniero Global, p.46-61, en ASOBANCARIA, Desafíos del Riesgo Cibernético en el Sector Financiero para Colombia y América Latina. (2018)

[34] La jurisprudencia y la doctrina ha llamado a esta formulación la teoría del riesgo creado. En ese sentido ver el extenso y profundo estudio de Luis Humberto Ustariz que menciona las decisiones de la Corte Suprema de Justicia. USTARIZ, Luis H. Responsabilidad Bancaria. Legis, 2021P. 130-141.

Ahora bien, la Corte Suprema de Justicia ha dejado claro que la creación del riesgo no significa el reconocimiento automático de la responsabilidad del banco. Lo anterior por cuanto este puede probar que la situación que ocasionó el daño fue consecuencia en todo o en parte de acciones u omisiones del mismo consumidor. El ejemplo puesto por la Corte es el del cuentahabiente que pierde su tarjeta y deja el número de clave con el plástico. En ese caso, las medidas de seguridad establecidas por el banco habrían sido vulneradas por hechos propiciados por el mismo consumidor[35] y, por lo tanto, la institución financiera no debería asumir la pérdida de los recursos. Se trata del incumplimiento de los deberes de diligencia y cuidado que debe observar el consumidor y que asume al contratar o adquirir un producto financiero. La falta de cuidado en el entorno digital comprende nuevos comportamientos diferentes al descrito por la Corte. Así pues, a manera de ejemplo, en un caso que falló la Delegada de asuntos jurisdiccionales de la Superintendencia Financiera se identificaron responsabilidades compartidas tanto del consumidor como de la institución financiera por transferencias hechas a través de una sucursal virtual –Internet-. En este caso, de la cuenta de un pequeño municipio se retiraron fraudulentamente $31.450.000 y se transfirieron a cuentas de terceros. El fallo ordenó restituir al municipio el 50% de los dineros transferidos, por cuanto nunca hizo el mantenimiento adecuado a los equipos ni instaló las herramientas para impedir intrusiones de tercero. Pero también se condenó a la institución financiera porque las transferencias no correspondían al perfil transaccional del municipio y no fueron identificadas ni bloqueadas oportunamente[36].

Pretender que, en estos casos, la institución financiera asuma siempre y en su totalidad las pérdidas económicas de municipios con controles frágiles, sería exonerar a estos del cumplimiento de sus deberes. La ausencia de deberes contradice la esencia misma del Estado social de derecho[37], y en este caso particular significaría trasladar la consecuencia de los descuidos y omisiones de un consumidor al sistema financiero. Es decir, las instituciones financieras asumirían las consecuencias económicas de pérdidas que no han provocado.

Ahora bien, de lo anterior se deduce que es deber de las entidades financieras adelantar investigaciones sobre los fraudes que les informen sus consumidores, tanto para asumir las responsabilidades que les corresponden como para identificar descuidos u omisiones en la conducta de los consumidores. En ese sentido, con base en los hallazgos debe determinarse la procedencia o no del reconocimiento de la pérdida. Obrar de otra forma, es decir, no investigar o acceder sin elementos de juicio a los reclamos de los ahorradores, sería no actuar profesionalmente.

En los casos de ciberdelitos, de nuevo se presenta una asimetría entre las entidades vigiladas y otros prestadores de servicios financieros digitales. Aquellas han sido afectadas con decisiones que las obligan a responder a pesar de haber obrado en forma diligente, con el argumento de que su obligación es de resultado, es decir, que solo se liberan probando que el fraude no es atribuible a su acción u omisión, sino al consumidor. En cambio, no hay norma ni precedente que haga extensivo ese criterio, tan favorable al consumidor, a las entidades de servicios similares no vigiladas. La diferencia de supervisor y de jurisdicción para unas y otras ha contribuido a crear regímenes y efectos diferenciales que perjudican al

[35] El ejemplo es mencionado por la Sentencia del 18 de diciembre de 2020. Corte Suprema de Justicia, Sala de Casación Civil. Magistrado ponente: Luis Alonso Rico Puerta.
[36] Superintendencia Financiera. Rad. 2021196769
[37] Artículo 95 de la CP.

consumidor de las no vigiladas.

De ahí la necesidad ya expresada de ampliar el concepto de consumidor financiero para incluir en esa categoría a todos aquellos que se relacionen no solo con las entidades vigiladas sino con prestadores de servicios financiero-digitales no vigilados. Lo dicho permitiría, además, aplicar los mecanismos de supervisión que se han venido implementado –Smartsupervision- y la mitigación del riesgo de conducta en los términos empleados por el White Paper. En el mismo orden de ideas, sería aplicable la teoría del riesgo creado y podría ejercerse la acción del consumidor ante la Delegada con funciones jurisdiccionales de la Superintendencia Financiera.

4. Conclusiones

4.1 La categoría de consumidor financiero no puede limitarse, como hoy lo hace la legislación, a las personas que se relacionan con entidades vigiladas. Es necesaria una ampliación del concepto que permita extenderlo a quienes se relacionan con otros actores que realizan actividades idénticas.

4.2 Los avances en materia de supervisión, garantías, proceso -incluidos los desarrollos jurisprudenciales- deben aplicarse a todos los consumidores.

4.3 Los riesgos inherentes al uso de nuevas tecnologías no deben conducir a un intervencionismo desproporcionado que impida su desarrollo o utilización en el sector financiero. Lo que se requiere es el fortalecimiento de los mecanismos hoy vigentes y su extensión a todos los actores.

4.4 La calificación constitucional de la actividad financiera como de interés público exige los mayores niveles de protección al consumidor financiero. Protección que se alcanza en gran medida con el cumplimiento de los deberes de información y comunicación como instrumentos que no solo garantizan una decisión económica racional, sino que también mitigan los riesgos de sesgos que distorsionan la decisión del consumidor.

Bibliografía

Blanco Barón, Constanza. La protección del consumidor financiero en la era digital: retos para los reguladores. (en línea) Bogotá: Universidad Externado de Colombia, 202133 páginas ISBN 9789587905847. P 657 (Fecha consulta: 22 de julio 2022).

Buckley Ross; P. Malady, Louise. Building consumer demand for digital financial services–the new regulatory frontier. *Journal of Financial Perspectives*, 2015, vol. 3, no 3., Available at SSRN: https://ssrn.com/abstract=3084037

Center for financial inclusion. *Prevención del sobreendeudamiento*. https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2019/06/Digital-Credit-Standards_ES_August-2021-update.pdf

Comisión para el mercado financiero. Desarrollo de estándares y principios generales en materia de Conducta de Mercado referidos a Protección al Cliente Financiera (2021) https://www.cmfchile.cl/portal/principal/613/articles-47839_doc_pdf.pdf

Cortada de Kohan, Nuria; Macbteh, Guillermo. Los sesgos cognitivos en la toma de decisiones. [en línea]. Revista de Psicología, 2(3). Disponible en: http://bibliotecadigital.uca.edu.ar/repositorio/revistas/sesgos-cognitivos-toma-de-decisiones-kohan.pdf.

Dewi Tsany, Ratna. The Promise and Perils of Digital Finance: Toward Financial Inclusion and Smart Consumer Protection. *University of Luxembourg Law Research Paper*, 2022, no 2022-002, Available at SSRN: https://ssrn.com/abstract=4095330 or http://dx.doi.org/10.2139/ssrn.4095330

G20 “G20 High-level principles on financial consumer protection”. Disponible en https://www.oecd.org/daf/fin/financial-markets/48892010.pdf

García-Tejeda, Enrique. ¿Alguien quiere una rebanada de pizza? Los sesgos cognitivos en la contratación de servicios digitales: el punto ciego de la regulación en México. *Latin American Law Review*, 2021, no 6, p. 175-194.

Hernández, Reche Vicente. *El sesgo de decisión en la inversión financiera*. 2017., https://www.tesisenred.net/handle/10803/457889#page=1 (last visited May 25, 2022).

Muriel, Irene Sabaté. Sobrendeudamiento, ejecuciones hipotecarias y cuestionamiento de la legitimidad de las deudas. Arbor, 2019, vol. 195, no 793, p. a516-a516. https://doi.org/10.3989/arbor.2019.793n3004

Niziol, Krystyna. The challenges of consumer protection law connected with the development of artificial intelligence on the example of financial services (chosen legal aspects). *Procedia Computer Science*, 2021, vol. 192, p. 4103-4111. https://www.sciencedirect.com/science/article/pii/S1877050921019244

Obrien, Esteban Carbonell. El consumidor sobreendeudado: Hacia una respuesta eficiente desde el derecho de la insolvencia.
https://www.institutoiberoamericanoderechoconcursal.org/images/eventos/congreso_peru/memorias/ARTICULO.%20El%20consumidor%20sobre%20endeudado.pdf

Palmer, Adam; Martins de A., Gilberto, Tendencias del Fraude Cibernético y Mejores Prácticas en el Sector Financiero Global, p.46-61, en ASOBANCARIA, *Desafíos del Riesgo Cibernético en el Sector Financiero para Colombia y América Latina*. (2018). https://www.asobancaria.com/wp-content/uploads/20191010-asobancaria-OEA_min.pdf

Rengifo G., Mauricio, "Derecho del Consumo: Problemas y Conceptos fundamentales". En VARON P., Juan Carlos, RENGIFO G, Mauricio, PEÑA B, Fernando, *Derecho del Consumo. Tomo I. Introducción al Derecho del Consumo*" Universidad de los Andes, 2022, p. 16. http://dx.doi.org/10.15425/2017.529

Wolton, Dominique. Informar no es comunicar: contra la ideología tecnológica. Informar no es comunicar, 2010, p. 1-144.

Ustáriz, L. H.. Responsabilidad Bancaria, Legis, 2021,

CAPÍTULO 10

Bancos digitales

Juan Sebastián Peredo Bernal[1]

Resumen

Los bancos digitales, si bien recientes, son fruto de décadas de adaptación tecnológica y social de la banca. Una adaptación que viene estrechamente ligada con un desarrollo legal y regulatorio permisivo de modelos de negocio digitales. De alguna manera, la intersección entre tecnología, mercado y regulación ha llevado al desarrollo de entidades que nacen digitales. Los bancos digitales responden a ese cruce de caminos que busca desplazar a la banca hacia el cliente, para ofrecerle los servicios y productos de manera instantánea y sin exigirle esfuerzo. En este capítulo se exploran los elementos de negocio, tecnología y regulatorios que caracterizan la existencia y razón de ser de los bancos digitales, especialmente aquellos que, por su naturaleza, los diferencian de lo que se concibe como banca tradicional. A la vez, se discute el camino natural que tendrán que recorrer y las tendencias que los podrán afectar y encauzar hacia nuevos rumbos. Finalmente, se analiza cómo el agnosticismo frente al tipo de tecnología y modelo de negocio continuará moldeando la forma de operar de los bancos digitales y, mejor aún, la forma en la que se prestan los servicios bancarios y financieros.

[1] Vicepresidente Jurídico de Lulo Bank S.A. Abogado de la Universidad del Rosario con especialización en derecho financiero de la Universidad Externado de Colombia y Master of Laws in Banking Law and Financial Regulation de The London School of Economics and Political Science.

1. Introducción

Los bancos digitales no son simplemente la culminación de un proceso de adaptación y adopción tecnológica por parte del sistema financiero. Representan el estado del arte de muchos procesos tecnológicos y culturales recorridos desde hace décadas. Son la combinación, por un lado, de avances tecnológicos que han permitido prestar servicios financieros de manera completamente digital, y por otro, de la adopción cultural de mecanismos digitales para consumir productos y servicios.

Los bancos digitales son una respuesta a la nueva forma de acceder a productos y servicios, una reformulación del modelo de negocio bancario a partir de utilizar la tecnología de manera integral y de entender la cultura digital de la sociedad. Y así ha sido para la mayoría de las industrias, no solo para la financiera, lo que ha hecho que migren a nuevos modelos de negocio y a operar de una manera diferente[2].

Más allá de un grupo de entidades que ofrecen servicios financieros de manera digital, los bancos digitales son entidades que retan el *statu quo* del sistema financiero, que replantean la forma de competir en el mercado bancario y buscan demostrar cómo, a través de tecnología, se puede alterar la forma en la que los clientes interactúan con la banca. No se trata simplemente de usar tecnología para que los consumidores accedan a servicios -una presentación digital de lo que ya conocen físicamente-, se trata de entender profundamente la tecnología y su relación con la sociedad para proponer una nueva forma de hacer banca a partir de las oportunidades que trae la tecnología.

Retar ese *statu quo* por parte de los bancos digitales se ha revelado como un desafío interesante, porque tienen que lograr operar de manera nativa en una cultura digital siendo, a su vez, una entidad sometida a la regulación bancaria. Es un reto en sí mismo coexistir como entidad nativo-digital y como entidad regulada.

Revisaremos la existencia de los bancos digitales a partir de su definición, su naturaleza, sus características y su búsqueda por un nuevo modelo de negocio.

2. Definiendo a los bancos digitales

Para asignarle a una institución la denominación de banco digital se debe partir de que esté habilitada para la prestación de servicios bancarios, para la realización de la actividad de intermediación financiera, que consiste en recibir depósitos para realizar préstamos. Las únicas instituciones autorizadas para realizar esta actividad en Colombia son los establecimientos de crédito, y entre ellos, los bancos. Por esta razón, los bancos digitales -o neobancos, término que se usa en este texto de manera intercambiable-, por su naturaleza de bancos, deben estar autorizados por la Superintendencia Financiera para realizar sus actividades. En ese sentido, para ser banco digital no basta que se preste algún tipo de servicio financiero, es necesario que se puedan prestar los servicios financieros que solo los bancos tienen permitido desarrollar.

[2] Peredo Bernal, Juan Sebastián. Capítulo 4: Los Bancos Digitales: Neobancos. Los mercados financieros ante la disrupción de las nuevas tecnologías digitales. Bogotá: Universidad Externado de Colombia. 2021.

Ahora bien, todos los bancos prestan sus servicios a través de tecnología, pero eso no los convierte en bancos digitales. La naturaleza digital no se trata simplemente de la adopción de herramientas tecnológicas para prestar servicios bancarios: esto nos llevaría a que casi cualquier banco pudiera autodenominarse digital cuando adopta tecnología. Se trata de una naturaleza digital derivada de la adopción social de tecnología y del replanteamiento del tipo de relaciones que tienen los clientes con sus bancos, del cambio de modelos de negocio a partir de estructuras que comprenden las nuevas formas de relacionamiento de las personas con la tecnología.

Entonces, los bancos digitales son entidades que nacen como los proponentes de una nueva forma de prestar servicios bancarios a sus clientes y buscan ser la forma más avanzada de digitalización de los servicios bancarios en este momento, llevando la tecnología a sus procesos de manera integral y nativa, tanto en el relacionamiento con el cliente como en la operación de la entidad[3].

3. Características de los bancos digitales

Al aproximarnos al concepto de banco digital, mencionamos la adopción de tecnología en la prestación de servicios financieros, por un lado, y por otro, que hacen parte de una cultura nativa-digital y de un reto al *statu quo* del sistema financiero. Por esa razón clasificaremos las características de los bancos digitales en dos conjuntos: aquellas que consideramos naturalmente objetivas y aquellas que conllevan un análisis subjetivo.

3.1 Desde lo objetivo

El primer grupo de características viene dado por el momento actual: una operación apalancada en un proceso maduro de adopción cultural de la tecnología en la sociedad. Esto se debe ver desde dos perspectivas que de manera acertada resume el Bank for International Settlements (BIS) cuando evalúa el impacto reciente de las nuevas tecnologías en la industria bancaria: *(i) la tasa de adopción de la tecnología en la sociedad, y (ii) el grado y la omnipresencia de los conocimientos tecnológicos dentro de la población general*[4]. Por esta razón, para que las personas puedan ver como una opción deseable utilizar los productos de bancos que prestan sus servicios de manera completamente digital, es necesario de un proceso mínimo de adopción y conocimiento tecnológico en la sociedad.

Que la operación se encuentre apalancada en la adopción cultural de la tecnología por las personas no implica únicamente la utilización de mecanismos digitales para prestar servicios. Este tipo de operación digital implica entender la forma de interactuar de las personas con productos y servicios, diseñar productos enfocados en el consumidor, resolver los problemas de los consumidores, hacer del banco un sistema habilitador de las necesidades financieras de las personas y ofrecer nuevos productos y servicios de manera constante y rápida: poner al consumidor en el centro de la operación. Por ejemplo, el diseño de la interfaz de usuario -lo que el cliente ve al abrir su app- y de la experiencia de usuario de un banco digital parte de entender la forma en la que las personas se relacionan con sus dispositivos, de buscar la forma en la que intuitivamente las personas utilizan las aplicaciones, algo que es difícil de

[3] Ibidem
[4] BANK FOR INTERNATIONAL SETTLEMENTS [BIS] Basel Committee on Banking Supervision. Sound Practices: Implications of fintech developments for banks and bank supervisors. Basilea: Bank for International Settlements. 2018.

encontrar en las aplicaciones bancarias de los bancos tradicionales. Así mismo, como un ejemplo adicional, los bancos digitales tienen una facilidad de apalancar su tecnología en nuevas tecnologías, de adoptar y reemplazar las que ya tienen, por cuanto su arquitectura se lo permite. Para los bancos tradicionales, esta adopción de nuevas tecnologías se torna compleja, implica la reestructuración de la arquitectura y años de trabajo: la infraestructura creada durante décadas hace significativamente más difícil adoptar nueva tecnología sin contratiempos.

3.1.1 Un diseño atractivo para los clientes

Decir que los consumidores se encuentran expuestos a tecnología siempre cambiante y a métodos de utilización de la tecnología que se desarrollan constantemente suena a simplificación. Esa exposición a tecnología por parte de los consumidores demanda de los proveedores de productos y servicios habilitar nuevas formas de proveerlos. El desarrollo de teléfonos móviles generó una tendencia en la utilización de estos dispositivos para realizar tareas diarias y mecánicas diferentes a solo comunicarse para llamadas[5].

Y en materia bancaria la historia no fue diferente. En los últimos años hemos tenido una evolución exponencial en los servicios digitales bancarios, atada, por un lado, a la madurez de la sociedad en la utilización de estos servicios, y por otro, a la demanda de los clientes de un mejor servicio. Esa evolución se ha hecho evidente en la disminución de la operación física y manual, dado que los clientes cuentan con mecanismos digitales y remotos para la realización de sus transacciones.

Los bancos digitales se diseñan a partir de los clientes. El diseño atractivo surge de poner al consumidor financiero en el centro de órbita del modelo de negocio. De entender sus necesidades y, a partir de ellas, diseñar la infraestructura operativa y tecnológica para satisfacerlas. De entender sus preferencias y lograr que la interfaz y experiencia de usuario del banco funcionen para él en todos sus aspectos. Esto se evidencia al hacer ejercicios comparativos de visualización de contenido, de ubicación, de acciones rápidas y fáciles y de utilización eficiente de tecnología. Incluir formas fáciles de visualización del pago de cuotas, permitir a las personas *jugar* con la selección de funcionalidades, hacer el proceso atractivo y claro visualmente son algunas de las bondades que se desprenden de este tipo de diseño atractivo para clientes.

Y es que la llegada de los teléfonos inteligentes constituyó un salto grande en las posibilidades de digitalización y construcción bancaria. Desde interfaces de usuario diseñadas para funcionar sin fricciones -sin exigirle más de lo natural al seleccionar acciones y esperar que estas sucedan-, pasando por la utilización de biometría para la seguridad de los dispositivos y la realización de transacciones, la geolocalización para la protección contra el fraude y mecanismos múltiples de autenticación para asegurar que las personas que están utilizando los dispositivos son los dueños de los productos. A esto se le debe sumar la potencialidad de escalar el número de servicios constantemente y de integrar nuevos desarrollos de tecnología a las operaciones que se realizan desde el teléfono inteligente: la adopción de *chatbots* -sistemas automatizados para resolver consultas de clientes-, la posibilidad de realizar transacciones a través de parlantes con asistentes de voz inteligentes -dentro de lo que se entiende como Internet de las cosas-, la utilización de relojes inteligentes para los

[5] Ibidem.

servicios bancarios, entre muchos otros. La frase clave es *escalar el número de servicios constantemente, y le agregaría: rápidamente*. Si bien un banco tradicional podría -y puede y lo han hecho- adoptar estas nuevas opciones que mencionamos, la arquitectura tecnológica que los subyace, la infraestructura operativa, el gobierno interno, hacen que el proceso difícilmente pueda ser catalogado como rápido. La oferta de servicios de un banco digital crece de manera constante y con una velocidad de desarrollo y ejecución mayor que la de la industria bancaria tradicional -como un ejemplo, la incursión de varios bancos digitales extranjeros en múltiples segmentos en cuestión de dos años-. Si se hacen algunas preguntas, este párrafo hará más sentido: ¿Cuántos años les ha tomado a los bancos tradicionales implementar su oferta digital? ¿Qué de esa oferta digital es diferente a la oferta física que tienen? ¿Es la oferta digital de los bancos tradicionales libre de fricciones? ¿Es la oferta digital libre de elementos adicionales físicos que la hagan híbrida, es decir, que impliquen que el proceso no sea totalmente digital y que el cliente tenga que interactuar de manera física con el banco, como cuando se firma un pagaré en papel?

Por esto, que una de las características de los bancos digitales sea proveer un diseño atractivo para los clientes significa entender las dinámicas de tecnología en el mercado, las demandas de sus clientes en relación con lo que consumen y cómo lo consumen y tener la capacidad de ofrecer servicios acordes con esas demandas sin fricciones y de manera casi automática. Entender las capacidades atadas al *hardware* disponible en el mercado y aprovecharlas de forma que beneficien la relación de sus clientes con sus productos financieros. Quien no entiende rápidamente esas dinámicas se expone a tener que adoptarlas después de que las compañías nativo-digitales las han usado y explotado. Un ejemplo, que se ha podido evidenciar en los últimos años, es la adopción de blockchain por el mercado financiero tradicional colombiano y la adopción de blockchain por el mercado nativo-digital. En el mismo ejemplo, la población ha visto cómo los servicios de transferencia de recursos internacionales a través de empresas que operan con criptomonedas han venido sustituyendo en costo y rapidez los servicios de transferencia internacionales implementados desde hace décadas por los bancos. Más allá de si la razón es regulatoria, de riesgo o de implementación, la adopción de tecnología por parte de entidades nativo-digitales es significativamente más rápida que la del mercado financiero tradicional, lo que hace que la oferta de productos y servicios sea, a su vez, mayor.

