REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

VOL. 11 NÚM. 2 (2022) • PÁGS. 211-244 • DOI 10.5354/0719-2584.2021.65972
RECIBIDO: 1/6/2022 • APROBADO: 23/11/2022 • PUBLICADO: 31/12/2022

DOCTRINA

Open data y *open banking*: El derecho en el contexto de los mercados digitales. Un modelo regulatorio por definir en el ordenamiento jurídico colombiano

Open data and open banking: Law in the context of digital markets. A regulatory model to be defined in the Colombian legal system

Laura Victoria Puentes Trujillo y Lucidia Amaya Osorio
Universidad Externado de Colombia

RESUMEN Colombia aún no cuenta con un modelo regulatorio de *open banking;* sin embargo, con la Ley 1.955 de 2019 se facultó al Gobierno Nacional para crear un *regulatory sandbox* —por dos años— que permitiera evaluar y medir el comportamiento de los mercados y el nivel de innovación financiera del país, antes de adoptar un modelo definitivo. En uso de las facultades dadas por el legislador se expidió el Decreto 1.234 de 2020, en el que se fijaron de manera general los objetivos, requisitos y etapas de funcionamiento del espacio controlado de prueba, como una herramienta para promover la innovación en la prestación de los servicios financieros y facilitar a las autoridades de supervisión y regulación la identificación de nuevos desarrollos financieros. En este escenario este artículo argumenta que, si bien las reglas vigentes en Colombia de *open banking* son transitorias, el regulador no puede olvidar, al definir el modelo regulatorio que adoptará, que los principales riesgos de su implementación son asegurar el cumplimiento de las normas de protección de los derechos a la intimidad personal, *habeas data* y datos personales. En ese sentido, se requiere complementar el régimen de protección de datos personales para llenar algunos vacíos relacionados con la calidad y responsabilidad de los agentes financieros y no financieros que participan en esta nueva forma de innovación financiera.

PALABRAS CLAVE *Open banking*, regulación financiera, datos personales, *habeas data*, derecho a la competencia, consumidor financiero.

ABSTRACT Colombia does not yet have an Open banking regulatory model; However, with Law 1955 of 2019, the National Government was empowered to create a regulatory sandbox -for a term of two years- that would allow evaluating and measuring the behavior of the markets and the level of financial innovation in the country, before adopting

a definitive model. In use of the powers given by the legislator, Decree 1234 of 2020 was issued, in which the objectives, requirements and stages of operation of the controlled test space were generally set, as a tool to promote innovation in the provision of financial services and make it easier for supervisory and regulatory authorities to identify new financial developments. In this scenario, this article argues that, although the open banking rules in force in Colombia are transitory, the regulator cannot forget when defining the regulatory model that it will adopt that the main risks of its implementation lie in ensuring compliance with the rules regarding the protection of the rights to personal privacy, habeas data and personal data. In this sense, it is necessary to complement the personal data protection regime to fill some gaps related to the quality and responsibility of the financial and non-financial agents that participate in this new form of financial innovation.

KEYWORDS Open banking, financial regulation, personal data, habeas data, right to competition, financial consumer.

Introducción

Con el desarrollo de las redes de comunicación en los años sesenta se dio paso a la creación del *Advanced Research Projects Agency Network* (ARPAnet) en 1969 —lo que hoy conocemos como el internet—, con estas redes de comunicación las sociedades y las formas de vida se transformaron progresivamente hasta llegar a la era de la digitalización. Los cambios originados en la interacción virtual también incidieron en la forma en la se llevan a cabo las transacciones en los mercados real y financiero.

Para el sector real tales cambios implicaron que las empresas tuvieran que desenvolverse en un mercado competitivo distinto, marcado por la agilidad en las decisiones empresariales. De la misma forma, la digitalización tuvo incidencia en los agentes financieros, por ejemplo, permitiendo la participación de otros actores en el diseño e invención de nuevos servicios y en la evolución de productos existentes, para que con ellos las entidades financieras pudieran reconsiderar su posición en el mercado y repensar la propuesta de valor que ofrecen a sus clientes.

El escenario reciente en el que se dan estos cambios es el de la «cuarta revolución industrial», expresión usada por primera vez por Klaus Schwab y que refiere a la fusión de las tecnologías disponibles para la interacción a través de los dominios físicos, digitales y biológicos (2016: 29). Tal como lo afirma Nydia Remolina (2019: 4), la cuarta revolución industrial crea una economía basada en el uso de los datos, por lo que en la transformación de la banca tradicional a la banca de servicios (*banking as a service*) es indispensable contar con una banca abierta (*open banking*), la que mediante el uso de interfaces de programación y aplicaciones exponen los datos que se tratan en la intermediación de los servicios financieros, creando nuevas formas de

relacionarse entre los agentes de los distintos mercados, incluidos los nuevos servicios no financieros diseñados a partir de la información del sector.

A pesar de que, en principio, el uso de las tecnologías para el diseño de nuevos productos y servicios tiene por objetivo brindar a los clientes mayor agilidad y oportunidad en acceso a la banca, en su implementación no se abordaron de manera directa algunos de los problemas que subyacen a las nuevas formas de vinculación de nuevos clientes mediante el uso de las nuevas tecnologías y al diseño de nuevos servicios. En el caso del *Open banking* uno de los principales aspectos de los que se han ocupado muchos de los ordenamientos jurídicos que poseen una regulación vigente, sin ser el caso de Colombia, es el uso de los datos personales de los clientes o consumidores financieros. El debate en este ámbito se ha centrado en responder cuáles son o deberían ser los límites y las restricciones para su tratamiento de los datos personales —incluida su circulación—, cuáles de ellos tienen el carácter de datos públicos, privados, semiprivados, estos últimos con un componente importante para asegurar la estabilidad económica de los mercados.

Otro de los aspectos que se han identificado como riesgosos en la definición de un modelo de *Open banking* es cómo se asegurará la pluralidad de agentes en el mercado financiero, de tal manera que no haya una indebida concentración tanto en el tratamiento de los datos como en la oferta de los nuevos servicios, y de ahí que sea necesario la articulación de la regulación financiera específica del *Open banking* con las reglas del derecho de la competencia, que impidan la concentración en ambas esferas.

Teniendo en cuenta lo anterior, en el presente artículo nos ocuparemos de identificar las problemáticas relacionadas con cuál debe ser el modelo regulatorio que emita el Estado colombiano para la definición de las reglas y límites aplicables a la implementación del *open banking* y su suficiencia respecto del proceso de transformación de la banca comercial al *banking as a service*, abordando cuatro elementos centrales: el tratamiento de los datos personales, la articulación de la regulación del sector financiero abierto con el derecho de la competencia, los riesgos de ciberseguridad y el modelo regulatorio contractual, estos últimos desde la perspectiva del cumplimiento de las condiciones en materia de protección de los derechos fundamentales a la intimidad personal, *habeas data* y datos personales.

Para cumplir con el objetivo de este artículo —relacionado con mostrar los aspectos legales más relevantes que deberá considerar el regulador financiero en Colombia (Congreso de la República y la Unidad de Regulación Financiera) al momento de definir el modelo de regulación para habilitar el funcionamiento de *Open banking*, respecto de la protección de los derechos fundamentales a la intimidad personal, *habeas data* y datos personales— emplearé una metodología que considerará las disposiciones y la jurisprudencia vigentes en estas materias, destacando desde el punto de vista doctrinal cuál es su alcance para asegurar que los beneficios por el uso de las nuevas tecnologías de la información en el sector financiero sean obtenidos tanto por

las entidades que conforman el sector como por los consumidores y titulares de los datos que son tratados en el contexto de la banca abierta.

El concepto de *Open banking*: Orígenes, antecedentes y perspectivas regulatorias

En el contexto de las economías liberales el papel del regulador está asociado a la corrección —mediante la fijación de reglas de comportamiento para los agentes— de las fallas del mercado. En el caso del sector financiero una de esas fallas es la asimetría de la información, que impone a los actores el deber, por ejemplo, de divulgación de información relevante al mercado a través del mecanismo dispuesto por el órgano de inspección, vigilancia y control.[1]

Los avances de la tecnología de la información tuvieron un impacto en los servicios financieros en la creación del *fintech,* término con el cual se denomina a las «nuevas compañías especializadas en la prestación de servicios financieros a través de desarrollos tecnológicos en plataformas electrónicas y móviles» (Arias Barrera, 2019), que ofrecen servicios financieros de forma paralela a las entidades tradicionales, tales como servicios de capitalización, negociación de valores, compensación y liquidación, sistemas globales de pago, depósitos y mecanismos de financiación, proceso de verificación de siniestros y pago de indemnizaciones, manejo de identidad digital y autenticidad, soluciones RegTech, etcétera (Arias-Barrera, 2020a).

Con el objetivo de crear un escenario más competitivo entre los agentes tradicionales y las empresas que hacían parte del ecosistema de *fintech,* nace el *Open banking* como un instrumento que permite no solo corregir la asimetría de la información entre las entidades financieras y las empresas de base tecnológica dedicadas a prestar servicios financieros, sino también crear un mecanismo para generar equidad en el mercado.

El caso emblemático que ejemplifica lo que es el *Open banking* y las decisiones regulatorias que han adoptado los estados es el del Reino Unido. En 2016 se tomó la decisión de facilitar la entrada de nuevos proveedores de servicios financieros considerando la gran diversidad de *fintech*. Adoptar una decisión similar implica para los ordenamientos jurídicos como el colombiano flexibilizar las reglas de entrada al mercado financiero, en lo que concierne, primero, a la definición del objeto social exigible a las entidades partícipes en el mercado y a la habilitación gubernamental para prestar servicios financieros; ambos aspectos se traducen en que los servicios financiaros no necesariamente son aquellos se prestan por entidades financieras.

Mientras el Reino Unido les abría las puertas a agentes no tradicionales y avanzaba en la definición de este nuevo concepto (*Open banking*), el Parlamento Europeo creaba el ambiente regulatorio conocido como *Payment Services Directive 2* (PSD2),

1. Para el caso colombiano la autoridad en la materia es la Superintendencia Financiera de Colombia.

que tuvo como principal objetivo crear un ambiente de libre competencia para todos los proveedores de servicios de pago, con estándares de seguridad y confiabilidad que permitiera la protección del consumidor financiero.

Con la incursión de nuevos actores al mercado financiero las agencias, unidades y entidades regulatorias tuvieron que tomar la decisión de cuál modelo emplear. Recordemos que la regulación vigente para el momento en el que nacen las *fintech* tiene una estructura compuesta por tres pilares (Dionne, 2003: 2-3): i) definición de mínimos de capital (inversión) y cobertura de riesgos (control máximo), como parte de una regulación prudencial; ii) procesos de seguimiento autorregulatorios conjugados con las exigencias a las entidades por riesgos no cubiertos por los mínimos prudenciales; y iii) máxima información pública disponible para que los agentes del mercado puedan hacer un análisis de la situación financiera de las entidades y puedan tomar decisiones informadas.

