FORSETI
Revista de Derecho

Forseti. Revista de Derecho. Volumen 13, Nº 20, Lima, 2024, pp. 06 – 43

Alcance, fundamentos y objetivos del *Open Banking*: planteamiento de las problemáticas de su implementación y posibles soluciones

José Alonzo Jiménez Alemán*

Resumen. – Este trabajo establece las bases conceptuales del Open Banking y analiza su situación en Perú y otros países. Para ello, se examinan argumentos técnicos y aspectos regulatorios necesarios para su implementación, como la seguridad y eficiencia en la transmisión de datos. En Perú, se define el modelo adecuado, tipo de información a compartir, los riesgos asociados y la compensación para las entidades que compartan datos.

Palabras clave. – Open Banking – Open Data – Fintech – Seguridad – Regulatorio

Abstract. – This work establishes the conceptual foundations of Open Banking and examines its status in Peru and other countries. It explores technical arguments and regulatory aspects necessary for its implementation, such as security and efficiency in data transmission. In Peru, it defines the appropriate model, the type of information to be shared, associated risks, and compensation for entities that share data.

Key words. – Open Banking – Open Data – Fintech – Security - Regulatory

* El autor es abogado por la Pontificia Universidad Católica del Perú y Magister en Derecho de los Sectores Regulados por la Universidad Carlos III de Madrid. Actualmente trabaja como especialista legal senior de la Gerencia Jurídica del Banco Central de Reserva del Perú. Las opiniones, interpretaciones y conjeturas del autor no representan la posición institucional del Banco Central de Reserva del Perú.

Un especial agradecimiento a Javier Quinteros Zarzoza por los comentarios y aportes en la perspectiva adecuada para el presente trabajo. Es un agradecimiento que trasciende este artículo, pues tengo aún la suerte de seguir aprendiendo de él en la Gerencia Jurídica del Banco Central de Reserva del Perú.

I. Introducción

El sistema financiero tiene un rol protagónico en el funcionamiento de los mercados y la sociedad en general, pues atiende una serie de necesidades de los agentes económicos, tales como promover el ahorro y distribuirlo a los sujetos que lo requieren para la realización de actividades productivas, la ejecución de pagos privados y de servicios públicos, transferencia de recursos, realización de inversiones, la gestión de riesgos a través de la contratación de seguros[1].

Desde la perspectiva de un proveedor de servicios financieros, hoy en día la información es un insumo valioso, pues les permite identificar la demanda de los usuarios con mayor certeza y, de esa forma, crear o modificar productos o servicios financieros que satisfagan esas necesidades. Hablamos de la creación de servicios financieros que atiendan de forma más eficiente el interés de los consumidores, por ejemplo, con el diseño de servicios de pago (por ejemplo, remesas al exterior) más económicos y rápidos. En este ámbito es que ingresan empresas con propuestas disruptivas que pretenden cambiar el alcance y la forma de cómo se vienen prestando los servicios financieros, a través de herramientas tecnológicas, que hoy en día conocemos como *Fintech*[2].

Para el diseño de servicios disruptivos, las *Fintech* requieren información sobre el comportamiento y características de los consumidores; para ello es fundamental tener acceso a data que proviene de una amplia variedad de fuentes: empresas prestadoras de servicios públicos, administración tributaria, aplicativos de pago digital, entidades bancarias, entre otros. En su gran mayoría se trata de información personal que se encuentra protegida por la normativa sobre protección de datos personales, por lo cual es indispensable el consentimiento expreso, informado e inobjetable del titular.

En este contexto, surge la interrogante: ¿cómo un tercero puede acceder a información que usualmente es custodiada o administrada por las entidades que proveen esos productos o servicios? Para responder esta pregunta debemos partir de la premisa de que la información no es de propiedad de las entidades privadas o públicas, si no de los clientes, quienes son los titulares de la misma y poseen el derecho de autorizar su utilización. En términos constitucionales se trata del

---

1 Comisión Nacional de los Mercados y la Competencia. (2018). Market study on the Impact of Technological Innovation in the Finantial Sector. Madrid: CNMC.

2 El término Fintech se refiere a las tecnologías digitales con potencial de transformar la provisión de servicios financieros, mejorando o creando nuevos modelos de negocio, aplicaciones, procesos y productos. FEYEN, E.; FROST, J.; GAMBACORTA, L.; NATARAJAN, H.; SAAL, M. (2021). *Fintech and the digital transformation of financial services: implications for market structure and public policy.* Bank For International Settlements. Monetary and Economic Department. BIS Papers N° 117.

ejercicio del derecho fundamental a la **autodeterminación informativa** consagrado en el numeral 6 del artículo 2° de la Constitución Política del Perú, cuyo contenido fue desarrollado por el Tribunal Constitucional[3], y supone la facultad de toda persona de requerir y utilizar información privada que consta en un registro administrado por una persona jurídica de derecho privado o público, para los fines que crea conveniente.

¿Por qué el Estado debe involucrarse en el desarrollo del derecho de autodeterminación informativa de los particulares, a fin de exigir a los custodios o administradores de la información mayores facilidades o esfuerzos para compartir información con terceros? La respuesta se encuentra en la promoción de políticas públicas como el *Data Access* u *Open Data*[4], que tiene por objeto maximizar el acceso e intercambio de información como un medio para promover la productividad, a través del desarrollo de nuevos productos, procesos, métodos organizacionales e incluso mercados; así como para la mejora de la gestión pública de los Estados (por ejemplo, advirtiendo ineficiencias en el ejercicio de sus funciones que impactan en la vida de las personas y empresas). Como lo explica la OCDE[5], el acceso a información es crucial para promover la competencia y la innovación en la era de la economía digital, no sólo para los comercios, sino también para los gobiernos e individuos. La información nos permite identificar demandas sociales en el ámbito de la salud, educación, transporte, infraestructura y, en general de los servicios públicos. En este contexto es que tiene cobertura el *Open Banking* o esquema de **finanzas abiertas**[6].

El *Open Banking* se desarrolló en el Reino Unido a mediados del 2016 como una herramienta para promover la competencia en el ámbito de los servicios financieros. Esta iniciativa se aplicó inicialmente a los nueve (9) bancos más grandes del país[7] y facilitó el acceso de nuevos agentes al mercado con esquemas de negocio disruptivos, tales como la **iniciación de pagos**, planificación financiera o servicio de *scoring*. La regulación exigió que las nueve (9) entidades financieras cumplan con compartir la información de sus clientes a terceros de forma segura y en línea.

El tema es aparentemente muy sencillo, sin embargo, existen muchos aspectos que deben ser evaluados para su correcta implementación, como es el caso de fijar los

---

3 En otras sentencias, basta con referirnos a la recaída en el Expediente 04739-2007-PHD/TC, fundamentos 2 al 4.

4 El enfoque del *Open Data* se sustenta en un principio fundamental: la información que administran o custodian las empresas prestadoras de servicios o proveedoras de bienes es de titularidad de las personas, por lo cual la decisión de compartirlas sólo les atañe a éstas, no a las empresas. Plaitakis y Staschen definen el *Open Data* en los siguientes términos: "*the exchange of consumer data between private sector institutions, including financial institutions and nonbank financial institutions such as mobile money issuers, utility providers, and telecoms, with other such institutions on the basis of costumer consent*". PLAITAKIS, A., & STASCHEN, S. (2020). Open Banking: how to designs for financial inclusion. Washington: Consultative Group to Assist the Poor; pp. 4.

5 OCDE. (2019). *Enhancing access to and sharing of data: reconciling risks and benefits for data reuse across societies*. Paris: OECD Publishing.

6 En el presente trabajo se utilizará de forma indistinta los términos *Open Banking* o finanzas abiertas.

7 Fue voluntario para las demás instituciones.

objetivos específicos que pretenden conseguirse, establecer el modelo más adecuado para la realidad del país, desarrollar el régimen de responsabilidad para los terceros proveedores de soluciones financieras, elaborar o plantear el protocolo para la interoperabilidad entre los agentes que administran la información financiera del cliente con los terceros que la demandan, la protección de los datos personales de los clientes, entre otros.

Actualmente, es probable que muchas personas estén utilizando aplicaciones que funcionan bajo el enfoque del *Open Banking* aun desconociéndolo, en tanto es una tecnología que permite el funcionamiento de servicios de uso cotidiano como las plataformas de **Rappi, Pedidos Ya, Didi, Uber**, entre otros. En el *New Payment Index 2022* de Mastercard[8] se presentó una encuesta dirigida a consumidores y respondida por más de 35 000 personas de 40 países, en las que se revela que más del 50% de los encuestados usan aplicaciones elaboradas sobre un enfoque de *Open Banking* sin conocerlo.

En esa línea, el presente trabajo tiene por objeto establecer bases conceptuales y prácticas sobre el funcionamiento y beneficios que implicaría la implementación de una visión o perspectiva de *Open Banking* o finanzas abiertas en el sector bancario. Asimismo, se ensayan los argumentos técnicos necesarios para promover el *Open Banking*, así como para regular ciertos aspectos indispensables para garantizar la seguridad y eficiencia en el traslado de información de los clientes. Finalmente, se desarrollan algunos retos pendientes en caso se pretenda implementar un régimen de *Open Banking*, considerando el estado de cosas vigente en Perú, tales como el arreglo institucional, el modelo más adecuado para nuestra realidad, el tipo de información que se debe compartir, los riesgos asociados a las finanzas abiertas (y su respectivo tratamiento), así como el discutible tema de la contraprestación o reconocimiento de los costos a las entidades que custodian o administran la información de los clientes.

II. Alcances conceptuales sobre el *Open Banking*

Como adelantamos, el *Open Banking* forma parte de un enfoque o concepción del funcionamiento del mercado más general, denominado *Open Data,* que -a nuestro juicio- tiene tres objetivos claros: (i) mejorar la productividad del país a través de la creación de nuevas oportunidades de negocio y promoción de la innovación; (ii) empoderar a los consumidores respecto del uso de su información (optimización del derecho a la autodeterminación informativa); y, (iii) aportar a la mejora de la gestión pública a través de información que beneficie la toma de decisiones de los burócratas.

El *Open Banking* se concentra en mejorar la experiencia del usuario y el proceso de creación de productos o servicios financieros, a través de la información de los

[8] Consultado el 01 de agosto de 2023: https://www.mastercard.com/news/eemea/en/newsroom/press-releases/press-releases/en/2022/august/mastercard-new-payments-index-2022-consumers-in-mena-embrace-digital-payments/

propios clientes, a la que pueden acceder terceros, previa autorización del titular de los datos. Esto se materializa a través del consentimiento de los propios usuarios, que no es otra cosa que el ejercicio del derecho fundamental a la **autodeterminación informativa,** que en el campo especializado se denomina derecho de acceso y a la **portabilidad de datos**[9] [10], el cual tiene raigambre constitucional. La información a la que nos referimos no necesariamente tiene que circunscribirse al ámbito bancario o financiero (que es el objeto del *Open Banking* u *Open Finance)*, sino que es deseable que se expanda a otros ámbitos como el de servicios públicos (por ejemplo, la información de los clientes que es administrada o custodiada por empresas prestadoras de servicios de telecomunicaciones, suministro de energía, entre otros).

De acuerdo con Azar, Mejía y Valdez[11], el *Open Banking* se refiere a la apertura de los productos, los servicios y los datos de los clientes de los bancos a otras organizaciones (otros bancos o terceros), con el objetivo de aumentar la oferta de los servicios financieros. Es el proceso que promueve que los proveedores de servicios financieros compartan los datos de sus clientes, previa autorización de éstos. Se diferencia del *Open Finance* debido al alcance de la obligación de compartir información, pues éste incluye no sólo a las entidades bancarias, sino también a los fondos de pensiones, *Fintechs*, aseguradoras, y en general todas las empresas que prestan algún tipo de servicio financiero. Por su parte, el denominado *Open data* incluye a las empresas que prestan servicios públicos, los *e-commerce*, las empresas del sector salud, las entidades gubernamentales, entre otras. Se trata de un enfoque más general, que -a nuestro juicio- es el más apropiado para crear bienes o servicios más alineados a las necesidades de las personas.

Los terceros proveedores de soluciones financieras (o de cualquier otro sector, incluso) utilizan esta información para innovar, lo cual constituye un valor clave para promover la competencia en el mercado, más aún si se incorporan componentes de disrupción tecnológica. Para explotar este enfoque de *Open Data* debemos partir de la premisa de que la información es dúctil a nuestras necesidades, por ende, puede ser acopiada de una empresa del sector de

---

9 OCDE. (2019). Enhancing access to and sharing of data (…); op. cit. pp. 43. De acuerdo a la OCDE, la portabilidad de datos puede ser conceptualizada como una herramienta para el ejercicio del derecho a la autodeterminación informativa, la cual consiste en el poder de las personas de exigir que su información personal pueda ser compartida con terceros a través de un formato práctico y sencillo, evitando así un nuevo registro.

10 El derecho a la portabilidad de datos, como expresión del derecho fundamental a la *autodeterminación* informativa y el derecho de acceso, aún no goza de reconocimiento expreso. Sin embargo, creemos que su reconocimiento es inminente, pues el proyecto de Reglamento de la Ley de Protección de Datos Personales (pre publicado el 26 de agosto de 2023, mediante Resolución Ministerial 0270-2023-JUS) lo incorporó. Cabe indicar que hubo un intento anterior a través del Proyecto de Ley N° 7870/2020-PE, que propuso crear la Autoridad Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, y además pretendía modificar la Ley de Protección de Datos Personales, Ley N° 29733, incluyendo el derecho a la portabilidad de datos. Sobre el particular, recomendamos revisar: Gabriela Bolaños Vainstein (2022). *La incorporación del derecho a la portabilidad de datos personales en el ordenamiento jurídico peruano*. Tesis para optar por el título de abogado, Universidad de Lima.