La regulación se ha enfocado en entender la tecnología, en la mayoría de los casos relacionada con los canales. Así, en el caso colombiano se encuentran instrucciones para las operaciones que se realicen a través de cajeros automáticos, Internet, banca móvil y otros[6]. Sin embargo, en la medida que la tecnología desplegada siga evolucionando y que los bancos digitales y tradicionales la adopten, pensar en regular canales podrá generar fricciones con la adopción de la misma. Tal vez pensar en regular objetivos más que actividades concretas sería lo ideal, y en la medida que estos objetivos se satisfagan con una u otra tecnología, el resultado sería óptimo.

3.1.2 Una operación rápida y eficiente basada en tecnología

La segunda característica, naturalmente ligada a lo anterior, consiste en la habilidad de los bancos digitales de operar de forma rápida y eficiente al encontrarse apalancados de manera nativa en tecnología -por ejemplo, poder pasar de 1 a 10 millones de clientes en un tiempo corto por tener una arquitectura en nube-. Esta rapidez y eficiencia se traduce

[6] Ibidem.

en el despliegue de nuevos productos, funcionalidades y servicios de manera constante, en escalar las líneas de negocio sin mayor impacto para la operación y en la capacidad de iterar el banco para que responda a las necesidades de usuario -arquitectura de tecnología que permite añadir componentes sin afectar la operación bancaria desplegada anteriormente-. Nos hemos acostumbrado a escuchar las historias del crecimiento en millones de clientes de entidades digitales, sin que en esas historias se hable de una dificultad en la operación por el crecimiento.

La condición de digitales desde su nacimiento les permite a este tipo de bancos tener una arquitectura tecnológica diseñada para evolucionar constantemente y para escalar el banco sin necesidad de mayores inversiones adicionales. Cuentan con procesos automatizados, analítica avanzada, arquitectura en nube, entre otros componentes, lo que les da la posibilidad de evolucionar continuamente.

La tecnología *legacy*[7], esa tecnología de antaño que todavía algunos bancos usan y muchos reencauchan, continuará siendo una desventaja competitiva para las entidades tradicionales que busquen participar de ecosistemas digitales. Esto implica que los bancos digitales están -y deben estar- desplegados en tecnología que en todo momento represente su versión más actualizada. Actualmente se pueden encontrar puntos comunes en tecnología que representan la base de los bancos digitales: automatización, analítica avanzada y *machine learning*, blockchain y arquitectura en nube. Mientras los bancos tradicionales incursionan en estas, los bancos digitales nacen adoptándolas. Sin embargo, la naturaleza nativo-digital de estos bancos deberá estar diseñada de manera que la operación sea fácilmente migrable a nuevas tecnologías. Los bancos digitales, en esencia, deben ser agnóstico-digitales: no preferir una tecnología sobre otra por el simple hecho de haberla adoptado antes.

Como lo hemos mencionado en otros textos, esto hace que *la magia de la digitalización y tecnología de las operaciones bancarias sucede en lo que no se puede ver o no es del todo evidente para el cliente*[8]. El cambio en el paradigma de cómo opera un banco tradicional a cómo opera un banco digital ocurre en el *back-office*[9], en la forma como estos operan y en la tecnología e información en la que se encuentran soportados.

Ha sido común ver cómo los bancos tradicionales se han apresurado a crear un *front-office*[10] digital, soportando en tecnología *legacy* las operaciones. Este tipo de operación trae consigo costos mucho más altos, limitaciones a la escalabilidad, ineficiencia en las operaciones y limitación en el uso y manejo de la información. Un ejemplo: en distintos países, los bancos tradicionales ofrecen créditos digitales que la persona solicita en línea -a través de Internet o de un dispositivo móvil-, pero el estudio del crédito, su formalización y el desembolso no se realizan en ese mismo momento, por cuanto tienen que surtir un proceso soportado en tecnología o procesos más antiguos. Para ponerlo en blanco y negro, imagine un crédito digital que se aprueba al día siguiente y le envían un funcionario del banco a su casa a tomar la firma de los documentos. No parece ser tan digital.

Y esto redunda en el punto: la infraestructura tecnológica para ofrecer servicios digitales debe comprender desde la interfaz del usuario hasta la forma como se opera el banco

[7] Término que se utiliza para describir tecnología que ya no se puede considerar actual o actualizada.
[8] Ibid.
[9] El conjunto de áreas que se encargan de la operación bancaria.
[10] Lo que interactúa directamente con el cliente.

en el *back office*. Solo así se logrará el estándar de operación que demanda el cliente, así como la posibilidad de escalar -crecer en productos, servicios, clientes- continuamente, tener los más altos estándares de seguridad, capacidad más rápida de recuperación de la infraestructura y reducción de los costos de operación de los clientes.

Aunque partimos del agnosticismo tecnológico y de no preferir una tecnología sobre otra por su momento de adopción, es importante analizar, así sea sucintamente, cuatro fenómenos tecnológicos que marcan la pauta de la operación actual de los bancos digitales:

3.1.3 Automatización

La automatización *consiste básicamente en crear un hardware o software que sea capaz de hacer las cosas automáticamente, sin intervención humana*[11]. Es decir, realizar operaciones utilizando tecnología y de manera automática, sin necesidad de la intervención de personas.

A través de la automatización, los bancos digitales logran mayor eficiencia y agilidad en sus procesos, en su capacidad de procesamiento de información, en el volumen de operaciones y transacciones que se pueden realizar y en la capacidad de dedicar las personas que contratan a procesos que le aportan mayor valor al banco:

> *La automatización tiene un único propósito: permitir que las máquinas realicen tareas repetitivas y monótonas o en palabras de algunas personas ´sacar al robot del humano´. Esto libera tiempo para que las personas se concentren en tareas más importantes y creativas que requieren el toque personal y el juicio. El resultado final es un negocio más eficiente, rentable y una fuerza laboral más productiva*[12].

La condición nativo-digital de los bancos digitales hace que sus fundamentos se encuentren atados a la automatización de procesos desde el inicio.

3.1.4 Analítica avanzada, *machine learning* e inteligencia artificial

La industria financiera ha tenido que migrar hacia una madurez en la utilización de información y datos. Hoy en día es imposible pensar en un escenario de digitalización y de prestación de servicios financieros sin pensar en analítica avanzada de datos. Los bancos reciben los datos de todo tipo de fuentes y en diferentes formas.

La analítica avanzada de datos aplicada a la operación de los bancos favorece su rendimiento al mejorar la forma en la que segmentan, dirigen, adquieren y retienen clientes y, en general, la forma en la que opera el banco[13]. En definitiva, *tendrá una mejor oportunidad en el mercado una institución que tome sus decisiones basadas en datos que aquella que no las toma de esta manera*[14]. Utilizar analítica avanzada de datos es una condición *sine qua non* de operación de bancos digitales que no todos los bancos tradicionales han adoptado.

---

[11] Kamila HANKIEWICZ. What Is The Real Difference Between Automation And AI? Becoming Human. Disponible en línea: https://becominghuman.ai/what-is-the-real-difference-between-automation-and-ai-366513e0c910 [Consultado el 26 de marzo de 2020]. Traducción del autor.
[12] Kamila HANKIEWICZ. Op. Cit.
[13] Ajit SINGH. Predictive Data Analytics and Banking. Patna Women's College. Bihar, 2019, p. 1.
[14] Peredo Bernal, Juan Sebastián. Capítulo 4: Los Bancos Digitales: Neobancos. Los mercados financieros ante la disrupción de las nuevas tecnologías digitales. Bogotá: Universidad Externado de Colombia. 2021.

Cuando se habla de *machine learning*, nos referimos al fenómeno mediante el cual un algoritmo -código- se mantiene actualizado al tener la capacidad de aprender a partir de datos y sin la necesidad de interferencia humana. Por otro lado, la inteligencia artificial se entiende como el fenómeno que le permite a una máquina tomar decisiones como un humano y simular sus acciones, es decir, tomar decisiones con inteligencia.

La nueva generación de servicios financieros está alineada con una utilización profunda de datos, como se mencionó, y con la incorporación de *machine learning* e inteligencia artificial:

> *Servicios financieros diseñados a partir de datos, a partir de la ingesta de enormes cantidades de datos que es procesada de manera automática y que permite, mediante el uso de herramientas tecnológicas, el constante aprendizaje y evolución, de manera que todos esos beneficios que se mencionaban arriba en relación con analítica avanzada continúen siendo actualizados y permitan a las instituciones tomar decisiones*[15].

Esta capacidad aumentada respecto de la información y su capacidad de procesamiento representa una ventaja en términos de conocimiento del cliente y de ofrecimiento de productos diseñados a la medida, lo que nos permite volver al eje central de los bancos digitales: los clientes.

3.1.5 Computación en la nube

El fenómeno de computación en la nube, consistente en dejar de lado los servidores *on-premises* -servidores administrados por la entidad-, de permitir almacenamiento de datos, *software*, plataformas de desarrollo de *software*, a través de Internet, sin la necesidad de una gestión activa por parte del usuario del servicio[16], es algo especialmente relevante a la hora de hablar de los bancos digitales. En la computación en la nube los centros de cómputo no se encuentran ubicados en la infraestructura del banco; están ubicados en diferentes países, con funciones distribuidas en servidores en distintos lugares y a los cuales se accede a través de Internet[17].

La magia de todo esto reside en que los proveedores de servicios en la nube administran completamente la infraestructura física. El usuario, que es el banco, paga por los servicios que consume. Cualquier discusión del pasado sobre adquisición de servidores y nuevas oficinas para ubicarlos, así como el presupuesto para su mantenimiento, queda olvidada. Queda olvidado también el miedo de no poder escalar los servicios del banco al no tener una capacidad instalada de servidores suficiente para responder a incrementos de demanda. Con la arquitectura en la nube, el proveedor de servicios solo cobrará por la cantidad consumida por el banco. No existe, desde la perspectiva del banco, una limitación natural dada su capacidad instalada.

El fenómeno de la arquitectura en la nube, en tanto permite diseñar la arquitectura tecnológica del banco para que su capacidad esté soportada en los proveedores de esos servicios, es particularmente interesante al analizar la infraestructura de bancos digitales y bancos

[15] Ibid.
[16] Definición a partir de la descripción de servicios de computación en la nube provistos por empresas como Microsoft, Amazon Web Services y Google.
[17] Peredo Bernal, Juan Sebastián. Capítulo 4: Los Bancos Digitales: Neobancos. Los mercados financieros ante la disrupción de las nuevas tecnologías digitales. Bogotá: Universidad Externado de Colombia. 2021.

tradicionales. Los bancos digitales traen consigo, naturalmente, este tipo de tecnología que permite economías de escala, mayor eficiencia en el gasto en tecnología, mitigación de riesgos y mejores tiempos de recuperación -ante eventos de indisponibilidad del servicio-. Los bancos tradicionales, soportados desde hace décadas en tecnología *on-premises*, han buscado aceleradamente movilizarse hacia infraestructura en la nube, con la diferencia de que su arquitectura tecnológica no fue diseñada así desde el inicio. Esta diferencia ha hecho más compleja su movilización hacia tecnología en la nube.

Es interesante ver cómo el British Bankers' Association en el 2017 identificó tres motivos para la adopción de tecnologías en la nube para los bancos[18]: (i) innovación ágil: al mejorar la agilidad, eficiencia y la productividad; (ii) mitigación de riesgos: la tecnología en la nube permite reducir los riesgos asociados con la tecnología tradicional, tales como la capacidad, redundancia -replicar la información en más de un lugar- y resiliencia -su capacidad de recuperación-, y (iii) costo-beneficio: el ahorro es significativo, especialmente al tener en cuenta la reducción en la inversión de capital frente a la inversión requerida en tecnología tradicional.

Esto hace que la arquitectura en nube sea uno de los grandes diferenciadores de competencia en la operación de bancos digitales y bancos tradicionales. No solo una entidad nueva puede partir de un territorio equilibrado frente a los incumbentes -aquellos que operan desde hace años-, sino que puede comenzar su operación con la posibilidad de escalar rápidamente y de tener una capacidad de procesamiento aún mayor que la de un banco tradicional con décadas de adquisición, renovación y mantenimiento de servidores propios. Todo desde una perspectiva nativa, sin necesidad de llevar a cabo complejos procesos de transición.

Por último, entendiendo que una de las necesidades principales de los bancos digitales es el procesamiento de información continuo, la tecnología que se utilice para este propósito es fundamental. Los negocios basados en datos tienen una necesidad intrínseca de capacidad de procesamiento. A mayor cantidad de información, mayores volúmenes para analizar y, por lo tanto, mayor la capacidad de procesamiento requerida. La arquitectura en la nube está diseñada para permitir esta capacidad de procesamiento.

3.1.6 Blockchain

Blockchain es uno de los avances más importantes en materia tecnológica del último siglo. Los bancos digitales, por su misma condición, y en general el sistema financiero han adoptado gradualmente esta tecnología para diferentes etapas de sus procesos. También los bancos digitales y el sistema financiero internacional han comenzado a incluir en su balance bitcoins y otros criptoactivos -situación que todavía no se ha podido presentar en Colombia-. El constante desarrollo de productos relacionados con criptoactivos por parte de bancos en Estados Unidos, la compra por parte de empresas que cotizan en la Bolsa de Nueva York, la adopción de bitcoin como moneda de curso legal, son tan solo algunos ejemplos de la penetración de los criptoactivos y las criptomonedas en el día a día del sistema financiero y monetario.

Los bancos digitales, en tanto hacen parte de un sistema regulado, son el actor por excelencia para generar una simbiosis entre blockchain como tecnología, los criptoactivos y

[18] BRITISH BANKER'S ASSOCIATION. Banking on Cloud: A discussion paper by the BBA and Pinsent Masons. London: BBA, 2016, p. 3.

el sistema financiero tradicional. La capacidad tecnológica instalada, su desarrollo a partir de la demanda de nuevos productos y servicios por parte de sus clientes, y el afán constante de los bancos digitales de explorar nuevas fronteras tecnológicas hacen que sea natural su participación en procesos relacionados con blockchain.

Por su impacto en diferentes esferas de la operación financiera, se ha vuelto esencial comprender tanto el blockchain como los criptoactivos y los NFTs, especialmente al evidenciarse el sinnúmero de casos de uso. Los invito a leer el capítulo de *Metaverso y los servicios financieros* para explorar un poco más sobre este tema.

3.2 Desde lo subjetivo

Después de ver algunas características objetivas con las que se puede identificar a los bancos digitales, es necesario hablar de las subjetivas. Subjetivas porque son difícilmente medibles y parten de la apreciación que cada uno le dé a un banco digital particular.

Fácilmente podríamos encontrar bancos tradicionales que viren sus modelos de negocio, su infraestructura tecnológica y su forma de operar a lo digital, de manera que cumplieran cada una de las características objetivas vistas. Sin embargo, eso no los haría bancos digitales o neobancos.

Los bancos digitales deben retar el *statu quo* de la industria. Esta es su esencia, una esencia que busca soluciones diferentes de las que se encuentran en la industria y que logra a través de la tecnología y a partir de la adopción cultural de la misma. No tiene mayor sentido pensar en bancos digitales que simplemente traigan tecnología para replicar modelos de negocio tradicionales.

Esta característica, subjetiva en su esencia, resulta fundamental al momento de evaluar si un banco es verdaderamente digital. Y es fundamental porque la llegada de los bancos digitales debe constituir una reformulación de la industria y no una continuación de lo mismo a partir de tecnología.

Es decir, la adopción tecnológica es simplemente un paso conforme al cual los bancos digitales operan. Lo que los vuelve realmente interesantes, lo que los hace diferentes frente a la operación digital de bancos tradicionales es esa capacidad retadora que pueden traer a la forma como se concibe el sistema financiero. No se trata de incorporar un banco, con operación digital, para afrontar el negocio bancario de la misma manera en que los otros bancos lo vienen haciendo. Se trata de bancos nativos de una cultura digital arraigada en la sociedad y de un entendimiento profundo de las demandas de esa sociedad frente a la forma en la que le son prestados los servicios financieros. Esa cultura retadora se evidencia cuando los costos asociados a productos desparecen porque la operación digital más eficiente los hace innecesarios, cuando las tasas ofrecidas en los productos de crédito bajan, cuando las variables de información para el otorgamiento de créditos se multiplican y dejan de lado las tradicionales variables que ha venido utilizando la banca, cuando se llega a todos los rincones del país porque no se necesita de sucursales para ofrecer productos.

Como todo lo que corresponde a un criterio subjetivo, será cada uno quien juzgue, con el paso del tiempo, si un nuevo operador bancario digital es o ha sido retador frente al sistema

financiero, si ha logrado cambiarlo a partir de sus nuevas ideas, de su nueva forma de relacionarse con el mercado.

Entonces, agregar todas las características objetivas que hemos mencionado más un diseño que responde a las necesidades de los clientes, una operación rápida y eficiente que parte de la tecnología, un uso intensivo de datos para entender el mercado y a sus clientes, más un fundamento retador al estado actual del sistema financiero da como resultado un banco digital, un neobanco.

4. En la constante búsqueda de un nuevo modelo de negocio

Los bancos digitales han traído un modelo de negocio en el que el cliente se encuentra en el centro de la operación. Esto ha hecho que el desarrollo de las plataformas, los productos y servicios tengan en cuenta esas demandas de los clientes -rapidez, eficiencia, facilidad de uso, constantemente operativos, sin cargos extra- al momento de ser construidos. No es que se replantee el negocio de la intermediación financiera, sino que se exploran nuevos modelos que tengan una relación más natural y menos distante con los consumidores.

Al estar en el centro de su negocio, entender al cliente y ofrecer lo que necesita ha pasado a ser una condición *sine qua non* para la operación de los bancos digitales. Lo vimos al hablar de la analítica avanzada de datos como elemento central de los bancos digitales. Entender al cliente y sus necesidades y características permite ofrecer productos y servicios adecuados a las mismas y evitar, al mismo tiempo, productos y servicios que no se necesitan.

Como parte de esa búsqueda, los bancos digitales se han vuelto los grandes exploradores de tres modelos que, aunque con algunas similitudes, son al final diferentes: *Open Banking, Banking-as-a-Service y Platform Banking*. Cada uno con su capacidad de ofrecer nuevos productos y servicios a los clientes. Cada uno rompe con la visión tradicional en la que el banco o el grupo de sus entidades afines están encargadas de desarrollar y ofrecer todos los productos y servicios a los clientes.

Open banking como ese modelo a través del cual los bancos les permiten a determinados terceros acceder a la información de los clientes que tienen en común, de manera que, a partir de la información que reciben de los bancos, los terceros puedan ofrecerles a esos clientes productos y servicios.

La experiencia financiera del cliente se expande al permitir que la información que tiene en su banco pueda ser compartida con terceros que le proveen otro tipo de servicios. Esto nutre los modelos de negocio de los bancos digitales, al lograr, mediante *Open Banking*, la ampliación de la oferta de productos, servicios, funcionalidades, apalancados en su operación bancaria. El mercado migrará hacia aquellas entidades que ofrezcan un portafolio propio y de terceros mayor, beneficiando este tipo de bancos.

En esta misma línea, mencionamos los modelos de *Banking-as-a-Service* que les permiten a terceros acceder a las funcionalidades del banco, de manera que las puedan utilizar con sus clientes. Es decir, los terceros acceden a las funcionalidades asociadas a una licencia bancaria -que solo son utilizables por quien tiene este tipo de licencia- para efectos de prestar un servicio. Es similar a un esquema de marca blanca en el que el tercero ofrece

servicios a sus clientes apalancado en la estructura de una entidad con licencia bancaria. Como ejemplo de esto se ven aplicaciones que ofrecen cuentas corporativas totalmente digitales, en las que la operación del *front-office* lo realiza esa aplicación digital y la cuenta es abierta en un banco, es decir, los recursos se encuentran en un banco, pero la gestión del cliente se realiza por la aplicación digital corporativa.

Nuevamente, desde la perspectiva del banco digital y de su modelo de negocio se explota la licencia bancaria, de manera que se gana capilaridad en el sistema a través de la integración de terceros. Los terceros prestarán sus servicios, lo que a su turno redundará en beneficio del banco, permitiéndole ganar clientes.

Sin embargo, esta búsqueda de nuevas formas de integrar a terceros en la oferta de productos y servicios que se ponen a disposición de los clientes de los bancos no se queda ahí. Los bancos digitales alrededor del mundo han venido encontrando en sus plataformas una posibilidad de vinculación de nuevos productos y servicios, plataformas que no obliguen a los consumidores a desplazarse a diferentes lugares y que busquen, en un solo sitio, ofrecer una multiplicidad de servicios. Esto nos lleva al fenómeno del *Platform Banking*, que es una historia completamente diferente. Se refiere a los bancos que integran servicios de otras empresas para aumentar su oferta existente. Tener en una sola plataforma, en una sola app, una multiplicidad de servicios bancarios y no bancarios, que permitan la profundización de la oferta y la satisfacción de necesidades de sus clientes. Por ejemplo, encontrar en una aplicación bancaria la posibilidad de comprar productos ofrecidos por el *marketplace* de un tercero y, a su vez, poder gestionar la cuenta bancaria.

Con esos tres modelos, *Open Banking, Banking-as-a-Service y Platform Banking* podemos empezar a entender por qué la relación de los bancos digitales con el mercado es mucho más abierta. Es una relación en la que se busca expandir los horizontes de lo que puede hacer el banco por sus clientes, de lo que puede ofrecerles. Se distancia de esa concepción de décadas atrás en la que los bancos desarrollaban todos los productos que querían ofrecer.

Estos nuevos modelos les permiten a los bancos ahondar en su digitalización, al permitir a terceros con otras capacidades tecnológicas prestar servicios, desde la plataforma del banco o la propia del tercero. Desde estos nuevos modelos de negocio las limitaciones regulatorias de ser banco dejan de serlo, porque ser banco se convierte en un activo adicional -la licencia bancaria como habilitador de nuevos negocios-. En palabras del BIS: *La adopción de API*[19] *públicas para el intercambio de datos podría generar oportunidades para que los bancos y terceros obtengan información y estimulen la innovación en los servicios financieros. Una economía de intercambio de datos podría cambiar el modelo de negocio bancario tradicional*[20].