En este ambiente de regulación los datos personales y los datos financieros de los clientes tenían una connotación de información custodiada por las entidades financieras, lo que significa que no eran, en principio, un activo que fuera susceptible de generar más ingresos y utilidades.

Tanto los pilares de la regulación aplicables a la banca tradicional como el papel de los datos personales y financieros en el mercado implicó una redefinición en el contexto de las fintech y del *Open banking*. En ese sentido, en la actualidad se han identificado tres modelos regulatorios aplicables: i) enfoque de desarrollo de mercado (*Market development approach*), ii) enfoque de aproximación obligatoria (*Compulsory approach*) y iii) enfoque de la caja de arena (*Sandbox approach*).

El modelo de enfoque de desarrollo de mercado establece un criterio de plena libertad para el desarrollo de actividades y de aplicaciones que permitan el desarrollo de nuevas actividades derivadas del *Open banking*. En ese sentido no hay exigencias mínimas o máximas de entrada o salida del mercado, y de parte del Estado hay un apoyo al desarrollo de nuevas iniciativas con datos abiertos, al tiempo de que se imparten unas directrices, no obligatorias, que brindan orientación acerca de la materia. Este es el modelo que se ha adoptado en Singapur.

Por su parte, el enfoque de aproximación obligatoria establece un marco legal base para la interacción entre proveedores, entidades bancarias y terceros. Este modelo fue el adoptado por el Reino Unido. La Unión Europea regula el intercambio de datos de cuentas bancarias de los consumidores con terceros proveedores de servicios de pago (PISP y AISP) a través de la Directiva de Servicios de Pago revisada (PSD2, por sus siglas en inglés), con la cual se proporcionó la base legal para un mercado único de pagos. «La PSD2 tiene como objetivo, por ejemplo, mejorar el campo de juego para los proveedores de servicios de pago (incluidos los nuevos jugadores), hacer que los pagos sean más seguros y proteger a los consumidores» (Remolina, 2019: 39) y son obligatorias dentro de la respectiva jurisdicción.

Finalmente, el enfoque de la caja de arena parte de la decisión del regulador de crear un ambiente de innovación y creación, una especie de simulador, en un entorno de prueba que le permita observar y valorar antes de definir las reglas que se aplicarán de manera definitiva.

La búsqueda del mejor modelo regulatorio para Colombia: La caja de arena de la innovación financiera[2]

En el contexto del *Open banking* la Unidad de Regulación Financiera (URF), órgano adscrito al Ministerio de Hacienda y Crédito Público de Colombia, evidenció la importancia que tienen las tecnologías en el mundo financiero, por lo que expidió el documento de trabajo *Open banking y Portabilidad en Colombia* (2020) con el objetivo de establecer la agenda que permita definir el mejor modelo regulatorio para el funcionamiento de la banca abierta.

A partir del estudio adelantado por la autoridad regulatoria, en esta primera parte nos ocuparemos de mostrar cuáles fueron las del Congreso de la República como del Gobierno Nacional para crear un ambiente de prueba temporal relacionado con la invención de bienes y servicios financieros por parte de terceros y competidores en el contexto del *Open banking*; esto, antes de expedir las disposiciones que regularán de manera permanente algunas de las actividades que hacen parte de la industria *fintech*, caracterizada como aquella que adelanta actividades de implementación de tecnologías digitales para optimizar los servicios financieros.

De la misma forma que ocurre en muchos otros países de Latinoamérica, en Colombia la necesidad de regular las actividades de *Open banking* se justifica en el avance de las nuevas tecnologías de la información y en los desafíos para el sector financiero que exigen, además de adecuar el marco normativo, promover la innovación como aspecto a través del que se traslada a los consumidores mejores condiciones de acceso a los servicios que ofrece este ramo de la economía. Es por lo que, a partir de las directrices del Banco Interamericano de Desarrollo, se ha señalado que la industria *fintech* ofrece alternativas que: i) incrementan la competencia, ii) mejora la experiencia del usuario, iii) impulsa la inclusión financiera y, iv) facilita a las entidades financieras su transformación tecnológica (Arias-Barrera, 2020b: 8).

Ahora, considerando que el avance de las tecnologías de la información es más rápido que las respuestas regulatorias de los Estados, las posibilidades que la industria

2. Acudiendo a la metáfora de la caja de arena que se usa para el desarrollo de las habilidades de los niños en los jardines infantiles, las cajas de arena de innovación se usan para crear condiciones que favorezcan el desarrollo de nuevos modelos de negocio en el contexto de mercados regulados que se encuentran sometidos a la irrupción de la tecnología. El objetivo, es crear un escenario en el que la regulación no se constituya en un impedimento para la creación de nuevos servicios y productos.

fintech ha creado derivaron en un alto grado de incertidumbre, por lo que es posible reconocer al menos tres riesgos relevantes: i) el uso indebido de la información de los consumidores que incrementa el riesgo de fraudes relacionados con la suplantación del cliente y, de manera general, con la vulneración de los derechos a la privacidad, los datos personales y el habeas *data*;[3] ii) riesgos de ciberseguridad y, iii) riesgo sistemático, entendido como aquel que no solo afecta a un consumidor o cliente o a una entidad del sector financiero, sino al sistema mismo (Arias-Barrera, 2020b: 9).

Dentro de las actividades que integran la industria *fintech* se encuentra la posibilidad del aprovechamiento de los datos (personales y abiertos) que son tratados por el sector financiero, dando así surgimiento al *Open banking*, descrita como la actividad práctica en la cual los establecimientos bancarios y demás entidades que conforman el sector financiero abren sus sistemas para que la información de los consumidores o clientes pueda ser compartida, previa autorización del titular, con el objetivo de que dichas entidades o terceros provean servicios autorizados por las respectivas autoridades.

La circulación de la información del sector financiero se efectúa a través de una *application programming interface* (API, por sus siglas en inglés) que garantizan la interoperabilidad entre los sistemas de almacenamiento y transferencia de datos empleados por cada una de las entidades financieras que participan de la actividad abierta y el acceso a las entidades y terceros interesados en la información (third party providers), quienes son principalmente empresas no financieras especializadas en el desarrollo de servicios tecnológicos para la prestación de los servicios en los que se especializan las *fintech*.

Una vez identificados los riesgos y las ventajas de la banca abierta, además de los actores que participan, la agenda de trabajo de la Unidad de Regulación Financiera partió del reconocimiento de cuatro modelos de regulación que se han implementado en otros ordenamientos jurídicos: voluntario u obligatorio, cada uno con o sin estandarización.

En el *modelo regulatorio voluntario con estándares*, según lo señala Unidad de Regulación Financiera, la construcción de las reglas aplicables a la actividad es liderada por la industria, con un estándar consensuado con el Estado y cuya adopción es voluntaria, ya que su valor jurídico además de autorregulatorio es el de una buena práctica en materia de innovación. Por su parte, en el *modelo voluntario sin estándares* la autoridad gubernamental suministra la información y las guías a ser adoptadas,

3. En el ordenamiento jurídico colombiano, a partir de lo previsto en el artículo 15 de la Constitución Política y la jurisprudencia de la Corte Constitucional se ha entendido que la privacidad, los datos personales y el *habeas data* son derechos fundamentales independientes, que pueden verse afectados por el tratamiento de los datos personales sin el consentimiento del titular. Sobre el asunto, puede consultarse la Sentencia C-094 de 2020, Magistrado Ponente: Alejandro Linares Cantillo.

pero las entidades financieras deciden si acogen las condiciones contenidas en los documentos provistos por el Estado. De otro lado, el *modelo regulatorio obligatorio con estándares* implica que existe un marco normativo sólido en el que es imperativo adoptar las condiciones de funcionamiento del *Open banking*, así como los estándares aplicables al esquema definido por el Estado. Finalmente, el *modelo obligatorio sin estándares* fija un marco normativo en el que se contempla su obligatoriedad, sin que se definan criterios de interfaces técnicas por parte de la autoridad pública.

Estos cuatro modelos no implican una variación de la estrategia de regulación basada en el riesgo, en cuanto pilar en la estructuración y definición de las reglas aplicables al sector financiero, en la medida en que se ha demostrado que es la herramienta más eficiente para garantizar que la intervención de agencias regulatorias y de supervisión logre el equilibrio entre los objetivos regulatorios, a saber: promoción de la innovación, protección al inversionista, competencia en el mercado *fintech*, y mantenimiento de la estabilidad financiera (National Economic Council, 2017).

En la definición de cuál de esos modelos es mejor para Colombia y siguiendo los estándares de innovación pública, el Estado colombiano optó por no tomar una decisión aún, por lo que el artículo 166[4] del Plan Nacional de Desarrollo 2018-2022, adoptado mediante la Ley 1.955 de 2019, creó un *regulatory sandbox* y facultó al Gobierno Nacional para reglamentar dicha disposición y así definir las reglas transitorias que permitan crear un escenario de prueba temporal para observar y evaluar cuál es la respuesta que el mercado y los agentes darán al excepcionar algunas reglas que rigen el funcionamiento del sistema financiero. En este tránsito normativo se permitió la creación de empresas de desarrollos tecnológicos innovadoras para realizar activida-

4. «Artículo 166. Constitución de empresas de desarrollos tecnológicos innovadores. Quienes se propongan implementar desarrollos tecnológicos innovadores para realizar actividades propias de las entidades vigiladas por la Superintendencia Financiera, podrán constituir una de estas entidades y obtener un certificado para operar temporalmente, de acuerdo con las condiciones, requisitos y requerimientos prudenciales, incluyendo la determinación o aplicación de capitales mínimos, de acuerdo con la reglamentación que para el efecto expida el Gobierno nacional. Dicho certificado de operación temporal no excederá de dos años y podrá ser revocado en cualquier momento por la Superintendencia Financiera. La Superintendencia Financiera autorizará la constitución de estas entidades y otorgará el respectivo certificado de funcionamiento, conforme al procedimiento que se establezca para el efecto. En desarrollo de esta disposición, el Gobierno nacional podrá determinar los montos mínimos de capital que deberán acreditarse para solicitar la constitución de las entidades sometidas al control y vigilancia de la Superintendencia Financiera de Colombia, el cual podrá estar diferenciado en función de las operaciones autorizadas por la Superintendencia Financiera de Colombia, en los términos del numeral 2 del artículo 53 del Estatuto Orgánico del Sistema Financiero. Parágrafo primero. Con sujeción a las condiciones, requisitos y requerimientos prudenciales que establezca la reglamentación a la que se refiere el presente artículo, las entidades vigiladas por la Superintendencia Financiera de Colombia podrán implementar desarrollos tecnológicos innovadores para probar temporalmente nuevos productos o servicios, bajo la supervisión de dicha Superintendencia, por el término indicado en este artículo».

des propias de las entidades vigiladas por la Superintendencia Financiera de Colombia, previa habilitación por parte de este órgano de control.

