
Fintech: entre la inclusión financiera y el cibercrimen. Análisis de su *status* jurídico y su vinculación con los ciberdelitos: panorama y soluciones.

Autora: **Evangelina Natalia Negro***

Una empresa crece por la capacidad que tiene para atender a un mercado siendo rentable, pero actualmente, la habilidad de crecer y ser rentable radica fuertemente en la capacidad de prevenir, mitigar y atender riesgos informáticos de manera precisa y con planes que no detengan la operación del negocio y los clientes.

SUMARIO

I. Introducción. II. Fases de evolución del concepto Fintech. Consumers International (2017). III. Conceptos actuales. III.1. Startups. III.2. Crowdfunding. III.3. Criptomonedas. III.4. *Blockchain*. IV. ¿Qué es una Fintech? V. Clasificación de las Fintech. VI. Mejores Fintech en nuestro país. VII. ¿Cuáles son los beneficios de las Fintech? VIII. Los sectores que poseen mayor presencia en nuestro país. IX. Importancia de la seguridad de la información en las *Fintech*. IX. *Fintech* o Banca Tradicional. X. Regulación de las *Fintech*. XI. Postura de las entidades financieras. XII. Siete áreas estratégicas del futuro *Fintech*? XIII. ¿Qué es el Cibercrimen? XIV. ¿Cuáles son los ciberdelitos más denunciados en los últimos años? XV. Algunos ejemplos de cibercrímenes. XVI. Impacto del cibercrimen. XVII. ¿Qué medidas ha tomado el sector financiero para combatir el cibercrimen? XVIII. Opinión del GAFI (Grupo de Acción Financiera Internacional). XIX. ¿Cómo pueden actuar las *Fintech* para mejorar sus soluciones tecnológicas y cuáles son los desafíos de cara a la postpandemia? XX. El 2023 para las *Fintechs*: lo que se viene. XXI. Conclusiones.

RESUMEN

El presente artículo hace referencia a las empresas Fintech, su evolución, y su vinculación con la banca tradicional, analizando también su regulación legal o marco normativo, su estrecha vinculación con los ciberdelitos, la importancia de proteger nuestra información personal, y cómo pueden estas *startups* actuar para mejorar sus soluciones tecnológicas.

* Abogada y Docente de la UBA en Contratos Civiles y Comerciales en la cátedra de los Dres. Heriberto Hoczman y Alan Gobato. Miembro de los Institutos de Derecho Civil, Comercial, Concursal, Laboral, Previsional y de la Seguridad Social, Derecho Informático del CASI. Miembro de la Comisión del Instituto de Derecho Informático del CASI. Miembro del Instituto

PALABRAS CLAVE

Fintech. Sector financiero. *Startup*. Banca tradicional. Innovación. Tecnología. Cibercrimen. Ciberdelitos.

I. INTRODUCCIÓN

El presente trabajo de investigación tiene la finalidad de desarrollar una descripción completa de las organizaciones “*Fintech*” con el objeto de dejar una base teórica que sirva de punto de partida para futuros análisis, con fines académicos o laborales, que busquen profundizar sobre algunos de los campos en los que se desarrollan. Lograr una descripción que las defina y analice su estructura. Además, determinar en qué situación se encuentran actualmente en nuestro país, cuál es su posición frente a los bancos tradicionales y su perspectiva futura.

Uno de los caracteres principales del comercio y uno de los principios básicos del derecho comercial es la celeridad. Sería necio negar los innumerables beneficios de la tecnología puesta al servicio del comercio nacional e internacional. Sin embargo, resulta prioritario para aquellos que nos encargamos de interpretar la ley, poder encuadrar dentro del ordenamiento jurídico argentino cualquier avance tecnológico para así estar en condiciones de determinar el status legal de los mismos y la consecuente interpretación que debemos darle sobre un caso concreto.

El exponencial crecimiento de los últimos años de la industria Fintech es innegable, tanto a nivel global como regional. Lastimosamente, la suplantación de la identidad, la usurpación de la data de los clientes y los ciberdelitos han sabido evolucionar a un ritmo casi tan acelerado como las mismas transformaciones digitales del sector bancario.

En medio de este panorama, saber encontrar el balance perfecto que permita procurar seguridad digital sin por eso perjudicar la fluidez de la experiencia del cliente (CX) pareciera todo un arte que las *Fintech* de hoy deberán aprender -sí o sí- a dominar. Frente a esto, varios expertos de la industria se han expresado al respecto para dar con una misma conclusión: del buen uso de la analítica y de la inteligencia artificial -dispuestas a través de tecnologías y soluciones omnicanales y con base en la nube- dependerá en gran medida el éxito de la difícil ecuación seguridad + CX = satisfacción.

Es por ello que, veo tan problemático como necesario determinar en la actualidad con exactitud qué entidad le da nuestro sistema jurídico al uso de la tecnología en los servicios financieros y, en consecuencia, si los mismos son lícitos o violan regulaciones vigentes.