[19] Interfaz de programación de aplicaciones que permite conectarse entre entidades.
[20] BANK FOR INTERNATIONAL SETTLEMENTS [BIS] Basel Committee on Banking Supervision. Report on open banking and application programming interfaces. Basilea: Bank for International Settlements, 2019, p. 9.

5. El ambiente regulatorio que permite prosperar a los bancos digitales

Se pueden encontrar muchos retos regulatorios al evaluar las características que tienen los bancos digitales y los modelos de negocio que persiguen. Retos que pasan, principalmente, por asegurar un diseño normativo que permita la innovación, iteración -constante prueba y cambio- de tecnología y modelos de negocio.

Para lograr este propósito, es imperativo que la regulación se diseñe bajo el respeto al principio de neutralidad tecnológica tanto en la expedición de nuevas normas como en la evaluación de las normas existentes.

Evidentemente, al hablar de bancos digitales se deberá hablar de las reglas prudenciales que atañen a la actividad bancaria. Sin embargo, esa regulación sobre la actividad bancaria no debe ser excusa para que se regule sobre tecnología generando una preferencia sobre un tipo de tecnología o de otro. Al final, los bancos, sean digitales o no, deberán hacer un diseño juicioso de su gestión de riesgos, lo que implica necesariamente la exposición a tecnología.

Un ambiente regulatorio amigable con la tecnología permite la existencia de entidades financieras digitales.

La existencia de por lo menos un banco digital en el país demuestra que el estado de maduración tecnológico y regulatorio ha derivado en la capacidad de que Colombia pueda tener este tipo de entidades en operación.

Esto en el marco de entender que las normas que rigen a los bancos digitales son las mismas que rigen a los bancos tradicionales. Es decir, en su actuar, los bancos digitales en Colombia deberán seguir la normativa aplicable a los bancos, en especial la relacionada con el cumplimiento de las normas prudenciales y de protección de los consumidores financieros. En este punto regresamos a la concepción inicial de banco y a la actividad de intermediación financiera: la importancia de que un banco digital sea una entidad sometida a la regulación bancaria -sin perjuicio de que la misma se adapte en los diferentes países para permitir el correcto despliegue tecnológico- radica en que se le atribuye, como a un banco tradicional, la protección del ahorro de las personas y la estabilidad del sistema financiero. Esta perspectiva es similar a la de otras jurisdicciones. La actividad bancaria, en una buena parte, es una actividad regulada.

Sin embargo, la regulación de los bancos digitales o, mejor, las normas que afectan su operación sobrepasan naturalmente la regulación bancaria propiamente dicha. Tener un modelo de negocio basado en datos -tomar decisiones a partir de la información existente, las métricas y los resultados que esta ofrece- con tecnología particular para habilitar dicho modelo, trae consigo múltiples retos frente a la protección de los datos personales de clientes.

Al analizar este aspecto, se debe entender que *(e)n el caso de modelos de negocio basados en datos, la discusión para efectos de cumplir con las normas de protección de datos implicará un ejercicio detallado de la infraestructura de datos, incluyendo específicamente:*

los datos que se utilizarán, la identificación del tipo de datos de acuerdo con la legislación aplicable, los lugares donde se procesarán los datos, los acuerdos que se tendrán con los terceros que tienen encargado el procesamiento de datos y las finalidades para las cuales esos datos serán utilizados[21].

En un modelo de negocio basado en datos, el diseño para cumplir con la obligación de obtener la autorización previa y expresa para el tratamiento de datos personales de sus clientes es más complejo y solo puede responderse desde el análisis de la infraestructura de datos del banco digital. Si habláramos de un modelo de negocio tradicional, es mucho más fácil identificar las fuentes y usos de los datos; al final, el número es significativamente menor. En un modelo de negocio basado en datos, solo a partir del análisis y construcción de la infraestructura de dicha información se podrá entender cuál usará el banco, qué tipo de datos tratará, si necesitará procesar información en países diferentes y para qué se utilizarán los datos.

A esto se debe sumar la seguridad desplegada para la protección de la información. En el caso de los bancos, la regulación bancaria fija estándares en relación con los parámetros de cumplimiento que deben tener, los que se deberán complementar con la regulación de protección de datos aplicable en otros países. Sin embargo, la responsabilidad es de cada entidad, serán su arquitectura de tecnología y las características de almacenamiento y tránsito de información las que darán la pauta respecto de la mejor manera de proteger la información.

También se debe tener en cuenta, tomando lo que vimos atrás, que al habilitar modelos de negocio que se apalancan en *Open Banking, Banking-as-a-Service y Platform banking* se presentan retos adicionales. Básicamente, el punto crucial frente a este tipo de modelos está dado por el acceso que se les otorga a terceras partes a información del consumidor para la prestación de servicios. Es decir, permitir que terceros accedan a la información financiera de clientes en un banco. De nuevo, citando al BIS: *Sin embargo, a pesar de las oportunidades potenciales, la expansión del intercambio de datos también podría exponer al sector bancario a un conjunto ampliado de riesgos operativos y de reputación*[22].

La legislación y regulación en los diferentes países es diferente: algunos exigen el *Open Banking* de sus instituciones, otros lo facilitan o lo restringen, y algunos más están aún buscando qué camino seguirán[23], en el intento de encontrar normativamente ese balance que menciona el BIS: salvaguardar la innovación y el avance de tecnología, y al mismo tiempo preservar la seguridad en la prestación de servicios financieros.

En el caso colombiano, estará a cargo de cada entidad determinar los estándares de protección y control de riesgos para gestionar modelos de apertura singulares.

Esto nos da pie para mencionar otro de los asuntos relevantes de los bancos digitales, especialmente en su relación con la regulación existente para bancos tradicionales: la gestión

[21] Ibid.
[22] BANK FOR INTERNATIONAL SETTLEMENTS [BIS] Basel Committee on Banking Supervision. Report on open banking and application programming interfaces. Basilea: Bank for International Settlements, 2019, p. 9.
[23] Peredo Bernal, Juan Sebastián. Capítulo 4: Los Bancos Digitales: Neobancos. Los mercados financieros ante la disrupción de las nuevas tecnologías digitales. Bogotá: Universidad Externado de Colombia. 2021.

de riesgos. La infraestructura tecnológica, el modelo de negocio y la forma de vinculación de clientes traen varios retos nuevos para la perspectiva regulatoria.

La administración de los riesgos operativo y de ciberseguridad a partir de estructuras digitalizadas, de arquitectura en la nube, de conexión con terceros genera que las entidades deban tener clara la estructura de gestión y medidas de control. Como se mencionó, la administración de estos riesgos dependerá de cada entidad. Con la llegada de nueva tecnología, estará en cada entidad el análisis correcto de beneficios, riesgos y controles para su adecuada gestión. Para los reguladores, exige el entendimiento de estos nuevos modelos de operación, la tecnología subyacente, sus beneficios y riesgos. Los marcos regulatorios deben tender a la adopción de nueva tecnología facilitando la información, pero sin perder de vista que será responsabilidad de la entidad la adecuada gestión del riesgo y el cumplimiento de los estándares mínimos exigidos por la regulación. En Colombia, la actuación del supervisor se ha traducido en instrucciones relacionadas con la gestión y seguridad en los canales y la tecnología que se utiliza para efectos de realizar transacciones por parte de los clientes.

En materia de riesgo de crédito, el análisis parte de una visión en analítica de datos y *machine learning* de las herramientas que se diseñan para el modelo de otorgamiento, así como la tecnología que acompaña la administración de este riesgo. A esto se debe sumar la adecuada gestión de la cartera, con un especial énfasis en la originación. Para los bancos digitales, la originación digital pasa por la habilitación legal que surge de la Ley 527 de 1999. Corresponderá a cada entidad la adecuada administración de los protocolos para la celebración de actos jurídicos por medios electrónicos. De esta forma, la cobranza no se ve afectada por la utilización de mecanismos digitales[24].

Finalmente, en materia de riesgo de lavado de activos y financiación del terrorismo, la regulación colombiana y las instrucciones de la Superintendencia Financiera han buscado adaptarse a las nuevas realidades en materia de conocimiento del cliente. Los primeros pasos se dieron con una reducción de la carga obligatoria para productos como los depósitos electrónicos, permitiendo su adquisición por los clientes a través de un trámite simplificado. Posteriormente, la Superintendencia Financiera replanteó la relación que se tenía con los mecanismos tradicionales de conocimiento del cliente y evolucionó hacia un sistema que, soportándose en el análisis de las entidades reguladas, buscara el control del riesgo de lavado de activos y financiación del terrorismo.

De alguna manera, a través de los riesgos se ha podido evidenciar una evolución en la postura regulatoria y de supervisión que propende por un marco mayor de innovación y de adaptación a nueva tecnología.

Lo que nos lleva nuevamente a esa frase del inicio de este título: un ambiente regulatorio amigable con la tecnología es uno que permite la existencia de entidades financieras digitales.

Un aspecto fundamental de la regulación amigable con la tecnología se basa en defender en todo momento el principio de neutralidad tecnológica. Defender que la tecnología es un medio para la prestación de los servicios financieros. Y recordar constantemente que se debe buscar esa *aplicación analógica del derecho cuando la actividad realizada es exactamente la*

[24] Ibidem.

misma independientemente del soporte utilizado, lo que supone implícitamente la existencia de límites en la aplicación de normas vigentes para actividades novedosas y, por tanto, la posibilidad de establecer nuevos regímenes jurídicos para las nuevas actividades, posibilidad mediada por el principio de proporcionalidad (…)[25].

La evolución, innovación y continua búsqueda de nuevas fronteras por parte de los bancos digitales, y por parte de la industria financiera en general, deben estar respaldadas por un marco regulatorio que permita que esas nuevas herramientas sean adoptadas sin necesidad de esfuerzos adicionales. Ese marco regulatorio deberá estar diseñado para permitir a los consumidores satisfacer sus nuevas demandas, en el marco de la evolución de cultura digital.

6. Conclusiones

A lo largo de este texto surgen una serie de conclusiones. Los bancos digitales resultan de la integración de una arquitectura tecnológica para prestar servicios financieros de manera completamente digital y de la adopción cultural de mecanismos digitales por parte de la sociedad para consumir productos y servicios. Son una respuesta acertada a la exigencia del mercado de poder utilizar dispositivos móviles para la realización de sus actividades diarias, incluyendo la actividad financiera.

Sin embargo, esto último no es lo único que hace que un banco digital sea considerado como tal. Dentro del ámbito subjetivo, los bancos digitales retan el *statu quo* del sistema financiero, replantean la forma de competir en el mercado bancario y buscan demostrar cómo, a través de tecnología, se puede alterar la forma en la que los clientes interactúan con la banca. Esto nos lleva a que los bancos digitales deben integrar factores objetivos -tecnológicos- y factores subjetivos -culturales y de razón de ser del modelo de negocio-.

Al combinar estos factores, la llegada de los bancos digitales y sus novedosos modelos de negocio derivan en una nueva ola de competencia en el sistema financiero. Estos nuevos modelos de negocio basados en tecnología traen consigo un reto a la forma de operar de los bancos tradicionales, que tendrán que adaptarse de manera que puedan sobrevivir a la *ola de disrupción habilitada por la tecnología*[26].

Y esa ola de disrupción habilitada por la tecnología no frena con la llegada de bancos digitales. Esa ola viene de la mano de modelos de negocio financieros descentralizados, de nuevas formas de prestar servicios financieros ágiles por parte de entidades no reguladas, de la agregación de servicios financieros por empresas de tecnología.

Esto implica que los bancos digitales deberán estar diseñados para poder competir con nuevos modelos de negocio no regulados que reemplazan, de una manera u otra, servicios tradicionalmente financieros. Los bancos digitales deberán estructurarse de manera que puedan estar constantemente en la punta de lanza de la innovación tecnológica y financiera. Los bancos digitales deberán estructurarse de manera que comprendan constantemente el estado de adopción cultural de la tecnología y las demandas de la sociedad.

[25] Carles Alonso ESPINOSA. "La información en la red y el principio de neutralidad tecnológica: la libertad de expresión y la difusión de información administrativa." Revista Derecho del Estado: Bogotá, Universidad Externado de Colombia, No. 22, 2009, p. 87.
[26] BANK FOR INTERNATIONAL SETTLEMENTS [BIS] Basel Committee on Banking Supervision. *Sound Practices: Implications of fintech developments for banks and bank supervisors. Basilea: Bank for International Settlements. 2018.*

Bibliografía

Bank for International Settlements [BIS] Basel Committee on Banking Supervision. *Sound Practices: Implications of fintech developments for banks and bank supervisors*. Basilea: Bank for International Settlements. 2018.

Bank for International Settlements [BIS] Basel Committee on Banking Supervision. *Report on open banking and application programming interfaces*. Basilea: Bank for International Settlements, 2019.

British Banker's Association. *Banking on Cloud: A discussion paper by the BBA and Pinsent Masons*. London: BBA, 2016.

Espinosa, Carles Alonso. La información en la red y el principio de neutralidad tecnológica: la libertad de expresión y la difusión de información administrativa. Revista Derecho del Estado: Bogotá, Universidad Externado de Colombia, No. 22, 2009.

Hankiewicz, Kamila. *What Is The Real Difference Between Automation And AI?* Becoming Human. Disponible en línea: https://becominghuman.ai/what-is-the-real-difference-between-automation-and-ai-366513e0c910 [Consultado el 26 de marzo de 2020]. Traducción del autor.

Peredo Bernal, Juan Sebastián. Capítulo 4: Los Bancos Digitales: Neobancos. Los mercados financieros ante la disrupción de las nuevas tecnologías digitales. Bogotá: Universidad Externado de Colombia. 2021.

Singh, Ajit. Predictive Data Analytics and Banking. Patna Women's College. Bihar, 2019.

CAPÍTULO 11

La regulación de los prestadores de servicios de pagos digitales

María Fernanda Quiñones Zapata[1]

Resumen

La regulación refleja la evolución que han tenido los prestadores de servicios de pagos digitales en la vida económica, el papel que han jugado en las dinámicas de consumo de las personas y la capacidad que tienen para contribuir al desarrollo y a la competitividad del país. Los pagos digitales han trascendido el carácter instrumental relativo a la extinción de obligaciones dinerarias y se han convertido en un articulador de los roles que los diferentes agentes juegan en la economía. Los prestadores de servicios de pago digitales han estado a la base de los hitos más relevantes de la reglamentación, desde la perspectiva del control de los riesgos asociados a su operación y su incorporación a la arquitectura del sistema financiero como agentes con una función propia y transcendente, hasta el reconocimiento de su capacidad para impulsar la real implementación de políticas públicas sobre inclusión financiera. Estas entidades deben regularse desde una perspectiva holística, que incluye no solo aquello que pueda plantearse desde el regulador financiero, sino también aspectos como la protección de los datos personales, el derecho al consumo, las normas sobre protección de la competencia, el comercio electrónico y los temas tributarios que les incumben, entre otros.

[1] Abogada de la Universidad de los Andes. MBA y especialista en derecho administrativo, constitucional y financiero. Durante once años trabajó como secretaria general, directora jurídica y gerente jurídica en CredibanCo. Actualmente es presidente ejecutiva en la Cámara Colombiana de Comercio Electrónico, donde lidera acciones y estrategias para fortalecer el comercio electrónico en el país.

1. Introducción

Un pago digital es una operación que conecta a proveedores y consumidores en un ambiente virtual. Para que las transacciones se den en este entorno, el proveedor pone a disposición alternativas de pago diferentes al dinero en físico, en las que el consumidor encuentra posibilidades más convenientes para gestionar sus recursos y satisfacer sus necesidades.

Entre los principales instrumentos que permiten el pago de bienes y servicios en ambiente digital están, en esencia, las tarjetas débito y crédito y las transferencias electrónicas -débito y crédito-[2]. Nos centraremos en las tarjetas e instrumentos de pago electrónicos, que se utilizan para transferir fondos desde la cuenta que un pagador tiene en una entidad financiera hacia el beneficiario del pago, por razones como la compra de bienes, la prestación de servicios o la transferencia de recursos por sí misma. En este capítulo veremos justamente aquellos sistemas que procesan transacciones con instrumentos de pago electrónicos y entenderemos los roles de los diferentes agentes que participan de estas operaciones.

La evolución de estos instrumentos de pago y de los sistemas de pago en donde se utilizan se explica en tres grandes hitos: (i) los sistemas de pago comienzan a ser vigilados por la Superintendencia Financiera; (ii) se regulan los instrumentos de pago buscando su masificación, y (iii) se reconoce la capacidad de los sistemas de pago para promover y materializar la inclusión financiera y, por ende, el desarrollo económico del país.

En las dinámicas económicas actuales los pagos cumplen un nuevo rol. Su función va más allá de cancelar obligaciones. Se han convertido en parte importante de la cotidianidad de los usuarios, al evidenciar sus preferencias y generar información sobre su forma de perfilarse en la vida económica[3].

Así mismo, los desarrollos tecnológicos y cambios culturales de las últimas décadas han transformado las formas de consumo, modificando el relacionamiento de los agentes del mercado: las empresas, las familias y el Estado. Estos avances también han generado una mayor interdependencia entre diferentes industrias especializadas en segmentos específicos del proceso de consumo. Resulta imposible pensar, por ejemplo, en una operación de comercio electrónico sin la incidencia del *marketing digital* como determinador de la decisión de consumo del comprador, o de la industria logística como facilitadora para el cumplimiento de la promesa de valor al cliente y de los pagos como la ruta para lograr una experiencia segura y fácil, sin fricciones, que permita el efectivo proceso de transferencia del bien o servicio.

A su turno, el progresivo avance de la digitalización, acompañado de regulaciones que lo facilitan y promueven su masificación, ha transformado de manera importante las relaciones económicas. Para lograrlo, se ha buscado crear ecosistemas que provean servicios de procesamiento de información, que funcionen como centros de datos y perfeccionen las transacciones financieras, favoreciendo la movilización efectiva de recursos.

Sobre estas premisas, resulta entonces innegable la correlación entre la madurez de los sistemas de pago y el desarrollo de una economía, pues a medida que aumenta el valor de

[2] Banco de la República de Colombia. (2020). *Reporte de Sistemas de pago 2020*. Bogotá: Banco de la República de Colombia.
[3] Muñoz, M. C.-M. (2021). *Derecho de las Obligaciones - Cap 13 Pago por Medios Electrónicos*. Bogotá: Universidad de Los Andes - Temis.

la actividad económica de un país se complejizan las relaciones entre los distintos actores y la necesidad del flujo de capital. Las consecuentes presiones de economía de escala -en la que la actuación de una empresa produce efectos económicos favorables para ella o para su industria- llevan a una mayor innovación y competencia de los proveedores de pagos, con reducción de los costos marginales, esto es, el costo unitario del procesamiento.

Aportamos el siguiente diagrama, con el objetivo de ilustrar los roles, actividades y alcance de las interacciones entre los agentes que participan en los pagos digitales de manera que, a lo largo del texto, podamos comprender más fácilmente las múltiples relaciones que se derivan de la realización de una transacción digital.

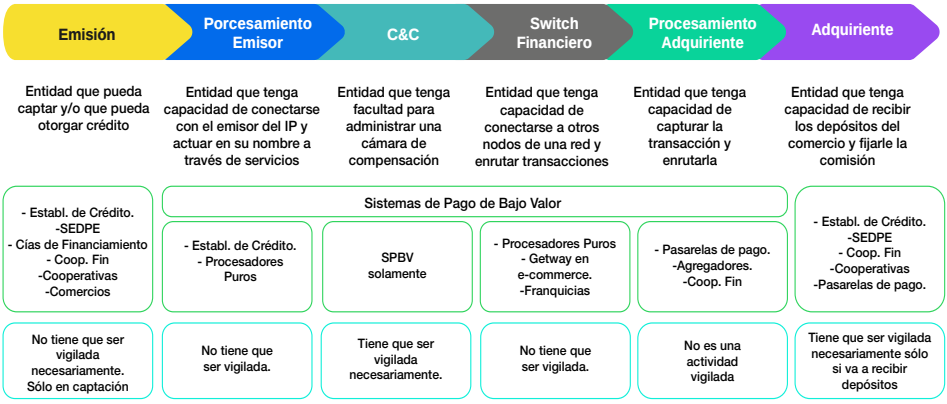


Figura 1. Actores y Roles en un Ecosistema de pagos. Elaboración Propia.

A continuación, describiremos en tres secciones cómo la regulación ha acompañado la evolución de los pagos electrónicos o digitales, dada la relevancia que han venido adquiriendo para el desarrollo de la vida económica.

2. Primera etapa. De la autorregulación a la regulación

La aparición de los pagos digitales se da con la llegada de las tarjetas de crédito como una forma diferente al efectivo, para satisfacer obligaciones dinerarias, que resultaba más práctica y segura. La idea fundamental alrededor de estos instrumentos de pago era lograr su aceptación en la mayor cantidad de comercios posible. Así las cosas, para el procesamiento de estas transacciones se establecieron acuerdos sobre la forma en la que cada actor -entidades financieras, comercios y tarjetahabientes - debía desarrollar su rol. Por muchos años fue a través de la ejecución de estos reglamentos que pudo garantizarse y extenderse la utilización de los pagos electrónicos que luego evolucionaron a los pagos digitales.

Las entidades que procesaban en principio estas transacciones en Colombia eran las redes como Credibanco y en su momento Red Multicolor, que fueron creadas por el sector financiero, pero no estaban vigiladas por la Superintendencia Financiera -Superintendencia Bancaria, para la época-. Eran entidades organizadas como sociedades de servicios

técnicos y administrativos, que cumplían un rol meramente instrumental para facilitar los pagos realizados con tarjetas débito y crédito emitidas por los bancos; estas redes eran las encargadas de lograr la aceptación de tarjetas en los comercios, proveyéndoles de herramientas para poder perfeccionar los pagos.

A la base del procesamiento de transacciones digitales se encontraban entonces estas entidades, encargadas de expandir el uso y la aceptación de instrumentos de pagos electrónicos, que para la época se reducían a las tarjetas de crédito y débito. Este procesamiento consistía en poner a disposición de las entidades financieras un sistema de mensajería que permitía el viaje de toda la transacción desde la tecnología que tuviera a disposición el comercio para lograr su autorización, por ejemplo, una llamada telefónica o un datáfono, hasta el envío de la misma a la entidad financiera con la que tuviera cuenta bancaria el comercio, para su respectivo abono.