En ejercicio de la facultad reglamentaria el Gobierno Nacional expidió el Decreto 1.234 de 2020, por medio del cual se adicionó el Decreto 2.555 de 2010 —Estatuto del Sistema Financiero— en lo relacionado con el espacio controlado de prueba para actividades de innovación financiera, en el que definió que los objetivos de este ambiente son el aprovechamiento de la innovación en la prestación de servicios y productos financieros, sin perjuicio de la protección de los intereses de los consumidores. El segundo objetivo es preservar la integridad y estabilidad del sistema financiero y prevenir los arbitrajes regulatorios (artículo 2.35.7.1.2.).

Una de las condiciones más importantes que impuso el Decreto 1.234 de 2020 es aquella relacionada con la finalidad con la cual se habilita a las empresas de desarrollos tecnológicos para realizar actividades propias de las entidades vigiladas por la Superintendencia Financiera de Colombia, ya que según lo prevé el artículo 2.35.7.1.3. los desarrollos que se acepten deberán aumentar la eficiencia en la prestación de servicios u ofrecimiento de productos financieros, resolver una problemática para los consumidores de este sector, facilitar la inclusión financiera, mejorar el cumplimiento normativo, desarrollar los mercados financieros o mejorar su competitividad. Si la iniciativa empresarial y tecnológica no logra demostrar el cumplimiento de alguno de estos propósitos el operador potencial no obtendrá el certificado de operación temporal de que trata la disposición del Plan de Desarrollo Nacional.

Esto significa que en Colombia se optó por darle continuidad a la habilitación gubernamental si se trata de actividades financieras o conexas con estas. Este criterio de conexidad permite mantener el control en un sector que desde el punto de vista estratégico apalanca una parte significativa del desarrollo del país, en la medida en que en el primer semestre de 2022 el crecimiento económico fue de 10,6%, en el que las actividades financieras y de seguros aportaron cerca de 4,8% del PIB, una cifra aunque parezca menor no toma en cuenta el número de empleos que genera el sector y los beneficios colaterales de la intermediación con el sector real (Banco Interamericano de Desarrollo, 2021).

En lo que concierne a la circulación de los datos para hacer posible la operación del *sandbox*, el artículo 2.35.7.3.1 establece, entre otros, que son deberes de los participantes «informar y obtener el consentimiento de sus consumidores financieros por cualquier medio verificable, donde manifiesten haber sido informados de las características y riesgos del producto o servicio al que está accediendo» y asumir las pérdidas ocasionadas a sus consumidores financieros, siempre que estas se produzcan como consecuencia de su participación en las pruebas.

Como puede observarse, las disposiciones que habilitan el desarrollo de actividades de innovación para la prestación de servicios financieros en el esquema del *open banking* se centran de manera principal en las condiciones de habilitación de

los agentes financieros y no financieros, adoptando las reglas de protección de datos personales contenidas en la Ley Estatutaria 1.581 de 2012 y protección de datos personales financieros de que trata la Ley 1.266 de 2008, mediante la inclusión del deber de obtener del respectivo titular la autorización para el tratamiento de sus datos personales en un ambiente de banca abierta.

Con base en los antecedentes normativos antes señalados, puede observarse que en la actualidad Colombia no ha definido cuál es modelo regulatorio que implementará para el funcionamiento del *open banking*, con lo cual la medición de la suficiencia de los aspectos regulatorios en el caso concreto debe hacerse, en primer lugar, con base en las reglas generales de transición existentes (incluidos los documentos de trabajo de la URF) y, en segundo lugar, a partir del contraste de las particularidades normativas del ordenamiento jurídico colombiano en materia de protección de datos, ciberseguridad, derecho a la competencia y protección de los consumidores financieros con los resultados que han obtenido otros países en la expedición de las disposiciones que permitan el funcionamiento del *open banking* y *que* dieron paso a la *banking as a service*.

La circulación de los datos en la banca de servicios: El *Open Data*, los derechos a la privacidad personal, el *habeas data* y los datos personales

En el ordenamiento jurídico colombiano con la entrada en vigencia de la Ley 1.266 de 2008 se creó el marco normativo que regula el derecho constitucional de conocer, actualizar y rectificar la información que se hayan recogido en bancos de datos (*habeas data* financiero), y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales.

Tratándose de la normativización de un derecho fundamental (artículo 152 de la Constitución Política) el proyecto de ley estatutaria tuvo control previo y automático por parte de la Corte Constitucional, y en la Sentencia C-1011 de 2008[5] se fijaron las reglas jurisprudenciales que se constituirían en el precedente constitucional sobre la materia, de tal forma que con la expedición de la Ley 1.581 de 2012 —por la cual se dictan disposiciones generales para la protección de datos personales— la Corte Constitucional, mediante la Sentencia C-748 de 2011,[6] reiteró muchas de las reglas jurisprudenciales que venían aplicándose desde el 2008.

Conforme con las disposiciones legales y las reglas jurisprudenciales de la Corte Constitucional que constituyen el precedente, uno de los pilares para el tratamiento legítimo y válido de los datos personales, sean estos o no financieros, es el consentimiento del titular. Para que dicho principio sea plenamente satisfecho se ha entendi-

5. Corte Constitucional. Sentencia C-1011 del 2008. Magistrado Ponente: Jaime Córdoba Triviño.

6. Corte Constitucional. Sentencia C-748 del 2011. Magistrado Ponente: Jorge Ignacio Pretelt Chaljub.

do que este debe: i) darse de manera expresa, previa al tratamiento e informada; ii) en virtud de la ley, de un contrato, o directamente por parte del titular y, iii) constar por escrito, verbalmente o por conducta inequívoca.

Teniendo en cuenta las anteriores condiciones, quizá la mayor problemática que debe enfrentar la autoridad regulatoria, respecto de los temas de *open banking* y b*anking as a service,* es la articulación del modelo por definir con las reglas sobre el tratamiento de los datos personales existentes en Colombia, en la medida en que no podría el Congreso de la República expedir una ley ordinaria para modificar las condiciones contenidas en las leyes estatutarias 1.266 y 1.581; de ahí que pueda entenderse porqué en el Decreto 1.234 de 2020 solo se hace referencia al deber de obtener el consentimiento del titular de los datos conforme con las disposiciones aplicables.

Si bien podrían modificarse las dos leyes estatutarias que regulan los derechos fundamentales de *habeas data* y datos personales, el proyecto de ley requeriría la aprobación de la mayoría absoluta de los miembros del Congreso de la República y su trámite deberá efectuarse en una misma legislatura; es decir, entre julio de un año y junio del siguiente. Por esta razón, además de los aspectos relacionados con la imposibilidad de que las modificaciones desconozcan las reglas jurisprudenciales de la Corte Constitucional, pues lo contrario daría lugar a que se declare la inexiquibilidad de las disposiciones, el regulador financiero deberá al momento de definir el marco normativo sobre *open banking* tener presente las restricciones en materia de protección de los derechos fundamentales relacionados con la intimidad personal, los datos personales y el habeas data.

Con el propósito de identificar algunos de los límites legales que debe tener en cuenta el regulador, a continuación, haremos una breve presentación de la clasificación de datos contenidos en las disposiciones legales y reglamentarias, para mostrar con ello los principales debates jurídicos respecto de cuáles datos pueden ser tratados sin consentimiento del titular y cuáles tienen un régimen de protección reforzado.

Datos personales públicos

En primer lugar, es necesario aclarar que en Colombia se adoptó el criterio de exclusión al momento de definir qué se entiende por un dato público. De acuerdo con la estipulación contenida en la Ley 1.266 de 2008 artículo 3 literal f), los datos públicos son aquellos que la constitución o la ley califican como tales y «todos aquellos que no sean semiprivados o privados». Además, señala la citada disposición a manera de ejemplo que son datos públicos los contenidos en «documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas».

Si revisamos uno a uno los criterios contenidos en el artículo 3, tendrían la connotación de públicos los datos distintos a los semiprivados, entendiendo por estos

últimos aquellos que no tienen naturaleza íntima o reservada, pero tampoco son públicos en estricto sentido, aun cuando el conocimiento de estos puede interesar no solo a su titular sino a cierto sector o a la sociedad, «como el dato relacionado con el comportamiento financiero y crediticio de la actividad comercial o de servicios». Por su parte, los datos privados, que por estipulación legal son aquellos que por su naturaleza íntima o reservada solo es relevante para el titular.

Es decir, los datos públicos son aquellos que la ley o la constitución definen como tal en razón a la satisfacción del interés general de permitir su acceso irrestricto o exigir su publicación de manera proactiva, conforme con los criterios previstos en la Ley 1.712 de 2014.

De igual manera, en la enunciación que trae el literal f) del artículo 3 de la Ley 1.266 de 2008, se fija un segundo criterio de catalogación de los datos públicos: los relativos al estado civil y los contenidos en «documentos públicos».[7] En relación con este criterio, podemos afirmar —solo de manera provisional y atendiendo de manera principal a la literalidad de la disposición— que si el nombre y el número de identificación (ID) están contenidos en un documento público constituirían datos personales públicos, respecto de los cuales no se requiere del consentimiento de su titular para su acceso y tratamiento.

Ante las dudas que generó la inclusión del referido criterio en relación a si el nombre y el número de identificación constituían datos públicos, teniendo en cuenta que no hay duda de que se tratan de datos personales, la Superintendencia de Industria y Comercio, en calidad de autoridad en materia de control respecto al tratamiento de datos personales, conceptuó que teniendo en cuenta lo consagrado en el artículo 213 del Código Electoral (Decreto 2.241 de 1986) «toda persona tiene derecho a que la Registraduría le informe sobre el número, lugar y fecha de expedición de documentos de identidad pertenecientes a terceros», por lo que el número de cédula (ID) es un dato público.

A pesar de estar vigente la disposición del Código Electoral, en la conclusión presentada por la Superintendencia de Industria y Comercio no se consideró que el artículo 213 es una disposición previa a la Constitución Política de 1991, lo que implica que su interpretación está sujeta a los criterios fijados en la carta política, especialmente, a lo previsto en su artículo 15.[8] Esto significa que con la entrada en vigencia de

7. Según lo prevé el artículo 243 del Código General del Proceso, el «documento público es el otorgado por el funcionario público en ejercicio de sus funciones o con su intervención. Así mismo, es público el documento otorgado por un particular en ejercicio de funciones públicas o con su intervención. Cuando consiste en un escrito autorizado o suscrito por el respectivo funcionario, es instrumento público; cuando es autorizado por un notario o quien haga sus veces y ha sido incorporado en el respectivo protocolo, se denomina escritura pública».

8. Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar

la actual carta política la constitucionalidad de las disposiciones expedidas en vigencia de la Constitución de 1886 está dada siempre que una o más de sus interpretaciones sean coherentes con los principios y derechos contenidos en la Constitución de 1991, cuestión que no fue verificada por la Superintendencia al momento de precisar el alcance de la mencionada disposición.

En relación con el alcance de la definición legal de «dato público» la Corte Constitucional en Sentencia C-1011 de 2008 precisó que tal estipulación no contraría las normas constitucionales, en la medida en que una interpretación sistemática de las definiciones contenidas en el artículo 3 de la Ley 1.266 permite inferir que el interés al que remiten es el interés público, que en el caso de la información personal relativa al *habeas data* financiero está relacionado con las actividades sociales que buscan satisfacer finalidades constitucionalmente reconocidas, como lo son las operaciones comerciales y de crédito.