11 AZAR, K., MEJÍA, D., & VÁLDEZ, M. (2021). Banca abierta: lecciones, desafíos y oportunidades para América Latina. Caracas: CAF.

telecomunicaciones y utilizada en sectores como la banca para crear productos o servicios que cierren la brecha de inclusión o profundización financiera. Piénsese en servicios de control de gastos, optimización de las finanzas, consolidación de deudas, comparación de productos financieros.

En el caso específico del *Open Banking* u *Open Finance*, la información que se puede acopiar de los clientes permite a los terceros conocer una serie de características de su comportamiento financiero, sobre la base de lo cual se pueden mejorar las experiencias, ofrecer productos más competitivos (por ejemplo, mejorar las tasas de interés, consolidar préstamos, o prestar servicios de administración de finanzas personales). Por otro lado, el acceso a las cuentas del cliente también constituye hoy en día un insumo fundamental para la prestación de determinados servicios por terceros, como son las billeteras digitales o los denominados servicios de iniciación de pagos.[12] [13]

El enfoque *Open Banking* tiene como principal efecto la promoción de la competencia en el mercado, pues elimina la asimetría informativa existente entre los proveedores de servicios financieros tradicionales (bancos) y los terceros proveedores de soluciones financieras (*Fintech*), y les permite a éstos competir e innovar en los segmentos del mercado más atractivos, como lo explican Zhiguo He, Jung Huang y Jidong Zhou[14]. De forma casi *apocalíptica*, estos autores vaticinan que la presión competitiva que ejercerán las *Fintech* sobre las instituciones financieras será tan fuerte que en algunos ámbitos (como el caso de los préstamos a favor de deudores calificados) las empresas de disrupción tecnológica desplazarán a los bancos tradicionales.

III. Reconociendo su impacto: principales servicios prestados a la luz del *Open Banking*

Hasta el momento, sabemos que las finanzas abiertas básicamente son un mecanismo para promover la competencia en el mercado bancario. Ahora bien, con el objeto de entender la utilidad práctica del *Open Banking,* en el presente acápite se realizará una revisión de los principales casos de uso, lo cual nos permitirá entender y dimensionar el aporte de una medida de esta naturaleza en beneficio del proceso competitivo y lo consumidores. Se utilizará como referencia el mapeo realizado por la Alianza Fintech del Pacífico[15]. Para este propósito se

---

12 ZUNZUNEGUI, F. (2018). *La digitalización de los servicios de pago.* Revista del Derecho del Mercado Financiero, Working Paper 1/2018.

13 Los servicios de iniciación de pagos (también conocidos como "PIS") por sus siglas en inglés fueron reconocidos formalmente en Europa a través de la Directiva N° 2015/2366 sobre servicios de pagos en el mercado interior (también conocida como PSD II). Este servicio permite al proveedor iniciar el pago de servicios con cargo en la cuenta que el cliente mantiene en un banco. Como explica Zunzunegui, este tipo de servicios permite ofrecer prestaciones complementarias para mejorar la gestión de las finanzas personales.

14 HE, Z., HUANG, J., & ZHOU, J. (2020). *Open Banking: credit market competition when borrowers own the data*. Journal of Financial Economics, 147(2), pp. 449-474.

15 Alianza Fintech del Pacífico. (2023). *Estándares Open Finance como palanca de conversión regional.* Santiago de Chile: Alianza Fintech del Pacífico.

puede identificar los casos de uso en tres grandes áreas: datos, pagos y finanzas embebidas.

Los casos de uso vinculados a **datos** buscan ampliar o mejorar la oferta de los productos o servicios financieros, a fin de adecuarlos a las necesidades de los consumidores. Para este propósito sólo se requiere tener acceso a datos personales y demográficos, información sobre los movimientos bancarios, información financiera en general. Los principales casos de uso basados en data son los siguientes:

a. Agregación de cuentas bancarias, inversión y seguros: este tipo de servicios permiten analizar los movimientos financieros, bursátiles y de seguros, a fin de optimizarlos. Se trata de un servicio que -por lo general- genera recomendaciones para mejorar las finanzas del cliente, incluso al nivel de sugerir consolidación de préstamos, o las mejores formas de endeudarse o realizar cambio de divisas. Esta función ha sido habilitada, por ejemplo, por el BBVA en Argentina o Bankinter en España, quienes han incorporado la función de **mis otros bancos**, a fin de incluir la información de medios de pago emitidos por entidades distintas.

b. Agregación de facturas de servicios públicos: este tipo de servicios implica el análisis y auditoría de las facturas de servicios públicos, a fin de validar y ratificar el cobro realizado. Te permite realizar un análisis para comparar el rendimiento y costos en relación con otros usuarios. Asimismo, te presentan oportunidades para mayor eficiencia y productividad del consumo del servicio. Este tipo de servicios es prestado por empresas como *Enel X* en España.

c. Planificación financiera y conciliación contable para personas naturales y jurídicas: en este tipo de servicios se operan con cuentas y productos de diferentes entidades financieras, de tal forma que se pueden conciliar los datos de los distintos proveedores y productos en una sola aplicación. De esta forma se puede simplificar la gestión de contabilidad, se tiene mayor control sobre las finanzas de las personas naturales o jurídicas, se ahorra tiempo en el análisis de la data y se toman mejores decisiones. Este tipo de servicios es prestado por empresas como *Sothis* en España.

d. Marketing de pagos: es un modelo de negocio donde la clave es la agregación de un número considerable de comercios para ofrecer al consumidor ventajas, ofertas, promociones. La plataforma se hace atractiva a través de una consistente red de comercios, con lo cual los clientes se afilian por las ventajas que se ofrecen en términos de ofertas, promociones, descuentos. La información del cliente es importante para efectos de ofrecerle productos o servicios más acordes a sus necesidades. Un caso de éxito de este tipo de modelos de negocio es la empresa *WayPay* que viene funcionando en España desde el 2019, y tiene una visión de apoyo al comercio local.

e. Servicios de *scoring* para *lending* y para inquilinos: este tipo de servicios procesa la información de potenciales clientes para realizar operaciones de préstamo o arrendamiento. Este tipo de servicios, con la información correcta, pueden cumplir un rol importante en el cierre de brechas de inclusión financiera, pues permitiría visibilizar a las personas excluidas del sistema financiero, a partir de información externa al sistema tradicional. Este es el caso de *Abaco* que es una plataforma de *credit score* cuyo objetivo es la inclusión financiera en América Latina. Por medio de información alternativa a la banca tradicional han desarrollado un modelo de negocio que incluye a las personas que no cuentan con un historial crediticio. En el caso de los inquilinos, encontramos el servicio prestado por *Quota Rent* denominado *QuotaScore*, el cual consiste en una evaluación voluntaria a la que se somete el potencial inquilino sobre la base de la información requerida por el aplicativo, en virtud del cual se emite un certificado digital, que le permite mostrarse como inquilinos de calidad ante los propietarios.

Por su parte, los casos de uso vinculados a **pagos** requieren que el cliente autorice al tercero proveedor de soluciones tecnológicas un acceso a sus credenciales para poder realizar operaciones en su nombre. Los servicios ofrecidos por los terceros aportan valor en términos de rapidez y conveniencia, por lo cual se suelen utilizar billeteras digitales que permitan centralizar en un solo lugar todos los medios de pago de los que dispone el cliente. En este ámbito, es preciso mencionar a los siguientes casos de uso:

a. Pagos directos de cuenta a cuenta: este servicio -también conocido como *account to account (A2A)* - permite que las transferencias de fondos se realicen directamente a la cuenta del banco del comercio o beneficiario. Se prescinde de intermediarios como en el caso de las tarjetas. Una de las herramientas que los terceros proveedores de soluciones tecnológicas utilizan son los sistemas de transferencia instantánea de fondos (este es el caso de *Pix* en Brasil). En este tipo de servicios se advierten dos tipos de pagos A2A: *push* y *pull*. En el primer caso los fondos se envían en tiempo real y son iniciados desde la cuenta del cliente, consumidor o pagador (cuenta de origen) hacia la cuenta del comercio o beneficiario del pago (cuenta de destino). En el caso de las *pull* A2A, el comercio o beneficiario de la transferencia es quien solicita retirar los fondos directamente del cliente, consumidor o pagador, lo cual es utilizado usualmente en el ámbito de créditos, seguros o suscripciones. Este modelo de negocio lo han desarrollado Fintechs como *Fintoc* en Chile o *PrometeoApi* que viene prestando el servicio en gran parte de Latinoamérica.

b. Iniciación de pagos (automatizados y posfechados): este servicio permite iniciar pagos directamente desde las propias cuentas del cliente de forma centralizada, automática y segura. Para este propósito el proveedor de soluciones tecnológicas debe acceder a las cuentas de su cliente, y los fondos deben viajar directamente a su destino. Con esta facilidad, las personas naturales o jurídicas ya no deben interactuar con tantos portales bancarios

como cuentas mantienen. Este servicio viene siendo prestado en Colombia a través de la Fintech *DRUO*.

c. Compras en línea: esta facilidad permite a los comercios cobrar por la prestación de sus servicios o venta de bienes a través de su propio portal, sin requerir el acceso directo a la banca por internet o móvil de su entidad financiera. En algunos casos se utilizan la infraestructura de las tarjetas de pago, y en otras se realiza directamente con la identificación de la cuenta, o incluso a través de transferencia de fondos. Este servicio es prestado en Europa por empresas como *Paysera*, o *Payu* que tiene operaciones en Perú (en general su operación se expande a América Latina, Europa, África).

Finalmente, el último grupo está vinculado a las **finanzas embebidas**, y se refiere a los supuestos en que los terceros proveedores de soluciones tecnológicas ofrecen servicios y productos financieros o de seguros, directamente en sus canales digitales. Se trata de simplificar el acceso a este tipo de bienes o servicios (en comparación con el habilitado por la banca tradicional), y atender una necesidad de forma práctica y célere. En este ámbito encontramos principalmente los siguientes casos de uso:

a. Validación de identidad de personas naturales o jurídicas: se trata de un servicio que forma parte del *onboarding digital*, en el que se validan los datos críticos de una persona, para lo cual se realiza una captura, lectura y validación de los documentos de identidad del usuario. Asimismo, en este ámbito se ofrece un registro de biometría facial, así como la confirmación de datos personales como correo electrónico, celular. En este ámbito también se ofrece la conexión a bases de datos que permitan identificar el perfil de la persona (antecedentes). Este servicio es prestado en España por empresas como *Veritran* o *Seon*.

b. Identificación de números de cuenta: este servicio permite a los comercios verificar la titularidad de las cuentas de sus clientes o potenciales clientes, lo cual tiene utilidad para efectos de abrir una nueva cuenta bancaria, o vincular un nuevo método de pago o completar una solicitud de préstamo. Este proceso es ofrecido por empresas como *Belvo*.

c. Localización de oficinas y cajeros automáticos e información de productos de la entidad: se trata de una facilidad que las propias entidades financieras ponen a disposición de las *Fintech* para que, a través de éstas, se puede facilitar determinada información a sus potenciales clientes. Se trata de descentralizar los canales de comunicación y promoción, aprovechando la escala y atención que hoy en día tienen determinados emprendimientos digitales.

d. Tipo de cambio y gestión de posiciones en divisas: Se trata de poner a disposición de los clientes una plataforma de cambio de divisas, en el que pueda evaluarse las mejores opciones y tu posición en términos históricos.

e. Todos los servicios involucrados en el denominado *Banking as a service*: a partir de este modelo es que se ha permitido que las *Fintech* ofrezcan servicios financieros que, en principio, son prestados exclusivamente por entidades autorizadas o con licencia para el ejercicio de dicha actividad. Esto les ha permitido a las entidades bancarias tradicionales extender la demanda de sus servicios, en complemento con los desarrollos puestos en marcha por los proveedores de soluciones tecnológicas. En este caso, las interfaces entre la entidad bancaria y el tercero proveedor sirven para poner a disposición de éstos las funcionalidades bancarias pactadas, por ejemplo, para otorgar una tarjeta de crédito, una tarjeta de débito, un préstamo (vehicular o hipotecario). Un caso bastante ilustrativo es el de *Rappi*, quien se alió con la institución financiera *Interbank*, a fin de tramitar o procesar directamente desde su canal las solicitudes de una tarjeta de crédito (que se denominó *RappiBank*).

En términos prácticos, y a la luz de la experiencia comparada, podemos señalar que son dos los casos de uso más importantes que incluso han requerido reconocimiento legal en la Unión Europea y Chile[16] que son los servicios de iniciación de pagos y los servicios basados en información, cuyos principales rasgos característicos a continuación podemos recapitular:

a. El servicio de iniciación implica ejecutar el pago de una determinada operación con cargo a la cuenta de pago del cliente. El servicio se presta *online* y se prescinde del instrumento de pago, pues éste se realiza a través de la plataforma del iniciador, en la que se almacenan los datos bancarios del cliente, respecto de cada una de las instituciones financieras con las que mantiene una cuenta o línea de crédito. Al momento de realizar un pago, el cliente tiene a su disposición una especie de billetera digital, de tal forma que puede elegir con qué medio de pago realizar la operación.

b. Por su parte, los servicios de información sobre cuentas tienen por objeto brindar un análisis agregado y desagregado de las operaciones del consumidor, sobre la base de la información financiera que éste pone a disposición del proveedor tecnológico, a través de las entidades bancarias que administran su información financiera. Esta información se asocia con una relación de los ingresos, gastos o compras, lo cual permite prestar una asesoría automatizada para optimizar sus gastos e inversiones. La Ley Fintec chilena define este servicio como una prestación que comprende la consulta, acceso y recepción de datos para efectos de proveer servicios a clientes.