Ahora bien, las redes procesaban transacciones de muchos comercios y de muchos tarjetahabientes, por lo que debieron sofisticar tecnológicamente este envío y recepción de mensajes, lo que además implicaba una definición de roles que permitiera garantizar el descuento y abono de recursos.

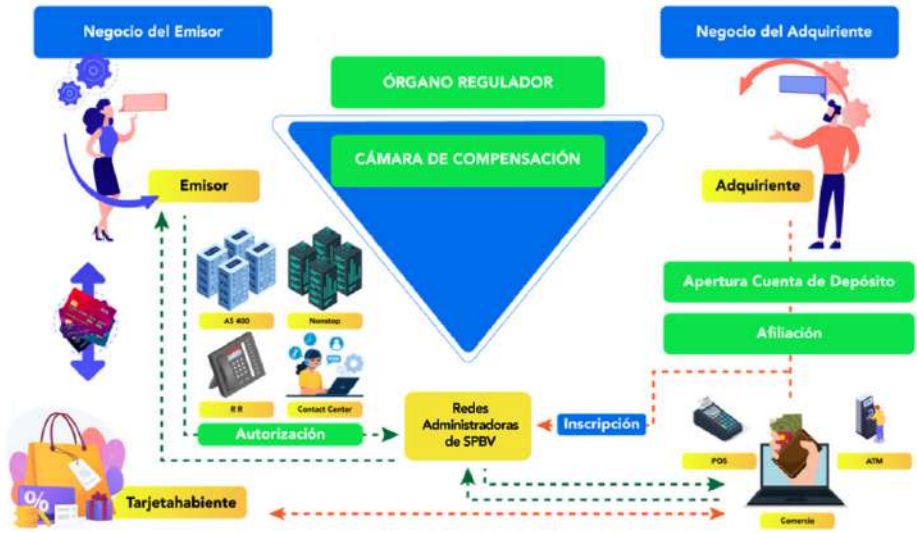
Así las cosas, tenemos la figura del Banco Emisor, cuyo cliente es una persona a quien se le entrega una tarjeta para que en ella se representen los recursos que tiene depositados en el banco o que provienen del otorgamiento de un crédito. Por otro lado, está la figura de Banco Adquirente, cuyo cliente es el comercio, y lo que hace es recibir los dineros provenientes de las operaciones de intercambio económico que se perfeccionen con el pago realizado por medio de las tarjetas. Aunque los sistemas y los instrumentos de pago han venido evolucionando con el tiempo, estos roles se mantendrán como la base del procesamiento de las transacciones digitales.

En una primera etapa, estas dinámicas tuvieron un alcance doméstico en Colombia. Con ese fin se crearon sistemas de marca nacionales administrados local y directamente por las redes del sector financiero. Así, hacia los años 70 las entidades financieras crearon Credibanco y Credencial, que, respaldadas por los bancos, se constituyeron como las primeras tarjetas de crédito que tuvieron los colombianos y que sólo tenían aceptación en los comercios nacionales.

Así surgió el primer ecosistema de pagos, enfocado inicialmente en el desarrollo de lo que se denominó dinero plástico -tarjetas de crédito y débito-, que buscaba entregarle a un consumidor de alto poder adquisitivo, con sólidas relaciones de confianza con el sector financiero, acceso a alternativas de pago más seguras y cómodas.

En este ecosistema se construyen una serie de relaciones jurídicas entre los diferentes intervinientes, tanto las del intercambio económico como aquellas necesarias para que el procesamiento de las transacciones pueda hacerse efectivo. Así, el emisor -banco que emite la tarjeta- es el encargado de entregar al adquirente -banco en el que el comercio tiene su cuenta- los dineros correspondientes a la compra realizada con la tarjeta. Esta labor asociada a los pagos implica, desde ese entonces, acuerdos de remuneración entre el banco emisor y el banco adquirente, que buscan cubrir los costos de procesamiento y seguridad del pago y que, a su vez, dependen de si la operación de intercambio económico se hace de modo presencial o virtual.

Figura 2. Relaciones Jurídicas en un Sistema de pago de Bajo Valor. Elaboración Propia.



Al comienzo, en relación con las tarjetas de crédito específicamente se utilizó un sistema de autorización telefónica a través del cual los comercios verificaban con los bancos la disponibilidad de cupo de los tarjetahabientes y solicitaban que posteriormente se efectuara el pago de las compras. Al tarjetahabiente se le exigía presentar la tarjeta física, de la que se tomaba una impresión en una máquina dispuesta para ese efecto.

Luego, vista la conveniencia de estos pagos para el desarrollo de nuevas formas de consumo, aparecieron en el país las tarjetas de aceptación global, es decir, tarjetas franquiciadas como Visa, Diners Club o Master Card. Estas tarjetas se convirtieron en la alternativa para consumidores viajeros que querían sustituir los tradicionales cheques de viajeros -*traveler's checks*- o evitarse el engorroso cambio y transporte de efectivo en distintas monedas También constituyó una solución para consumidores que querían acceder localmente a bienes de alto valor, pero con la opción de diferir su pago.

Posteriormente, con la aparición de los primeros datáfonos, se habilitó para la realización de pagos el uso de las tarjetas débito, y la autorización de las transacciones empezó a darse por la lectura de la información contenida en la banda magnética que estas portaban.

Como comentamos al inicio, este desarrollo de la industria de pagos electrónicos en Colombia funcionó bajo un esquema de autorregulación en el que las redes del sector financiero definían las condiciones para las entidades que participaban en estas dinámicas como emisores o adquirentes. Básicamente, se utilizaban las políticas definidas por los sistemas de marca de tarjetas de aceptación global.

En el desarrollo de los pagos en Colombia, se fueron apropiando estas regulaciones y adaptando algunas a la práctica nacional, de cara a hacer una oferta de estos servicios más atractiva para los consumidores.

Aunque, como veremos más adelante, las operaciones de los sistemas de pago fueron adquiriendo cada vez más relevancia, hasta constituirse en materia de una regulación propiamente dicha, los reglamentos siguen teniendo vigencia e incluso se mantienen prácticas de autorregulación particulares de la industria colombiana. Un ejemplo de esto son justamente los pagos diferidos con tarjetas de crédito.

En Colombia, los pagos diferidos han tenido una particular forma de liquidarse: los deudores acuerdan previamente con el banco diferir sus compras a un determinado número de cuotas mensuales que se definen al momento de la compra, con una tasa de interés que será también la del día de la compra. En la práctica internacional, en cambio, la liquidación de este tipo de créditos suele hacerse bajo la modalidad de crédito revolvente, consistente en que para cada periodo mensual se liquida nuevamente el valor del crédito hasta el plazo fijo que se pacta en el momento en que se adquiere el crédito y a la tasa vigente para el corte mensual en el cual se hace la liquidación.

Es claro, entonces que, en el caso de los pagos diferidos, aun cuando no ha existido una norma específica que defina sus reglas de operación, la práctica del sector financiero ha establecido un esquema de autorregulación que se atiene a lo que pacten el banco y el tarjetahabiente.

Retomando, las redes del sector financiero operaban y operan hoy como facilitadoras de las relaciones entre las entidades financieras y sus clientes -personas naturales o comercios-. Esto, en razón a que realizan procesos operativos que implican transmitir mensajes de datos para solicitar autorización y procesar, liquidar y compensar todas las operaciones que se hacen cada día. De este modo, al final se asigna a cada entidad financiera la suma que le corresponde.

Las redes, que cuando empezaron a ser reguladas se denominaron administradoras de sistemas de pago de bajo valor o simplemente sistemas de pago de bajo valor, tenían varias relaciones jurídicas autónomas e interdependientes. Por un lado, celebraban separadamente contratos de licenciamiento con las franquicias y/o sistemas de marca -es decir, con Master Card o Visa, que eran y son las más relevantes por tener mayor aceptación de los comercios-. Por otra parte, establecían relaciones con los comercios encaminadas a garantizar la aceptación de pagos con tarjetas de crédito, así como su abastecimiento tecnológico para que este objetivo fuera posible. Con este fin, proveían los dispositivos o herramientas de comunicación necesarios, como los ya mencionados datáfonos. Así comenzó a materializarse la oferta de alternativas de pago diferentes al dinero en efectivo, articuladas con innovaciones tecnológicas que, además, buscaban entregarle cada vez mayor seguridad al sistema.

2.1 Análisis de los riesgos – Tránsito a un esquema regulado

La tecnificación y consecuente masificación de estas operaciones supuso asumir mayores riesgos, como que alguna entidad no pudiera cumplir sus obligaciones y afectara, a su vez, el cumplimiento de otras obligaciones suyas o de otros actores. Como vimos, en un principio estos riesgos fueron administrados a través de mecanismos de autorregulación, derivados de las mejores prácticas definidas por los sistemas de marca, en el sentido de constituir, por parte de las entidades financieras, fondos de contingencia o colaterales para garantizar el cumplimiento de las obligaciones.

Pero, con ocasión de la crisis financiera de 1998, varios bancos fueron intervenidos por el Estado debido a problemas de liquidez y a la consiguiente imposibilidad de atender obligaciones que debían cumplirse a través de las redes. Esta situación evidenció que las operaciones de compensación podían resultar cada vez más relevantes para el correcto funcionamiento y estabilidad del sector financiero y, por ende, que podían afectar su operación. Con este criterio se concluyó que, aun cuando su actividad continuaba siendo instrumental para las entidades financieras, debían ser vigiladas por el Estado -la Superintendencia Financiera-, y este es el primer gran hito de la regulación de los pagos electrónicos -decreto 1400 de 2005-.

Así las cosas, vemos que, inicialmente, la regulación de los servicios de pagos digitales en Colombia se concentró en el rol de las infraestructuras tecnológicas y en la administración de los riesgos inherentes al desarrollo de su actividad, es decir, en esta primera etapa la regulación buscó establecer los cimientos de un procesamiento seguro de las transacciones hechas con tarjetas, en términos de garantizar el adecuado cumplimiento y respaldo de las obligaciones que se traban entre bancos emisores y adquirentes.

El citado decreto define los sistemas de pago de bajo valor como entidades que permiten la transferencia de fondos entre los participantes mediante la recepción, el procesamiento, la transmisión, la compensación y/o la liquidación de órdenes de transferencia y recaudo, todo lo cual ocurre en virtud del acuerdo que hacen estos participantes de aceptar un conjunto organizado de políticas, reglas, acuerdos, referidos a los instrumentos de pago, entidades y componentes tecnológicos, que concurrirán al sistema.

Vale la pena detenerse en las actividades definidas en este decreto para entender su funcionamiento y la razón de ser de la vigilancia de la Superintendencia. Comencemos por la compensación, que es un modo de extinguir total o parcialmente las obligaciones. Puede ser bilateral, es decir, entre dos personas que sean recíprocamente deudoras y acreedoras, o multilateral, esto es, entre más de dos personas que ostenten las calidades mencionadas. Esta es la que naturalmente ocurre al interior de un sistema de pago de bajo valor, entre las entidades que allí concurren, por decirlo de alguna manera, para cruzar sus cuentas, en función de los roles que ejerzan de adquirente o emisor.

La liquidación, por su parte, constituye la finalización de una operación o conjunto de operaciones mediante cargos y abonos en las cuentas de depósito que los bancos tienen en el Banco de la República. Las operaciones a las que se hace referencia son justamente las órdenes de pago y transferencia que se cursan entre los participantes del sistema, bien sea que jueguen el rol adquirente o emisor.

El decreto 1400 de 2005 describió por primera vez las operaciones esenciales de los sistemas de pago de bajo valor, concebidos en principio como proveedores de infraestructura, pero que también asumían el procesamiento de las transacciones que por esta cursaban. Incluso les eran encomendadas, por parte de las entidades financieras, funciones propias del manejo de los pagos que, por supuesto, trascendían las actividades de canje y compensación y los ubicaba como protagonistas de otros eslabones de la cadena de valor, como el procesamiento adquirente y emisor.

Desde el concepto de adecuada gestión del riesgo, inicia la regulación de los pagos electrónicos en el país. El decreto 1400 de 2005 define los riesgos asociados a la operación de la siguiente manera:

Riesgo Operativo: errores humanos o de falla en los equipos, los programas de computación o los sistemas y canales de comunicación que se requieran para el adecuado y continuo funcionamiento de un sistema de pago. También incluye el riesgo de lavado de activos y la financiación del terrorismo.

Riesgo Crediticio: posibilidad de que un participante incumpla definitivamente con la obligación resultante de la compensación y/o liquidación a su cargo, en forma total o parcial a su vencimiento.

Riesgo de Liquidez: posibilidad de que un participante incumpla total o parcialmente la obligación resultante de la compensación y/o liquidación a su cargo en la fecha de vencimiento, pero que pueda cumplir en un momento posterior.

Riesgo sistémico: se presenta cuando el incumplimiento total o parcial de una o varias obligaciones de un participante en un sistema de pago, o la interrupción o el mal funcionamiento de dicho sistema pueda originar: (i) que otros participantes en el mismo sistema de pago no puedan cumplir con las obligaciones a su cargo; (ii) que otros participantes de otro sistema de pago, ya sea de bajo valor o de alto valor, no puedan cumplir con las obligaciones a su cargo, y (iii) que otras instituciones o personas que operen en el sistema financiero o en el mercado público de valores no puedan cumplir con las obligaciones a su cargo, y en general, que tal incumplimiento pueda causar problemas significativos de liquidez o de crédito, lo cual podría amenazar la estabilidad del sistema financiero.

Riesgo Legal: posibilidad de que un participante incumpla total o parcialmente una obligación resultante de la compensación y/o liquidación a su cargo por causas imputables a debilidades o vacíos del marco legal vigente, los reglamentos o los contratos, que, por lo tanto, afectan la exigibilidad de las obligaciones contempladas en estos últimos.

Adicionalmente, uno de los objetivos fundamentales del decreto era lograr que a través de planes de contingencia y de seguridad informática pudiera garantizarse la continuidad de la operación en el sistema de pagos de bajo valor -SPBV-. Así, los estándares operativos y técnicos con que debía contar la entidad administradora del sistema, así como aquellos con los que debían contar quienes concurran a él, resultaban esenciales para su funcionamiento adecuado. Por consiguiente, es de la esencia del sistema de pagos la estructuración de planes de contingencia y de recuperación que aseguren, cuando menos, el procesamiento y terminación del ciclo de compensación y/o liquidación ante situaciones tales como fallas de los equipos, programas de computador o canales de comunicación, interrupciones o variaciones excesivas en el suministro de energía eléctrica, interrupciones en la prestación

de los servicios de telecomunicaciones o en el suministro de cualquier otro insumo u otros eventos de la misma índole.

El decreto 1400 de 2005 permitió, entonces, darles mayor solidez a las relaciones jurídicas entre las entidades financieras y el sistema de pago. Las entidades financieras, en calidad de participantes, celebran un contrato de vinculación, que implica adherirse al reglamento que el sistema obligatoriamente debe establecer. Este reglamento busca sentar las bases para la descripción de la operación y de los componentes del sistema, lo que deviene en protección del riesgo propio de una actividad de esta naturaleza.

Adicionalmente, el decreto precisa las características de los intervinientes en el procesamiento de pagos digitales. Por ejemplo, que los sistemas de marca o franquicias, es decir, Visa y MasterCard, son agentes diferentes a los sistemas encargados de procesar las órdenes de pago y transferencia, en nuestro caso los sistemas de pago de bajo valor representados por Credibanco y Redebán. Significa que las actividades de procesamiento no están necesariamente atadas a las actividades de licenciamiento o administración de una marca, lo que tiene efectos positivos en la competitividad de los pagos digitales y la conformación del mercado de pagos en Colombia.

Otro elemento importante del decreto 1400 de 2005 es la exigencia de que haya tres o más entidades participantes para la formación del sistema. Por participante se entiende cualquier entidad autorizada por el administrador de un sistema de pago de bajo valor para tramitar órdenes de transferencia o recaudo en el respectivo sistema. Este decreto permitió que los participantes en las entidades administradoras de sistemas de pago de bajo valor puedan ser o no entidades financieras, en tanto acrediten el cumplimiento de los estándares derivados de los sistemas de protección de los riesgos reseñados.

Del decreto 1400 de 2005 se derivaron varias circulares de la Superintendencia Financiera de Colombia, orientadas a precisar las exigencias relacionadas con la protección de los riesgos propios de la actividad. Vale la pena aludir a ellas por ser desarrollos que contribuyeron a la regulación de los proveedores de pagos digitales y, por consiguiente, a la tecnificación de su operación[4]. En esencia, son instrumentos de regulación que buscaron hacerle frente e incluso impulsar la evolución de la industria de pagos que, como resultado de la innovación tecnológica, tomaba cada vez un mayor alcance. Piénsese, por ejemplo, en la forma como fue cambiando la captura de la transacción en los datáfonos o medios de acceso: pasamos de la banda magnética a la tecnología del chip, al código QR y a los pagos sin contacto. Todas estas alternativas, que pueden convivir actualmente, fueron concebidas siempre para llevar condiciones de seguridad cada vez más robustas al consumidor y para mejorar su experiencia.

3. Los ecosistemas de pago para profundizar la bancarización

Durante los años posteriores al decreto 1400 y casi hasta el año 2016, la discusión se centró en cómo crear una oferta de servicios financieros que llegara a la base de la población y le permitiera a esta servirse de las ventajas de estar bancarizada. En su momento se pensó que ese objetivo pasaba necesariamente por la activación de dinámicas de pagos y consumo digitales.

[4] Las normas relativas a los sistemas de pago pueden consultarse en https://bit.ly/regulacion_sistemas_de_pago_bajo_valor

Un par de circunstancias contextualizaron las discusiones de esta fase de la regulación; en esencia, definieron el camino para entender la real contribución que tienen los ecosistemas de pago en el desarrollo económico del país.

El decreto 1400 fue incorporado al decreto 2555 de 2010 -Decreto único del sistema financiero-, un paso importante para entender a los sistemas de pago de bajo valor como integrantes del sector financiero, así como un reconocimiento al papel protagónico que cumplen en el funcionamiento y la estabilidad de dicho sistema.

Ya no se miraban los sistemas de pago de bajo valor como meros proveedores de infraestructura, sino también desde los beneficios que se derivan del fortalecimiento de los instrumentos de pago. En ese sentido, a fin de lograr su masificación, la regulación simplificó el trámite para adquirir los productos asociados a los instrumentos de pago. Además, creó un nuevo tipo de entidad que hiciera posible la conformación de un verdadero ecosistema.

Entre el 2008 y el 2016 se promovieron productos y servicios financieros mucho más coherentes con las realidades de la base de población, enfocados en permitir un acceso fácil, oportuno y adecuado. Nos referimos a los depósitos electrónicos y las cuentas de ahorro y de trámite simplificado, así como a la corresponsalía bancaria y las sociedades de depósitos y pagos electrónicos -SEDPE-.

Los depósitos electrónicos constituyen un nuevo tipo de depósito, diferente de las cuentas de ahorros y corriente. Aunque también son a la vista, su vocación es en esencia transaccional. Se diferencian de los productos tradicionales de la banca, primero, por la forma en la que puede disponerse de los recursos, que es, por un lado, desmaterializada, es decir, que no requiere de una tarjeta u otro instrumento físico, y por otro, que están diseñados para mantener el dinero dentro del sistema financiero y ser un vehículo para el ordenamiento de pagos y transferencias. Los trámites para su apertura, disposición y cierre son mucho más fáciles que los de otros depósitos, pero con algunas restricciones en cuanto a los montos de saldos y transacciones.

Otra figura relevante, que tuvo un amplio despliegue regulatorio y que promovió la mayor utilización de los servicios financieros y la llegada de estos a segmentos previamente desatendidos, fue la corresponsalía bancaria. Permitió abrir la ruta para que las entidades financieras pudieran innovar en la prestación de servicios financieros, algunos de ellos transaccionales, de manera mucho más asequible a la realidad de la población colombiana.

Esta figura permitió aprovechar las interacciones de las personas con los desarrollos tecnológicos, como el uso del teléfono celular para acercar al consumidor financiero con el sistema, sin necesidad de desplegar una capacidad instalada en cada lugar del país, ya que la capilaridad se fue conquistando a partir de las relaciones de confianza ya establecidas entre una comunidad determinada y la persona con la que al final el banco podía elegir como su corresponsal.

El decreto 2672 de 2012[5] incorporó nuevas reglas sobre el servicio de corresponsalía que vale la pena destacar:

[5] Modifica el decreto 2555 de 2010 en lo relacionado con los servicios financieros prestados a través de corresponsales.

- Se regularon los servicios financieros prestados a través de corresponsales, definiendo de esta forma los establecimientos o sociedades que bajo su responsabilidad podrán prestar sus servicios a través de terceros corresponsales sin que esto implique la exoneración de los deberes propios de su actividad.
- Se estableció que le corresponde a la Superintendencia Financiera determinar las condiciones que deberán cumplir los corresponsales.
- Se definieron las modalidades de servicios que podrán prestar los corresponsales con sus respectivas condiciones, así como la información que al respecto deberá entregarse a los clientes y usuarios.

Ahora bien, en relación con las sociedades especializadas para pagos y depósitos electrónicos, SEDPE, la ley 1735 de 2014, denominada Ley de inclusión financiera, tenía como propósito la creación de un tipo de entidad que permitiera la utilización de esta nueva forma de depósitos electrónicos en el marco de una dinámica transaccional, para desarrollar ecosistema de pagos de una misma entidad.