En ese sentido, aun cuando los datos financieros de un sujeto están contenidos en un documento público no necesariamente por esta circunstancia deja de ser un dato semiprivado y, por ende, no muta *per se* a un dato público, ya que legalmente tales datos solo pueden ser tratados conforme con las reglas contenidas en la Ley 1.266 que prevé su administración por parte de un operador de información, la autorización del titular para su consulta a través de las bases de datos dispuestas para ello, y demás condiciones que aseguren la protección del derecho al habeas data.

Con el propósito de garantizar, entonces, tanto el derecho al acceso a la información pública (dentro de la cual están incluidos los datos personales públicos) cuando el nombre y el número de identificación son tratados por la Registraduría Nacional del Estado Civil en virtud de las funciones que constitucional y legalmente le han sido asignadas, tales datos tienen la connotación de públicos; pero esto no implica que cualquier persona, natural o jurídica, pueda tratarlos sin la autorización expresa de su titular, ya que el derecho de acceso a la información no implica el derecho al tratamiento de los datos personales públicos. En otras palabras, debe entenderse que en virtud de la ley la única entidad autorizada para entregar información respecto del número de identificación de una persona es la Registraduría Nacional del Estado Civil, las otras entidades requieren de autorización expresa del titular para la circulación de los datos respecto de los cuales son titulares.

La anterior condición incluye a las entidades que hacen parte del sistema financiero quienes, en calidad de particulares, no cuentan con autorización legal para tratar los datos relativos al nombre y el número de identificación sin autorización del titular.

Otro aspecto que es relevante en el análisis del alcance del tratamiento de los datos públicos es que por definición estos «son aquellos que conciernen a un interés

y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

general» (SIC, 2017: 7), de ahí que cuando son tratados por entidades públicas gozan de presunción de publicidad conforme con lo previsto en la Ley 1.712 de 2014, que garantiza la satisfacción del principio de transparencia en las actuaciones de las entidades públicas y de los particulares que administran o ejecutan recursos públicos.

Sin embargo, en estos casos, el nombre y el número del documento de identidad de las personas naturales son un tipo de información (datos personales) que, conforme con los criterios que define la misma Ley 1.712, puede excepcionarse del principio de publicidad conforme con lo señalado en el artículo 18, por ser «información pública clasificada» en los casos en los que estos datos sean tratados por entidades públicas distintas a la Registraduría Nacional del Estado Civil.

Datos abiertos

El Estado colombiano mediante el Decreto 1.151 de 2008 definió la Estrategia de Gobierno en Línea, que inicialmente tuvo como objetivo que las entidades obligadas a su implementación contaran con las herramientas tecnológicas necesarias que permitieran la interacción entre las distintas entidades que hacen parte del Estado y los ciudadanos en un escenario de inclusión social y competitividad. En el 2019, esta estrategia mutó a la Política del Gobierno Digital, que tiene por objetivo transformar digitalmente el Estado colombiano, permitiendo que las entidades públicas sean más eficientes para atender las necesidades y problemáticas de los ciudadanos y que estos sean los protagonistas en los procesos de cambio a través del uso y apropiación de las tecnologías digitales.

A partir del año 2011, en la segunda versión del Manual de Implementación del Gobierno en Línea, expedido por el Ministerio de las Tecnologías de la Información y las Comunicaciones, se incluyó la posibilidad de aprovechar los datos abiertos generados por las entidades públicas en el cumplimiento de sus funciones. Finalmente, en el artículo 6 de la Ley 1.712 de 2014 se indicó que los datos abiertos son:

aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Conforme con la definición legal, los datos abiertos son datos públicos no personales. Corresponde a un tipo de información que se reporta al Departamento Administrativo de la Función Pública en forma estructurada, que permite que sean procesados, reutilizados y analizados para el desarrollo de aplicaciones, investigaciones, periodismo de datos y control social[9] por cualquier persona, sin que ninguna entidad

9. A través de las veedurías ciudadanas o por cualquiera de los otros mecanismos de participación democrática previstos en el ordenamiento jurídico.

posea el control exclusivo. Los datos abiertos hacen parte de los ocho principios de la Política de datos gubernamentales abiertos escritos por el grupo de trabajo convocado por Carl Malamud en 2007 en Sebastopol, California.

Los otros siete criterios de la Política de datos gubernamentales abiertos son: i) principio de publicidad: los datos son públicos y deben estar disponibles para su acceso de manera permanente, por lo tanto, no están sujetos a limitaciones de privacidad, seguridad o reserva legal; ii) dato en bruto: los datos se publicarán tal y como se recogen en la fuente, propendiendo por el mayor nivel de detalle posible; iii) actualizados: el valor de los datos abiertos está en garantizar su acceso lo más rápido posible; iv) accesibles: los datos deben estar disponibles para que sean consultados por el mayor número de usuarios y para la más amplia gama de propósitos; v) estructurados: los datos deben poder ser procesados de manera automática por un ordenador; vi) sin registro: el acceso a los datos debe ser de forma anónima y, vii) libres: los datos no deben estar sujetos a las normas de derechos de autor, patentes o *copyright*.

El aprovechamiento de los datos de las entidades públicas para la corrección de fallas o para mejorar los niveles de eficiencia del Estado sin duda es un aprovechamiento legítimo de la información. Sin embargo, tal como lo relata Joshua Tauberer, la obligación en la publicación de esta información puede conducir al principio de incertidumbre de transparencia de Heisenberg, según el cual las «observaciones pueden alterar e incluso proyectar una sombra sobre los mismos eventos sobre los que estamos tratando de arrojar luz» (2014: 24).

En el ámbito de las funciones estatales el principio de incertidumbre de transparencia se expresa en que los servidores públicos y políticos pueden alterar su comportamiento para jugar con los datos y las estadísticas calculadas por los defensores de la transparencia y los periodistas; es por ello que no es suficiente con mejorar las leyes de divulgación y acceso de la información pública porque tan pronto como se expiden «nuevas reglas de transparencia, los eventos que pretendían descubrir ya no son visibles para ese centro de atención. La transparencia en algunos casos es imposible y, en casos excepcionales, incluso puede ser perjudicial» (Tauberer, 2014: 113).

Ahora, en un contexto de derecho privado y de entidades que no manejan o administran recursos públicos las reglas acerca de los datos abiertos y los datos públicos están sometidos a las reglas propias del mercado. Esto implica que, por ejemplo, la divulgación de los datos de contracto de los servidores públicos, empleados del Estado, que están relacionados con el cumplimiento de las funciones públicas estén siendo usados por el sector financiero para ofrecer bienes y servicios, sin que el servidor pueda decidir si restringe el tratamiento de tales datos, que se han entendido como de propiedad de la entidad pública y no del trabajador.

Datos personales

Colombia al momento de definir qué se entiende por un «dato personal» adoptó la definición internacional, según la cual este tipo de datos corresponden a cualquier información relacionada con una persona natural que pueda ser identificada o identificable. En ese sentido, el artículo 4 de la Ley 1.581 de 2012 señaló que los datos personales, salvo la información pública, no podrán estar disponibles en Internet o cualquier otro medio de comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados por el respectivo titular.

En concordancia con lo previsto en la Ley 1.266 de 2008, la Ley 1.581 permite interpretar que en el ordenamiento jurídico colombiano hay algunos datos personales que tienen el carácter de datos personales públicos (información pública), respecto de los cuales señalamos nuestra posición y entendimiento en uno de los acápites previos.

Otra subcategoría de datos personales son los datos sensibles. En el régimen colombiano se ha previsto que se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación. En esta subclasificación se encuentran los datos relacionados con 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 de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

En las exigencias legales para el tratamiento de los datos sensibles Colombia adoptó como regla general que se prohíbe el tratamiento de estos datos, salvo que su titular lo autorice, lo que en términos efectivos equipara el tratamiento de los datos personales con el de los datos sensibles, salvo en lo que concierne a la interpretación de los principios definidos en la ley y aplicables en la resolución de un caso concreto, en el que debe prevalecer una interpretación restrictiva respecto del tratamiento de los datos sensibles en mayor grado que el cumplimiento de los requisitos para el tratamiento de datos personales que no sean sensibles.

A partir de la distinción entre datos públicos, datos abiertos y datos personales, las disposiciones del Decreto 1.234 de 2020 exigen una articulación con las reglas referentes a los datos personales y de *habeas data* contenidas en las leyes 1.581 de 2012 y 1.266 de 2008, respectivamente. Estas leyes constituyen el marco normativo que la Unidad de Regulación Financiera consideró para la construcción del documento *open banking y Portabilidad en Colombia* (2020), en el que concluye que las mencionadas leyes son adecuadas y suficientes para la implementación del modelo de banca abierta, ya que ellas están en sintonía con los estándares internacionales relativos a la primacía el principio de autonomía en el tratamiento de datos personales.

No obstante, después de verificar la inclusión de algunos deberes que deben cum-

plir los participantes en el espacio controlado de prueba, encaminados a la protección de los intereses de los consumidores financieros,[10] es necesario analizar cuál es el entorno en el que el titular de los datos personales dará autorización para su tratamiento en la banca abierta.

Así, pues, las disposiciones que regulan el *sandbox* permiten la participación en el escenario de pruebas tanto de entidades públicas como de entidades privadas;[11] ahora, teniendo en cuenta que el tratamiento de datos personales es una condición necesaria para que los terceros proveedores de tecnología (TPPS) puedan impulsar los nuevos desarrollos y servicios, es indispensable que los titulares den su consentimiento previo, expreso e informado (URF: 2020) a cada uno de los participantes, sin importar si se trata de entidades públicas o privadas.

Lo anterior, en la medida en que si bien tanto la Ley 1.266 como la Ley 1.581 establecen que no se requiere el consentimiento del titular para el tratamiento de sus datos cuando sean solicitadas por autoridades estatales para el cumplimiento de sus funciones, en el ámbito financiero el sistema jurídico ha unificado el régimen de derecho aplicable tanto a las entidades públicas como a las privadas, lo que significa que tratándose de un escenario en competencia regido por el derecho privado, no podrán las entidades públicas del sector financiero poner de presente su condición de entidades estatales para quedar exceptuadas del deber de solicitar la autorización del titular de los datos.

Ahora, si bien la autorización del titular de los datos personales legitima su tratamiento por parte de las entidades financieras y por los terceros proveedores, uno de los principales interrogantes está relacionado con la suficiencia de este requisito en los casos en los que los proveedores de servicios tecnológicos están ubicados por fuera del territorio colombiano.

Según lo prevé el artículo 2 de la Ley 1.581 de 2012 esta se «aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales».