[16] La Ley Fintec chilena define al servicio de información sobre cuentas como un conjunto de prestaciones que comprenden la consulta, acceso y recepción de datos para efectos de proveer servicios a clientes (artículo 19, Ley N° 21521, Ley que promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros). Asimismo, los servicios de iniciación de pago son definidos como una prestación a favor de clientes titulares de cuentas, la cual consiste en instruir, a nombre del cliente y ante la entidad proveedora de la cuenta, la ejecución de órdenes de pago o transferencias electrónicas de fondos, con cargo a sus respectivas cuentas o medios de pago.

IV. Fundamentos técnico-legales para regular el *Open Banking*

Como ha explicado Muñoz Machado[17] frente a la creencia que el mercado puede por sí mismo ordenar los intereses de todos los operadores y los consumidores, así como establecer los equilibrios perfectos entre la oferta y la demanda, nace la teoría de la competencia imperfecta en virtud de la cual se considera que las imperfecciones y fallos de mercado son normales. Es comúnmente aceptado que la regulación tiene como justificación la presencia de fallas de mercado, y lógicamente su objetivo es corregirlas[18].

Además de las fallas de mercado, existen otras razones de orden económico o incluso social que facultan al Estado a intervenir en la economía a través de regulación. Para efectos del presente artículo mencionaremos dos fundamentos adicionales a la regulación: la gestión de riesgos y la implementación y desarrollo de políticas públicas. Respecto de la gestión de riesgos, resaltamos el desarrollo conceptual elaborado por Esteve Pardo[19], quien explica que este enfoque nace a partir de la necesidad de anticiparse a la afectación del interés público. Ante la falta de evidencia, nos ubicamos en un escenario de desconocimiento e incertidumbre sobre el funcionamiento de un determinado sector, por lo cual se propone regular la actividad sobre la base de los riesgos que han podido advertirse en la experiencia comparada o desde un plano hipotético, de cara al cumplimiento de objetivos de política pública o fallas de mercado. En este contexto, la regulación se puede conceptualizar como una herramienta de gestión de riesgos de los sectores sociales o económicos que requieren una intervención **ex ante** a este nivel (claramente no todos los ámbitos requieren este tipo de intervención). Más adelante abordaremos un acápite en particular sobre la gestión de riesgos en el *Open Banking*.

Respecto del desarrollo de políticas públicas, se ha explicado que usualmente éstas se materializan en mandatos programáticos, principios, directivas u objetivos explícitos que se establecen en la normativa. Esteve Pardo[20] explica que la propia Constitución establece parámetros a la regulación como es el mandato de cumplir con los objetivos expresamente establecidos. Estos mandatos también pueden emanar de una norma infra-constitucional que aprueba una política pública, o incluso de normativa de naturaleza reglamentaria que establece las políticas

---

17 MUÑOZ MACHADO, SANTIAGO (2009). *Fundamentos e instrumentos jurídicos de la regulación económica*. En ESTEVE PARDO, J. & MUÑOZ MACHADO, S., Derecho de la Regulación. Madrid: Iustel; pp. 113.

18 OGUS , ANTHONY (2007). *Estructuras e instituciones regulatorias*. Revista de Derecho Themis (54); pp. 274-275.

19 Esteve Pardo sostiene hace más de dos décadas que el enfoque propuesto sobre la regulación de riesgos inevitablemente incorpora a la actividad administrativa de policía, la cual se ve *desplazada* por el contenido más amplio de la regulación por riesgos. Si bien es cierto se usan técnicas o herramientas similares, se han realizado importantes modulaciones que -a su criterio- justificarían superar la clásica actividad de policía por la actividad de regulación de riesgos. Por ejemplo, el desarrollo de la técnica autorizativa ha excedido totalmente las características de la actividad administrativa de policía, pues no puede brindar explicaciones sobre el alcance de algunas herramientas debido a sus particulares características. PARDO, ESTEVE (2009). *El encuadre de la regulación de la economía en la sistemática del Derecho Público*. En MUÑOZ MACHADO, S., & PARDO, E., Derecho de la Regulación (pp. 387-404). Madrid: Iustel.

20 PARDO, E. (2009). *El encuadre de la regulación de la economía en la sistemática del Derecho Público*, op. cit.; pp. 399.

públicas y directrices de funcionamiento de determinado sector. El Estado pasa a cumplir un rol de garante del funcionamiento de la economía, por lo cual su tarea no se puede limitar a seguir manuales de economía clásica, sino al bienestar de la sociedad materializado en mandatos de orden constitucional y legal.

Uno de los principales objetivos o directrices de la intervención del Estado en la economía es su orientación para proteger y promover las libertades individuales (principalmente la económica), la libre competencia, la protección al consumidor. No es necesaria una falla de mercado para que aparezca naturalmente la regulación, pues el fundamento también pasa por el cumplimiento de objetivos de orden público, legalmente establecidos por la normativa vigente. En este escenario, el Estado interviene en la economía a fin de compatibilizar el funcionamiento de la industria con el cumplimiento de las metas de política pública establecidas por el legislador o el propio gobierno.

En el caso del *Open Banking*, a nuestro juicio, la regulación se justificaría como una herramienta con dos propósitos. En primer lugar, facilita el ejercicio del derecho fundamental de autodeterminación informativa (portabilidad de datos), de tal forma de que los particulares libremente puedan compartir su información personal para que terceros puedan crear productos alineados a sus necesidades (lo que podría entenderse en el marco de una política pública de **datos abiertos**). En segundo lugar, el *Open Banking* promueve la competencia, pues fomenta la innovación para crear nuevos servicios, y además elimina las asimetrías informativas que se mantenían con los terceros proveedores de soluciones tecnológicas, con lo cual –por ejemplo- se intensificaría la competencia en los sectores más atractivos (es el caso de personas naturales o jurídicas con índices de cumplimientos altos).

El *Open Banking* procura eliminar esa brecha de información entre la banca tradicional y las *Fintech*, lo cual no ha podido revertirse incluso con la información proporcionada por las centrales de riesgos, pues la data que poseen los bancos y otras entidades sobre sus clientes se extiende a la información protegida por el secreto bancario o la regulación sobre datos personales, como es el caso de hábitos de consumo, el detalle de las cuentas de ahorros, cuentas corrientes, depósitos a plazo fijo y demás activos financieros que puede adquirir una persona natural. El *Open Banking* elimina esta especie de **asimetría informativa**, con el objeto de que nuevos actores puedan ingresar al mercado para competir con la banca tradicional (por ejemplo, en el sector de banca de personas), o para ofrecer nuevos servicios financieros como la **iniciación de pagos** o los servicios **información sobre las cuentas.**

Dependiendo de su alcance y enfoque, el desarrollo el *Open Banking* podría incorporarse como un objetivo de la Política Nacional de Inclusión Financiera[21]. No podemos defender que la inclusión financiera sea el objetivo inicial, si es que antes no se reformula el alcance de la data a la que pueden acceder los terceros

[21] La Política Nacional de Inclusión Financiera fue aprobada por el Decreto Supremo N° 255-2019-EF.

proveedores de soluciones financieras. Con la información del sector bancario o incluso financiero, no se cuenta con el insumo suficiente para identificar a las personas excluidas del sistema. Analícese el supuesto de incorporar dentro de las entidades obligadas a compartir información de sus clientes a las empresas que prestan servicios de telecomunicaciones o los servicios de cambio de divisas. Con la información que administra un operador de telecomunicaciones o las denominadas **casa de cambio**[22], se puede validar la identidad de una persona no bancarizada, conocer su récord de pagos de servicios y créditos (usualmente para adquirir un equipo celular). Esta información es un insumo importante para ofrecer una cuenta bancaria al titular del servicio, proponer una solución de pagos más ágil o incluso créditos.

Este es el caso, por ejemplo, de los servicios prestados por empresas como *Mojo mortages* o *Canopy* en el Reino Unido, en los que -sobre la base de información que no proviene del sistema financiero- se genera un antecedente verificado que sirve como un sustituto del récord crediticio para personas que nunca han accedido a un servicio financiero. Una de las fuentes de información más importantes para desarrollar la inclusión financiera es aquella provista por las compañías que prestan servicios públicos, pues a partir de esta data algunos emprendimientos han creado herramientas de ahorro[23], como es el caso de *Digit* en Estados Unidos. También se facilita la creación de cuentas bancarias aprovechando la regulación de los servicios públicos donde se aplica un protocolo de autenticación fuerte del titular. Claramente esto representa un reto por la compleja red de coordinaciones que se debe implementar para que este tipo de información pueda ser compartida.

V. Principales retos en la implementación de un régimen de *Open Banking*

i. El arreglo institucional

Uno de los primeros asuntos que debe determinarse es el organismo competente para promover, vigilar y dirigir el *Open Banking*. De acuerdo con la información proporcionada por el Banco Mundial[24], existen tres (3) tipos de formas de gobierno:

a. El modelo implementado por México o la Unión Europea, en el que la promoción, vigilancia y dirección es encargada a un organismo regulador. En el caso de México es la Comisión Nacional Bancaria y de Valores, mientras que en la Unión Europea es el regulador de cada país (por ejemplo, en España es el Banco de España). Es un modelo rápido y confiable, aunque se requiera recursos públicos para su implementación. Chile ha seguido esta línea, pues asignó a la Comisión para el Mercado Financiero (regulador

[22] Este es el caso de la *Fintech "Kambista"*, empresa especializada en el servicio de cambio de divisas. Esta empresa suscribió una alianza estratégica con Interbank, a fin de facilitar el proceso de apertura de una cuenta en la entidad bancaria, lo cual constituye una necesidad en un servicio de cambio de divisas digital.

[23] PLAITAKIS, A., & STASCHEN, S. (2020). Open Banking: how to designs for financial inclusion. Washington: Consultative Group to Assist the Poor.

[24] ALIÑO, NURIA (2022). *Hacia un marco de Open Finance*. Lima: Grupo Banco Mundial.

bancario) la competencia para regular y supervisar el cumplimiento de la normativa sobre finanzas abiertas.

b. El modelo implementado por un organismo de la industria: este es el caso de Nueva Zelanda en el que se creó un *API Centre*, y una entidad denominada *Payments NZ*, las cuales coordinan la promoción, vigilancia y dirección del *Open Banking*. Es también un modelo que se caracteriza por ser rápido, contiene estándares y procedimientos; sin embargo, se advirtió que los terceros proveedores de soluciones financieras (*Fintech*) no tienen una participación. En el caso de Brasil se trata de una entidad financiada y gobernada por el sector privado, la cual es supervisada por el Banco Central.

c. Una nueva entidad pública: esta fue la fórmula implementada por el Reino Unido cuando crea la OBIE (*Open Banking Implementation Entity)*, la cual es gobernada por la *Competition and Market Authority*, y financiada por los nueve bancos más grandes del país. Se ha observado que la implementación del *Open Banking* se realiza de forma más técnica, aunque toma un poco más de tiempo.

Como puede advertirse, en algunos casos la entidad a cargo de implementar el *Open Banking* es el regulador bancario, mientras que en otros casos es la autoridad de la competencia. Se ha podido advertir que incluso se ven involucrados las autoridades nacionales de protección de datos personales en el campo que les corresponde.

En la práctica puede ocurrir que la implementación del *Open Banking* deba ser vigilada no sólo por el organismo especializado en materia bancaria, sino también por la entidad a cargo de la protección de datos personales, por los riesgos que se generan respecto de la data de los clientes. Como veremos más adelante, en el caso peruano se deberá considerar un grupo de entidades públicas que deberán coordinar sus actuaciones, a fin de alcanzar los objetivos públicos propios de las finanzas abiertas.

ii. Sobre el modelo más adecuado: una revisión sobre la experiencia comparada

En la actualidad se han identificado dos modelos para la implementación del *Open Banking:* obligatorio o voluntario. En algunos países como Colombia[25] decidieron observar de cerca el desarrollo de la industria, a través de un régimen de *sandbox*, el cual les permitirá tomar una decisión sobre el enfoque exigido **a posteriori.**

En el modelo voluntario existe absoluta libertad por parte de las entidades del sistema financiero y los terceros proveedores de soluciones financieras para el desarrollo del *Open Banking*, con lo cual no existe barreras de acceso o permanencia en el mercado, sin perjuicio de lo cual el regulador puede aprobar directrices o

[25] PUENTES TRUJILLO, L. V., & AMAYA OSORIO, L. (2022). *Open Data y open banking: el derecho en el contexto de los mercados digitales. Un modelo regulatorio por definir en el ordenamiento jurídico colombiano*. Revista Chilena de Derecho y Tecnología, 11(2), pp. 211-244.

lineamientos referenciales para encaminar la industria. Bajo esta perspectiva (visión de la industria), el *Open Banking* se desarrolla en función de la evolución del mercado, es decir, atendiendo a la necesidad de las entidades financieras de compartir información con los terceros proveedores de soluciones por motivos de innovación tecnológica, o para expandir el alcance de sus servicios. Este es el caso de Estados Unidos, Canadá y Nueva Zelanda, quienes han decidido dejar en manos del mercado el desarrollo del *Open Banking*. Por su parte, en Singapur y Hong Kong el modelo es voluntario, pero se brindaron ciertas pautas para su implementación con guías técnicas sobre seguridad y modelos de gobierno.