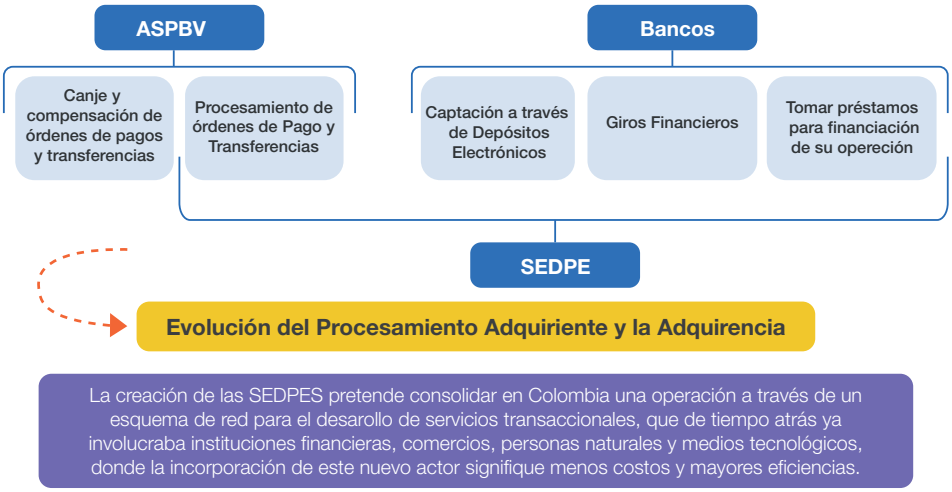
Las SEDPE se incorporaron a la estructura del sistema financiero como entidades vigiladas con menos requisitos de capital y, por ende, con un marco regulatorio más liviano. Aunque no tienen posibilidades de prestar ni, por lo tanto, de realizar las actividades de intermediación, pueden captar en la modalidad de depósitos electrónicos y se les abre la posibilidad de procesar pagos digitales, hacer giros y transferencias. A través de realizar las operaciones de pago de manera digital, se pretende mantener el dinero dentro del sistema financiero.

Estas entidades no se limitan, entonces, a ser únicamente un vehículo especializado para el denominado depósito electrónico. Su espectro de operaciones es más amplio. Se entienden como un verdadero centro de servicios transaccionales, que puede originar operaciones en diversidad de canales a través del uso de nuevas tecnologías, logrando una oferta más eficiente y a menores costos, con estándares de seguridad y operativos que permitan mantener protegido el sistema de pagos de los riesgos que le son inherentes.

La idea es que constituyan una alternativa para que entidades no financieras también puedan proveer servicios de pagos digitales de manera segura. Se permite incluso que puedan ser constituidas por toda suerte de entidades, como operadores de servicios postales, proveedores de redes y servicios de telecomunicaciones, bancos o cualquier persona. Adicionalmente, las SEDPE permiten interacciones entre los tenedores mismos de los depósitos electrónicos, lo que hace mucho más económico el traslado de fondos entre personas.

Las SEDPE se concibieron como entidades que debían estar inmersas en el sistema financiero para competir en la prestación de servicios de pagos digitales, dado que los bancos habían desatendido segmentos de la población cuya inclusión financiera era necesaria. En la figura 3 se observa cómo, a partir de esta nueva regulación, se habría estructurado una verdadera evolución en la competitividad del procesamiento adquirente, entendido como la captura de la transacción y el envío de la misma al banco emisor para lograr su respectiva autorización -tradicionalmente a cargo de las administradoras de sistemas de pago de bajo valor-, y la de la adquirencia, que consiste en la administración de los depósitos de los comercios derivados de sus ventas pagadas con instrumentos de pago electrónicos y que se encuentra a cargo de los bancos.

Figura 3. Alcance de la Licencia de las SEDPE vs. ASPBV y Entidades Financieras. Elaboración Propia.



Las SEDPE constituyen, así, un tipo de entidad con gran potencial de profundizar la inclusión financiera, en tanto estimulan dinámicas digitales en los comportamientos de pago de las personas, desincentivando el uso de efectivo. Están destinadas a crear ecosistemas de pagos que permiten una transaccionalidad con costos marginales, es decir, con menor inversión en función del aumento que vaya teniendo el procesamiento de esas transacciones. Esto es posible, pues operan las transacciones sobre su propia red -pago entre clientes de una misma SEDPE-, sin necesidad de incurrir en costos asociados a la prestación del servicio de los bancos.

Sin embargo, la figura de la SEDPE no ha tenido la acogida que se esperaba, por lo que no ha generado la masificación en la aceptación y el uso de los pagos electrónicos. En cambio, durante estos años se han venido teniendo desarrollos paralelos por parte de algunos bancos que, a través de la implementación del depósito electrónico, han desplegado rutas de inclusión financiera. Como resultado, parte de la población que antes no tenía acceso a productos financieros ha podido adquirirlos. También se ha logrado algo más complejo: hacer que estas personas realicen transacciones con sus productos, de forma que mantengan dentro del sistema sus hábitos de pago y de consumo. Alguna de estas alternativas son Daviplata y Nequi.

Lo propio han hecho entidades que no son vigiladas y que, como parte de la industria Fintech proveen servicios de aceptación y facilitación de pagos, por ejemplo, las pasarelas de pagos. Justamente, vale la pena resaltar que la industria Fintech, conformada por empresas que hacen uso de componentes tecnológicos para ofrecer eficiencias en la prestación de servicios financieros, ha venido desarrollando un rol determinante en lo local y en lo global para impulsar la competitividad de los servicios de pagos y su incursión en el mercado. Esto ha supuesto desafíos regulatorios encaminados a mantener un balance entre la seguridad

y la confiabilidad de que debe gozar el sistema financiero, por ser administrador de los recursos del público, y la incursión de actores no vigilados pero que tienen la capacidad de complementar la oferta del sector y llegar a más segmentos de la población.

4. Los sistemas de pago como articuladores decisivos en la inclusión financiera

El contexto de la siguiente etapa de regulación de los sistemas de pago está marcado por un exponencial desarrollo de los pagos digitales y dinámicas que trascienden la provisión de infraestructura para la aceptación de los instrumentos de pago, que como vemos, ya en esta fase pueden o no estar materializados en tarjetas, o ser, por ejemplo, representados a través de nuestros celulares o con otros atributos tecnológicos más dinámicos como los códigos QR.

Ya no era suficiente que se demandara seguridad en el procesamiento de las transacciones, sino que se requería una regulación que condujera verdaderamente a la masificación de los servicios financieros y, por consiguiente, de las transacciones digitales.

Como antecedente de este planteamiento, podemos reseñar que la crisis económica global de 2008 también tuvo importantes efectos en la provisión de servicios financieros y de pagos en Colombia. Originada en la exposición del sistema financiero global a activos de alto riesgo, resultó en serios problemas de liquidez para las principales instituciones financieras del mundo y generó importantes cuestionamientos sobre la credibilidad del sistema financiero y la conveniencia de los servicios ofrecidos. Esta situación conllevó replanteamientos sobre la forma en la que debían ofrecerse los servicios y, en particular, sobre la necesidad de hacerlos mucho más cercanos a la sociedad. Igualmente, determinó la entrada de nuevos actores, no vigilados, pero con capacidad de solventar estos requerimientos del mercado a través de soluciones disruptivas, no solo en términos de acceso, sino en esquemas de gestión y asunción del riesgo que hacen también mucho más liviano para el consumidor el acceso al servicio propiamente dicho.

El objetivo era ir más allá de la bancarización, entendida como la colocación de productos del sistema financiero, y pasar a promover avances más decididos en inclusión financiera, que implican no solo la adquisición de un producto sino su efectiva y constante utilización.

Esta nueva regulación tiene la mayor relevancia, porque trasciende el entendimiento meramente instrumental que se daba a los proveedores de servicios de pagos digitales para pasar a verlos como agentes que hacen parte del sistema y, por ende, que están en capacidad de proveer soluciones más eficientes y competitivas para la realización de los intercambios económicos de las personas y, aún más relevante, facilitan la trazabilidad de dichos intercambios, lo que permite comprender los hábitos de consumo de las personas para entregarles, a partir de ese perfilamiento, posibilidades reales de inclusión económica a través del crédito.

Esta trazabilidad también mejora la fiscalización y, por ende, la optimización del gasto social. Además, desde una perspectiva macroeconómica, se incorpora al país en un círculo transaccional virtuoso que le habilita además su inserción en dinámicas de comercio globales.

Con este cambio de criterio se abandona la clasificación de sistemas de pago de bajo y de alto valor en función de un criterio cuantitativo -decreto 1400 de 2005, incorporado en el decreto 2555 de 2010- y se adopta un criterio orgánico, es decir, ya no asociado al volumen o valor de las transacciones procesadas en la respectiva infraestructura de los sistemas de pago sino en función de si tales operaciones son de aquellas que maneja o no el Banco de la República a través de sus propias infraestructuras.

Este cambio en la conceptualización también se da en las definiciones sobre quienes concurren a los sistemas de pago. El decreto 1692 de 2020 establece una diferencia entre usuario y participante: define al usuario como la persona que utiliza los servicios financieros para ejecutar una orden de pago o transferencia de fondos. Y al participante del sistema de pagos, en su rol emisor o adquirente, como aquel que haya sido autorizado para tramitar órdenes de pago o transferencia de fondos. Otra novedad es que se incluye como posibles participantes a los patrimonios autónomos.

Paralelamente, el comercio electrónico aparece como un inequívoco dinamizador de los pagos digitales y con él la entrada de nuevos agentes que abren mayores posibilidades de aceptación de estos pagos. Las pasarelas de pagos, que funcionan como portales para conectar una cuenta bancaria con un proveedor de servicios de pago, aparecen como una solución para los establecimientos de comercio virtuales. A través de estas plataformas, los comercios electrónicos pueden aceptar los pagos digitales o bien hacerse representar por ellas ante el sistema de pago, a través de los modelos de agregación.

4.1 Proveedores de servicios de pagos, nuevos agentes

Esta figura ha venido tomando cada vez más relevancia en la industria de pagos en el país, debido, por un lado, a la expansión de la industria digital, y por otro, porque ofrece al comercio rutas más económicas de acceso a los servicios de aceptación de pagos digitales. En este último caso, ha implicado que quien tenga la relación con el sistema financiero, tanto con el banco adquirente como con el sistema de pago de bajo valor, sea la pasarela, que, a través de su capacidad para desplegar economías de red, busca agrupar comercios que directamente no podrían establecer una relación con el sistema financiero y de esta manera hacerles más eficientes los costos.

Este nuevo decreto reconoce así la existencia de otros actores que participan de las dinámicas transaccionales, cuya actividad es relevante para los objetivos de política pública en inclusión financiera. Se les reconoce el rol que cumplen en el ecosistema, sin que su actividad esté sujeta a la vigilancia de la Superintendencia Financiera.

Este reconocimiento dado por el decreto a las pasarelas de pago como agentes de los ecosistemas de pago ha estado acompañado de normas expedidas por la mencionada Superintendencia, en términos que muchos han denominado supervisión indirecta, pero que no es otra cosa que una forma de mantener control sobre los riesgos que puedan afectar la estabilidad del sistema.

El decreto 1692 de 2020 introduce a los proveedores de servicios de pagos como entidades que, en función de su relación con el banco adquirente y, por supuesto, con el comercio -que siempre será su cliente- podrán prestar todo tipo de servicios en cualquier eslabón de la cadena de valor de los pagos digitales. Como señalamos en la Figura 1, el procesamiento

de pagos digitales implica el ejercicio de distintos roles que pueden ser desarrollados por diferentes tipos de entidades y soportados por otras que se profesionalizan en el desarrollo especifico de esa actividad.

Este decreto hace especial énfasis en reconocer el rol de agregación bajo las siguientes modalidades:

Proveedores de servicios de pago: *agente del sistema de pago que por delegación del adquirente o la entidad emisora desarrolla una o varias de sus funciones. Se incluye dentro de esta definición, entre otros, al procesador emisor, al procesador adquirente, al agregador y al proveedor de tecnologías de acceso.*

Agregador: *proveedor de servicios de pago del adquirente que vincula a los comercios al sistema de pago de bajo valor, le suministra tecnologías de acceso que permitan el uso de instrumentos de pago y recauda en su nombre los fondos resultantes de las órdenes de pago o transferencia de fondos a su favor.*

En esta línea, el decreto 1692 de 2020 buscó simplificar la forma en la que los comercios acceden al sistema de pago de bajo valor, para que su relación sea solo con el banco adquirente, que es quien deberá trasladarle los dineros correspondientes a la aceptación de pagos digitales. El objetivo es buscar eficiencias en la asunción de costos por parte de los comercios y modificar los esquemas de relacionamiento tradicionales, que siempre le habían supuesto al comercio la administración de distintas relaciones: por un lado, con el banco adquirente, lo que le implica al comercio el pago de una comisión de adquirencia que se cobra contra sus saldos; y por otro, una relación accesoria con el sistema de pago de bajo valor o con proveedores de servicios de pago para tener la tecnología que le permitiera habilitar la aceptación de pagos.

Esta previsión supuso en su momento algunas dificultades interpretativas, puesto que no resultaba claro si la aludida simplificación implicaba que las relaciones que pudiera tener el comercio con los proveedores de servicios de pago o con las redes administradoras de sistemas de pago de bajo valor quedaban subordinadas a la relación con el banco adquirente, lo que a la postre podría suponer dificultades de acceso a servicios por parte de comercios que justamente habían utilizado a los agregadores para poder acceder a los pagos digitales. Por suerte, el recientemente expedido decreto 1297 de 2022, sobre *Open Finance*, resuelve en su artículo 1 esta problemática al establecer que la relación contractual del comercio podrá ser con el adquirente o con el agregador o proveedor de servicios de pago, sin perjuicio de que el adquirente siga siendo responsable ante el sistema de pago, los participantes y sus usuarios por el cumplimiento de las funciones de adquirencia.

Adicionalmente, el decreto 1692 de 2020 admite que los proveedores de servicios de pagos puedan participar del proceso de compensación y, si es de su interés, operar dentro del sistema como adquirentes, para lo cual deberán informar de tal circunstancia a la Superintendencia Financiera. Establece entonces que las actividades de las entidades no vigiladas que desempeñen un rol de adquirente, serán las siguientes:

- *Vincular a los comercios al sistema de pago de bajo valor. (*Actividad delegable en PSP).
- *Suministrar al comercio tecnologías de acceso que permitan el uso de instrumentos de pago.* (Actividad delegable en PSP).
- *Procesar y tramitar órdenes de pago o transferencia de fondos iniciadas a través de las tecnologías de acceso.* (Actividad delegable en PSP).
- *Abonar al comercio o al agregador (…).* (Actividad indelegable).

De este modo, junto con las entidades financieras y las SEDPE, los actores no financieros -proveedores de servicios de pago- podrán desarrollar la actividad de adquirencia, que consiste en recibir en un depósito los dineros provenientes de las ventas que se paguen de forma electrónica o digital. Tales dineros deben a su vez ser depositados en establecimientos de crédito o en una SEDPE. También deben cumplir con los registros y requisitos de patrimonio que señala la norma.

No se requiere que el abono en cuenta a quienes concurren al sistema de pago de bajo valor se haga en cuentas del Banco de la República. De acuerdo con el decreto, este proceso se podrá surtir en las cuentas bancarias que los proveedores de servicios de pago -PSP- tengan dispuestas para el efecto. Algunos temas que el decreto 1692 de 2020 busca resolver podrían haberse solventado con la regulación existente, como es el caso de la participación de actores no financieros en los sistemas de pago de bajo valor, que hemos reseñado anteriormente. Si bien es cierto la obligación de tener una cuenta en el Banco de la República para poder compensar era una barrera -por lo demás no impuesta por el sector financiero-, dicha limitación habría podido superarse mediante la fijación de estándares de control de riesgo claros, que han sido recientemente especificados por la autoridad de vigilancia. Sin embargo, aporta claridad y seguridad jurídica que la regulación incorpore expresamente, como parte del ecosistema, la interacción natural que debe darse entre los diferentes actores con capacidad para expandir la penetración de los pagos, independientemente de que sean o no vigilados.

Con ocasión del decreto 1692 de 2020, la Superintendencia Financiera ha expedido normas orientadas a controlar la forma en la que se desarrolla esta actividad de procesamiento adquirente.

Adicionalmente, sobre la discusión de cuál debe ser la interacción de los agentes que participan de los servicios de pago para lograr su masificación, se introduce en el decreto de 2020 el concepto de interoperabilidad, que no es otra cosa que la determinación de un lenguaje común entre todos los intervinientes para lograr que las personas puedan pagar y recibir pagos en uno u otro sistema a su libre elección. En ese sentido, la interoperabilidad se erige como una variable fundamental para hacer efectiva la inclusión financiera.

Se otorga a esta discusión toda la trascendencia, y se faculta a los actores, tanto del sector financiero como a quienes no están ajenos a la vigilancia del Estado, para establecer mejores prácticas con ese fin, y reserva a la Superintendencia Financiera la posibilidad de conformar un comité consultivo para impulsar el tema.

Una preocupación adicional se relaciona con temas de gobierno corporativo, asociados fundamentalmente: (i) a las estructuras de propiedad de las sociedades administradoras de sistemas de pago de bajo valor, en la medida en que han sido conformadas por entidades

del sector financiero, y (ii) a los conflictos de interés relativos a la admisión de nuevos agentes que puedan competir con dichas entidades en la prestación de alguno de los servicios de la cadena de valor de los ecosistemas de pago.

El decreto separa, del objeto primario de este tipo de entidades, la actividad de procesamiento, por cuanto establece, como actividad central, que podrán ser proveedores de servicios de pago de adquirentes y entidades emisoras, ofrecer sus servicios y productos de manera desagregada y cobrar tarifas individuales por cada uno de dichos servicios y productos. Ahora bien, el decreto también les permite realizar procesamiento y suministro de tecnología para actividades conexas con el procesamiento de pagos digitales. Este cambio se relaciona con la prohibición de las entidades administradoras de sistemas de pago de bajo valor de realizar actividades de adquirencia, a menos que actúen como proveedores de servicios de pago de los adquirentes.

Adicionalmente, se busca impulsar la entrada en el mercado de nuevos agentes, productos y soluciones tecnológicas con capacidad para competir en la captura de transacciones y su correspondiente procesamiento. Sobre esta base, las Fintech, como entidades que no están bajo la vigilancia del Estado, tienen un gran potencial para desarrollarse como sociedades de innovación y tecnología financiera y, por consiguiente, de promover la transformación digital de los colombianos a través de la masificación de los pagos electrónicos y el incentivo del uso de nuevas tecnologías para los servicios financieros.

Un último tema, que reviste una importancia capital dentro de este nuevo cuerpo normativo, es la alusión a los precios inherentes al funcionamiento de los pagos digitales en el país. Como se señaló, entre los bancos emisores y los adquirentes existe un acuerdo de remuneración asociado a las transacciones digitales. Esta remuneración, denominada Tarifa Interbancaria de Intercambio -TII-, está asociada a muchas variables relacionadas generalmente con el sector y/o la actividad que realice el respectivo comercio, así como los riesgos que le sean inherentes, en función de lo cual se determina la comisión de adquirencia -precio que, como también señalamos, el banco adquirente le cobra al comercio-.

El decreto establece que la fijación de la TII estará a cargo de las franquicias para el caso de los instrumentos de pago franquiciados. Para otro tipo de instrumentos que cursen en el sistema de pago, será la respectiva junta directiva de la entidad administradora del sistema quien la fije.

La TII tiene un comportamiento relacionado directamente con la comisión de adquirencia, por ser un costo. Es un tema sensible en el relacionamiento con el comercio, que siempre busca disminuir al mínimo los costos de transacción asociados a la aceptación de pagos digitales. Esto implica evaluar que las medidas regulatorias relacionadas con el precio mantengan en el tiempo una correspondencia con el logro de los objetivos de política pública sobre transformación digital y trazabilidad de los pagos, ya que, dependiendo de cómo se aborde, puede incidir negativa o positivamente en la mayor aceptación de los pagos digitales.

5. Regulación transversal a los servicios de pago digitales

Además de las normas que específicamente regulan la operación de los sistemas de pago y de los instrumentos que cursan a través de ellos, son relevantes las regulaciones relacionadas con el funcionamiento en general del sistema financiero, el comercio electrónico, la protección de datos personales, el derecho de la competencia y la protección del consumidor, determinantes en la operatividad de los sistemas de pago.

La provisión de los servicios financieros se enmarca en lo que establece la Constitución Política respecto de la actividad financiera y la democratización del acceso al crédito, el habeas data, los derechos de los consumidores y la protección de la libre competencia.

La denominada Ley de Comercio Electrónico, Ley 527 de 1995, definió los fundamentos en virtud de los cuales es posible procesar los mensajes de datos que están en la base de cualquier transacción digital. Estableció que el mensaje de datos debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, se les debe reconocer la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos atributos de un documento. Tiene, entonces, plena validez jurídica respecto de los datos trasmitidos siempre que para dicha trasmisión se haya utilizado un método que permita identificar al iniciador y pueda asegurarse que este ha dado efectiva aprobación del contenido, que es lo que ocurre cuando se procesa una transacción y se estandariza tecnológicamente su ruta a través del sistema. Así mismo, se le atribuye eficacia probatoria si se logra que el método sea confiable y apropiado al propósito para el cual el mensaje fue generado o comunicado.

En cuanto a la Ley de Habeas Data, en el marco de la actual economía digital los datos representan un insumo fundamental. A partir de su utilización, pueden tomarse decisiones tanto de negocio como para atender más eficientemente a un consumidor que demanda servicios más informados y que interactúa con multiplicidad de canales para nutrir sus decisiones de consumo. Así las cosas, los datos y su libre flujo se erigen como fundamentos esenciales para definir ofertas que favorezcan el bienestar de los titulares, sobre todo estructurando perfiles virtuales para la prestación más asertiva de servicios o la provisión de bienes.

El tratamiento indebido de los datos personales vulnera derechos fundamentales, por lo que los responsables de ese tratamiento tienen obligaciones de índole constitucional y legal. La información registrada con ocasión de estas operaciones debe ser tratada de acuerdo con las finalidades conocidas por el titular. La regulación sobre protección de datos personales se funda en conferir a las personas el poder jurídico para conocer e incidir sobre el contenido y la difusión de la información personal que les concierne y que se encuentra archivada en un banco de datos; así mismo, establece un conjunto de principios en torno a los cuales debe girar todo el proceso de acopio, uso y transmisión de datos personales[6].

Sobre protección del consumidor financiero, la ley 1328 de 2009 -Reforma Financiera- y la ley 1480 de 2011 establecen criterios para la protección del consumidor, fundados en que la relación de este con las entidades financieras es, por naturaleza, asimétrica. Por lo tanto, el objetivo de la normatividad es garantizar un balance en el desarrollo de la relación de consumo, que, en esencia, se consigue asegurando que la entrega de información

[6] Remolina, N. (2013). *Responsabilidad por el tratamiento de los datos personales de clientes, empleados, proveedores y terceros*. Bogotá: Universidad de los Andes - Temis.

sea suficiente, clara, oportuna y veraz, para que las decisiones de consumo sean lo más ajustadas posible a las reales necesidades del consumidor. Sin duda, los avances en relación con la protección del consumidor han sido relevantes en términos de cómo se define la oferta de los servicios de pago.