A raíz de la pandemia del 2020, reconocidas entidades bancarias comenzaron a innovar utilizando tecnología aprovechando la masificación del acceso a internet con el fin de ofrecer una amplia gama de servicios financieros a sus clientes por esta vía. De esta forma, cualquier cliente de un banco podía acceder a su estado de cuenta por medio de una computadora con acceso a internet sin necesidad de trasladarse.

Una vez que este sistema logró consolidarse, comenzaron a surgir sociedades ad-hoc que ofrecían este tipo de servicios a nivel mundial pero que no estaban encuadradas estrictamente bajo el formato y los requisitos de aquellas sociedades comprendidas en las distintas leyes que regulan a las entidades financieras por no poderse detectar prima facie si efectivamente realizan intermediación financiera y/o captación de ahorro público. Este tipo de empresas son conocidas mundialmente como “*Fintech*” (acrónimo de *Financial*

de Derecho Comercial del CASM. Participante y ponente de diversas ponencias y trabajos académicos en los Encuentros de los Institutos de Derecho Comercial de los Colegios de Abogados de la Provincia. Diplomatura en Gestión Educativa y Representación Legal de la Universidad Austral. Posgrado en Asesoramiento Empresarial y Corporativo (CASI-UBA). Seminario de actualización de Neurociencias y Derecho del CASI. Programa de Inteligencia Artificial y Derecho (CASI). Programa de Inteligencia Artificial – Laboratorio de Innovación e Inteligencia artificial de la UBA. Título de Especialista en Gobernanza de Datos.

Technology o “Tecnología Financiera”), en virtud de la utilización de tecnología para ofrecer servicios financieros.

Asimismo, y a raíz del acelerado avance tecnológico, la Asociación Argentina de Lucha Contra el Cibercrimen (AALCC) ha presentado varios informes haciendo notar el aumento desmedido de denuncias por casos de estafas virtuales.

En un informe de mediados del 2021, la AALCC expuso que el crecimiento de las herramientas digitales y el aumento de usuarios en la banca impulsaron el crecimiento de este tipo de delitos, que afecta a todos los estratos sociales con instrumentos bancarios. Si bien en 2022 se observó una disminución del 40% en las consultas/denuncias que llegan a la asociación debido al esfuerzo de entidades financieras en realizar campañas de prevención, los delitos de fraude online y suplantación de identidad están en la actualidad a la orden del día.

La modernización acelerada impuesta por la coyuntura ha cambiado totalmente los procesos y el esquema de servicios en bancos y *Fintechs*. Sus principales retos en el contexto actual se centran principalmente en la “educación financiera de sus personas usuarias”, pero también en “fortalecer sus sistemas de seguridad para prevenir el ciberdelito”.

Los pagos a través de internet y las comunicaciones móviles es un área donde las *Fintech* enfocan sus esfuerzos. De la misma forma, la infraestructura para las operaciones de valores y liquidación y para el comercio de derivados del OTC (Operaciones OTC o “*Over the Counter*”) son claves para el sector *Fintech* y es donde las empresas de telecomunicaciones y de tecnologías de información buscan sus oportunidades.

En la actualidad no podemos hablar de tecnología y de trabajo en red si no pensamos en la “seguridad de los datos que se manipulan”, ya que éstos son vulnerables al ciberdelito y el espionaje. Por lo tanto, es un tema importante y una gran preocupación pensando a futuro, debido a que cada vez más son los servicios que se prestan digitalmente y con ellos los datos que se manejan en un entorno virtual. En este sentido, las grandes bases de datos con las que cuentan los bancos son una ventaja competitiva sobre las organizaciones no tradicionales que surgen ofreciendo servicios financieros.

Para concluir, podemos decir que este concepto, que nos parece enteramente novedoso y perteneciente a nuestro siglo, ha tenido sus antecedentes. La tecnología y las finanzas han tenido su relación y se han influido mutuamente desde los albores de la historia financiera mundial.

II. FASES DE EVOLUCIÓN DEL CONCEPTO FINTECH. CONSUMERS INTERNATIONAL (2017)

1) Fintech (1866-1967)

- Tendido del primer cable transatlántico.
- Telégrafo.
- Transmisión rápida de información financiera, transacciones y pagos.

2) Fintech (1967-2008)

- Pagos electrónicos y sistemas de liquidación.
- Cajeros automáticos y banca on line.
- Uso de la tecnología de información por instituciones financieras tradicionales para mejorar sus productos y servicios.

3) Fintech (2008 – Presente)

- Uso de la tecnología por parte de nuevos ingresantes a la industria para proveer servicios sin intermediación, al cliente.

-Nuevo panorama competitivo para las instituciones financieras.

III. CONCEPTOS ACTUALES

Analizaremos en este apartado algunos conceptos surgidos actualmente que no necesariamente están ligados exclusivamente al sector financiero.

III.1. Startups

Una definición precisa de este concepto es la que nos dan Steve Blank y Bob Dorf (2013): “una organización temporal en busca de un modelo de negocio rentable, repetible y escalable”.