En el modelo obligatorio la regulación exige a las entidades financieras que compartan la data de sus clientes con los terceros proveedores de soluciones financieras. Este modelo fue adoptado por la Unión Europea (2015) y el Reino Unido (2016), con algunos matices. Por ejemplo, en el Reino Unido se exigió el cumplimiento de este régimen -en una primera etapa- a los nueves bancos más grandes, además de crearse un organismo especializado (*Open Banking Implementation Entity, "OBIE"* por sus siglas) y fijarse estándares técnicos para la transmisión de la información. Por su parte, en la Unión Europea se aplicó a todas las entidades financieras y los estándares técnicos no fueron fijados por la autoridad, sino por la propia industria.

La principal resistencia a un modelo obligatorio obviamente son las entidades bancarias que custodian o gestionan la información del cliente por dos razones básicamente: (i) deben compartir la información de sus clientes, lo cual implica que terceros pueden ofrecer servicios más atractivos o competitivos en términos de precio y calidad; y, (ii) las cargas que impone la regulación para la implementación del *Open Banking*, tales como el desarrollo, gestión y mantenimiento de las interfaces de programación de aplicaciones (APIs) para permitir la interoperabilidad con terceros.

Una mención especial merece el caso chileno, que mediante Ley N° 21521 del 03 de enero de 2023, que promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros (denominada Ley Fintec), aprobó un régimen jurídico especial para incentivar la prestación de servicios financieros a través de medios tecnológicos (sistema de finanzas abiertas). Esta norma establece un régimen obligatorio de **finanzas abiertas** a las instituciones proveedoras de información, que incluye a los bancos, emisores de tarjetas de créditos, tarjetas de pago con provisión de fondos, entre otras.

Finalmente, en términos de modelos, es saludable promover el *Open Banking,* incluso, desde una perspectiva programática como en el caso colombiano, en el que se incluyó dentro de los objetivos del Plan Nacional de Desarrollo 2022-2026 el desarrollo del *Open Data,* a partir del cual se promoverá que las entidades estatales y las empresas brinden acceso y suministren toda aquella información que pueda ser empleada para facilitar el acceso a productos y servicios financieros.

iii. Las entidades obligadas a compartir información de sus clientes

Este acápite parte de la premisa de la implementación de un modelo obligatorio. En este punto, tenemos dos experiencias. La primera es la propuesta del Reino Unido, que fue seguida por el Banco Central de Brasil, que en una etapa inicial sólo aplicó el régimen de *Open Banking* a algunas instituciones importantes de su ecosistema financiero, siendo voluntario para los demás. Por otro lado, tenemos el esquema implementado por la Unión Europea o México, en los que la obligación se extiende a todas las entidades que custodian o administran la información financiera de sus clientes.

Los criterios que pueden utilizarse para definir a las entidades que deben compartir la información de sus clientes dependerá de la profundidad, enfoque o alcance del régimen que pretenda implementarse. En este momento es que debe decidirse si se pretende implementar un modelo de *Open Banking* o se prefiere un régimen de *Open Finance*, o incluso uno de *Open Data* dirigido a determinados sectores (por ejemplo, que incluya a las empresas proveedoras de servicios públicos, *fintechs,* empresas de *retail* que prestan servicio de crédito, entre otros).

Por ejemplo, en el caso chileno[26] se ha cubierto principalmente a todas las entidades que componen el sistema financiero. Además de los bancos, se han incorporado a los operadores de tarjetas de pago autorizados, las cooperativas de ahorro y crédito fiscalizadas por el regulador, los agentes administradores de mutuos hipotecarios, corredores de bolsa, administradores de cartera, entre otros. La Comisión del Mercado Financiero podrá ampliar esta lista, sin embargo, en principio no se incluye a entidades fuera de su ámbito de acción.

Otro de los aspectos que debe considerarse es analizar si todas las entidades bancarias pueden implementar los mecanismos exigidos para la transmisión de la información, así como su mantenimiento (como veremos más adelante, en oportunidades se trata de herramientas de costosa implementación, a fin de garantizar la seguridad de la información). En ese orden de ideas, también debe advertirse si el impacto de la medida en las entidades bancarias más pequeñas justifica la carga regulatoria que deberán soportar.

iv. Los riesgos asociados al *Open Banking*

En este acápite queremos plantear algunas notas introductorias sobre los riesgos asociados al *Open Banking*. Es indiscutible el escenario de riesgos al que se exponen los clientes y las entidades financieras cuando se permite que terceros proveedores de soluciones tecnológicas puedan acceder a la información y a sus sistemas, incluso con su consentimiento. Nos referimos a riesgos vinculados con la ciberseguridad, interoperabilidad entre las entidades financieras y el tercero

[26] Véase el artículo 18 de la Ley Fintec chilena.

proveedor, el uso indebido de la información personal del cliente, o la ejecución de operaciones no reconocidas o fraudulentas[27].

En primer lugar, nos debemos referir a la protección de la información personal del cliente. En este ámbito se debe procurar que el consentimiento del titular de los datos personales se realice, conforme lo exige el ordenamiento jurídico vigente[28], es decir, debe ser previo, informado, expreso e inequívoco. En ese sentido, el mecanismo que se plantea para requerir el consentimiento del titular de la información debe cumplir esta exigencia.

En este ámbito también debe procurarse que la información sólo pueda ser utilizada para los fines expresamente autorizados por el titular de la data. Asimismo, deberá especificarse quiénes pueden ser los destinatarios de la información, así como si se almacenara en un banco de datos[29]. Todas estas exigencias representan un riesgo de cumplimiento que debe ser dimensionado al momento de implementar un régimen de *Open Banking*. Por tratarse de un nuevo enfoque sería de utilidad ratificar la competencia de la Autoridad Nacional de Protección de Datos Personales en este ámbito, así como de la aplicación de la normativa especial.

En segundo lugar, se advierten problemas vinculados a la ciberseguridad. Como ha explicado Puentes y Amaya[30], la indispensable interoperabilidad entre las plataformas de las entidades financieras y los terceros proveedores de soluciones financieras ha provocado la aparición de puntos débiles en la seguridad de la red de las entidades que custodian o administran la información de los clientes. Esta situación exige un rol más activo de las entidades financieras -principalmente-, a fin de no perder la confianza del público sobre los beneficios de la banca digital. En este contexto aparece la necesidad de contar con interfaces de programación de aplicaciones (APIs) que garanticen un acceso seguro y acotado a la información administrada por la entidad financiera, y que se valide la capacidad del tercero proveedor para poder implementar y cumplir estos estándares. Para ello, se plantean soluciones como exigir un tipo de certificación privada o pública.

Como explica la Alianza Fintech del Pacífico[31], en este ámbito es importante establecer dos tipos de directrices de seguridad, como mínimo: (i) primero: aquellas que garanticen conexiones seguras; y, (ii) segundo: aquellas que establezcan procesos de captura y gestión de los consentimientos explícitos de los usuarios para poder acceder a sus datos. Por ejemplo, respecto del perfil de

---

27 Tanto la SBS como el MEF han llamado la atención de estos riesgos al momento de analizar el Proyecto de Ley N° 1584/2021-CR, que más adelante analizaremos a detalle.

28 Ley N° 29733, Ley de Protección de Datos Personales. El numeral 13.5 del artículo 13° de la Ley establece que "*los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco*".

29 Ley N° 29733, Ley de Protección de Datos Personales. Artículo 18° derecho de información del titular de los datos personales.

30 PUENTES TRUJILLO, L. V., & AMAYA OSORIO, L. (2022). *Open Data y open banking: el derecho en el contexto de los mercados digitales*; op. cit. (…); pp. 234.

31 Alianza Fintech del Pacífico. (2023). *Estándares Open Finance como palanca de conversión regional*. Santiago de Chile: Alianza Fintech del Pacífico.

seguridad para gestionar los consentimientos de forma segura y ordenada, a la fecha se cuenta con una propuesta denominada **perfil de seguridad de *Financial-grade API (FAPI)***[32], que fue planteada por el grupo de trabajo *Open ID Foundation*. Esta herramienta garantiza el cumplimiento de los estándares de seguridad más altos, con lo cual se resguarda la confidencialidad, integridad y disponibilidad de los datos.

De forma referencial, debemos indicar que, en Perú, la Superintendencia de Banca, Seguros y AFP aprobó el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, mediante Resolución SBS N° 504-2021, el cual desarrolla -entre otros aspectos- el uso de interfaces de programación de aplicaciones (APIs) y disposiciones vinculadas sobre ciberseguridad. Esta medida es prospectiva y se adecúa al escenario de disrupción tecnológica que vivimos, la cual más adelante analizaremos.

En tercer lugar, advertimos el riesgo de realización de operaciones no reconocidas o fraudulentas, que desarrollaremos más adelante. Basta con decir en este punto que corresponde implementar mecanismos de autenticación reforzada del cliente, así como canales de denuncia rápida ante episodios de pérdida, robo u operaciones no reconocidas.

v. El mecanismo para compartir información: aspecto clave para la seguridad del *Open Banking*

Uno de los elementos claves en la implementación del *Open Banking* es determinar el tipo de mecanismo para la transmisión de la información de forma segura y eficiente. En el ámbito de la protección de datos personales, este asunto está vinculado con el ejercicio del derecho a la **portabilidad de los datos**, es decir, aquella facilidad para transferir la información del cliente sin la necesidad de volver a registrarla, para su posterior reutilización.

Actualmente, las empresas que requieren la información de un determinado cliente utilizan herramientas como el *screen-scraping*[33] (también conocida como **captura digital de datos**) o el *reverse engineering*[34] para acceder a los datos

---

32 Utiliza el *Outh* 2.0 y *OpenID Connect (oidc)* como base y define requisitos técnicos adicionales para el sector financiero y otros sectores que requieren una mayor seguridad de las APIs. FAPI no sustituye a otros estándares como OAth2 y OpenID Connect, sino que, introduce controles más rigurosos que obligan a realizar acciones de seguridad adicionales. Alianza Fintech del Pacífico (2023).

33 De acuerdo al BIS, la práctica del screen scraping se puede explicar en los siguientes términos: *The practice of screen scraping, a form of extracting data from websites, first began as manual copying-and-pasting and evolved into an automated process. To collect customer-permissioned data from banks, screen scraping methods require that a customer provides the third party with their authentication credentials (eg username and password) that the customer uses to log into their bank's internet banking website*. Comité de Basilea en Supervisión Bancaria. (2019). *Report on open banking and application programming interfaces*. Basilea: Banco Internacional de Pagos; pp. 9.

34 El BIS también describe el *reverse engineering* en los siguientes términos: *The practice of reverse engineering, decompiles the code of the mobile banking applications to figure out which information is exchanged between the application and the banks' servers (through the non-public API) and subsequently build a 'reverse engineered' version of the mobile application which is capable of directly exploiting the communication from and to the banks' servers. It requires a second enrolment of a mobile application (in this case the reverse engineered version) upon receipt of the customer's authentication credentials and the*

administrados por sus respectivas entidades financieras, lo cual ha sido calificada como una práctica poca segura (principalmente el acceso a cuentas o servicios de crédito). El Comité de Basilea en Supervisión Bancaria[35] explica que ambas técnicas son inseguras, en la medida de que el tercero proveedor de soluciones financieras mantiene la información de las credenciales del cliente y con ello acceso total a sus cuentas, incluyendo -por ejemplo- la posibilidad de realizar operaciones o cargos no autorizados, así como cambiar datos sensibles en la configuración de la cuenta. Esta situación puede dificultar las labores de las entidades financieras para identificar transacciones fraudulentas, así como distinguir cuando una operación es aprobada directamente por el cliente, o a través de un proveedor de servicios de pago.

Sin perjuicio de ello, queremos rescatar algunos aspectos positivos del uso de este tipo de técnicas de **captura digital de datos**, que probablemente justificaron los avances de las finanzas abiertas en Europa y América Latina[36]:

a. Muchos proveedores de servicios de captura digital de datos mantienen estándares de seguridad de nivel bancario, por lo que se limita el riesgo de fraude a los consumidores.

b. El impacto positivo del uso de la captura digital de datos se manifiesta con la aparición y desarrollo de emprendimientos digitales que hoy en día han cambiado muchas industrias como las plataformas de *streaming*, servicios de transporte, servicios de comida, entre otros.

c. No hay pruebas significativas de que se produzcan perjuicios para los consumidores o violaciones de la seguridad como resultado del uso de estas técnicas.

d. Las técnicas de captura digital de datos no podrán ser sustituidas fácilmente, o a corto plazo, por la implementación de APIs, debido a los costos que generará para los principales involucrados.

e. De hecho, la *Select Committee on Australia as a Technology and Financial Centre* emitió un reporte en abril del año 2021, en el que abordó el tema de los mecanismos de captura digital de datos y su impacto en el desarrollo del *Open Finance*[37], concluye que (a pesar de la existencia de variados

subsequent use of these credentials or even the creation of a proprietary set of authentication credentials (to the third party). This technique is often favored by data aggregators over screen scraping because it is much more scalable and robust as its performance is not influenced by changes made by banks to their customer interface. Comité de Basilea (2019). *Report on open banking and application programming interfaces*; op. cit. p. 9.