A su turno, las leyes sobre protección de la competencia han buscado estructuras más dinámicas y menos concentradas en el sector de servicios financieros, pues la competencia es el motor de la eficiencia y la innovación. En contraste, una mayor concentración de los mercados podría impactar negativamente la liquidez de los mercados interbancarios.

Garantizar la competencia en el sistema financiero es, por lo tanto, clave para brindar la estabilidad que el sistema necesita y mantener un equilibrio en los costos. En el caso colombiano, el principio de libre competencia cuenta con rango constitucional por los efectos que su transgresión produce para el mercado.

Sumado al rango constitucional, el derecho de competencia en Colombia se encuentra regulado desde hace varios años: la ley 155 de 1959 sobre prácticas comerciales restrictivas, el decreto 2153 de 1992 y la ley 1340 de 2009, que establece las normas en materia de protección de la competencia. En 2022, se publicó la ley 2195 de 2022, que aumentó de manera importante las multas por prácticas anticompetitivas.

Otro aspecto relevante que sin duda ha afectado la aceptación de los pagos digitales en el país es la regulación tributaria. En los últimos años, dicha regulación no ha sido precisamente favorable a la masificación de los pagos electrónicos; por el contrario, sus planteamientos no han sido consecuentes con las políticas de inclusión financiera del Gobierno. Debido a que valora con criterio de corto plazo las bondades que en términos de recaudo ofrece el sector financiero, establece medidas altamente regresivas como el gravamen a los movimientos financieros o las retenciones en impuesto de renta, IVA y en algunos casos extendido al ICA, lo que hace más costosa la aceptación de los pagos digitales y aumenta la preferencia por el uso de efectivo.

Lo cierto es que la urgencia fiscal que caracteriza a las iniciativas tributarias de los gobiernos no ha permitido abordar, para el largo plazo, una regulación fundada en incentivos tributarios que promuevan la digitalización de los intercambios económicos, lo que desestimularía el uso del efectivo y traería consecuencias positivas en términos macroeconómicos para el país.

6. La experiencia internacional

En esta sección se detallan experiencias internacionales relacionadas con el desarrollo de innovaciones en materia de pagos digitales en diferentes países:

6.1 Europa

6.1.1 Reino Unido

Con el ánimo de contar con un sistema de pagos que satisfaga las diversas necesidades de las empresas y los consumidores, la industria de pagos de Reino Unido ha propuesto el desarrollo y entrega de la Nueva Arquitectura de Pagos -NPA, por sus siglas en inglés-, la cual reemplazará la arquitectura utilizada para los sistemas de pagos interbancarios actuales

de Reino Unido. Con la NPA se busca organizar la compensación y liquidación de pagos interbancarios y, de esta manera, alcanzar una infraestructura sólida y sostenible en la cual la innovación y la competencia puedan prosperar[7].

Con este desarrollo se espera que la compensación y liquidación de los pagos se realicen por medio de una única infraestructura central, en lugar de la infraestructura separada que se utiliza en la actualidad. Su diseño permitirá que las empresas de pago puedan desarrollar servicios que beneficien a los consumidores y empresas que utilicen el sistema. A su vez, permitirá una evolución continua de los pagos interbancarios minoristas del Reino Unido.

6.1.2 Alemania

Según el Estudio de Comportamiento de Pago en Alemania para 2021, realizado por el Deutsche Bundesbank (2022), cerca del 98% de los alemanes mayores de 18 años posee una cuenta corriente o producto de banca en línea, un alto nivel de inclusión y acceso a servicios financieros. Dado lo anterior, mucha de la innovación en sistemas de pago se ha enfocado en eficiencia tecnológica, por ejemplo, el pago móvil ha sido prioridad como parte del cubrimiento de comercio electrónico. Entre otros, Applepay cuenta con el 38% de los usuarios de pagos digitales, seguido de aplicaciones de banco con un 25% y GooglePlay con 18%[8].

Uno de los grandes avances para el dinamismo del sistema de pagos digitales es la creación de los Pagos SEPA, que son un tipo de cuenta utilizada en la Zona Euro para realizar transferencias y pagos en tiempo real y de forma ágil, independiente de la región en donde se encuentre el usuario, pero que funciona con la misma seguridad, eficiencia y condiciones que en un ámbito nacional. Otra tendencia que se ha presentado en Alemania es el de los tokens criptográficos que, si bien es un método nuevo y con una falta importante de cubrimiento, para el 2021 cerca del 4% de los alemanes mayores de 18 años ya había realizado algún pago con este sistema -Deutsche Bundesbank, 2022-.

6.2 Asia

6.2.1 India

Dentro de las estrategias adelantadas en India con el propósito de impulsar el desarrollo del ecosistema de pagos, se destaca el programa establecido en 2016 por el cual el primer ministro, Narenda Modi, anunció que los billetes de 500 y 1000 rupias dejaban de ser legales en ese país, medida que canceló el 86 % del valor efectivo en circulación. La política tuvo como propósito alcanzar cuatro objetivos específicos: i) frenar la corrupción; ii) frenar la falsificación del efectivo; iv) eliminar el uso de billetes de alta denominación para actividades terroristas, y iv) eliminar la acumulación de dinero negro generado por los ingresos que no habían sido declarados ante las autoridades fiscales. A la par de esta política, el Banco de Reservas de India -RBI, el banco central de ese país- desarrolló el Unified Payments Interface -UPI- para facilitar los pagos P2P interbancarios y de consumidor a comercio. Esta es una plataforma que funciona sobre el Immediate Payment Service y que permite la conexión a

[7] PSR. (2021, diciembre 31). *New Payments Architecture (NPA).* https://www.psr.org.uk/our-work/new-payments-architecture-npa/
[8] Deutsche Bundesbank. (2022). *Zahlungsverhalten in Deutschland 2021.* https://www.bundesbank.de/en/publications/reports/studies/payment-behaviour-in-germany-in-2021-894118

partir de APIs, lo que ha facilitado su masificación para el uso con billeteras virtuales y otros instrumentos de pago digitales.

En lo relacionado con el sistema de pagos, desde el año 2020 el RBI desarrolló el Índice de Pagos Digitales -DPI, por sus siglas en inglés-, a fin de capturar el grado de digitalización de pagos en todo el país. El RBI-DPI se compone de cinco parámetros que permiten medir la profundización y penetración de los pagos digitales durante diferentes periodos. Los parámetros que componen este índice son: (i) habilidades de pago: 25%; (ii) infraestructura de pago: factores del lado de la demanda: 10%; (iii) infraestructura de pago: factores del lado de la oferta: 15 %; (iv) rendimiento del pago: 45 %, y (v) experiencia del consumidor: 5 % (RBI, 2021). Para el mes de marzo de 2022, el RBI-DPI se situó en 349,30 frente a la cifra de 207,84 del mes de marzo de 2021, lo que da cuenta de un crecimiento significativo y la rápida adopción y profundización de los pagos digitales en India durante los últimos años. En términos de crecimiento, los pagos digitales han aumentado cerca de un 216 % en términos de volumen y un 10 % en términos de valor, en el mes de marzo de 2022 frente a marzo de 2019[9].

Con el propósito de promover un ecosistema de pagos a escala global e impulsar un sistema de pagos nacional a través de la colaboración de los distintos agentes participantes en el sistema, en junio de 2022 el Departamento de Sistemas de Pago y Liquidación del RBI presentó su Visión de Pagos 2025. En este documento, el RBI detalla cada una de las metas y objetivos que quiere alcanzar durante los próximos tres años, para dinamizar y fortalecer el ecosistema de pagos nacionales. La visión se enmarca en torno a cinco pilares claves: integridad, inclusión, innovación, institucionalización e internacionalización, a través de los cuales espera incrementar las transacciones de pago digital más de tres veces y a su vez fomentar la aceptación de medios de pago diferentes al efectivo. El RBI también desarrollará un nuevo sistema de pagos diseñado específicamente para procesar pagos de comercio electrónico y banca móvil.

6.2.2 Corea del Sur

Recientemente, Corea del Sur ha trabajado en su Ley de Transacciones Financieras Electrónicas, puesta en vigencia desde diciembre de 2020 y mediante la cual busca garantizar la seguridad y confiabilidad de las transacciones electrónicas y así mismo promover este tipo de sistema. Una de las ideas novedosas que incluye dicha ley es la obligatoriedad por parte de las compañías financieras o entidades comerciales financieras electrónicas de presentar anualmente un plan para el sector de tecnologías de la información[10].

Una de las mayores apuestas del Banco Central de Corea es la creación de su propia moneda digital denominada CBDC -Moneda Digital del Banco Central-; por ende, una de sus principales políticas durante los últimos años ha sido enfocada a la investigación y desarrollo, para de esa manera sentar unas bases que sirvan para el cubrimiento y finalmente una funcionalidad universal de la moneda[11].

[9] RBI. (2022, julio). *Reserve Bank of India announces Digital Payments Index for March 2022*. https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR602DPI147FB19811794BBB8CCBF29AF13B09CA.PDF

[10] Bank Of Korea. (2022a). *ELECTRONIC FINANCIAL TRANSACTIONS ACT.* https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=1&query=electronic+financial+transactions+act&y=0&x=0#liBgcolor0

[11] Bank Of Korea. (2022b). *Payment and Settlement Systems Report 2021*. https://www.bok.or.kr/viewer/skin/doc.html?fn=202207130212437470.pdf&rs=/webview/result/E0000866/202207.

6.3 Latinoamérica

6.3.1 Uruguay

Dado el establecimiento de la ley de inclusión financiera, este país inició una etapa de crecimiento respecto a bancarización, digitalización y uso de comercio electrónico en muchos aspectos, destacando una mayor inclusión e innovación en su sistema de pagos. Primeramente, se estructuraron políticas para un acceso universal a medios que permitan la utilización del sistema, esto es, condiciones básicas obligatorias respecto a tarifas de adquisición de productos financieros, beneficios tributarios para pagos a través de Internet y programas para acercar a población vulnerable. Otra de las novedades es la creación del Índice de Pagos Electrónicos elaborado por el Banco Central del Uruguay, que busca realizar una comparación con los pagos tradicionales y de esta manera guiar políticas públicas en la materia[12].

6.3.2 Chile:

En los últimos años y con el impulso de la crisis sanitaria, el uso de pagos electrónicos y la sustitución de los medios de pago físicos es una realidad en Chile. Los avances tecnológicos se han convertido en una herramienta esencial para la inclusión financiera y la universalidad del sistema de pagos. Durante los últimos años, una de las principales políticas del Banco Estatal Comercial de Chile o BancoEstado, ha sido la de proveer medios de pago electrónicos mediante un producto conocido como Cuentas RUT. Estas cuentas tienen facilidades de acceso, dado que no tienen requisitos de ingresos, documentos, costos de apertura o manutención. A diciembre de 2021, contaban con 13,6 millones de usuarios[13]; para muchos, esta cuenta es el único instrumento financiero al que tienen acceso.

La flexibilidad del Banco Central también ha aportado a la innovación de políticas que incrementen el número de los pagos electrónicos. Desde 2017, y con un incremento significativo a la fecha, se permitió que empresas que proveen servicios de procesamiento de pagos puedan afiliar comercios de manera excepcional, prestando servicios de subadquirencia para ampliar el uso de medios de pago electrónico[14].

6.3.3 Brasil

Brasil es uno de los países líderes de Suramérica en cuanto al desarrollo e impulso de un ecosistema de pagos moderno que responde a las tendencias globales de pagos. Para el 2020, de los 210 millones de habitantes del país, alrededor del 75 % tenía acceso a Internet, 70 % de las personas tenía al menos una cuenta bancaria y 27 % contaba con al menos una tarjeta de crédito. De igual manera, de 2019 a 2020 Brasil experimentó la mayor caída en el uso de efectivo por parte de la población adulta, al pasar de 82,8 % a 62,8 %, lo que contrastó con el incremento del uso de tarjetas tradicionales: 61,6 %, que duplicó al uso de tarjetas *contacless*: 38,4 %[15].

---

[12] Banco Central del Uruguay. (2021). *Sistema de Pagos Minorista Reporte Informativo No 25*. https://www.bcu.gub.uy/Sistema-de-Pagos/Paginas/Reporte-Sistema-Pagos-Minorista.aspx

[13] Banco Central Chile. (2022). *Informe de Sistemas de Pago 2022*. https://www.bcentral.cl/documents/33528/3652920/Informe_de_sistema_de_pago_julio_2022.pdf/037fea7f-ce7f-1257-0025-62d71871a4b6

[14] Ibidem.

[15] Asobancaria. (2021). Ecosistema de pago Brasil y su importancia para la region.pdf. https://www.fintechgracion.com/wp-content/uploads/Ecosistema-de-Pago-Brasil-y-su-importancia-para-la-region-.pdf

Dentro de los factores claves en el impulso y consolidación del sistema de pagos de Brasil se encuentran los desarrollos regulatorios y las medidas adoptadas desde distintos organismos de competencia y el Banco Central de Brasil -BCB-, las cuales han conducido al fortalecimiento del sistema de pagos y el dinamismo del sector. Uno de los desarrollos más recientes es la creación del Sistema de Pagos Instantáneos -SPI-, también conocido como PIX, el cual es operado por el BCB y se consolidó como la única infraestructura centralizada para la liquidación de pagos instantáneos entre los diferentes actores del sistema de pagos. De esta manera, a través de PIX los diferentes actores de dicho sistema pueden operar y ofrecer a sus clientes soluciones de pago que se liquidan al instante. Sumado a estas ventajas, PIX tiene el potencial de: (i) aprovechar la competitividad y eficiencia del mercado; (ii) reducir los costos, aumentar la seguridad y mejorar la experiencia de los clientes; (iii) fomentar la digitalización del mercado de pagos minorista; (iv) promover la inclusión financiera, y (v) llenar una serie de vacíos en la canasta de instrumentos de pagos que actualmente están disponibles para la población -BCB, 2021-.

7. Conclusión

Hemos buscado entregar, a través de este capítulo, una aproximación a lo que han implicado las regulaciones de los sistemas de pago de bajo valor, de los instrumentos que cursan en él y de los actores que participan; en definitiva, entregar desde los instrumentos normativos un registro de cómo ha sido la evolución de los pagos digitales en el país, de cómo se relaciona con regulaciones adyacentes pero al final determinantes para su desarrollo y de los retos que plantea para un regulador una industria tan activa, en constante cambio y con una inmensa capacidad de contribución para el desarrollo de las dinámicas económicas.

Bibliografía

Arango, C., Arias, F., Rodríguez, N., *Suárez, N., & Zárate, H. (2020). Efectivo y pagos electrónicos. Ensayos sobre Política Económica, 93*, 1-76. https://doi.org/10.32468/espe.93

Arango-Arango, C. A., Zárate-Solano, H. M., & Suárez-Ariza, N. F. (2017, mayo). Determinantes del acceso, uso y aceptación de pagos electrónicos en Colombia. 999, 59. https://doi.org/10.32468/be.999

Asobancaria. (2021). *Ecosistema de pago Brasil y su importancia para la region.pdf.* https://www.fintechgracion.com/wp-content/uploads/Ecosistema-de-Pago-Brasil-y-su-importancia-para-la-region-.pdf

Banca de las Oportunidades. (2018). *Reporte de Inclusión Financiera 2020.* https://bancadelasoportunidades.gov.co/sites/default/files/2020/1.pdf

Banco Central Chile. (2022). *Informe de Sistemas de pago 2022*. https://www.bcentral.cl/documents/33528/3652920/Informe_de_sistema_de_pago_julio_2022.pdf/037fea7f-ce7f-1257-0025-62d71871a4b6

Banco Central del Uruguay. (2021). *Sistema de pagos Minorista Reporte Informativo No 25.* https://www.bcu.gub.uy/Sistema-de-Pagos/Paginas/Reporte-Sistema-Pagos-Minorista.aspx

Banco de la República de Colombia. (2020). *Reporte de Sistemas de pago 2020*. Bogotá : Banco de la República de Colombia.

Bank of Korea. (2022a). *ELECTRONIC FINANCIAL TRANSACTIONS ACT.* https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=1&query=electronic+financial+transactions+act&y=0&x=0#liBgcolor0

Bank of Korea. (2022b). *Payment and Settlement Systems Report 2021.* https://www.bok.or.kr/viewer/skin/doc.html?fn=20220713021243747O.pdf&rs=/webview/result/E0000866/202207

BCB. (2021). *Pix Powered by Banco Cental.* Pix Powered by Banco Central. https://www.bcb.gov.br/estabilidadefinanceira/pix

Decreto 1400 del 2005, (2005).

Decreto 2555 del 2010, (2010)

Decreto 1692 del 18 de diciembre de 2020, (2020). https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%201692%20DEL%2018%20DE%20DICIEMBRE%20DE%202020.pdf

Deutsche Bundesbank. (2022). *Zahlungsverhalten in Deutschland 2021.* https://www.bundesbank.de/en/publications/reports/studies/payment-behaviour-in-germany-in-2021-894118.

Muñoz, M. C.-M. (2021). *Derecho de las Obligaciones - Cap 13 Pago por Medios Electrónicos.* Bogotá: Universidad de Los Andes - Temis.

Pérez, C.; Pacheco, B. H., & Salazar, N. (2016). *BENEFICIOS POTENCIALES DE UN INCREMENTO EN EL USO DE LOS MEDIOS DE PAGO ELECTRÓNICOS EN COLOMBIA.* Fedesarrollo. https://www.repository.fedesarrollo.org.co/bitstream/handle/11445/2947/Repor_Abril_2016_Perez_y_Pacheco.pdf?sequence=3&isAllowed=y

Prieto, Ana María; Torres, David; Martínez Estela, José, & Gutiérrez, David. (2018). *Estudio sobre los sistemas de pago de bajo valor y su regulación.* URF. http://www.urf.gov.co/webcenter/ShowProperty?nodeId=%2FConexionContent%2FWCC_CLUSTER-106608%2F%2FidcPrimaryFile&revision=latestreleased

PSR. (2021, diciembre 31). *New Payments Architecture (NPA)*. https://www.psr.org.uk/our-work/new-payments-architecture-npa/

RBI. (2021, enero). *Banco de la Reserva de la India—Comunicados de prensa.* https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=50901

RBI. (2022, julio). *Reserve Bank of India announces Digital Payments Index for March 2022.* https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR602DPI147FB19811794BBB8CCBF29AF13B09CA.PDF

Remolina, N. (2013). *Responsabilidad por el tratamiento de los datos personales de clientes, empleados proveedores y terceros.* Bogotá: Universidad de los Andes - Temis.

CAPÍTULO 12

Metaverso y los servicios financieros

Juan Sebastián Peredo Bernal[1]

Resumen

El metaverso trae consigo una nueva iteración de Internet, sea que se plantee como parte de la evolución de la Web hacia Web3 o que se vea como una nueva forma de interacción social. Esta iteración presenta una nueva visión de la forma en la que concebimos las dinámicas sociales y económicas en Internet. Naturalmente, para las empresas, para las entidades financieras y, en general, para aquellos que buscan estar en el lugar donde se encuentran sus clientes, requiere de un nuevo planteamiento frente a la forma en la que se concibe la prestación de sus servicios. Para abordar la relación del metaverso con la prestación de servicios financieros, se analiza la evolución de la Web y de las iteraciones de Internet, las implicaciones de la centralización y descentralización de los metaversos, lo que las plataformas plantean como nueva forma de interacción social y, finalmente, la forma como la banca y los servicios financieros se conciben -y se podrán concebir- dentro del metaverso.

[1] Vicepresidente Jurídico de Lulo Bank S.A. Abogado de la Universidad del Rosario con especialización en derecho financiero de la Universidad Externado de Colombia y Master of Laws in Banking Law and Financial Regulation de The London School of Economics and Political Science.

1. Introducción

La discusión sobre el metaverso y su relación con la banca implica desligarnos de nociones preconcebidas sobre la forma como se prestan servicios financieros.

Desligarnos de pensar en un mundo de únicamente actividades reguladas y entidades vigiladas; de la necesidad de encontrarle un símil jurídico local a una actividad digital; de pensar en un mundo con tan solo algunos medios para la prestación de servicios financieros. Y, para los que han empezado a explorar el metaverso, desligarnos de la idea de que la única forma en la que el mundo bancario actuará en el metaverso corresponde a la apertura de sucursales bancarias.

También debemos abandonar toda prevención con el metaverso. Abandonar la prevención sobre la dificultad de programar un contrato inteligente. Abandonar los aparentes conflictos y estar dispuestos a aceptar los evidentes beneficios de concebir un mundo financiero con múltiples alternativas.

Una vez desligados de todo esto, podremos abordar cualquier discusión sobre el metaverso. Una discusión que viene dada por muchas variantes, formas de entenderlo y representarlo. A través de este texto, habremos recorrido de manera sencilla los principales aspectos del metaverso, bajo la lupa de los servicios financieros.

El desarrollo de múltiples metaversos ha derivado en un portafolio de diferentes plataformas, con diferentes mercados objetivo, diferentes usuarios, diferentes usos, diferentes formas de concebirse a sí mismos. Y esto, naturalmente, ha causado dificultad para entender el metaverso.

Para abordar la relación entre el metaverso y los servicios financieros, haremos un recorrido buscando primero entender qué es el metaverso, su forma de construcción y sus principales caracterizaciones, así como los choques naturales entre la estructura de gobierno de los metaversos y la que conocemos en el mundo físico, la identidad digital y la pseudonimidad, y a partir de esto daremos forma a la relación entre metaverso y servicios financieros. Esta discusión hay que darla desde la neutralidad tecnológica. (Ver la explicación de este concepto en el capítulo de Bancos Digitales).

2. Entendiendo el metaverso

No existe una definición exacta y tampoco un listado de requisitos que deban cumplirse para ser metaverso. El concepto se entiende desde lo abstracto y se aplica en lo concreto. Lo más importante: no existe un solo metaverso, no es un lugar único, no es una sola plataforma. El metaverso son múltiples lugares digitales, operados en múltiples plataformas, que proveen una alternativa a la realidad física en la que interactúan las personas. Por esto, al hablar de metaverso nos referimos a la multiplicidad de plataformas que ofrecen y ofrecerán este nuevo lugar de interacción social. El metaverso trae consigo un cambio paradigmático en la forma de interactuar en la Web, una conversación similar a la que se tuvo sobre Internet en la década de los 90: ¿Cuáles son las fronteras qué vamos a encontrar en los próximos años?