---

10. Deberes «1. Informar y obtener el consentimiento de sus consumidores financieros por cualquier medio verificable, donde manifiesten haber sido informados de las características y riesgos del producto o servicio al que está accediendo. 2. Atender de manera oportuna la solicitud de cancelación del producto o servicio por parte de sus consumidores financieros en el momento en que éste lo solicite. […] 5. Asumir las pérdidas ocasionadas a sus consumidores financieros como consecuencia de su participación en las pruebas en caso de presentarse, de acuerdo con el régimen de responsabilidades aplicables».

11. De acuerdo con la norma transcrita, los principios y disposiciones en materia de protección de datos personales aplican a cualquier base de datos de naturaleza personal, sin distinción de que quien realice el tratamiento sea una entidad de derecho público o privado. En particular, se resalta que los principios expuestos en la Ley 1.581 de 2012 son aplicables incluso a los datos regulados en la Ley 1.266 de 2008, tal y como lo dispone el artículo 2 del régimen general de protección de datos personales.

Con base en este ámbito de aplicación puede afirmarse que en los casos en los que el tercero proveedor esté ubicado en un país que no haga parte de los tratados internacionales que permiten la incorporación de reglas de derecho externo en el orden jurídico interno, el titular podría verse sometido a condiciones en el tratamiento de sus datos distintas a las reglas que garantizan el principio de autonomía.

De esta manera, y considerando que precisamente los servicios de naturaleza tecnológica pueden prestarse desde cualquier parte del mundo, se puede inferir que la decisión del regulador y el Gobierno Nacional no es suficiente para establecer cuál es el mejor modelo con el que se definan las reglas aplicables al *open banking*, especialmente en el evento en el que el tratamiento de datos sea efectuado desde el exterior. Se requiere, pues, de una ley estatutaria especial en la que se contemplen normas de carácter transfronterizo, que permitan verdaderamente regular situaciones globales como la del suministro de servicios tecnológicos.

Teniendo en cuenta lo anterior, parece que no es suficiente que la regulación encuentre que las normas de *habeas data* y datos personales existentes garantizan el tratamiento legítimo de los datos de los clientes financieros en el *open banking*. La Ley 1.581 de 2012 contempla una serie de principios —aplicables también a las bases de datos de información financiera, crediticia, comercial y de servicios de que trata la Ley 1.266 de 2008— entre los que se encuentran el principio de finalidad, el de libertad, el de acceso y circulación restringida, todos ellos orientados a que el titular no solo imparta su autorización, sino que esté debidamente informado de cuál será la finalidad del tratamiento.

Bajo la premisa de que los terceros proveedores de servicios obtienen los datos de los clientes por intermedio de las API de las entidades financieras, se plantea el cuestionamiento de a quién y de qué manera le corresponde informar al consumidor cuál será el destino final y la utilización de sus datos. Aunque la respuesta más fácil sería la de que es a la entidad financiera a la que compete suministrar tal información al titular, tal solución no resulta obvia y evidente, toda vez que de acuerdo con la forma en que fue redactado el deber contenido en el artículo 2.35.7.3.1. del Decreto 1.234 de 2020 puede interpretarse que los desarrolladores en condición de participantes también están obligados a cumplir con este requisito legal.

Otra de las cuestiones que se desprende del funcionamiento de la banca abierta, es el relativo a la suficiencia de la regulación respecto de la circulación de los datos. El riesgo que se evalúa en este caso está asociado al eventual abuso de las condiciones contenidas en la política de privacidad por parte de las entidades financieras, de tal manera que sea deficitario el régimen de protección de los derechos de los consumidores en un escenario contractual de adhesión y en el que la autorización para el tratamiento de los datos no sea lo suficientemente informado o, en caso de que lo sea, su no aceptación incondicional se constituya en una restricción para el acceso a los servicios de la banca por servicios y del *open banking*.

Así, por ejemplo, puede evidenciarse que, a diferencia de lo que ocurre en la Unión Europea, en Colombia no existen disposiciones que impongan a las entidades financieras la obligación de compartir los datos de sus clientes con terceros; la circulación de los datos entre distintas personas tiene como condición que en la respectiva autorización se incluya la posibilidad de entrega de ellos a terceros con los que la entidad financiera tenga relaciones comerciales, legales o contractuales, caso en el cual los terceros tendrán la calidad de encargados y tendrán las mismas obligaciones que los responsables.

Pero qué ocurre cuando abrir la banca implica que los datos puedan estar a disposición de personas con las que la respectiva entidad financiera no tenga ningún vínculo contractual o legal y, además, que sea una condición para el acceso a los servicios financieros dar la respectiva autorización del tratamiento abierto de los datos personales; cómo se garantizarían los derechos de los titulares, por ejemplo, el derecho de retiro de la autorización para el tratamiento de los datos personales a todos o a algunos de los responsables y/o encargados partícipes en la cadena de producción de servicios financieros y no financieros del *open banking*.

Por su parte, dentro de las condiciones de circulación y uso puede incluirse la posibilidad de monetización de los datos personales. El principal interrogante es quién está legitimado para explotar económicamente y con fines distintos a la prestación de servicios financieros los datos de las personas naturales que participan en condición de consumidores en el mercado financiero. En este punto, se ha señalado que la monetización de los datos no puede prohibirse para los titulares, pero no se tiene aún definido si los responsables o encargados también pueden acceder a esta posibilidad, más aún cuando los volúmenes de información que reciben y procesan de los clientes les permite crear *big data* con las que se pueden predecir los comportamientos de pago, capacidad financiera de los usuarios, entre otros aspectos.

Lo que sí es cierto, es que la reciprocidad (la transferencia de los datos de los clientes a una empresa) es una condición necesaria para el desarrollo de la banca de servicios, y eso es precisamente lo que permite el *open banking*. Las dudas están en la posibilidad de que la reciprocidad se dé solo en condiciones mercantiles que beneficien principalmente a los intermediarios y terceros, aun cuando se establezca la irrenunciabilidad de los derechos de los titulares de los datos personales.

Con base en lo anterior, es importante, entonces, que se prevea expresamente que las entidades financieras no son las propietarias de los datos del cliente, y, por ende, no pueden cobrar por la misma. Esto, en la medida en que el derecho de *habeas data* que consagra el artículo 15 de la Constitución Política es de carácter fundamental, y de ahí que sea universal, indisponible e inenajenable. El permitir a las entidades financieras percibir una retribución económica por compartir los datos de sus clientes sería seguir patrocinando el monopolio que han venido detentando durante décadas, además de desdibujarse la finalidad perseguida con la arquitectura financiera abierta,

que es fomentar la competencia y la provisión de nuevos productos y servicios en pro de los consumidores financieros.

De igual forma, tener un control en la circulación de los datos personales entre las entidades financieras y los terceros desarrolladores implica definir con claridad cuál es el rol que asumen los terceros proveedores de servicios financieros tecnológicos de acuerdo con la legislación vigente.

Al respecto, el artículo 3 de la Ley 1.266 de 2008 establece y define cada uno de los actores que participa en el manejo y tratamiento de los datos personales incluidos en bases de datos financieras, y el artículo 3, literales d y e, de la Ley 1.581 de 2012, a su vez, consagra otros intervinientes. Sin embargo, ante la posibilidad de que otros actores puedan participar en la cadena de generación de valor agregado para el sector financiero se hace indispensable determinar con claridad, particularmente en el caso de las *fintech* y las *BigTech,* qué calidad asumen estas, de acuerdo con las clasificaciones hechas en las respectivas leyes.

Lo que se desea destacar es que el hecho de que se tenga un concepto de titular de los datos, fuentes de información, operadores de información, usuarios, encargados y responsables del tratamiento de datos, no significa necesariamente que se tenga absoluta certeza de cuál es el papel que cumplen los terceros proveedores de servicios tecnológicos. A manera de ejemplo, se podría decir que una *fintech* se considera fuente de información porque recibe o conoce datos de los titulares, a través de la información a la que tienen acceso por medio de las API. Sin embargo, dichas *fintech* no transmiten la información recibida de un operador y por ello no serían fuentes de información. Por otra parte, podría afirmarse que los *fintech* o *BigTech* se consideran solamente usuarios, por cuanto acceden a la información exclusivamente para efectos de prestar servicios de iniciación de pagos o de información de cuentas del consumidor financiero.

La ambigüedad que generan las categorías existentes respecto de la forma cómo se accede a los datos en un ambiente de banca abierta, permite advertir la necesidad de crear una reglamentación específica sobre la protección de los datos en el campo del *open banking*, o al menos el desarrollo de una reglamentación de la ley de *habeas data* y de protección de datos personales, en la que se determinen los alcances de esas disposiciones frente a los denominados TPPS, en aras de evitar interpretaciones diversas y de tener claridad acerca de las responsabilidades de los intervinientes en la órbita del *open banking*. Sin definirse estos aspectos existe el riesgo de no hacer valer responsabilidades y de no poder fijar sanciones a los terceros proveedores de servicios tecnológicos.

En relación con el tratamiento de los datos personales en la banca abierta y tal como lo propone José Miquel de la Calle (2021), el punto de partida es la necesidad de una nueva autorización del titular en la que estén presentes todos los elementos que garanticen la prevalencia de los intereses de los consumidores, de ahí que haya

necesidad de consagrar de manera expresa la aplicación del principio de responsabilidad demostrada; además de la exigencia legal de que la autorización que dé el titular de los datos, al momento de firmar un contrato con la entidad financiera, no incluya finalidades múltiples y abiertas, que lleven a una cadena indefinida de encargados o que prevea la posibilidad de que terceros puedan acceder y circularlos solo en razón de las relaciones comerciales o contractuales de las entidades participantes de la banca abierta, sin que se le comunique o notifique al titular tal circunstancia.

En concordancia con las reglas internacionales, especialmente con el Reglamento General de Protección de Datos de la Unión Europea, la regulación debe tener un enfoque de riesgos, cuya administración y mitigación estén dadas por el cumplimiento de estándares de seguridad y de cumplimiento de las condiciones que aseguren que el consentimiento sea informado. Con esto, es indispensable exigir a las entidades participantes que conforman el sistema de *open banking* un Oficial de Protección de Datos ante el cual se lleve el registro de quiénes están tratando los datos y que deban notificar al titular cuando un nuevo agente los tratará, de tal manera que pueda asegurarse la efectividad de los derechos fundamentales involucrados en la circulación de los datos y su tratamiento por diversos agentes financieros y del sector real, con finalidades que pueden ser claramente distintas a las informadas al momento de la obtención de la respectiva autorización.

Otro punto que es relevante en la necesidad de reglas más precisas, adicionales a las existentes en el ordenamiento jurídico colombiano, es cuando el titular de los datos personales autoriza el tratamiento con una finalidad abierta y amplia que cubra no solo la exploración comercial de tales datos sino diversas finalidades, dependiente de si se trata de un actor financiero o del sector real.

Nuevamente, atendiendo a la protección de los derechos fundamentales, es necesario que se prohíba la inclusión de finalidades que paradójicamente no permitan conocer al titular de manera clara cuál será el uso que se le dará a sus datos. Los casos en los que las finalidades han sido de este tipo, por ejemplo, las incluidas por algunas entidades públicas, han probado que la afectación a los derechos fundamentales se presenta porque el titular no tiene la posibilidad de realmente elegir cómo pueden o no ser tratados sus datos, siendo estos empleados, por ejemplo, para fines electorales.