35 Comité de Basilea (2019). *Report on open banking and application programming interfaces*; op. cit. pp. 9.

36 Alianza Fintech del Pacífico. (2023). *Estándares Open Finance como palanca de conversión regional*. Santiago de Chile: Alianza Fintech del Pacífico.

37 Este organismo fue designado por el Senado de Australia para revisar el tamaño y alcance de las oportunidades para los consumidores australianos respecto del desarrollo de las tecnologías financieras y regulatorias. Por su parte, el reporte abordó el ejercicio del derecho de autodeterminación informativa del consumidor, y contó con la participación de reguladores

argumentos en contra, que hemos explicado) no es pertinente una prohibición de este tipo de prácticas, pues permiten que las empresas sigan innovando e incentiven el proceso competitivo en el mercado financiero.

Sin perjuicio de lo anterior, y considerando el inminente escenario de riesgos de ciberseguridad, aparecen las interfaces de programación de aplicaciones (APIs), las cuales deben garantizar la interoperabilidad entre los sistemas de almacenamiento y transferencia de datos empleados por cada una de las entidades financieras y las plataformas de las entidades y terceros interesados en la información. Las APIs son mecanismos adecuados para que los sistemas de dos o más entidades independientes puedan interoperar y se facilite la entrega de información, en términos de rapidez, seguridad y eficiencia. Desde un punto de vista jurídico, las APIs viabilizan el ejercicio del derecho a la **autodeterminación informativa**, en su manifestación del derecho a la portabilidad de datos, pues habilitan un formato estándar o compatible que permite la transmisión de la información entre distintos agentes, sin la necesidad de reingresar la información.

Las APIs pueden ser definidas como herramientas informáticas que habilitan a dos o más sistemas para interoperar o comunicarse entre sí. Están compuestas por un grupo de conceptos y protocolos que son empleados para desarrollar e integrar el *software* de las aplicaciones, lo cual permite que dos o más aplicaciones puedan interrelacionarse para cumplir una o varias funciones. Es una especie de **intermediario** entre dos sistemas, que viabiliza la comunicación entre aplicaciones independientes. Si bien es cierto existen otras formas de compartir información, las APIs son herramientas que garantizan la seguridad, escalabilidad y flexibilidad; asimismo, su arquitectura les permite atender las necesidades del cliente, actualizarse o incluso reemplazarse[38].

El tema de la **apificación** es uno de los aspectos más resaltantes en el ámbito del *Open Banking*, lo cual siempre se ha justificado en la seguridad necesaria para la transmisión de la información. Las APIs proporcionan un mecanismo seguro para interconectar dos sistemas, a través de reglas y controles que garantizan el uso de la información del cliente en los términos en que autorizó. De hecho, la Unión Europea desde septiembre de 2019 prohibió el uso de herramientas como el *screen scraping* para acceder a la información de los clientes. En Chile también se consideró un modelo de **apificación** obligatoria, aunque no advertimos prohibiciones radicales con el uso de los mecanismos de captura de datos digital.

De acuerdo a los expertos[39], existen tres tipos de API actualmente:

a. APIs privadas: son utilizadas por desarrolladores al interior de una organización, a fin de integrar sus propios sistemas.

financieros, de competencia y de protección al consumidor, incumbentes, entrantes de la industria financiera.

38 AZAR, K., y otros (2021). *Banca abierta: lecciones, desafíos y oportunidades para América Latina*; op. cit., pp. 9.

39 ALIÑO, N. (2022). *Hacia un marco de Open Finance; op. cit.; y AZAR, K., y otros (2021).* Banca abierta: lecciones, desafíos y oportunidades para América Latina.

b. APIs abiertas: son empleadas para viabilizar la comunicación e integración de empresas con la que se tiene un acuerdo comercial. Este es el caso de las entidades financieras que crean portales de desarrolladores en las que se pone a disposición del público en general las APIs, a fin de que otras empresas puedan integrarse eficientemente (caso Interbank en Perú, el BBVA en México y España, el BCP en Bolivia).

c. APIs públicas: este tipo de herramientas se ponen a disposición de cualquier organización, sin la necesidad de suscribir un contrato o mantener una relación comercial, y tiene por objeto transmitir información y funcionalidades de uno o varios sistemas y aplicaciones de la empresa, a fin de que terceros puedan interoperar.

Asimismo, la demanda por APIs ha generado un nicho de mercado para la aparición de los denominados **agregadores de APIs** (una especie de *hub* de APIs), que son empresas que ofrecen APIs a terceros, de forma tal que la integración o interoperabilidad se materializa sin que la entidad financiera desarrolle sus propias APIs (este es el caso, por ejemplo, de *Prometheo Open Banking*[40] o SIBS[41]). En estos casos no estamos frente a APIs abiertas, sino más bien a desarrollos *ad hoc* a cargo de empresas especializadas que conocen la forma de **apificarse** con las entidades del ecosistema financiero. Un tema importante es que el tercero que pretende acceder a la información de la entidad financiera es quien sostiene una relación con el **agregador de APIs**, quien se compromete a cumplir con la regulación aplicable, como los protocolos de autenticación del cliente, el tiempo y forma de los accesos.

De acuerdo a lo expuesto, cada jurisdicción debe tomar una decisión sobre la base de los siguientes modelos: (i) voluntario sin estándares de comunicación; (ii) voluntario con estándares API; (iii) obligatorio sin estándares de comunicación; o, (iv) obligatorio con estándares API. Es muy importante diferenciar cuándo estamos frente a un modelo que fija estándares API, y cuando se implementan guías de instrucción, las cuales no aportan un detalle técnico, sino un parámetro de funcionamiento.

Como explica la Alianza Fintech del Pacífico[42], es recomendable establecer directrices y especificaciones básicas para las APIs de *Open Finance*, a fin de garantizar interacciones seguras entre los terceros proveedores de soluciones tecnológicas y las entidades que custodian la información de los clientes. Dentro de las principales áreas encontramos las siguientes:

---

40 Esta plataforma de *Open Banking* brinda acceso a información bancaria e iniciación de pagos en 10 países.

41 Es una empresa creada en Portugal la cual ha creado un *Marketplace* donde los usuarios pueden encontrar nuevos servicios y los bancos pueden compartir sus aplicaciones. Interconecta comercios y entidades financieras, para lo cual procura tener una relación comercial con los custodias o administradores de la información.

42 Alianza Fintech del Pacífico. (2023). *Estándares Open Finance como palanca de conversión regional*. Santiago de Chile: Alianza Fintech del Pacífico.

a. Especificaciones para APIs de lectura y escritura: este tipo de interfaces permite a los terceros proveedores acceder a la información del cliente no sólo para revisar sus movimientos o información personal, sino también efectuar pagos autorizados.

b. Especificaciones para APIs de datos abiertos: esta herramienta te permite acceder, de forma segura, a los datos públicos disponibles, tales como ubicación de los cajeros automáticos, sucursales o información sobre productos. No cubre la transferencia de datos sensibles.

c. Marco de confianza: se trata de establecer un protocolo para confirmar la identidad de los terceros proveedores de soluciones tecnológicas que podrán acceder a la información de los clientes. En este ámbito se ha sugerido la implementación de un directorio (que involucra un análisis *ex ante* de cada uno) o certificaciones de las propias entidades que administran o custodian la información.

d. Registro dinámico de clientes: este mecanismo debe permitir a los terceros proveedores de soluciones tecnológicas obtener, de forma segura, las credenciales necesarias a los datos de la cuente del cliente.

Por su parte, como lo indica el BIS[43], la principal desventaja de exigir la implementación de APIs en el *Open Banking* es la inversión en términos de tiempo y dinero que se tiene que realizar para crear y mantener una API, particularmente en esquemas donde no se ha estandarizado el lenguaje y se requiere de acuerdos comerciales. Tómese en cuenta también el impacto de estos costos para pequeñas instituciones financieras para desarrollar APIs y mantenerlas.

Por ejemplo, en la Unión Europea se implementó un modelo obligatorio de *Open Banking*[44], sin embargo, sus normas de desarrollo brindaron mucha flexibilidad a los Estados Miembros para establecer los estándares de comunicación segura a través de APIs. Esto conllevó algunas dificultades (problemas de coordinación) y resistencias por parte de las entidades financieras que custodian o administran la información de los clientes, y no lograron ponerse de acuerdo con los terceros proveedores de soluciones financieras para aplicar una determinada API. Esta situación se quiso revertir con alternativas impulsadas por el sector privado para presentar un estándar de la industria como es el estándar *Berlin Group*, lo cual tampoco garantizó la armonización.

Por su parte, el Reino Unido, a través de la OBIE, estableció un estándar API (a través de diccionarios de datos[45], lineamientos de arquitectura[46], lineamientos de

43 Comité de Basilea en Supervisión Bancaria. (2019). *Report on open banking and application programming interfaces.* Basiela: Banco Internacional de Pagos; pp. 6.

44 A través de la Directiva N° 2015/2366 sobre servicios de pagos en el mercado interior, la cual fue desarrollada en ese extremo por el Reglamento Delegado (UE) 2018/389 de la Comisión Europea, en virtud del cual se aprobaron normas técnicas de regulación para la autenticación reforzada de clientes y unas guías de comunicación abiertas, comunes y seguras.

45 Descripción estándar de la información.

46 Especificaciones sobre el diseño de la API.

seguridad de la información[47]), lo cual facilitó su implementación y provocó un desarrollo inicial del *Open Banking* cuya evidencia consta en los servicios ofrecidos en dicha jurisdicción gracias a este enfoque[48]. En Japón también se han documentado problemas en el desarrollo del *Open Banking*, producto de la falta de un estándar y la dificultad para alcanzar acuerdos entre la industria financiera tradicional y los terceros proveedores de servicios que requerían información de sus clientes[49]. La estandarización de las API puede generar un proceso de implementación más rápido y pueden beneficiar a las entidades financieras más pequeñas e incluso a los terceros proveedores de soluciones financieras.

Sin perjuicio de los beneficios que pueda generar la estandarización de las APIs, es necesario recapitular las dos desventajas identificadas: (i) primero: las APIs pueden perder flexibilidad o adaptabilidad al desarrollo tecnológico si se fijan expresamente en una norma; y, (ii) segundo: que la infraestructura tecnológica de algunas instituciones financiera no está preparada para la creación de APIs, por lo cual aún se prefiere soluciones como el *screen scraping*.

vi. Los terceros proveedores de soluciones financieras a quienes se les debe permitir el acceso a la información

En este ámbito se han planteado varias soluciones, tales como la exigencia de un registro o autorización a cargo de la autoridad competente, o que las entidades financieras sean quienes acrediten la idoneidad del tercero proveedor de soluciones, o esta situación se sujete al acuerdo entre las partes. El propósito de este control es acreditar que los terceros proveedores cuenten con los mecanismos de seguridad e interoperabilidad necesarios para enlazarse con las entidades que custodian o administran la información de los clientes, como explicaremos.

No obstante, de acuerdo al BIS[50], en un estudio realizado a 17 países, la mayoría no exige la obtención de un registro o autorización para que los terceros puedan acceder a los datos del cliente, por lo cual se siguen utilizando herramientas como el *screen scraping* o el *reverse engineering*.

Claramente, la herramienta más restrictiva es exigir un registro o autorización previa a los terceros proveedores para poder acceder a la información de los clientes a través de APIs. El objetivo de esta exigencia es que la autoridad corrobore el cumplimiento de una serie de requisitos que se consideren necesarios para la adecuada protección del interés público, cuyo cumplimiento le corresponde supervisar. Este es el caso del Reino Unido (cuyo registro es administrado por la OBIE), la Unión Europea (a través de la Autoridad Bancaria Europea y cada organismo regulador competente en el país miembro), Australia (por medio de la *Australian Competition and Consumer Commission*), Brasil (a cargo del Banco Central

47 Lineamientos de seguridad de la información.

48 Plaitakis, A., & Staschen, S. (2020). *Open Banking: how to designs for financial inclusión*; op. cit.; pp. 20

49 *Idem.*

50 Comité de Basilea en Supervisión Bancaria. (2019). *Report on open banking and application programming interfaces*. Basiela: Banco Internacional de Pagos; pp. 12-13.

de Brasil), o recientemente el caso chileno a través de la Comisión del Mercado Financiero.

Principalmente nos referimos a requisitos vinculados con los protocolos de seguridad de la información con que debe contar el tercero proveedor de servicios, requisitos de ciberseguridad, o los acuerdos que debe mantener con las entidades financieras para el intercambio de información. En este extremo, es necesario preguntarnos ¿es lo más adecuado exigir un registro o autorización previa para acceder al mercado? ¿cuáles son las ventajas que se obtendrían con esta exigencia? ¿No se estaría desincentivado el crecimiento del *Open Banking* a propósito de la seguridad en la transmisión de la información que se pretende obtener? El impacto de la regulación en el desarrollo de la industria debe tomarse en consideración, más aún si se considera que su evolución aún es incipiente.