El metaverso se viene construyendo desde hace años, y en el último tiempo ha tomado una velocidad de exploración exponencial. Son lugares que existen, plataformas que operan, usuarios que las usan. Y así mismo, son lugares que existirán, plataformas que operarán y usuarios que las usarán. En la medida en que la gente explore más su identidad en el metaverso, más plataformas alternativas aparecerán y algunas desaparecerán.

El cúmulo de posibilidades parece imposible de listar, y por esta razón es difícil imaginar o anticipar un único camino a recorrer en el metaverso y su evolución en el corto, mediano y largo plazo.

Algo cierto es que el metaverso tiene muchas formas y expresiones y tendrá aún más: desde su gobernanza y economía, la soberanía del individuo sobre la identidad, la relación con los activos digitales y su arquitectura, hasta su *ethos* -razón de ser-. Las diferenciaciones y categorizaciones pueden resultar innumerables.

Al final, el metaverso plantea -y se le exige- desafiar las construcciones sociales a las que estamos habituados y también plantea -y se le exige- aprovechar su potencial que no se encuentra limitado por las leyes de la física -las limitaciones del mundo físico-.

3. La naturaleza del metaverso

3.1 Como parte de una nueva evolución de la Web

El metaverso ha venido tomando la forma de una nueva iteración -un nuevo modelo- de Internet y, más específicamente, de la Web. Hasta ahora, cuando se hablaba de esas iteraciones de la Web se mencionaban dos: Web1 y Web2. Cuando se habla del impacto del metaverso, algunos lo incluyen en lo que se denomina Web3.

Web1, la primera generación de la Web, fue mayormente construida desde la curiosidad académica y de los nuevos exploradores de las fronteras de Internet. La primera generación de la Web trajo consigo la construcción de lenguajes informáticos, estándares, protocolos interoperables. Esta fue la generación de los protocolos abiertos -no son propiedad de una empresa en particular y permiten ser usados libremente-, la generación de HMTL y SMTP. Es decir, la generación de las páginas web y de los correos electrónicos. La generación de personas y empresas que empezaron a construir sus primeras páginas web, los primeros blogs, y que empezaron a entender la Web como una nueva forma de comunicación social, como un nuevo lugar de interacción social.

Al principio fue ignorada, incluso se la tildó de una moda. Sin embargo, la sociedad poco a poco se fue volcando hacia la Web. Y ese nuevo lugar de interacción social empezó a mostrar muchas formas y a cautivar multiplicidad de intereses. Pasaron de ser lugares de interacción social académica y de un grupo de curiosos, a lugares de interacción social mucho más masivos. Esta masificación evidenció insuficiente capacidad de los equipos en los hogares para acceder a Internet, y por esto se volvió común escuchar de los café Internet y los lugares de juego *online*. La primera iteración de la Web logró atraer a una gran parte de la población.

Con la adopción precipitada de Internet, la Web empezó a consolidarse como un nuevo

lugar -y después *el lugar*- de interacción social y comercial de la sociedad, generando una explosión de nuevas creaciones, de nuevas empresas, de nuevos modelos de interacción social basados en Internet. Se masificaron los protocolos propietarios -protocolos cerrados- explotables por quienes los creaban y operaban su negocio. Esto llevó al surgimiento de las redes sociales, a la explosión de los *marketplaces*[2], al nacimiento de muchos de los gigantes de tecnología que conocemos hoy en día. Es lo que se conoce como Web2.

La Web se movió de una versión más académica y de exploración de algunos curiosos, a una versión en la que la interacción social masificada naturalmente llevó a que los intereses comerciales confluyeran en los nuevos lugares de reunión social. Esto implicó que de una Web basada en protocolos abiertos pasáramos mayormente a una Web que construía protocolos cerrados aprovechables económicamente por sus creadores. Y con esto, la carga y el deber de las nuevas plataformas, las redes sociales, de gobernar y administrar sus reglas de uso y su aprovechamiento dentro de una economía que se venía digitalizando. Estaban centralizadas la operación, la gobernanza, la administración y la explotación económica de sus creaciones.

Por supuesto, como parte esencial de esta operación, administración y explotación económica, empezamos a vivir en un mundo digital de aprovechamiento de datos, de analítica avanzada. Con Web2, los movimientos legislativos y regulatorios para proteger de forma más clara los datos fue natural. La normativa actual fue construida en esa época y para esa época. A su vez, las personas empezaron a tener una noción más clara de privacidad, de lo que implicaba dicha protección y de la razón por la que empezaban a aceptar todo tipo de términos y condiciones y autorizaciones para el tratamiento de sus datos. Que los negocios digitales se movían a través de datos fue evidente para todos y también que nuestros datos personales eran -y son- una fuente de explotación económica en el mundo digital.

De la mano de estas dos características de Web2, su gobernanza centralizada en las plataformas y la noción de privacidad, se erigieron los cimientos de lo que sería la Web3, cimientos que incluso se podrían rastrear desde muchos años antes:

> *La privacidad es necesaria para una sociedad abierta en la era electrónica. La privacidad no es sinónimo de secreto. Un asunto privado es algo que uno no quiere que todo el mundo sepa, pero un asunto secreto es algo que uno no quiere que nadie sepa. La privacidad es el poder de revelarse selectivamente al mundo*[3].

3.2 La relación del metaverso con Web3

Web3 parte de la idea de descentralización a partir de una tecnología muy particular: blockchain[4]. Bloomberg describió Web3 como una idea que *construiría activos financieros, en forma de tokens*[5], *en el funcionamiento interno de casi cualquier cosa que se haga en línea*[6]*. Más que una idea*, es una realidad que viene operando desde hace un tiempo.

[2] Plataformas digitales de compra y venta de bienes y servicios.
[3] Hughes, Erick. *A Cypherpunk's Manifesto*. 9 de marzo de 1993. Traducción propia.
[4] Es importante que el lector de este artículo se encuentre familiarizado con blockchain y lo que implica como tecnología y como modelo de gobernanza.
[5] La moneda de uso de un protocolo o de un contrato inteligente dentro de un protocolo.
[6] Kharif, Olga. What You Need to Know About Web3, Crypto's Attempt to Reinvent the Internet. Bloomber, US Edition. 10 de diciembre de 2021.

En este momento partimos en dos los metaversos: los centralizados y los descentralizados.

Los metaversos centralizados, con una gobernanza que sigue la forma de Web2, que centralizan la administración y explotación económica en la plataforma creadora del metaverso. No muy diferente de las actuales redes sociales. El desarrollo por supuesto es propietario, sus términos de uso y condiciones residen en la plataforma creadora y la explotación económica le pertenece a su creador.

Dentro de este concepto de metaverso se pueden incluir casi todos aquellos cuyo desarrollo no está basado en blockchain -sin que el solo hecho de que esté basado en blockchain haga que un metaverso sea considerado descentralizado-. Este tipo de metaversos construye la interacción social sobre los supuestos económicos y de gobernanza de Web2. De hecho, una gran parte de estos metaversos son desarrollados o están siendo desarrollados por muchas de las grandes compañías de Web2, por quienes están detrás de las redes sociales.

Entonces, entender un metaverso centralizado es mucho más sencillo que entender uno descentralizado. La razón es que llevamos más de una década de interacción a través de redes sociales, de gobernanza por términos y condiciones y de explotación económica a partir de datos personales.

Por su lado, los metaversos descentralizados se construyen a partir, precisamente, de la descentralización. El metaverso descentralizado se soporta en blockchain, tiene un token que lo gobierna y la privacidad se protege a partir de la pseudonimidad que otorga una billetera de criptoactivos. Veamos cada uno de estos componentes.

3.2.1 Un desarrollo a partir de blockchain y NFTs

Que un metaverso se desarrolle a partir de blockchain es el componente principal que lo habilita para tener un orden descentralizado. La descentralización que trae consigo blockchain -particularmente redes como Ethereum que han llegado a un estadio de descentralización de la red- le otorga el potencial al metaverso de organizarse de manera que su gobernanza sea, también, descentralizada. La gobernanza descentralizada de un metaverso está dada, palabras más, palabras menos, por otorgarle a sus usuarios el poder de convenir las reglas de uso y de convivencia del metaverso, las reglas de la economía que lo rigen y las que determinan su destino. Para lograrlo, parte de una base fundamental, apalancada en blockchain: *los tokens*.

Algo que maravilla a las personas sobre el metaverso es, precisamente, su operación a través de blockchain. Blockchain es primordialmente el habilitador que permite en el metaverso tener relaciones sociales digitales que funcionan como un reemplazo de determinadas relaciones sociales físicas. Cuando pensamos en una representación digital del mundo físico, más que avatares similares a las personas que los usan, hablamos de relaciones económicas y sociales similares a las que encontramos en el mundo físico[7].

Ha llegado al punto de permitir la adquisición de tierra digital y el desarrollo de esa tierra; la adquisición de bienes, activos digitales, que podrán ser usados o vendidos nuevamente,

[7] Peredo Bernal, Juan Sebastián. Entrando al metaverso – NFTs, blockchain y el metaverso – Parte 3/X. Publicación en LinkedIn. Abril, 2022.

como se haría en el mundo físico. Todo atado a tecnología que permite a las personas demostrar la titularidad sobre su identidad digital y la propiedad de sus activos digitales. Con un ingrediente adicional: permitir que las personas asuman la forma en que quieran construir y proyectar su identidad digital, que puede ser igual o diferente a su identidad real.

Estos mundos, metaversos creados a partir de blockchain e interoperables por esta misma razón, tienen la capacidad de permitirle a una persona visitar tiendas y lugares, asistir a eventos y conciertos, visitar museos, hablar con otras personas y recorrer el metaverso de manera similar a como lo haría en el mundo físico, pero sin las limitaciones de este.

Para esa representación digital del mundo en el metaverso se hace necesaria tecnología que lo entrelace, especialmente si queremos darle todas las cualidades que acabamos de mencionar[8]. La tecnología para hacerlo es blockchain.

Blockchain es esa telaraña en la que están todos los componentes del metaverso, como la identidad digital, la identificación, la moneda y cada uno de los activos digitales que lo componen. Blockchain es una red que lleva un registro de todo lo que va pasando. Permite llevar el registro del metaverso y de las transferencias, de los ingresos, de la identidad digital, de la propiedad de los activos digitales allí adquiridos y de la moneda que en su interior se utilice -*el token*-. Blockchain permite, además, tener mecanismos descentralizados de gobernanza[9].

Todo reside, en últimas, en la dirección de criptoactivos que cada usuario tenga -más adelante veremos algo de la práctica sobre el ingreso a los metaversos soportados en blockchain-; allí tiene los activos digitales que ha adquirido o recibido en el tiempo y que, a su vez, son utilizables en la plataforma; tiene los *tokens* -moneda- del metaverso y recibe las retribuciones, recompensas, premios derivados de utilizar la plataforma[10].

Blockchain también es la tecnología que habilita la existencia de NFTs. NFT significa *non-fungible token* o *token* no fungible. No fungible significa que no son reemplazables unos por otros. Por ejemplo, los dólares y los pesos colombianos son activos fungibles -reemplazables unos por otros-. A nadie le importa si le pagan con un determinado billete de 100 dólares, le importa que le paguen 100 dólares. En cambio, si yo compro una casa, espero esa casa, no cualquiera que me quieran dar. En blockchain, el equivalente al dinero son las monedas que soportan la operación del respectivo blockchain -por ejemplo, Ether en el caso de Ethereum o bitcoin en el caso de Bitcoin-[11]**,** y el equivalente a la casa que compré son los *tokens* no fungibles -los NFTs-. Entonces, un NFT es una representación única de un activo digital.

Los NFTs han tenido una explosión mediática derivada de uno de los casos de uso más relevantes: el arte. Sin embargo, los NFTs pueden estar en absolutamente todo, por ser tecnología que permite singularizar un activo de manera digital. El arte digital encontró una manera de garantizar con certeza la procedencia de los activos digitales a través de los NFTs -con mayor eficacia que los mecanismos de verificación de procedencia en el arte físico-.

[8] Ídem.
[9] Ídem.
[10] Peredo Bernal, Juan Sebastián. Entrando al metaverso – NFTs, blockchain y el metaverso – Parte 3/X. Publicación en LinkedIn. Abril, 2022.
[11] Además de la moneda del blockchain particular (las cuales son fungibles por su esencia), también lo son los tokens fungibles creados a partir de un contrato inteligente y que son usados como moneda para los fines propios de ese contrato inteligente.

¿Qué otra forma más segura de saber quién es el propietario de una obra artística digital que hacer que la misma viva en blockchain a través de un NFT? La representación a través de un NFT implica, *per se*, que todas las características de seguridad y de *inmutabilidad* de blockchain respaldan el activo.

El ejemplo clásico permite dar luz a este concepto: si se pintaran 100 representaciones exactas de la Mona Lisa y las mezclaran con la original, se necesitaría un grupo de expertos para determinar cuál es la real y habría que confiar en que la conclusión del grupo de expertos es correcta o en que dichos expertos no tuvieran interés en seleccionar una distinta de la original. En el caso de los NFTs, no se necesita un grupo de expertos para saber cuál es el original, simplemente nos remitimos a blockchain y al *smart contract* -programa- que dio origen a la obra para saber cuál es; así de sencillo.

Más allá del arte, los NFTs son la representación en blockchain de los activos digitales que ocupan y pueden ocupar el metaverso:

> *Si queremos comprar tierra digital en el metaverso, esta tomará la forma de un NFT. Si queremos comprar avatares, estos tomarán la forma de un NFT. Si queremos comprar arte, estos tomarán la forma de un NFT. Si queremos comprar accesorios, estos tomarán la forma de un NFT. Y así, todo lo que se imaginen*[12].

A esto se debe sumar uno de los ingredientes finales y tal vez más importantes del desarrollo de los metaversos en blockchain: la interoperabilidad. Las personas no están atadas al uso de una sola plataforma, los activos digitales son utilizables en tantas otras plataformas como se desarrollen en ese blockchain particular -naturalmente la tierra no, ya que es una representación de tierra digital de un metaverso específico, tal y como se ampliará más adelante-. Podría una plataforma dejar de funcionar, pero los activos continuarían existiendo en la medida en que seguirían estando en blockchain y podrían seguir siendo utilizados en otra plataforma.

3.2.2 El rol del *token* en el metaverso

Cada metaverso descentralizado tiene un *token* que cumple varias funciones: primero, es la moneda de uso en el metaverso. Esto hace que la economía gire alrededor del *token*, que tiene unas características económicas determinadas y programadas; segundo, es el mecanismo a través del cual se premia el uso del metaverso -algo particularmente interesante y tradicional en la forma de construcción de estos metaversos-. El usuario es el eje principal, por lo que su participación se recompensa a través de la asignación de *tokens* de ese metaverso, dependiendo de la estructuración económica del respectivo *token* -los *tokenomics*-, y, tercero, *el token* habilita al usuario para participar en el sistema de gobernanza del metaverso. El *token* otorga derechos de voto y le permite al usuario -poseedor de ellos- participar en los mecanismos descentralizados de gobernanza, tradicionalmente desarrollados a través de *descentralized autonomus organizations* -DAOs-[13]. Esta gobernanza descentralizada les permite a los usuarios decidir las reglas que regirán el metaverso y su economía, proponer ideas, votar sobre ellas, ordenar gasto. Se podría, y se debería, escribir un capítulo única y exclusivamente para desarrollar la estructuración técnica y legal de los DAOs.

[12] Peredo Bernal, Juan Sebastián. Entrando al metaverso – La tierra digital – Parte 6/X. Publicación en LinkedIn. Abril, 2022.
[13] Mecanismo de organización a partir de un *smart* contract que le permite a los participantes tomar decisiones sin la necesidad de un órgano central.

El *token*, entonces, es uno de los engranajes principales de un metaverso descentralizado por cuanto hace parte de todo lo que integra a ese metaverso. El *token*, a su vez, es el mecanismo de retribución principal que tienen los creadores del metaverso, el premio que reciben por su creación y su rol dentro del mismo.

3.2.3 La dirección de criptoactivos

La forma de acceder a todo lo que hemos mencionado son las direcciones de criptoactivos. Para tener acceso al metaverso, se inicia sesión utilizando la billetera de criptoactivos, lo que le permite al usuario conectar una dirección única -por ejemplo, una dirección de Ethereum- al metaverso. Este mecanismo de inicio de sesión es interoperable en la medida que se puede utilizar como mecanismo de autenticación de identidad en cualquier sitio web que utilice ese blockchain particular. Eso hace que no se requiera que en cada sitio web, en cada plataforma, una persona deba tener un usuario único con contraseñas diferentes. La billetera de criptoactivos o, mejor, la dirección de criptoactivos atada a esa billetera es la que provee ese mecanismo de inicio de sesión único para todos los sitios web[14].

La dirección de criptoactivos no será solamente el mecanismo identificador de quien accede al metaverso, también cumple otra serie de funciones: tiene los activos digitales que esa persona ha adquirido o recibido en el tiempo y que, a su vez, son utilizables en la plataforma y tiene los *tokens* -moneda- del metaverso y recibe las retribuciones, recompensas y premios derivados de utilizar la plataforma[15].

El acceso, interacción e identidad están alojados en esa llave que es la dirección de criptoactivos. La dirección -o direcciones cuando se tiene más de una- se convierte en su identidad y en el acceso a su patrimonio digital[16].

Así mismo, y en línea con una cita anterior, la dirección de criptoactivos es el mecanismo que busca que la privacidad sea uno de los ejes principales del funcionamiento de los metaversos. Al final, uno de los principales fundamentos de blockchain está en la privacidad.

Debemos mencionar, sin embargo, que en algunos casos, y muchas veces debido a regulación que no termina de sintonizarse con la tecnología actual, las plataformas requieren que se adelante un proceso adicional de KYC -*Know Your Customer, conozca a su cliente*-. Evidentemente, los principios sobre los cuales se ha erigido Web3 y los procesos de KYC son de alguna manera contraintuitivos. Como lo veremos más adelante, el mundo Web3, basado en la privacidad, y el mundo bancario regulado, basado en el conocimiento del cliente, tienen una colisión natural compleja de resolver.

Con esto, demos paso a la discusión para entender la naturaleza de la identidad digital en Web3.

[14] Peredo Bernal, Juan Sebastián. Entrando al metaverso – NFTs, blockchain y el metaverso – Parte 3/X. Publicación en LinkedIn. Abril, 2022.
[15] Ídem.
[16] Ídem.

3.3 Identidad digital en Web3

Si nos aproximáramos a una simple definición de identidad, podríamos decir que es aquello que caracteriza a una persona y que le permite diferenciarse de los demás. La identidad, por supuesto, debe ser vista como algo que supera la simple identificación a partir de rasgos físicos; es un cúmulo de características, cualidades, intereses y experiencias de un individuo que lo hacen identificable y único en la sociedad.

La identidad digital ha permitido a las personas presentarse de una manera diferente de la que estábamos acostumbrados en el universo físico, les ha dado la posibilidad de identificarse a partir de sus intereses, su cultura, su conocimiento, su forma de pensar, las comunidades en las que participa, entre muchos otros. Lo que ha logrado tocar fibras más profundas en materia de identidad individual y colectiva, y lo que cada una de estas conlleva.

Esta especie de nueva identidad nada tiene que ver con un tipo de identificación centralizada -el documento de identidad- o el nombre que se incluye en un registro estatal o el número de identificación ciudadana que se le haya asignado a alguna persona. Es muy importante diferenciar identidad e identificación. Diferenciar entre cómo nos representamos y cómo nos identificamos, cómo nos individualizamos frente a los demás.

La discusión de la identidad digital y el metaverso es fundamental. El metaverso, centralizado o descentralizado, pasa a ser un nuevo lugar de reunión social y de interacción en el que las personas confluyen por el interés que tienen de explorar una realidad digital alternativa. El metaverso es un lugar en el que se puede tomar cualquier forma y en la que las personas se expresan de la manera que quieren. Al haber multiplicidad de metaversos, siempre se podrá encontrar un lugar que se ajusta perfectamente a lo que cada uno busca.

Esto implica, necesariamente, que empezamos a tocar las fibras de la soberanía sobre la forma en la que alguien quiere identificarse y la soberanía en la decisión de los lugares en los que se quiere participar colectivamente. Al tocar esta fibra, comprendemos la existencia de múltiples metaversos, tan distintos entre todos ellos. Un único metaverso, un único lugar de interacción social en esta nueva forma de iteración de Internet, no sería muy diferente a lo que ya encontramos en el mundo físico[17].

En el metaverso, entonces, las personas asumen una identidad soberana y asumen también una soberanía respecto de la forma en la que son identificados -soberanía frente a la identidad y la identificación de cada persona-. La identidad depende de la construcción que cada uno realice y la identificación simplemente depende de la dirección de criptoactivos que utilice para asumir esa identidad. La pseudonimidad les permite a las personas elegir el nombre y forma que prefieran sin estar atados a una identificación como aquella a la que estamos acostumbrados. Esto no difiere mucho de lo que ha venido siendo tendencia en la Web desde su inicio, incluso en la época de las redes sociales. Sin embargo, en el caso del metaverso se ve reforzado por la posibilidad de hacer parte activa de la red social sin tener que mostrarse físicamente y con un aliciente adicional: poder interactuar socialmente en lugares alternativos al mundo físico sin estar atado a los rasgos físicos.

[17] Peredo Bernal, Juan Sebastián. Entrando al metaverso – Identidad digital y pseudonimidad – Parte 4/X. Publicación en LinkedIn. Abril, 2022.

La forma de identificación, como se vio, solo exige conectar una billetera de criptoactivos para validar el ingreso de una persona, para leer los activos digitales que tiene y hacerlos interoperables en el metaverso, para permitirle hacer parte de la gobernanza y adquirir bienes y servicios. La billetera de criptoactivos es, por lo tanto, la llave de acceso que contiene la información que necesitamos para operar en el metaverso. Y aún más importante, es la llave de acceso que permite operar en todo Web3, sin necesidad de hacer procesos de registro en cada plataforma y pudiendo utilizar el portafolio de activos digitales de manera interoperable.

Esa llave de acceso, al funcionar a partir de *blokchain*, provee un acceso en el que no se requiere que una entidad centralizada valide la identificación de sus participantes. La identificación viene validada por ser quien tiene esa llave que le da la entrada a la dirección de criptoactivos y su utilización. La identidad viene dada por todo lo que caracteriza a esa persona en el metaverso -la forma como se quiere representar, los grupos con los que quiere interactuar, los activos que compra, entre muchas otras cosas-.