Control de las externalidades de la banca abierta para impedir prácticas restrictivas de la competencia y la conformación de monopolios

El sector financiero ha estado tradicionalmente sometido a unas reglas especiales, debido a que la forma en la que se llevan a cabo las distintas transacciones exige, en pro de la estabilidad del sector, controlar y contener las amenazas originadas en los múltiples riesgos que se involucran en el ejercicio de la actividad financiera, tales como el riesgo de crédito y el de mercado, entre otros. Para ello, la regulación financiera ha

expedido normas dirigidas a resolver los problemas presentes en esta actividad, entre otros: i) la asimetría de información entre las instituciones financieras y sus clientes, que dificulta la evaluación de los riesgos de estos últimos en sus transacciones; ii) la inherente inestabilidad de sus operaciones; y iii) el efecto sistémico de las quiebras bancarias, que afectan no solo al banco fallido sino a otras entidades.

Ahora, tal como lo afirmamos previamente, uno de los objetivos centrales de la implementación del *open banking* es la promoción de la competencia, a través de impulsar la innovación y eficiencia en la prestación de servicios financieros. Paradójicamente, una de las externalidades que se presentan en las transacciones a través del *open banking* es la restricción de la competencia si en el futuro los clientes solo interactúan a través de plataformas digitales controladas por un solo agente. Esta eventual restricción puede presentarse a partir de la creación de nuevos monopolios por parte de, por ejemplo, los participantes que no son entidades financieras, pero que concentran en una sola base de datos los clientes de todas las entidades bancarias; es decir, detentan en mayor medida la información del sistema financiero en comparación con los agentes naturales de este sector económico.

La consecuencia que, por ejemplo, los *Bigtech* tendrían en el sector financiero puede llegar a afectar la estabilidad financiera del sistema al cambiar sustancialmente la estructura de este mercado. Estos cambios en la estructura pueden verse reflejados en el levantamiento de las restricciones en la capacidad jurídica u objeto social exclusivo de las entidades financieras que, en comparación con los actores del sector real, pueden desarrollar simultáneamente múltiples actividades de distintos sectores económicos. La idea, entonces, de un objeto limitado o específico ha estado justificada además de la especialización de la banca, en la mitigación de dos riesgos principalmente: i) la presencia de subsidios cruzados o intersectoriales y ii) el descuido en la prestación de servicios financieros por el desarrollo de actividades económicas con mayor grado de especulación, que pongan en riesgo las actividades financieras.

Es decir, en el escenario del *open banking* los agentes del sector real que participan como beneficiarios de pagos a través de los canales digitales, intermediarios no financieros o como terceros proveedores de nuevos servicios pueden llegar a tener un mayor control de la información de los clientes y con ella pueden determinar las acciones de las entidades financieras, sin que haya para las primeras unos estándares para la mitigación de los riesgos propios del sistema financiero.

Para evitar un efecto adverso que pueda llegar a tener la banca abierta en relación con la reducción de los agentes del mercado y la concentración de la información que impida la transparencia en las decisiones que se toman en el sector, se ha previsto que es necesario cierta madurez de los *fintech* antes de implementar un modelo regulatorio obligatorio. En ese sentido, en el caso colombiano parece ser una buena alternativa implementar un enfoque de caja de arena, en el que la banca abierta está

sometidas a algunas condiciones del regulador, pero estas condiciones están dadas para la operación controlada en un ambiente de prueba.

Ahora, una vez haya que tomar una decisión respecto de implementar un modelo obligatorio o voluntario no será suficiente la evaluación de los resultados obtenidos en las pruebas piloto, cuya supervisión está a cargo de la Superintendencia Financiera de Colombia, en la medida en que el control y la vigilancia respecto de la protección de los datos personales como del derecho de la competencia actualmente están a cargo de la Superintendencia de Industria y Comercio, de ahí que sea necesario la coordinación entre ambos organismos de control (Remolina, 2019), para asegurar un escenario regulatorio compatible.

En lo que concierne a las restricciones indirectas a la competencia originadas en la regulación prudencial, el regular colombiano en el escenario del *sandbox* adoptó para el *open banking* los mismos controles de ingreso al mercado exigidos a la banca tradicional; esto es, para llevar a cabo los desarrollos y la prestación de servicios financieros en el contexto de la innovación, se requiere habilitación gubernamental del supervisor basada en un capital mínimo de constitución definido en el Decreto 1.234 de 2020, la existencia de los sistemas de administración de los diversos riesgos financieros, según los desarrollos tecnológicos y los nuevos productos financieros ofrecidos, y la evaluación de idoneidad y solvencias de los accionistas y administradores. Estas condiciones de ingreso son consideradas por algunos como elementos que podrían ser usados «para inducir la concentración del mercado [financiero], considerada por algunos como fuente de estabilidad (tesis concentración estabilidad)» (Perilla Castro, 2020: 284).

Respecto de las restricciones de salida del mercado, otro de los aspectos que debe decidir el regulador es si incluirá mecanismos de apoyo y resolución de entidades en crisis, esto, por tratarse de desarrollos para la prestación de servicios financieros en el que pueden participar las propias entidades financieras. Por el momento, la separación del capital que se destinará al *open banking* de capital para la realización de las operaciones tradicionales indica que solo el sector financiero propiamente dicho tendrá barreras de salida del mercado.

Con base en lo anterior, la conclusión en materia de competencia para el sector financiero no es distinta a la que los expertos han anunciado para la banca tradicional, esto es, se requiere partir de la «premisa de que la competencia es permitida en el sistema financiero, y que su regulación y supervisión deben dirigirse a los sistemas de administración de riesgos de las instituciones y a la adecuación de capital conforme el perfil de riesgo involucrado en sus operaciones» (Perilla Castro, 2020: 288).

Suficiencia de la regulación sobre los problemas de ciberseguridad asociados a la implementación del *open banking*

Uno de los grandes beneficios del *open banking* será la personalización de los servicios. En el informe del *Accenture Banking Technology Vision 2019* (Accenture, 2021) se señala que «los registros distribuidos, inteligencia artificial, realidad aumentada y computación cuántica» conocidos como las tecnologías DARQ, así como los postulados de *Secure Us to Secure Me* serán las tecnologías que marquen el derrotero en la implementación del *open banking* en nuestro país.

En el citado estudio también se concluye que la tendencia global hacia el *open banking* amplía la interconectividad entre bancos y terceros, lo que crea puntos débiles en la seguridad de la red de las entidades bancarias. Ante el incremento del riesgo de que el sistema sea vulnerado, se ha señalado que:

> Los consumidores confían en sus bancos y están dispuestos a proporcionarles sus datos personales a cambio de productos y servicios adecuados. Para mantener esa confianza, los bancos deben repensar cómo enfocar la seguridad de la red, centrándose en un ecosistema más amplio. Por ello, los bancos deberán adoptar una postura mucho más activa en lo que respecta a ciberseguridad (Rufilanchas, 2019).[12]

Sin embargo, en esta época en la que incluso las empresas tecnológicas más grandes del mundo (Microsoft, Apple, Google, Facebook, etcétera) están perdiendo la confianza del público por el tratamiento que se le han dado a sus datos, los clientes dudan si entregarán el acceso de ellos a terceros para el desarrollo de nuevos productos, más aún cuando en la actualidad los riesgos de pérdida del dinero por fraude se incrementan. Una investigación acerca de la percepción de los consumidores potenciales sobre las consecuencias del *open banking* encontró que el 40% consideró que tales consecuencias eran positivas; mientras que el 48% se refirió a los riesgos por el tratamiento de sus datos y a las preocupaciones de ciberseguridad como razones de peso para sustentar opiniones negativas.

Teniendo en cuenta la percepción que las personas tienen de la banca abierta y con el propósito de medir la suficiencia de la regulación colombina también en este aspecto, en la medida en que uno de los principios contenidos en la Ley 1.581 de 2012 para el tratamiento de los datos personales es el de seguridad, se destacan como principales interrogantes los referentes a si las API para compartir datos financieros abiertos y datos transaccionales de los usuarios de *open banking* tendrán un estándar o metodología de programación que garantice la seguridad de los datos y, en caso de ser así, si esos estándares garantizan certeza respecto del acceso controlado por parte de los responsables.

12. Disponible en https://bit.ly/3X93TEo.

Así mismo, teniendo presente que el *open banking* implica en su operación un uso dependiente de *BlockChain*, para garantizar la trazabilidad y transparencia de una operación, el interrogante que surge es ¿cómo puede garantizarse el derecho al olvido y la aplicación de la ley de *habeas data* y de protección de datos personales en un ecosistema como *BlockChain*?

Para dar respuesta a estos y otros interrogantes relacionados de manera general con la seguridad y el cumplimiento de los derechos de los titulares contenidos en la Ley 1.581 de 2012, es necesario que exista una convergencia de todos los elementos que la garanticen en una política integral de ciberseguridad, esto es, que comprenda el proceso de recepción, almacenamiento, tratamiento, difusión y circulación de los datos personales y financieros.

La integración de cada uno de estos componentes requiere, por ejemplo, de credenciales especiales de autenticación con el banco, previa autorización expresa del usuario para el uso de su información por parte de terceros. Para obtener esas credenciales las empresas interesadas deberán estar acreditadas ante la entidad reguladora de su país de origen como *Account Information Service Provider*[13] para los servicios de agregación bancaria y como *Payment Initiation Service Provider*[14] para los servicios de iniciación de pagos.

Para obtener las respectivas licencias las entidades deberán también acreditar que cumplen con los requisitos necesarios en materia de seguridad, trato de la información y tecnología. Ahora, desde la perspectiva del cliente es indispensable que dentro de las condiciones contractuales esté la obligación del uso de dispositivos sin alteraciones de fábrica, con los cuales pueda implementarse métodos de autenticación reforzada.

En lo que concierne a los estándares de optimización de las API, es importante recordar que son los actores encargados de integrar, correlacionar, intercambiar, procesar y analizar toda la información personal y financiera de los clientes entre los diversos agentes del sector; por lo que estas API deberían ser programadas con base en altos estándares como The Software Security Framework, OWASP Software Assurance Maturity Model y/o Microsoft Security Development Lifecycle. Esta es precisamente una de las exigencias que debe hacer el regulador, sin que tal requisito se instituya en perjuicio del principio de neutralidad tecnológica que es aplicable a

13. Proveedor de servicios de información sobre cuenta. Prestador Financiero que obtiene información de varias entidades en nombre de un usuario de servicios de pago y se las presenta de forma consolidada.

14. *Account Servicing Payment Service Provider* (ASPSP) o Proveedor de servicios de iniciación de pago: prestador financiero de servicios de transferencia bancaria gestionados en nombre de un usuario de servicios de pago a través de una API ofrecida por su Proveedor de servicios de pago gestor de cuenta. Puede requerirse por parte del ASPSP la confirmación del usuario.

todas las relaciones del comercio electrónico y a los servicios digitales implementados tanto por el sector real como el financiero.