Una alternativa es que los terceros proveedores de soluciones financieras deban celebrar contratos o acuerdos con las entidades bancarias que administran o custodian la información, quienes deberán velar por el cumplimiento de los estándares mínimos en materia de ciberseguridad, protección de datos personales, continuidad operativa, entre otros aspectos que pueda definir el regulador. Es decir, las entidades bancarias deberían hacer cumplir la ley, y en caso de controversia debería participar el regulador (una estrategia muy parecida a la interoperabilidad implementada por el Banco Central de Reserva del Perú, la cual está acompañada de un régimen sancionador en caso de negativa de la entidad bancaria para brindar facilidades para la interoperabilidad[51]).

En le legislación nacional cabe observar lo planteado por el artículo 22° del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad (aprobado por la SBS), el cual exige que, en el caso de servicios provistos por terceros en aspectos referidos a la gestión de tecnología de la información, gestión de seguridad de la información o procesamiento de datos, la empresa del sistema financiero deberá evaluar las amenazas y vulnerabilidades de seguridad de la información e implementar medidas para su tratamiento. En esa línea, se exige que vía contractual se establezcan este tipo de obligaciones, así como los roles y responsabilidades.

vii. Contraprestación por el desarrollo y mantenimiento de las APIs

No todos los esquemas de *Open Banking* han sido diseñados tomando en cuenta su sostenibilidad. Uno de los aspectos que la regulación debe definir, en caso se quiera intervenir, es confirmar (o no) que el desarrollo y mantenimiento de las APIs deban ser cobrados a los clientes o terceros proveedores de servicios que pretenden interconectarse con los administradores de la información de los clientes. Es un tema bastante discutible, pues -desde la perspectiva de la protección de datos personales- el cobro por el ejercicio del derecho a la portabilidad de datos debe ser residual o excepcional, siendo la gratuidad la regla, en tanto la

[51] Nos referimos a la Circular N° 024-2022-BCRP, Reglamento de Interoperabilidad de los Servicios de Pago provistos por los Proveedores, Acuerdos y Sistemas de Pagos.

razonabilidad es establecer procedimientos sencillos para el ejercicio de los derechos de acceso a la información propia[52].

Como hemos explicado, las APIs abiertas y públicas facilitan la interoperabilidad entre plataformas, al igual que los **agregadores de API** que son organizaciones especializadas en tender el puente entre las entidades financieras y los terceros proveedores de soluciones financieras. En este contexto es lógico que el desarrollador y administrador de la API deba realizar una inversión que merezca ser recuperada. En el caso de las APIs abiertas y públicas, la inversión usualmente es realizada por la entidad financiera que custodia o administra la información de los clientes; mientras que en el caso de los **agregadores** se trata de empresas independientes de la entidad que custodia la información.

Como explicamos, en Japón hubo problemas en la implementación del *Open Banking,* pues las entidades financieras y los terceros proveedores de soluciones financieras no pudieron cerrar los acuerdos de servicio de lectura de datos, principalmente por asuntos vinculados a las tasas que se deberían cobrar a los usuarios finales por las API. Independientemente del esquema que se elija (si se cobra al tercero proveedor del servicio o al cliente), el cobro de una contraprestación para acceder a la información del cliente, o poner a disposición del tercero la información, es un asunto que merece ser discutido, pues puede constituirse en una barrera para la implementación del *Open Banking*.

Desde el punto de vista de la protección de datos personales, como hemos mencionado, en principio no se puede cobrar por atender las solicitudes de acceso, menos aún por implementar mecanismos como APIs para automatizar su atención; sin embargo, es preciso resaltar que la normativa no se diseñó para atender modelos como el *Open Banking,* por lo cual estamos de acuerdo con lo explicado por Bolaños[53], quien justifica un eventual cobro de una tarifa adicional siempre que se acredite la existencia de una inversión adicional que deba realizarse para atender las solicitudes de acceso.

De acuerdo al BIS[54], en la mayoría de las jurisdicciones no se establecen restricciones para que las entidades financieras que custodian o administren la información pueden cobrar tarifas a los terceros proveedores por compartir información de los clientes. De hecho, en algunos países como Brasil, Hong Kong, México y Singapur la normativa expresamente autoriza a las empresas financiera a cobrar tarifas por compartir la información de sus clientes a los terceros proveedores.

Hay dos casos particulares que nos gustaría comentar. El primero es el mexicano, pues la normativa estableció un control de las tarifas que cobran las entidades

52 BOLAÑOS VAINTEIN, G. (2022). *La incorporación del derecho a la portabilidad de datos personales en el ordenamiento jurídico peruano*. Lima: Tesis para optar por el título de abogado en la Universidad de Lima.

53 *Idem.*

54 Comité de Basilea en Supervisión Bancaria. (2019*). Report on open banking and application programming interfaces*. Basiela: Banco Internacional de Pagos; pp. 16-17.

financieras a los terceros proveedores de soluciones financieras. Cabe indicar que existen posiciones más radicales en el sentido de prohibir el cobro por la posición dominante de las entidades bancarias que custodian o administran la información[55]. En los demás casos se observa la adopción de esquemas basados en acuerdos bilaterales (Hong Kong), o multilaterales (en Brasil se hace a través de un comité organizado por empresas privadas).

El segundo caso es el chileno, en el que expresamente se ha proscrito que las instituciones proveedoras de información realicen cobros a los proveedores de servicios basados en información por concepto de transmisión de la información[56]. Sólo se podrá reconocer o reembolsar los costos incrementales directos en que incurran, los cuales deberán fijarse sobre la base de condiciones públicas, objetivas, equitativas y no discriminatorios. La norma chilena tampoco permite el reembolso de los costos asumidos por las entidades bancarias por el desarrollo y mantenimiento de las interfaces de aplicaciones por parte de los terceros proveedores de soluciones tecnológicas. Finalmente, para cerrar el círculo, se prohíbe que las entidades proveedoras de la información realicen algún cobro de comisiones o cobros adicionales a los clientes.

En nuestro caso, el ordenamiento jurídico peruano no permite la fijación de precios o tarifas, salvo en el caso de los servicios públicos, declarados como tal por una ley expresa[57]. En esa línea, lo que sí puede exigirse es que la contraprestación sea transparente, no discriminatoria y refleje la prestación efectiva de un servicio.

Desde nuestro punto de vista, ante la prestación efectiva de un servicio (como es el caso de poner a disposición de terceros un API para compartir la información de miles clientes, a fin de crear productos o servicios adecuados a sus necesidades) es indispensable una inversión de recursos (no sólo para desarrollar el API, sino también para mantenerla), por lo cual nos parece que una postura como la chilena podría contravenir nuestro ordenamiento jurídico, en tanto se estaría fijando precios vía normativa (en este caso como un servicio gratuito o precio cero). No estamos defendiendo una posición como la implementada en Japón (en la que se cobrara al titular de los datos), sino más bien que se evalúe la participación de los terceros proveedores de soluciones tecnológicas, máxime si cobran por algunos servicios que ofrecen sobre la base de esta información.

viii. El tipo de información que se debe compartir y la implementación progresiva del *Open Banking*

55 PUENTES TRUJILLO, L. V., & AMAYA OSORIO, L. (2022). *Open Data y open banking: el derecho en el contexto de los mercados digitales* (…); op. cit., pp. 229-230. Sobre el particular se ha dicho que 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.

56 Véase el artículo 25° de la Ley Fintec chilena.

57 Artículo 4 del Decreto Legislativo N° 757.

Debemos partir de la premisa de que la información es de titularidad de las personas naturales, por ende, -si lo creen conveniente a sus intereses- podrán compartir toda su información con terceros, y por ende las empresas o entidades que custodian o administran esa información no tienen por qué negarse a proporcionarla. Como hemos mencionado, se trata del ejercicio del derecho fundamental a la **autodeterminación** informativa, que consiste en el reconocimiento de una serie de facultades atribuibles a una persona para ejercer el control sobre su información personal contenida en registros de todo tipo, así como para requerir y utilizar esta información, o permitir que terceros puedan acceder.

Sin embargo, lo que se propone con regímenes como el *Open Banking* es **optimizar** el ejercicio del derecho a acceder y utilizar la información personal por parte de terceros, a través de protocolos o herramientas de funcionamiento más rápido, seguro y eficiente. Para ello, se debe **seleccionar o priorizar** el tipo de información que será transmitida con estas facilidades, pues resultaría imposible implementar infraestructuras tecnológicas para el tráfico de toda la información disponible de los clientes, por los recursos que ello implica. En el caso de las finanzas abiertas, se priorizará la información más útil para la creación o mejora de productos financieros.

Sin perjuicio de ello, y de forma general, a continuación se describen los tipos de información que se suele compartir en un esquema de *Open Banking*, así como su utilidad para los terceros proveedores*:*

a. Información sobre cuenta corriente: a partir de esta data se puede determinar los hábitos de consumo de los clientes, y con ello se pueden crear soluciones para la administración de las finanzas de los clientes. No hay discusión sobre la posibilidad de compartir esta información, sin perjuicio de lo cual se requiere el consentimiento del titular.

b. Información transaccional: al igual que en el caso anterior, esta información es útil para crear soluciones que puedan optimizar el gasto de los clientes. En la experiencia revisada no hubo resistencia para compartir esta información, y también requiere el consentimiento del titular.

c. Credenciales de acceso: en casi todos los países consultados se exige compartir esta información, sin embargo, en el caso de México no se obligó a proporcionar este acceso. La información sobre las credenciales de identidad o acceso le permite al tercero proveedor de soluciones financieras iniciar una operación de pago en nombre del cliente. Este es uno de los supuestos de información más crítica, por ende, es clave el cumplimiento de los protocolos para obtener el consentimiento del titular.

d. Información sobre productos, servicios, cajeros automáticos, oficinas: se trata de información general de la entidad bancaria, lo cual tiene como efecto inmediato facilitar su acceso a los clientes. Este tipo de información no requiere el consentimiento del cliente, sólo un acuerdo con la entidad bancaria.

e. Verificación de la identidad: en este caso los terceros proveedores de soluciones solicitan acceder a una facilidad implementada por las entidades financieras, la cual regularmente implica una inversión de recursos importante.

En algunos países se ha decidió implementar este enfoque sobre la base de fases como es el caso de Chile (lo cual se encuentra en proceso de formulación) y Brasil, que lo han previsto ejecutar en tres etapas[58]. En la primera etapa del modelo brasilero el intercambio de información recaería en productos y servicios ofrecidos por las instituciones financieras, lo cual implica detallar los canales de acceso, las características de sus productos y servicios relacionados con las cuentas de depósito o pago, así como las operaciones de crédito. En la segunda etapa se decidió brindar información sobre datos de registro de sus transacciones relacionadas con las cuentas de depósito y pago, así como las operaciones de crédito. Finalmente, en la tercera etapa, se proporcionó información sobre las credenciales de acceso y el detalle de créditos.

Siguiendo la lógica planteada en la experiencia comparada, el régimen de *Open Banking* debe iniciar con el acceso a información general o pública de la entidad financiera como es la ubicación de las agencias o cajeros automáticos, o información sobre los productos que ofrece. Seguidamente, debería procederse a compartir la información menos sensible del cliente, por ejemplo, los datos del consumidor (identificación, dirección), la información de saldos de sus cuentas o créditos, información transaccional agregada o desagregada, los productos que mantiene con la institución bancaria. Finalmente, se debería compartir los accesos a la cuenta del cliente, a partir de la cual se pueden realizar operaciones a su nombre. Es un régimen progresivo, lo cual responde a los riesgos que cada fase implica, y los necesarios períodos de adecuación que se requieren.

ix. Responsabilidad ante fallos operativos o pérdidas del cliente (caso de iniciación de pagos)

Un aspecto importante que debe ponerse en agenda cuando se decida discutir la implementación del *Open Banking* es el régimen de responsabilidad aplicable a la entidad bancaria que custodia la información del cliente y el tercero proveedor que accede a ésta. Si bien es cierto en algunos supuestos será discutible la determinación del responsable del fallo operativo o de la realización de una operación no autorizada, incorrecta o fraudulenta (para el caso de servicios de pago, principalmente), esta indefinición no puede perjudicar al usuario y el ordenamiento jurídico debe prever mecanismos que lo solucionen.

En este ámbito se sugiere establecer procedimientos claros para la autenticación del cliente, manifestación del consentimiento y la realización de la operación. Debe definirse con claridad cuál es el alcance de responsabilidad del usuario y del proveedor del servicio. Por ejemplo, debe precisarse la oportunidad que tiene el

[58] AZAR, K., y otros (2021). *Banca abierta: lecciones, desafíos y oportunidades para América Latina*; op. cit., pp. 24.

usuario para comunicar una operación no autorizada o incorrecta; así como la obligación del proveedor de contar con un canal disponible para realizar este tipo de comunicaciones.

En caso el error no sea atribuible al usuario, debe definirse con claridad quién responde respecto del reembolso o reversión de la operación. Véase el caso de un error en el que el proveedor de servicios de administración de cuenta procesó una operación que originó un proveedor de servicios de iniciación de pagos, a pesar de que el cliente previamente había cumplido con comunicar el robo del instrumento de pago y sus respectivas credenciales de acceso. En este tipo de casos la regulación no puede condicionar el resarcimiento del daño generado a la definición sobre qué proveedor fue el responsable.

Por ejemplo, la Directiva 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior, estableció que en este tipo de casos la devolución la debe realizar **inmediatamente** el proveedor de servicios de pago gestor de cuenta (la entidad bancaria). La norma señala que, si el verdadero responsable de la operación de pago **no autorizada** es el proveedor de servicios de iniciación de pago, éste deberá resarcir al gestor de la cuenta. El **iniciador de pagos** tiene la carga de la prueba de acreditar que la operación se autenticó de forma correcta, y por ende no es responsable de la operación no reconocida por el cliente (artículo 73°).