En este punto, es importante mencionar que la privacidad no es ni debe ser entendida como un sinónimo de libertad de actuación más allá de la ley y las reglas. Operar en Web3 identificándose a partir de direcciones de criptoactivos no implica de ninguna manera un anonimato irresoluble con una libertad de actuación sin responsabilidad. Los múltiples ejercicios forenses recientes han demostrado que la naturaleza pública de blockchain y las herramientas forenses adecuadas permiten la identificación de individuos cuando actúan al margen de la ley. El pseudónimo es una forma de representación, no una forma de ocultamiento. La pseudonimidad, en el estado del arte, representa la magia de proteger la privacidad de las personas sin perder la responsabilidad que a cada uno le corresponde por sus acciones[18].

Esto es supremamente importante, la naturaleza pública de blockchain hace que los metaversos soportados en esta tecnología sean intrínsecamente públicos también. Que la actuación de cada uno de los individuos, sus transacciones y sus operaciones sean identificables y rastreables. Entonces, una identificación basada en una dirección de criptoactivos permite a cualquier agente, público o privado, tener un registro histórico y en tiempo real de las actuaciones de un determinado individuo en blockchain. Y sí, esto ha hecho que la conversación respecto de blockchain y criptoactivos se haya podido alivianar con el tiempo. Que la pseudooscuridad que se le atribuía al inicio ahora sea descalificada por ser evidente su naturaleza pública.

Ahora, al pensar en el mundo de los servicios financieros tradicionales, se vuelve apenas lógico evidenciar esa primera colisión entre los dos mundos: el bancario tradicional y el de Web3. El mundo bancario tradicional tiene arraigados los sistemas de conocimiento de clientes que le exigen tener plena seguridad respecto de quién es la persona con la que están transando. Ese mundo del conocimiento del cliente exige la entrega de identificaciones, la realización de biometría, la plena individualización del individuo de acuerdo con sus registros estatales. Y esto es natural, desde la perspectiva de entidades que responden por las transacciones que se realizan a través de ellas y que tienen que observar un alto número de normas que las obligan a desplegar sus mejores oficios para asegurarse de saber con quién están transando.

[18] Ídem.

En el mundo de Web3, como han visto, no hay nada más lejano a esto. La identificación de las personas parte de la utilización de direcciones de criptoactivos. No hay necesidad de entregar evidencia adicional, no hay necesidad de entregar documentación ni de realizar pruebas biométricas que le permitan a una entidad corroborar que quien entrega una identificación es quien tratar de usar un servicio. En Web3 la identificación solo depende de tener la llave de acceso a la dirección de criptoactivos.

Entonces, nos encontramos con dos mundos: uno que exige un conocimiento individual del cliente a partir de registros centrales y otro que simplemente exige una billetera de criptoactivos para poder operar. El balance entre estos dos mundos lo veremos más adelante.

4. Los servicios financieros en el metaverso

Los servicios financieros en el metaverso tienen que verse desde dos perspectivas: a partir de la vinculación de instituciones a metaversos específicos -centralizados o descentralizados- y a partir de lo que se entiende como servicios financieros en Web3.

La primera parte del análisis se centrará en la integración en los metaversos existentes de los bancos o entidades financieras que ya conocemos y que operan en el sistema financiero como existe actualmente. La segunda parte se concentrará en el entendimiento de los servicios financieros en Web3.

Es una discusión sobre cómo abordar el metaverso a partir de lo que conocemos como servicios y productos financieros ofrecidos por bancos o entidades financieras y cómo abordarlo a partir de la construcción propia de servicios financieros que han nacido a partir de los criptoactivos y Web3.

4.1 La vinculación de las entidades a los metaversos

Para las entidades financieras tradicionales, los servicios financieros en un metaverso, centralizado o descentralizado, pueden verse como un canal adicional de contacto con los clientes. Un canal que puede tener diferentes funcionalidades, desde la educación financiera hasta la transaccionalidad. Seguramente, la realización de operaciones tendrá una forma similar a la que los usuarios se encuentran acostumbrados, y en cuanto a la identificación, el cliente deberá ser individualizado de acuerdo con mecanismos diferentes a Web3 y similares o iguales a los tradicionales bancarios.

Un ejemplo, tal vez muy sencillo pero ilustrativo de este asunto, son las apps bancarias y las sucursales virtuales accesibles a partir de exploradores de Internet. Hace un tiempo, y especialmente antes de la llegada de los teléfonos inteligentes, las personas comenzaron a utilizar masivamente la Web a través de sucursales virtuales a las que se accedía -y se accede- usando exploradores de Internet. Los teléfonos inteligentes, con tecnología que permitía la creación de apps bancarias, primero vieron un uso -no muy amigable- de sus exploradores para la realización de operaciones bancarias a través de las sucursales virtuales que ya se conocían. Solo después de un tiempo se empezaron a desarrollar estas apps utilizando los sistemas operativos de los teléfonos inteligentes. Es decir, lo único que un usuario de un teléfono inteligente lograba era utilizar lo que ya estaba disponible en Internet a

través del explorador de su celular. No había nada que se desarrollara a partir de esta nueva tecnología que apareció. No había mayor adaptación -tal vez alguna modificación de la interfaz en la Web para permitir visualizar correctamente la sucursal bancaria-. Entonces, no hubo una explotación de la capacidad tecnológica que permitían los teléfonos inteligentes, sino hasta unos años después de su lanzamiento.

Esto mismo se puede intuir -y ya se está viendo- en relación con el metaverso. La apertura de sucursales financieras es ese primer paso, pero no es el paso que realmente explota las capacidades tecnológicas que ofrece el metaverso.

En un metaverso centralizado, probablemente la apariencia transaccional y económica será similar a la que encontramos actualmente. Dependiendo del tipo de metaverso centralizado y de sus expectativas con sus usos y funciones, los metaversos podrán tener un componente activo en la realización de actividades financieras con los usuarios: financiación para la compra de funcionalidades adicionales, actividades financieras tradicionales realizadas en cabeza de la plataforma directamente, etc. De nuevo, es un uso y explotación del metaverso que no distaría mucho de lo que actualmente se les ofrece a los clientes y a lo que están acostumbrados.

Ahora, bajo esta perspectiva de creación de nuevas sucursales financieras, el modelo de las entidades financieras en metaversos descentralizados no distaría mucho de lo que se podría ver en un metaverso centralizado. Es decir, el modelo de explotación potencialmente sería similar y la integración a mecanismos de Web3, bajo este simple modelo de apertura de sucursales en el metaverso que integren los servicios bancarios y financieros tradicionalmente ofrecidos por estas entidades, no sería requerido -y probablemente no sería explotado-. Entonces, lo que empezamos a ver -y lo decimos en presente porque son modelos que ya vienen desarrollándose- es una tímida forma de ver la oportunidad del metaverso para las entidades financieras. Es tímida por cuanto plantea al metaverso como un canal de acceso, que realmente es más un canal de redireccionamiento de su portafolio de servicios bancarios y financieros tradicional: una especie de portal que dirige a quien se encuentra en el metaverso hacia los canales tradicionales de atención de las entidades financieras.

Esta es, sin duda, la versión más sencilla de exploración inicial que una entidad financiera puede tener del metaverso. Es tan sencilla que, en materia regulatoria, ese redireccionamiento hará que la transaccionalidad siga realizándose a través de los canales habituales y que las reglas tal y como se encuentran escritas actualmente sigan siendo útiles.

Los bancos tradicionales, solo en el caso de operar en metaversos descentralizados, tendrán un componente adicional a lo que ya están acostumbrados: tener, al menos parcialmente, una parte de su construcción en blockchain. Para poder tener una sucursal bancaria, necesariamente tendrán que vincularse de la manera que Web3 exige: una billetera de criptoactivos. Tener una sucursal bancaria también exigirá adquirir tierra en el metaverso y desarrollarla, todo lo que se hace a partir de activos digitales que se encuentran en blockchain. Y, seguramente, también tendrán que transar en criptoactivos para poder adquirir esos activos digitales. Entonces, la particularidad de construir sucursales bancarias en el metaverso obligará a muchos bancos a tener que vivir el mundo de los criptoactivos para poder operar esas sucursales, incluso bajo el modelo tímido que estamos discutiendo en este momento. Y esta conversación nos da pie para hablar, por lo menos brevemente, de tierra digital.

Cuando hablamos de metaversos descentralizados, metaversos que operan basados en blockchain, la tierra digital es un activo más que existe en el respectivo blockchain y que vive como un NFT. El hecho de que sea un NFT permite tener mecanismos de validación de propiedad y, a su vez, permite conectarse y tener mecanismos privados y públicos para poder venderlo, transferirlo, entregarlo en garantía y comprarlo. La seguridad dada por blockchain y su forma de construcción asegura que nadie diferente a su dueño -a quien tiene las llaves de la dirección de criptoactivos- pueda realizar algún tipo de operación con la tierra digital. Nadie diferente a su propietario puede hacer uso, transferir, desarrollar, construir en esa tierra digital.

En cambio, los metaversos centralizados, por su forma de construcción y desarrollo, poco campo dejan a que exista algún tipo de concepto de propiedad interoperable sobre los activos que existen en su plataforma. Lo que queremos decir es que básicamente el propietario de tierra digital en un metaverso centralizado lo podrá ser en tanto el diseño centralizado se lo permita y sujeto a la decisión de ese metaverso. Dentro de las decisiones de un metaverso centralizado podrá incluso existir la posibilidad de retirar la propiedad a una persona o empresa. Piensen, para esto, en el poder atribuido por los términos y condiciones de las plataformas en las que operan redes sociales. A una empresa o una persona podría prohibírsele el acceso a la red social. En un metaverso centralizado también podría prohibírsele el acceso y retirársele sus derechos; por supuesto, sujeto a los términos y condiciones de uso del metaverso que haya aceptado la empresa o a la persona. Evidentemente, todo variará entre metaversos, el nivel de seguridad sobre la propiedad en la tierra digital y los activos digitales estará dado por las atribuciones que se otorguen a cada una de las plataformas que operan el respectivo metaverso centralizado.

Decisiones, decisiones. Los bancos tendrán que tomar muchas decisiones al momento de explorar la adquisición de tierra digital para abrir sus sucursales. Y no estamos discutiendo la posibilidad regulatoria, sino las múltiples variables dados los múltiples metaversos. Habrá puntos en común entre metaversos, al momento de analizar el metaverso en el que se operará, el lugar o lugares donde se adquirirá tierra digital. Será interesante para los bancos colombianos, como lo ha sido para entidades financieras que han empezado a explorar el metaverso en el mundo, entender los nuevos territorios, las formas de explotación, el tipo de personas que hacen uso de metaversos, las ubicaciones deseadas en cada uno de ellos. Entender el tamaño de la tierra digital, los usos que se le pueden dar -y en algunos casos, en algunos metaversos, el tráfico de usuarios en ese metaverso y esa tierra digital-. De eso se trata descubrir los nuevos metaversos y hacer parte de ellos[19].

Cerrando esa breve referencia al concepto de tierra digital, necesaria para cualquier discusión sobre la apertura de sucursales bancarias en el metaverso, podemos llegar a una versión resumida de esta primera forma de exploración del metaverso por parte de las entidades financieras: los productos seguirán siendo los mismos. Es decir, los bancos y entidades financieras no estarían ofreciendo productos nuevos, simplemente estarían ofreciendo sus productos -ya operativos digitalmente- a través de un nuevo medio de contacto con sus clientes. Los productos del banco seguirían operando de la misma manera en la que operan de manera tradicional.

[19] Peredo Bernal, Juan Sebastián. Entrando al metaverso – La tierra digital – Parte 6/X. Publicación en LinkedIn. Abril, 2022.

Sin embargo, incluso en una versión tímida de exploración del metaverso, la neutralidad tecnológica se antoja fundamental. De no aplicarse, se limitaría la capacidad de evolución de las entidades financieras para su llegada a esta nueva iteración de la Web y de los servicios financieros -como se verá más adelante-. De no aplicarse, se le cerraría la entrada a los bancos y, más importante, se privaría a los clientes de poder usar un nuevo tipo de tecnología para el acceso a sus productos y servicios.

Al inicio de este capítulo se dijo que la apertura de sucursales bancarias no es la única forma para que los bancos actúen en el metaverso. Con esta idea, podremos explorar la forma de prestar servicios financieros en Web3.

4.2 El entendimiento de servicios financieros en Web3

Como vamos a hablar de los servicios financieros en Web3, nos tenemos que trasladar a metaversos que basen su operación en blockchain.

Los metaversos descentralizados basan su operación en blockchain y esto, *per se*, hace que la conversación sobre servicios financieros se expanda. Por supuesto, el potencial uso de tierra digital en el metaverso para construir sucursales bancarias sigue ahí -y así es en su forma más elemental como se ha venido trabajando-. Como lo veíamos, la exploración del metaverso para abrir sucursales bancarias no tiene mayores diferencias cuando se trata de metaversos centralizados y descentralizados.

Sin embargo, la integración de mecanismos de finanzas descentralizadas naturales de Web3 -DeFi, por su acrónimo en inglés- hace que los servicios financieros en los metaversos descentralizados ofrezcan un abanico más amplio de posibilidades: la integración de *Descentralized Exchanges* -plataformas de intercambio descentralizadas- al metaverso, la financiación a partir del apalancamiento en activos digitales, las transferencias de recursos sin intermediarios, servicios de inversión descentralizados y así podríamos continuar. Los metaversos descentralizados, entonces, ofrecen un abanico en el que compiten entidades tradicionalmente reguladas -como los bancos- con entidades -si se les puede llamar así- no reguladas. Esto quiere decir que las entidades reguladas se encuentran -y se encontrarán- con una competencia a la que no están habituados. Una competencia de naturaleza no regulada, completamente apalancada en blockchain y que opera bajo principios diferentes a los que tiene la banca tradicional.

Pensar, entonces, en que la oferta de servicios tradicionales bancarios sea suficiente para competir en el metaverso puede parecer y sonar ingenuo. Simplemente abrir una sucursal bancaria para ofrecer un nuevo punto de contacto, incluso un nuevo punto de transaccionalidad, parecería insuficiente. Y es que el espectro de servicios financieros descentralizados ofrecidos por Web3 trae consigo un nuevo tipo de competencia para los actores regulados que quieren aventurarse al metaverso: un portafolio de servicios digitales, apalancado en tecnología descentralizada y en activos digitales.

Haberse instituido en Web3, en blockchain y en criptoactivos hace que los metaversos sean un canal óptimo de llegada para que las personas satisfagan sus necesidades financieras haciendo uso de operaciones de finanzas descentralizadas.

Y es que DeFi puede entenderse como un sistema financiero paralelo al que conocemos y

que no depende del rol de los intermediarios a los que estamos acostumbrados. No requiere de bancos, no requiere de aseguradoras, no requiere de fiduciarias, etc. Las personas, apoyadas en desarrollos en blockchain, tienen la capacidad de realizar operaciones de crédito, de hacer transferencias, de apalancarse, de ahorrar, de invertir, de asegurarse, entre muchas otras, a través de contratos inteligentes, eliminando la necesidad de estos intermediarios. Todo esto se desarrolla bajo los principios de Web3 que hemos mencionado a través de este capítulo.

A través de DeFi se puede realizar la mayoría de las operaciones que estamos acostumbrados a ejecutar a través de entidades financieras. Solo que en este caso no se necesita de ningún intermediario y todo se basa en el paradigma de blockchain: *trustless* -sin necesidad de un intermediario de confianza que apruebe las operaciones-.

Entonces, para las entidades financieras, el metaverso implica tener un nuevo vector de competencia. Una competencia que se arraiga en los principios de Web3. Una competencia que ve muy natural conectarse a los diferentes metaversos descentralizados. Una competencia que, además, tiene la facilidad de hablar el mismo idioma de los metaversos descentralizados.

Y es que DeFi ha venido ganando terreno a pasos agigantados; solo dando el ejemplo de Ethereum -segundo blockchain por capitalización de mercado, detrás de *Bitcoin*- y el volumen estimado de operaciones de DeFi que ocurren en esa red, nos podemos dar cuenta: de un volumen de casi 400 millones de dólares en abril de 2019 ha pasado a un poco más de 80 billones de dólares mensuales en abril de 2022[20].

Entonces, la conversación se torna diferente y por eso se percibe tímido pensar en abrir sucursales bancarias como la forma de explotación del metaverso por parte de los bancos. DeFi ha crecido a pasos agigantados sin necesidad de integración con los metaversos, lo que hace pensar que la integración -absolutamente natural y sin fricciones- solo va a lograr atraer un mayor volumen y un mayor número de individuos que empezarán a realizar operaciones financieras desintermediadas.

Aquí es donde se requiere innovación por parte de los bancos, de los reguladores y supervisores, para empezar a concebir el rol de las entidades financieras dentro de DeFi o el rol de las entidades financieras como competencia a DeFi, eso que se presenta como el sistema financiero de Web3. Significa que no hay una única respuesta respecto de la forma en la que las entidades financieras tradicionales podrán hacer parte de los servicios financieros en el metaverso. Lo importante será reconocer que los vacíos que se vayan dejando los ocuparán nuevos actores integrados nativamente en Web3.

El camino que se tome, en cualquier caso, deberá ser comprensivo de las necesidades actuales de los clientes, que son distintos de los de hace diez años. De entender que el cliente que tiene como lugar de interacción social el metaverso tiene unas necesidades digitales diferentes a las que el sistema financiero tradicional está acostumbrado a ofrecer. Lo que significa que el camino que se tome, regulatoriamente y a partir del mercado, deberá tener claro cuál es el escenario de competencia que se plantea, y, desde allí, decidir si se permite a los bancos participar en esquemas de finanzas descentralizadas o si se busca

[20] Cifras de Statista, disponibles en (consultado el 12 de mayo de 2022):
https://www.statista.com/statistics/1237821/defi-market-size-value-crypto-locked-usd/

generar innovación que permita competir a partir de los actuales productos regulados.

Estas preguntas no son ajenas al sistema financiero. La competencia entre estructuras reguladas y estructuras no reguladas ha estado presente a través de los años y la respuesta también ha sido evolutiva en el tiempo. En este caso, la competencia se presenta de una nueva manera, con una capacidad de masificación sin precedentes y con una atracción para nuevas generaciones impactante. La interacción social en metaversos de personas menores de 20 años en países como Estados Unidos se acerca a la mitad, y conforme la edad es menor, el porcentaje de participación es mayor. La exposición de las nuevas generaciones a criptoactivos, NFTs, blockchain y finanzas descentralizadas crece cada día, lo que hace que su utilización sea natural en el momento en el que se acerquen a una madurez financiera.

7. Conclusiones

Llegar a conclusiones definitivas sobre el metaverso es complejo. Tan complejo como llegar a conclusiones sobre Internet en la década de los 90. La construcción del metaverso viene adelantándose desde hace varios años, pero su multiplicidad de posibilidades hasta ahora empezamos a visualizarlas y no parece razonable anticipar cuáles serán todas.

Cuando se trae la discusión del metaverso a los servicios financieros, la conversación se vuelve aún más compleja porque plantea un análisis de adaptabilidad de un mercado maduro como el financiero a una nueva iteración de Internet, a una nueva iteración de la Web.

Las entidades financieras tendrán un camino obvio: la apertura de sucursales financieras en los metaversos. Sucursales que probablemente comenzarán bajo un esquema informativo y que posteriormente empezarán a tener un carácter transaccional -sin perder de vista los comentarios que hicimos atrás-. De alguna manera, esa evolución de las sucursales financieras en el metaverso tendrá mucho en común con la exploración de las entidades financieras en los inicios de la Web.

Sin embargo, los bancos también tendrán que explorar el camino menos obvio: cómo competir con un sistema financiero paralelo y descentralizado, cómo participar de un sistema financiero que se aprecia a la lejanía y que todavía está por entenderse por parte de los actores financieros más tradicionales.

Las nuevas generaciones ven el metaverso dentro de su normalidad, y en cinco años e incluso menos, conforme lleguen a una edad en la que los productos financieros sean una necesidad, tendrán clara la posibilidad de elegir entre un sistema financiero centralizado y uno descentralizado. Más aún, podrán ver con mayor facilidad el acceso a través de mecanismos basados en Web3, por su interoperabilidad y por los pilares en los que se encuentra construido. Pero también por estar construidos dentro del ambiente que vienen explorando y con el que han venido creciendo.

Por esto debemos replantear lo que hemos creído hasta ahora. Replantearlo en función de la identificación e identidad de las personas, en torno a los activos, las operaciones financieras existentes. Los bancos tendrán que adaptarse al metaverso, porque el metaverso no se adaptará a ellos. Como el ejemplo que dimos, tendrán que aprovechar la tecnología disponible y que habilita el metaverso en toda su extensión y no solo en la forma más fácil e inmediata que encuentren.

Bibliografía

Hughes, Erick. A Cypherpunk's Manifesto. 9 de marzo de 1993.

Kharif, Olga. What You Need to Know About Web3, Crypto's Attempt to Reinvent the Internet. Bloomber, US Edition. 10 de diciembre de 2021. https://www.bloomberg.com/news/articles/2021-12-10/web3-is-crypto-s-attempt-to-reinvent-the-internet-here-s-what-you-should-know

Peredo Bernal, Juan Sebastián. Entrando al metaverso – NFTs, blockchain y el metaverso – Parte 3/X. Publicación en LinkedIn. Abril, 2022. https://www.linkedin.com/pulse/nfts-blockchain-y-el-metaverso-entrando-al-parte-3x-peredo-bernal

Peredo Bernal, Juan Sebastián. Entrando al metaverso – Identidad digital y pseudonimidad – Parte 4/X. Publicación en LinkedIn. Abril, 2022. https://www.linkedin.com/pulse/identidad-digital-y-pseudonimidad-entrando-al-parte-4x-peredo-bernal

Peredo Bernal, Juan Sebastián. Entrando al metaverso – La tierra digital – Parte 6/X. Publicación en LinkedIn. Abril, 2022. https://www.linkedin.com/pulse/la-tierra-digital-entrando-al-metaverso-parte-6x-peredo-bernal

Primera Edición, Septiembre de 2022
ISBN: 978-958-9040-85-0

Asobancaria
Acerca la Banca a los Colombianos