Así, con independencia de la forma como se integren las tecnologías a los servicios financieros, debe ser un requisito necesario el cumplimiento de las guías de programación segura, las cuales reducen la capa de exposición frente a eventuales fallas de programación que deriven en fugas de información personal: Guidelines for the use of the C language in critical systems (MISRA), C Secure Coding Standard, Secure Coding in C and C++ y Oracle Secure Coding Standard for Java. (CERT) y la Guía de referencia rápida para buenas prácticas de programación segura de OWASP.

Por último, respecto de la segunda interrogante, es necesario tener en cuenta que como medida de protección de datos personales el usuario de *open banking* que desee prescindir de estos servicios, sea cual fuere la razón, debe tener la tranquilidad absoluta de que la información o los datos que puedan identificarlo en la BlockChain deberán contar con medidas de pseudoanonimización que dificulten e impidan la violación de sus datos personales y transaccionales.

Banca abierta y sus agentes: En busca del modelo de relacionamiento contractual

Tal como lo señalamos previamente, uno de los requisitos para que el consentimiento o autorización dada por el consumidor financiero sea válida, es indispensable que este se dé en virtud de la ley, contrato o directamente por parte del titular. Este último caso se presenta cuando no media entre la entidad del sector financiero una relación contractual en la que se incluya la cláusula relativa al tratamiento de los datos personales para los propósitos exclusivos de la ejecución de la relación contractual. Este escenario podría presentarse en caso de que sean los TPP quienes obtengan la respectiva autorización.

Ahora, si son las entidades financieras las que obtendrán el consentimiento informado de sus clientes, el Estado colombiano al momento de definir el modelo regulatorio también deberá tener en cuenta los tres enfoques que se han implementado en otros países para definir el acceso a los bancos y proveedores de servicios de pago por terceros por parte de entidades financieras:

- *Centralizado,* en el que el tercero que accede a los datos financieros e información de los titulares lo hace conforme con los estrictos parámetros definidos por el regulador, datos que son administrados y aprobados por una entidad administrativa central para esos terceros.
- *Liderado por la entidad financiera*, en el que el tercero y la entidad financiera celebran un contrato, cuyas condiciones dependen del análisis de riesgos que haga la propia entidad financiera.

- *Mixto*, en el que el ente regulador establece un contrato estándar para las partes que se constituye en el mínimo de garantía para los usuarios, pero tanto entidad financiera como los TPP tienen la libertad de adicionar las cláusulas que sean necesarias.

De la aplicación de cada uno de estos modelos se han obtenido algunos resultados en varios países. Por ejemplo, Europa cuenta con una normativa que al estar estandarizada y en constante supervisión ofrece mejores mecanismos para implementar una regulación sólida, esta vez de carácter obligatoria a través de la directiva PSD2, mediante la cual obliga a los bancos a dar acceso a terceros ubicados en esta jurisdicción, transacción que es supervisada por la European Banking Authority,[15] a partir del establecimiento de mecanismos para hacer seguimiento a las actividades del sector financiero, entre los que se encuentran las directrices para la contabilización del crédito esperado, directrices sobre comunicación entre autoridades competentes y auditores, las Normas Técnicas Reglamentarias sobre métodos de consolidación prudencial, revisión de entre entidades bancarias y proveedores y *e-money*, constituyéndose como un modelo centralizado.

Así mismo, el Reino Unido cuenta con la Autoridad de Competencia y Mercados[16] la cual es un organismo que busca promover la libre competencia y la protección al consumidor en el Reino Unido, además de fomentar las buenas prácticas en el mercado para garantizar el mejor beneficio a los consumidores, las empresas y la economía en general.

Las virtudes de este modelo centralizado adoptado por el Reino Unido han mostrado algunas ventajas, de las que se destacan: [17]

- La creación de una entidad independiente: el regulador, la CMA, dispuso que la Entidad de Implementación de banca abierta (open banking, 2021) (OBIE) sería la encargada por delegación del diseño de las especificaciones para las interfaces de programas de aplicación; además de elaborar los lineamientos para que los participantes del nuevo ecosistema financiero puedan apoyarse en la implementación de los estándares del *open banking*.
- Una norma basada en API: con la vigencia de la directiva de pagos PSD2 y el Reglamento General de Protección de Datos, se dieron respuesta a dos interrogantes relevantes en la implementación del *open banking* en esta jurisdicción. Uno de ellos referente a la integración de API a los entornos propios de la banca abierta y el segundo relacionado con garantizar la interoperabilidad.

15. Disponible en https://bit.ly/3GkeViA.

16. Disponible en https://bit.ly/3WWy41k.

17. BBVA, Cinco lecciones de Reino Unido sobre open banking, *BBVA API Market,* 7 de agosto de 2018. Disponible en https://bit.ly/3Wwlzcv.

Con base en los instrumentos jurídicos disponibles, se tuvo certeza de que cualquier *fintech* autorizada puede utilizar un único estándar API para acceder, con el consentimiento de los clientes, a los datos de transacciones de las cuentas corrientes de consumidores y pymes, y pueden ejecutar también pagos únicos inmediatos.

- Protección al consumidor: Reino Unido definió que el éxito del modelo está en garantizar la protección del consumidor, por lo que fijó altos criterios de seguridad acompañadas de recomendaciones de uso, y la posibilidad de que el titular verifique con facilidad la lista de terceros a los que ha autorizado el acceso a sus datos, para asegurar el derecho de revocar la correspondiente autorización.
- Creación de un directorio de empresas: solo las entidades autorizadas pueden sumarse al ecosistema. La OBIE ha creado un directorio al que solo pueden sumarse *fintech* autorizadas, esto es «que tengan una licencia para realizar pagos por parte de las autoridades competentes».

Sin embargo, en el ecosistema de la banca abierta es muy frecuente el uso de otros modelos, entre estos el liderado por la entidad financiera, que adelanta de manera autónoma su propio análisis de riesgo y de evaluación de cada tercero participante en los procesos de banca abierta. Eºste esquema fue implementado en el ecosistema financiero de Asía,[18] principalmente apoyado por los operadores bancarios tradicionales. El ecosistema de banca abierta ha crecido hasta convertirse en parte del panorama financiero de ese territorio y ahora se encuentra entre uno de los más avanzados del mundo. El desarrollo de la banca abierta se ha visto facilitado por la infraestructura pública digital establecida por el gobierno.

India, por otro lado, ha optado por un enfoque híbrido en el que tanto el mercado como el gobierno toman roles activos en el desarrollo del ecosistema. En particular, el desarrollo de la infraestructura digital conocida como India Stack a menudo se elogia por ser un habilitador clave del floreciente ecosistema de banca abierta de la India.

Así, en ausencia de la implementación de un marco regulatorio estandarizado en lugares como Hong Kong también se ha optado por ceñirse a un modelo de implementación de banca abierta mixta, en virtud de que el regulador propone un contrato entre las entidades bancarias y los proveedores de servicios técnicos (2021), TSP, que son empresas que trabajan con proveedores regulados para ofrecer productos o servicios de banca abierta. Para que estos adopten en común acuerdo las medidas adicionales que a bien tengan considerar.

En síntesis, los modelos de implementación del *open banking* ofrecen una importante variedad de opciones, las cuales pueden ser consideradas, concertadas, priori-

18. Fintechnews, India's Open banking Landscape Thrives on the Back of Digital Public Infrastructure. *Fintechnews*, 15 de marzo de 2021, disponible en https://bit.ly/3FXdYg9.

zadas y ejecutadas de manera consecuente con el mercado, las entidades financieras y el regulador para dotar de dinamismo el ecosistema financiero, promoviendo un mejor uso de las bondades de la banca en los distintos eventos de ofrecimientos de productos y servicios, incentivando de esta manera una mayor y mejor inclusión financiera de todos los actores de la economía de una manera segura y confiable.

Lo anterior significa que la suficiencia de la regulación de la banca de servicios no puede medirse exclusivamente con base en un modelo ideal o referente teórico, sino que debe involucrar el análisis de las condiciones económicas, sociales y normativas del país específico, sin perder de vista que la banca abierta y la banca de servicios en la actualidad se ejecutan en un escenario de globalización, que implica tener en cuenta los mejores estándares de otros órdenes jurídicos.

Aun con las diferencias que existen entre los Estados respecto del modelo regulatorio y contractual a aplicar, la contratación dentro de las medidas del *open banking* puede asimilarse, en sus bases y en los principios, a los enfoques con base en los cuales se diseñaron las reglas del comercio electrónico, los contratos electrónicos y los relativos a las nuevas tecnologías; sin que a la fecha pueda afirmarse de manera definitiva que están resueltos todos los problemas de índole jurídico que de cada uno de ellos se desprenden.

Los principios de equivalencia funcional de los actos electrónicos, la neutralidad tecnológica, la no alteración del régimen de las obligaciones o de los contratos, la buena fe y libertad contractual, continuarán siendo los pilares del funcionamiento de las relaciona contractuales entre la banca, los TPP y los consumidores financieros, y también son relevantes para la definición del modelo que se escoja al introducir el *open banking* en el ordenamiento jurídico colombiano; en la medida en que no involucran un determinado número de partícipes o cierto modo de aplicativos, ya que se basan en la seguridad y la libertad contractual de las partes.

Retos de la modificación al servicio de intermediación bancario

La aparición de nuevos agentes con incidencia en el sector financiero y que no necesariamente se dedican a las actividades propias de este mercado, abre el camino para que haya una modificación en la forma de relacionamiento de los actores que tienen a cargo la intermediación bancaria.

Con base en todos los aspectos que hemos evidenciado en este artículo, y que generan algunos interrogantes en el caso colombiano, pero que parecen tener una solución en otros órdenes jurídicos, finalmente nos ocuparemos de sintetizar los retos que se desprenden de la modificación al servicio de intermediación bancario, en cada uno de los puntos previamente señalados, esto es, la protección de datos personales, el derecho de la competencia, ciberseguridad y modelo contractual.

Respecto de la protección de datos de los consumidores de servicios financieros,

son varios los retos que se presentan. El primero está relacionado con garantizar que el acceso a los datos del consumidor por parte de terceros respete el principio de finalidad consistente en cumplir el objetivo de generar mejores condiciones de mercado y de acceso a los servicios financieros, así como buscar el beneficio del consumidor en la creación de nuevos productos y servicios.

Aunque es natural que todos los actores comprometidos en el modelo de *open banking* quieran derivar un beneficio, no se puede perder de vista que la prioridad en todo caso debe ser el cliente o consumidor de servicios financieros. El promover la competencia entre prestadores de servicios financieros con productos y servicios de rango tecnológico favorecerá al consumidor al tener acceso a productos novedosos, más eficientes y a menores costos; pero sin olvidar que los controles respecto a la concentración de la información es una condición necesaria no solo para la estabilidad del propio sistema financiero sino para no ahondar en la asimetría de la información del mercado entre agentes y consumidores.