En ausencia de regulación, en este ámbito es de gran utilidad los acuerdos comerciales entre los bancos y los terceros proveedores, pues en estos documentos se puede identificar a los responsables de los fallos operativos y eventuales pérdidas del cliente. El regulador debe vigilar de cerca los incidentes de seguridad que se generen para tomar acción en caso sea necesario. Por ejemplo, en el ámbito de la protección de datos personales hoy en día se viene exigiendo que este tipo de incidentes deban ser reportados a la autoridad competente.

En las jurisdicciones donde existe regulación, como es el caso de la Unión Europea, a los terceros proveedores se les exige mantener una póliza de seguro por daños a terceros o una garantía equivalente en activos líquidos, a fin de cubrir eventuales situaciones de perjuicio al cliente como transacciones no autorizadas o no completadas (en el caso de la **iniciación de pagos**). Asimismo, a las entidades financieras que administran o custodian la información de sus clientes se les exige un régimen de autenticación reforzada, cuyo incumplimiento les obliga a reembolsar al cliente el monto por operaciones no reconocidas o fraudulentas.

VI. Avances y comentarios sobre el *Open Banking* en Perú

i. Organismos encargados de la implementación y supervisión del *Open Banking*

Como ha podido advertirse a partir de una revisión del alcance, los riesgos y los regímenes jurídicos aplicables al *Open Banking* es que podemos determinar los organismos involucrados en la implementación y supervisión de este enfoque.

Sobre la base de las siguientes premisas es que realizaremos nuestro análisis: (i) en primer lugar, el *Open Banking* involucra un servicio complementario a la intermediación financiera tradicional; (ii) en segundo lugar, hemos podido advertir la presencia de casos de uso vinculados a servicios de pago; (iii) en tercer lugar, se han observado riesgos vinculados con el tratamientos de datos personales de los clientes; y, (iv) en cuarto lugar, también se prevé la resistencia de determinadas entidades bancarias -con una posición importante en el mercado- a compartir la información de sus clientes.

En el Perú, el organismo a cargo de la protección del ahorrista (cliente financiero) es la Superintendencia de Banca, Seguros y AFP, al amparo de lo establecido en el artículo 87° de la Constitución Política de Perú y la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley N° 26702 (en adelante "Ley de Bancos"). Esta norma ratifica la competencia de la SBS para regular y supervisar a las entidades que realizan actividades de intermediación financiera (que son consideradas actividades principales), así como **actividades complementarias** a ésta, como es el caso de los servicios de pago, lo cual está vinculado con la protección del consumidor financiero (en este ámbito en término de la protección de su información).

Como explica Giovanna Prialé y Denise Díaz[59], la protección del consumidor financiero y la regulación de la conducta de mercado son funciones asumidas de forma completa por la SBS desde una perspectiva orgánica, pues forman parte de sus planes de supervisión y cuentan con atribuciones para enmendar los defectos en la gestión que se puedan observar. La regulación busca corregir fallos de mercado (como la asimetría informativa), así como mejorar la prestación de los servicios financieros, a fin de que se estructuren para efectivamente satisfacer la necesidad de los consumidores.

En segundo lugar, el Banco Central de Reserva del Perú tiene competencia para regular los servicios de pago, de acuerdo con lo establecido en la Ley N° 29440, Ley de los Sistemas de Pagos y de Liquidación de Valores. Expresamente el literal n) del artículo 10° dispone que el instituto emisor tiene atribuciones para **dictar normas, reglas principios y estándares a los Proveedores de Servicios de Pago para fomentar su operación segura y eficiente.** En este contexto, el Banco Central está interesado en que los servicios de pago se presten de forma segura, por lo cual le incumbe el mecanismo de transmisión de la información de los consumidores (como es el caso de sus credenciales de acceso, por ejemplo), y sería legítimo que opinara sobre los estándares aplicables para las interfaces de programación de aplicaciones (APIs) o los riesgos de ciberseguridad a los que se expondrían las entidades financieras con la implementación del *Open Banking*.

Asimismo, el Banco Central también debe procurar que el servicio de pago se preste de forma eficiente, por lo cual también podrá intervenir en aspectos como la rapidez del servicio o la contraprestación que deba pagarse, o no, al proveedor

[59] PRIALÉ REYES, G., & DÍAZ, D. (2010). *La protección al consumidor en el Perú y la banca sin sucursales*. Lima: SBS.

de las APIs. Como señalamos líneas arriba, el ordenamiento jurídico peruano no permite la fijación de precios o tarifas, salvo en el caso de los servicios públicos, declarados como tal por una ley expresa, por lo cual (a lo sumo) podría exigirse que la contraprestación sea transparente, no discriminatoria y refleje la contraprestación de un servicio efectivamente prestado.

En tercer lugar, contamos con la Autoridad Nacional de Protección de Datos Personales, que es un órgano adscrito al Ministerio de Justicia y Derechos Humanos, la cual tiene competencia para realizar todas las acciones necesarias para el cumplimiento de la normativa sobre protección de datos personales, lo cual incluye el ejercicio de la potestad sancionadora y la potestad coactiva, según corresponda[60]. Dentro de sus principales funciones se encuentra supervisar el cumplimiento de las exigencias establecidas en la normativa[61], resolver las reclamaciones formuladas por los titulares de los datos personales por la vulneración de sus derechos[62], o supervisar la sujeción del tratamiento de los datos personales que efectúen el titular y el encargado del banco de datos personales a las disposiciones técnicas que ella emita[63].

Considerando que la información que se transmitirá al tercero proveedor de servicios en su mayoría se tratará de información protegida por la normativa de protección de datos personales (secreto bancario, secreto bursátil, secreto comercial, información personal), corresponde la aplicación de la normativa especia. En este contexto, por ejemplo, deberán implementarse mecanismos para obtener el consentimiento previo, expreso e inobjetable del titular de la información, o que el tratamiento de los datos personales de los clientes se realice conforme a la finalidad comunicada o de la forma establecida en la normativa. No consideramos que sea conveniente, ni tampoco advertimos una justificación válida, para que este tipo de tratamientos de información personal sean exceptuados de la aplicación de este régimen jurídico.

Finalmente, consideramos que la implementación y funcionamiento del *Open Banking* también le debe incumbir al Instituto Nacional de Defensa de la Competencia y Propiedad Intelectual[64], organismo encargado de defender la libre y leal competencia, sancionando prácticas anticompetitivas y desleales, procurando que en los mercados exista una competencia efectiva. Cabe indicar que este organismo también tiene la atribución de proteger los derechos de los consumidores, asegurando la idoneidad de los bienes y servicios que se les prestan.

Desde nuestro punto de vista son tres los motivos que justificarían su participación. En primer lugar, porque el *Open Banking* es un mecanismo de

60 Artículo 32 de la Ley de Protección de Datos Personales, Ley N° 29733.
61 Numeral 8 del artículo 33 de la Ley de Protección de Datos Personales, Ley N° 29733.
62 Numeral 16 del artículo 33 de la Ley de Protección de Datos Personales, Ley N° 29733.
63 Numeral 19 del artículo 33 de la Ley de Protección de Datos Personales, Ley N° 29733.
64 La descripción de su naturaleza y funciones se encuentra prevista en el Decreto Legislativo N° 1033, que aprueba la Ley de Organización y Funciones del Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelecual (Indecopi).

promoción de la competencia para el ingreso de nuevos agentes al mercado, así como para intensificar el proceso competitivo en los sectores más rentables, como es el caso de los préstamos a personas con un buen historial crediticio. En segundo lugar, porque debe vigilar que no se cometan prácticas que restrinjan el acceso de nuevos agentes al mercado, por ejemplo, a través del establecimiento de estándares de muy complejo cumplimiento o, incluso, por medio de negativas injustificadas para contratar (que se pueden materializar a través de las asociaciones de bancos). Finalmente, como autoridad de protección al consumidor *ex post*, es decir, para atender las reclamaciones directas del consumidor financiero (labor que no ha asumido la Superintendencia de Banca, Seguros y AFP).

Es preciso indicar que, en la medida de que el enfoque de la intervención regulatoria incorpore otros objetivos como la inclusión financiera, se debe comprender a los organismos encargados de desarrollar esta política pública, como es el caso del Ministerio de Economía y Finanzas.

ii. Evolución del *Open Banking* en el Perú

Como la gran mayoría de países, el progreso de las finanzas abiertas en el Perú no ha dependido de la regulación o de una política de Estado (que a la fecha no existe), sino más bien del desarrollo disruptivo de la industria, que viene utilizando herramientas poco seguras -como el *screen scraping* o *reverse engineering*- para tomar, de forma consentida, la información bancaria de los consumidores. Véase el caso de todas las plataformas en las que ingresamos las credenciales de nuestras tarjetas de crédito o débito (*Rappi, Didi, Pedidos Ya,* entre otros[65]).

De otro lado, no puede negarse que existen entidades financieras que están promoviendo el uso APIs para compartir información (caso de *Interbank*), quien ha implementado un portal de desarrolladores con APIs abiertas. Es más, hemos podido advertir que modelos de negocio exitosos de determinadas *Fintech* han provocado una **interoperabilidad o colaboración empresarial natural**, como es el caso de *Kambista*, que es una empresa dedicada al cambio de divisas, que hoy en día facilita -a través de su banca por internet o sus aplicativos móviles- la creación de cuentas bancarias.

Esta situación claramente ha llamado la atención de la Superintendencia de Banca, Seguros y AFP que mediante Resolución SBS N° 504-2021 aprobó el Reglamento para la gestión de la seguridad de la información y la ciberseguridad, el cual tiene por objeto desarrollar un sistema de gestión de seguridad de la información aplicable a las entidades del sistema financiero[66]. Dentro de los principales aspectos en el rubro **ciberseguridad** advertimos la exigencia de uso de APIs para la provisión de servicios en línea a través de terceros. Como veremos a continuación, no se trata de exigir un determinado estándar, sino más bien un

[65] Sólo se está mencionando las aplicaciones que utilizo, y en las que puedo verificar que no se utilizan APIs con las entidades financieras para la transmisión de mi información, o que no aplican los mismos protocoles de seguridad para la validación de mi identidad que los aplicados por mi proveedor de servicios de pago gestor de cuenta.

[66] Aquellas comprendidas en los artículos 16 y 17 de la Ley de Bancos.

conjunto de procedimientos o protocolos. Concretamente, el uso de interfaces de programación de aplicaciones requiere (artículo 21°):

a. Análisis de riesgos asociados e implementación de medidas de mitigación.

b. La autenticación mutua de los sistemas y la de los usuarios.

c. La autorización de las operaciones por parte de los usuarios.

d. El cifrado de datos en almacenamiento o transmisión.

e. Prácticas de desarrollo seguro de API y revisión de prácticas de codificación segura.

f. Análisis de vulnerabilidades y pruebas de penetración.

g. La seguridad de la infraestructura tecnológica que lo soporta.

h. Los mecanismos de tolerancia ante fallos y de contingencia.

i. Control de accesos en el entorno de datos, sistemas e infraestructura.

j. Monitoreo de eventos de seguridad de la información y gestión de estos cuando se constituyan en incidentes.

Asimismo, la norma establece que se debe tomar como referencia estándares y marcos de referencia internacionales, y cuando sea factible adoptarlos en el marco de acuerdos gremiales o sectoriales, para la implementación del intercambio y encriptación de datos, así como la autenticación y la autorización de operaciones, sin que ello sea una lista restrictiva. Consideramos que es un avance importante de cara a la seguridad de la información de los clientes. Es preciso indicar que esta norma **a priori** no significa que técnicas como el *screen scrapping* se encuentren prohibidas, pues para ello se requerirá una prohibición expresa, en tanto esa herramienta no obedece a un acuerdo con las entidades financieras que administran la cuenta de clientes, sino más bien a un **acuerdo** entre el cliente y los terceros proveedores de soluciones tecnológicas.

iii. Avances normativos sobre el *Open Banking*

En el plano normativo no existe una disposición que permita o restrinja la utilización del *Open Banking*, sin embargo, siete congresistas presentaron en el mes de marzo de 2022 el Proyecto de Ley N° 1584/2021-CR, el cual tiene el propósito único de declarar de interés nacional y necesidad pública la implementación de la política pública que fomente la masificación de la banca abierta. Hasta la fecha no hemos identificado otra iniciativa legislativa de esta naturaleza. En la exposición de motivos de la norma -acertadamente- se reafirma el fundamento principal de toda política de finanzas abiertas: **los datos no son propiedad ni del banco ni del gobierno, son propiedad del cliente, y es por eso que debe tener el poder de decidir quién tiene su información y no al revés.**

Una crítica constructiva al enfoque del Proyecto de Ley es que se pretende promover la **inclusión financiera**, sin embargo, como hemos explicado, el *Open Banking* -en principio- no tiene ese propósito por lo acotada de la información que se exige compartir. De acuerdo a lo explicado, el principal objetivo del *Open Banking* es promover la competencia de dos formas: (i) intensificando el proceso competitivo respecto de los bienes o servicios que se vienen ofertando en el mercado, pues se elimina la asimetría informativa entre los proveedores, con lo cual las entidades financieras más pequeñas y los terceros proveedores de soluciones financieras pueden tener acceso a la misma información que manejan los bancos más importantes; y, (ii) facilitando o viabilizando la creación de nuevos productos financieros, como es el caso de la **iniciación de pagos**, la gestión discrecional de los créditos, servicios de asesoría financiera y optimización de gastos.

El propio Proyecto de Ley menciona[67] que la creación de productos o servicios más cercanos a la población excluida o desatendida por el sector financiero no es el objetivo primario del *Open Banking*, pues su objetivo principal es la **profundización de los servicios financieros**[68]. De forma expresa, la Exposición de Motivos indica que los sistemas de banca abierta basados en el acceso a los datos de las cuentas bancarias **no son los principales factores que impulsan la inclusión financiera,** pues contribuyen a incrementar la oferta y mejorar la calidad de los servicios que reciben las personas bancarizadas.

No obstante, también coincidimos con la Exposición de Motivos del precitado Proyecto de Ley, pues identifica que, si la información a la que pueden acceder los terceros proveedores de soluciones financieras tiene un alcance mayor, entonces sí podrían crearse productos o servicios bancarios que puedan contribuir a cerrar la brecha de inclusión financiera. Nos referimos concretamente a información sobre la declaración y pago de impuestos, sobre los contratos para la provisión de servicios públicos (principalmente telecomunicaciones), el uso de aplicativos móviles de servicios de pago, a partir de la cual se puede obtener o crear un récord de comportamiento crediticio del ciudadano no bancarizado.

Un enfoque que mejoraría la propuesta legislativa es desarrollar un régimen de *Open Data* u *Open Access*, en el que toda la información del ciudadano custodiada o administrada por determinados tipos de empresas deba ser compartida con los terceros proveedores de soluciones financieras que así lo requieran. Evidentemente esto involucra una serie de retos de coordinación, sin embargo, puede impulsarse esta iniciativa por etapas, por ejemplo, empezando con incluir a las empresas que prestan servicios públicos de telecomunicaciones. A partir de esta información, además de verificar la identidad del cliente, puedes analizar su comportamiento de pago de los servicios o créditos otorgados por las compañías (usualmente para la compra de equipos).

---

67 Véase la página 5 de la Exposición de Motivos del Proyecto de Ley N° 1584/2021-CR.

68 Esta es uno de los temas discutidos por Nuria Aliño en sus talleres de Open Banking realizados en Perú dirigido a los reguladores bancarios en el mes de noviembre de 2022 (Aliño, 2022).

También hemos observado que las entidades públicas involucradas se han pronunciado, casi todas a favor de su aprobación. La SBS[69] ha recomendado que el modelo de finanzas abiertas se efectúe por etapas, iniciando con las entidades bancarias y otras empresas de operaciones múltiples, para luego ampliar su ámbito a otras entidades. Asimismo, respecto de su operación, advierte la necesidad de gestionar los riesgos involucrados en la implementación del *Open Banking*, tales como ciberseguridad, interoperabilidad, uso indebido de la información personal de las personas. Esta preocupación por los riesgos de la banca abierta es compartida por ASBANC[70], quien además propuso que sea un modelo voluntario vista la inversión que se debe realizar para su implementación.

Por su parte, el Banco Central de Reserva del Perú[71] [72], también manifestó su conformidad con el Proyecto de Ley, y además resaltó los potenciales beneficios del *Open Banking* en el Perú, tales como el empoderamiento del cliente final, el impulso de la innovación, la promoción de la competencia y potencial reducción de tasas de interés, aceleración de la transformación digital. Asimismo, el instituto emisor recomendó que se le asigne la competencia para adoptar las medidas que se consideren necesarias para el desarrollo de la banca abierta en el país, en el marco de sus funciones constitucionalmente reconocidas.

En contraste, el Ministerio de Economía y Finanzas manifestó su opinión desfavorable sobre el Proyecto de Ley, pues consideró que esta declaratoria de interés forma parte de una política nacional que corresponde ser aprobada por el Poder Ejecutivo, y además ya existe una política nacional que promueve y facilita el proceso de inclusión financiera, por lo cual no es necesario la aprobación de la norma. Finalmente, indica que no se establecen criterios o parámetros básicos que protejan al ciudadano de riesgos asociados a la implementación de la masificación de la banca abierta, entre ellos el riesgo de fraude.

A nuestro criterio, el Proyecto de Ley pudo tener un mejor enfoque y constituirse como una herramienta para el impulso de la competencia y la inclusión financiera, y no simplemente una mera declaración de importancia[73]. Me refiero a que pudo establecerse un régimen jurídico general que, por ejemplo, les exija a las empresas proveedoras de servicios públicos el compartir la información de sus clientes, previa autorización, con terceros proveedores de soluciones financieras. Con esta medida sí se estaría brindado un impulso a la inclusión financiera, pues a partir de esta información se podrían crear nuevos productos o servicios dirigidos a la población desatendida por este sector, o simplemente creando oportunidades vista su comportamiento diligente en el pago de sus obligaciones.

---

69 Oficio N° 20688-2022-SBS del 20 de mayo de 2022.

70 Carta C0047-2022-GG-ASBANC del 20 de mayo de 2022.

71 Oficio N° 128-2022-BCRP del 16 de mayo de 2022.

72 Es preciso indicar que el suscrito, a la fecha de elaboración del presente artículo, no ha participado en ningún tema vinculado al *Open Banking* como parte de sus funciones en la Gerencia Jurídica del Banco Central de Reserva del Perú.

73 Nos referimos a la clásica declaración de interés público de una determinada actividad, la cual no tiene efectos prácticos en su desarrollo.

VII. Conclusiones y comentarios finales

El Open Banking o finanzas abiertas es una política pública que tiene por objeto maximizar el intercambio de información como un medio para promover la productividad a través del desarrollo de nuevos productos, procesos, métodos organizacionales; incluso para la mejora en la toma de decisiones por parte de entidades públicas (pues permite identificar demandas sociales en distintos ámbitos), o el cierre de las brechas en materia de inclusión financiera. Es un mecanismo para la promoción de la competencia e innovación en el mercado bancario, que se circunscribe en un esfuerzo mucho más estructurado y orgánico que es la política pública de datos abiertos (*Data Access* u *Open Data*).

Las finanzas abiertas optimizan el ejercicio del derecho a la autodeterminación informativa, en su manifestación del derecho de acceso y portabilidad de datos, pues no sólo facilita y garantiza el consentimiento de los titulares a disponer de su data personal, sino también viabilizan su transmisión a terceros en un formato práctico, que no exige un nuevo registro. Al amparo de este enfoque se exige que los administradores o custodios de la información desarrollen mecanismos para compartir la información de los clientes (previo consentimiento) con los terceros proveedores de soluciones tecnológicas u otras entidades financieras, a través de estándares o formularios comunes, a fin de que los sistemas de ambas partes sean compatibles y puedan interoperar. La idea es la compartición de la información de forma automática y segura.

Los principales fundamentos para regular el Open Banking se encuentran en la optimización del derecho a la autodeterminación informativa (que puede circunscribirse a una política pública de datos abiertos), la gestión de riesgos (cuyo alcance se abordará en una conclusión particular), y la promoción de la competencia en el mercado bancario, pues tiene por objeto fomentar la innovación en la creación de nuevos servicios, y además elimina la asimetría informativa entre las entidades del sistema financiero tradicional (quienes usualmente custodian o administran la información de los clientes) y los nuevos proveedores de soluciones tecnológicas (Fintechs). Dependiendo de su alcance (tipo de información y sujetos obligados a compartir), podría incorporarse como objetivo el desarrollo de la política pública de inclusión financiera.

El arreglo institucional es clave para la implementación de las finanzas abiertas. En algunas experiencias se encargó a un solo organismo su implementación (incluso de naturaleza privada como en Brasil), mientras que en otras se han distribuido las competencias en función de la especialidad, vistas las áreas transversales del régimen de finanzas abiertas. En el caso de Perú, la entidad con mayor protagonismo es la SBS, aunque se ha advertido la necesaria participación de entidades como el Banco Central, la Autoridad de Protección de Datos Personales y el Indecopi.

En la actualidad se han identificado dos modelos para la implementación del Open Banking: obligatorio o voluntario. En algunos países (Unión Europea, Reino Unido

y Chile) el modelo es obligatorio, por ende, el incumplimiento del deber de compartir información involucra la comisión de una infracción y por ende la aplicación de una sanción.

Los clientes y las entidades financieras se exponen a una serie de riesgos cuando se permite que terceros puedan acceder a la información y a sus sistemas, incluso con su consentimiento, por lo cual se deben adoptar medidas de ciberseguridad para garantizar una transmisión segura de la información que expresamente autoriza el cliente a transmitir. Precisamente, uno de los elementos claves en la implementación del Open Banking es determinar el tipo de mecanismo para la transmisión de la información de forma segura y eficiente. Actualmente, las empresas que requieren la información de un determinado cliente utilizan herramientas como el *screen-scraping* o el *reverse engineering* para acceder a los datos administrados por sus respectivas entidades financieras, lo cual ha sido calificada como una práctica poca segura, aunque su éxito y aporte en la promoción de la competencia es evidente.

En este escenario de riesgos de ciberseguridad, aparecen las interfaces de programación de aplicaciones (APIs), las cuales deben garantizar la interoperabilidad entre los sistemas de almacenamiento y transferencia de datos empleados por cada una de las entidades financieras y las plataformas de las entidades y terceros interesados en la información. Las APIs son un mecanismo adecuado para que los sistemas de dos o más entidades independientes puedan interoperar y se facilite la entrega de información, en términos de rapidez, seguridad y eficiencia. La principal desventaja de exigir la implementación de APIs es la inversión en términos de tiempo y dinero que se tiene que realizar para crear y mantener una API, particularmente en esquemas donde no se ha estandarizado el lenguaje y se requiere de acuerdos comerciales.

Uno de los temas más discutibles es la posibilidad de cobrar, o no, una contraprestación por el desarrollo y mantenimiento de las APIs. En este contexto, incluso se ha discutido a quién se le debería cobrar, en el supuesto de que proceda: por un lado, tenemos al cliente quien autoriza a la entidad financiera que comparta sus datos para gozar de una prestación; y -por otro lado- tenemos al tercero proveedor de soluciones tecnológicas que utiliza la información como un insumo para innovar en la creación de productos financieros. Nosotros consideramos que la contraprestación es necesaria para la sostenibilidad del esquema (siempre que responda a un servicio efectivamente prestado, sea transparente y no discriminatoria), y restringir su aplicación es una forma de regular tarifas, lo cual se encuentra proscrito por el ordenamiento jurídico peruano (como el caso del medio pasaje en el ámbito del transporte urbano). Si bien es cierto muchos países que abordaron el tema no han restringido su aplicación, nos llama poderosamente la atención el caso chileno, pues expresamente han prohibido el cobro de alguna tarifa, contraprestación o reconocimiento de costo a los terceros y clientes.

De acuerdo a la información consultada, el desarrollo de APIs abiertas aún es muy bajo en América Latina (particularmente en Perú sólo existe una entidad financiera

que ha implementado un portal de desarrolladores como parte de una política de *Open Banking*), lo cual sólo es un síntoma de que las entidades financieras administradoras de la información no tienen la necesidad de interoperar con los terceros proveedores de soluciones financieras, pues no le aportan valor a su negocio. El éxito de las APIs depende del nivel de innovación y desarrollo de negocios por parte de los terceros proveedores que provoquen impactos como el cambio en la forma de prestar determinados servicios, o el valor agregado que le puede aportar a la banca tradicional.

Como la gran mayoría de países, el progreso de las finanzas abiertas en el Perú no ha dependido de la regulación o de una política de Estado (que a la fecha no existe), sino más bien del desarrollo disruptivo de la industria, que viene utilizando herramientas poco seguras -como el *screen scraping* o *reverse engineering*- para tomar, de forma consentida, la información bancaria de los consumidores.

La SBS ha considerado que la regulación del *Open Banking* es sólo un posible componente de un ecosistema que requiere del desarrollo de gobierno, sistemas, procesos, seguridad, informática, APIs y estándares. Se maneja la posibilidad, como hasta la fecha, de que pueda prescindirse de la regulación o puedan crearse incentivos para su desarrollo orgánico[74].

Es importante reflexionar sobre las necesidades de regular el *Open Banking* considerando el desarrollo de la industria, la dinámica del mercado, los riesgos involucrados (principalmente el uso de información personal del cliente) y el impacto que tendría en la promoción de la competencia. Se ha visto que en los países donde no existe regulación, se aprecia mayor flexibilidad y libertad para innovar (creación de nuevos casos de uso). Piénsese en que la regulación conllevará una carga de cumplimiento normativo, lo cual supone un aumento en los costos operativos de empresas que no tienen el respaldo financiero de las empresas que administran o custodian la información de los clientes (operadores incumbentes).

Sobre la base de lo expuesto en el presente artículo, podríamos preguntarnos ¿hoy en día es necesaria la regulación para promover la competencia en el mercado o el acceso de nuevos agentes? ¿El enfoque de una regulación promotora de la competencia se puede desvirtuar con reglas de acceso al mercado destinadas a brindar seguridad a las operaciones (registro previo, directivas técnicas de seguridad)? Un régimen estricto de finanzas abiertas no siempre es necesario o conveniente si la industria está encaminándose por esa ruta, o cuando los terceros proveedores no han adquirido cierto grado de madurez. No debemos confundir una regulación promotora de la competencia, de una regulación que pretenda sustituir el mercado o descartar la innovación, a la que no estamos preparados.

[74] Superintendencia de Banca, Seguros y AFP. (2021). Servicios financieros digitales. Lima: SBS.