En esa medida, uno de los principales retos es el establecimiento de un modelo de responsabilidad para los intermediarios que no esté basado exclusivamente en el grado de diligencia formal con el que se mide sus actuaciones, sino en un modelo de responsabilidad probada o prospectiva que tenga en cuenta la incidencia del uso de la tecnología en los derechos individuales de los sujetos y que tome en cuenta las consecuencias colectivas para agentes y usuarios del sistema financiero.

Así, pues, la fijación de un modelo de responsabilidad para los terceros y para las entidades financieras cuando se aparten de la finalidad perseguida por el *open banking*, es fundamental. Contar con reglas claras es una condición imprescindible. La armonización de los distintos intereses en el mercado tratando de garantizar relaciones justas y equilibradas, será una gran exigencia tanto para el regulador como para el supervisor.

En articulación con el sistema de responsabilidad que sea coherente con las nuevas formas de interacción, es indispensable que se creen las acciones respectivas para que los consumidores puedan reclamar los perjuicios que les ocasionen los terceros por no atender la finalidad del *open banking*, esta posibilidad de reparación también debe tener en cuenta no solo la lesión material, sino la afectación a derechos fundamentales.

Es indispensable no solo asignar responsabilidades a los nuevos participantes en el mercado: *fintechs*, *Bigtechs*, bancos, sino también establecer las acciones que los titulares de datos personales podrán adelantar contra aquellos para hacer efectivas tales responsabilidades. Esto implicará analizar si conforme a la normativa vigente, a las entidades proveedoras les asiste una legitimación para ser sujetos pasivos de acciones de protección al consumidor.

Otro reto respecto de las implicaciones de los cambios en la forma tradicional de intermediación y que está en sintonía con el aseguramiento de un mercado en

competencia plena, está relacionado con el análisis de la conveniencia de mantener por separado las funciones de supervisión financiera, respecto de protección de datos personales.

En la actualidad se cuenta con una supervisión específica a las actividades financieras, a cargo de la Superintendencia Financiera de Colombia, y con una vigilancia al cumplimiento de las normas de protección de datos por parte de la Superintendencia de Industria y Comercio. Vale la pena preguntarse si este esquema de supervisión, a la luz del *banking as a service*, resulta efectivo y conveniente dadas las interacciones que se presentan bajo este formato de integración.

La Unidad de Regulación Financiera es partidaria de un esquema de coordinación entre las autoridades financieras y las autoridades de protección de datos y de protección al consumidor.[19] Nosotros estimamos que es más efectivo que en materia de servicios financieros suministrados a través del sistema de *open banking*, se le asignen funciones de supervisión a la Superintendencia Financiera de Colombia respecto de la vigilancia del cumplimiento de las normas de protección de datos por parte de los terceros proveedores de servicios financieros. De esta forma se canalizan en una única entidad las reclamaciones y sanciones derivadas de cualquier infracción cometida en el marco del *banking as a service*.

El mismo interrogante, respecto a la separación de las competencias en organismos distintos, se predica en relación con la inspección, vigilancia y control de los actos que atentan contra la libre competencia, tales como cartelizaciones, competencia desleal, acuerdos restrictivos de la competencia o integraciones económicas. Sin embargo, en este aspecto es importante que sea la Superintendencia de Industria y Comercio la autoridad que mantenga estas funciones, en la medida en que con independencia del mercado en el que se dé el acto que restringe la competencia, los efectos son los mismos para los demás agentes.

De otro lado, también se observa que en materia de seguridad es necesario el desarrollo de una Política de Ciberseguridad Integral para entidades y clientes de *open banking*, que permita ser aplicada de una manera fácil a todos los que participan en la transacción. Esto incluye, la expedición de directrices que lleven al uso obligatorio de API que cumplan tales guías y metodologías de programación segura y que se pueda comprobar de manera sencilla y eficiente dicha aplicación antes de pasar a entornos de producción.

19. La coordinación entre las autoridades financieras y las autoridades de protección de datos y protección del consumidor, considerando que el modelo involucra entidades financieras y no financieras.

Conclusión

Si bien en Colombia se ha decidido que el *open banking* tenga un enfoque de pruebas controladas, mientras se adelanta la agenda de trabajo que muestre todos los atributos de esta institución y que, además, identifique los riesgos propios de las condiciones normativas y económicas del país, es importante que el regulador tome en cuenta los resultados de otros países para incluir los aspectos normativos que han permitido obtener beneficios para los consumidores financieros, de tal manera que también puedan incluirse en nuestro ordenamiento teniendo en cuenta nuestro contexto social, económico y jurídico.

Para el caso colombiano y en articulación con las políticas de Gobierno digital y estandarización de las reglas de los mercados financiaros, de la protección de la competencia y del tratamiento de datos personales con las reglas que han adoptado otros países, podemos concluir que dicho espectro normativo no está lo suficientemente completo y por ello en la medida en que se avance en los resultados del entorno de pruebas también es necesario tomar decisiones respecto de reforzar o expedir un régimen especial aplicable al *open banking*, principalmente en lo que concierne a seguridad y datos personales.

En relación con el tratamiento de los datos personales en el contexto de la banca abierta es necesario que el regulador, específicamente el Congreso de la República, expida unas reglas especiales que exijan una mayor rigurosidad en la autorización del titular, de tal manera que estén presentes todos los elementos que garanticen la prevalencia de los intereses de los consumidores financieros, de ahí que haya necesidad de consagrar de manera expresa la aplicación del principio de responsabilidad demostrada tanto para los responsables, como para los encargados y los terceros que por cualquier razón tengan acceso a los datos.

De manera especial, debe prohibirse el diseño de políticas de privacidad y de cláusulas de tratamiento de datos personales que no permitan un control estricto en la circulación de los datos entre agentes del mercado, lo que requiere de que la autoridad y los partícipes del *open banking* lleve un registro que pueda ser consultado por el titular, para que pueda ejercer con mayor eficiencia los derechos de retracto y olvido de que trata la Ley 1.581.

En concordancia con las reglas internacionales, especialmente con el Reglamento General de Protección de Datos de la Unión Europea, la regulación debe tener un enfoque de riesgos, en el que la administración y mitigación estén dadas por el cumplimiento de estándares de seguridad y de cumplimiento de las condiciones que aseguren que el consentimiento sea informado. Con esto, es indispensable exigir a las entidades participantes que conforman el sistema de *open banking* un Oficial de Protección de Datos ante el cual se lleve el registro de quiénes están tratando los datos y tenga a cargo el deber de notificar al titular cuando un nuevo agente los tratará.

En materia de seguridad, derecho de la competencia y el modelo contractual que se habilitará en el relacionamiento entre las entidades bancarias y los TPP, conforme con la experiencia de otros países, se requiere que la regulación incluya la definición de estándares por parte del Estado, que permita a este ejercer un mayor control a partir de un enfoque en el que las competencias de los órganos de control estén dadas a partir de un criterio de especialidad.

Referencias

Accenture (2021). *The Post-Digital Era is Upon Us. Are You Ready For What's Next?* Obtenido de https://accntu.re/2Ot3lGU.

Arias-Berrera, Ligia Catherine, (2019). «El 'fintech' está generando cambios en la regulación financiera». Disponible en https://bit.ly/2Hyo6eK.

—. (2020a). «Los contratos inteligentes en el sistema financiero y la regulación realmente responsiva», en *Mercados financieros y nuevas tecnologías.* Bogotá: Universidad Externado de Colombia. Disponible en https://ssrn.com/abstract=3684831.

—. (2020b). *Problemáticas Asociadas a la Adopción de Contratos Inteligentes en el Mercado de Derivados Financieros*. Bogotá: Universidad Externado de Colombia.

Banco Interamericano de Desarrollo (2021). *Ensayos sobre inclusión financiera en Colombia*. Disponible en https://bit.ly/3YX1A8o.

Calle, José Miquel (2021). *Implicaciones de un nuevo régimen de Banca Abierta desde la perspectiva de protección de datos.* Disponible en https://bit.ly/3I7FlXn.

Diamond, Douglas y Raghuram Rajan (2001). «Liquidity Risk, Liquidity Creation, and Financial Fragility: A Theory of Banking». *Journal of Political Economy*, 109 (2): 287-327.

European Banking Authority (2018). *The EBA's Fintech Roadmap. Conclusions from the consultation on the EBA's approach to financial technology (fintech)*. Disponible en https://bit.ly/3jyC21g.

Michael Klein y Colin Mayer (2011). «Mobile Banking and Financial Inclusion: The Regulatory Lessons 7-8». *World Bank Policy Research Working Papers*, 5664. DOI: 10.1596/1813-9450-5664.

National Economic Council (2017). *A Framework for FinTech.* Disponible en https://bit.ly/3juoUap.

Open banking (2021). Obtenido de https://www.openbanking.org.uk/about-us/.

Perilla Castro, Carlos Andrés (2020). *Evolución del derecho de la competencia en el sector financiero: de la tolerancia a la sanción de prácticas restrictivas*. Disponible en https://bit.ly/3I47U8g.

Remolina, Nydia (2019). Open banking: Regulatory Challenges for a new form of Financial Intermediation in Data-Driven World. *SMU Center for AI & Data Gobernance Research Paper*, 5. Disponible en https://bit.ly/3C6Nnfm.

SIC. (2017). *Protección de datos personales: aspectos prácticos sobre el derecho de habeas data*. Superintendencia de Industria y Comercio. Disponible en https://bit.ly/3QrCMBM.

Unidad Regulación Financiera (2020). *Open banking y Portabilidad en Colombia*. Disponible en https://bit.ly/3Vzdwue.

Tauberer, Joshua (2014). *Open Government Data*. Second Edition.

Sobre las autoras

Laura Victoria Puentes Trujillo es abogada de la Universidad del Cauca, Especialista en Derecho Informático y Nuevas Tecnologías de la Universidad Externado de Colombia, magíster en Derecho con mención en Derecho Público de la Universidad de Chile, candidata a doctora en Derecho de la Universidad Externado de Colombia y la Universidad del País Vasco. Profesional jurídica de la Asociación Todos por Medellín. Miembro del Colegio de Abogados en Derecho Médico. Miembro de la International Network of Biolaw (Red Internacional de Bioderecho). Miembro colaboradora Observatorio de Salud, Universidad de Buenos Aires, Argentina. Su correo electrónico es lauvip12@gmail.com. https://orcid.org/0000-0003-1700-166X.

Lucidia Amaya Osorio es abogada Universidad de Antioquia, especialista en Derecho de los Negocios de la Universidad Externado de Colombia, magíster en Derecho de la Universidad Pontificia Bolivariana, candidata a doctora en Derecho de la Universidad Externado de Colombia. Es directora jurídica en Todos por Medellín, miembro del Comité Editorial Revista Letras Jurídicas, docente cátedra Teoría y Filosofía del Derecho. Su correo electrónico es lucesitamaos@gmail.com. https://orcid.org/0000-0001-6457-1564.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

DIRECTOR

Daniel Álvarez Valenzuela

(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).