Cuando hablan de organización temporal se refieren a que aún no cuenta con un modelo de negocio validado y aspira a ser una empresa real. “En busca de un modelo de negocio” marca la gran diferencia con una empresa madura o consolidada.

En cuanto a la *startup* como “modelo escalable” hace referencia al ritmo creciente que pueden alcanzar sus ingresos respecto a sus costos.

Montoya (2016) afirma en su artículo de investigación: “aunque la *startup* puede referirse a iniciativas de cualquier sector económico y sociocultural, normalmente está muy relacionada con el ámbito tecnológico, dado que es una empresa que suele hacer un uso intensivo del conocimiento científico y tecnológico o está relacionada directamente con el mundo de Internet y las TIC”.

III.2. Crowdfunding

El término *crowdfunding*, frecuentemente traducido como “financiación en masa o colectiva”, describe un amplio fenómeno consistente en la creación de un entorno (electrónico) para la agrupación de un colectivo, la aportación de ideas, recursos y fondos y la interacción en red dirigidas a apoyar conjuntamente proyectos, esfuerzos e iniciativas de individuos, organizaciones o empresas.

Este es un concepto muy relacionado a las *Fintech* a través de otro que es el P2P9 (Peerto-peer). Una *Fintech* pionera en microcréditos y préstamos entre pares es la estadounidense Kiva, una organización sin fines de lucro que permitía a los empresarios prestar fondos a personas u organizaciones en todo el mundo.

III.3. Criptomonedas

Las criptomonedas son un sistema de pago descentralizado que tiene como fin eliminar los intermediarios, no cuentan con la participación de bancos, uniones de crédito o prestamistas, pero pueden ser consideradas unidades monetarias al cumplir con las características del dinero: es un medio de intercambio, genera confianza y funciona como una unidad de cuenta.

Buscan asegurar las transacciones y controlar la creación de nuevas unidades de una manera descentralizada.

No tienen un emisor concreto.

La coherencia de la encriptación de esta moneda está protegida por los mismos usuarios en todo el mundo, pero su control se encuentra descentralizado, no cuenta con un respaldo bancario o institucional.

El Bitcoin, la criptomoneda de mayor auge en estos tiempos se apoya en un sistema digital denominado *Blockchain*.

Bitso es una de las plataformas más utilizadas en nuestro país para la compraventa de criptomonedas.

III.4. Blockchain

Es una cadena de bloques, como lo indica su nombre, que contienen información codificada de trans-

acciones en la red. Estos bloques están entrelazados por eso se le llama “cadena” lo que permite que se transfieran datos entre ellos. Su codificación es segura gracias a la criptografía.

Con los conceptos desarrollados anteriormente estamos en condiciones de comenzar a adentrarnos completamente en el concepto de Fintech.

IV. ¿QUÉ ES UNA FINTECH?

Partiendo de su etimología, Fintech surge de la combinación de las palabras en inglés *Finance* (finanzas) y *Technology* (tecnología). A este término podemos utilizarlo genéricamente para referirnos a la aplicación de la tecnología en el sector financiero.

El Consejo de Estabilidad Financiera (FSB11, por sus siglas en inglés) la define como “innovación financiera potenciada tecnológicamente que podría resultar en nuevos modelos de negocios, aplicaciones, procesos o productos con un efecto material pertinente en los mercados e instituciones financieras y en la provisión de servicios financieros”.

Las *Fintech* representan la transición de los modelos financieros tradicionales, como los bancos, hacia esquemas basados en tecnología, como las billeteras virtuales. Su crecimiento en el país se vincula, según analistas, con un alto grado de la población que aún no está bancarizada.

La gran diferencia entre las Fintech y las entidades financieras tradicionales radica en que el negocio en línea entre la entidad bancaria y su cliente se realiza en el marco de una relación contractual previa por la existencia de una cuenta corriente bancaria, caja de ahorro y/o solicitud presencial de un producto que ofrece la entidad en cuestión.

Por contraparte, en el caso de las Fintech si bien la voluntad de ambas partes para la celebración de un acuerdo también se exteriorizaría (mediante un *click* o envío de datos) no existe una relación contractual previa entre ambos contratantes al punto que la totalidad del acuerdo se celebra, se cumple y se extingue en forma on-line y sin la firma ológrafa de ninguna de las partes sobre documentación física.

De acuerdo con una encuesta realizada en nuestro país por la consultora Pricewaterhousecoopers (PwC), las empresas argentinas asignan en promedio el 23% de su facturación anual a proyectos relacionados con la industria Fintech. Asimismo, el 83% de las instituciones financieras argentinas espera ampliar sus asociaciones con empresas Fintech y el 78% incrementará sus esfuerzos internos para innovar en la materia.

La consultora PwC en su definición del concepto en un informe publicado en 2016 parece agregar algunos requisitos necesarios para que una organización sea considerada una Fintech.

Las define como “un segmento dinámico en la intersección de los servicios financieros y la tecnología donde las *startups* tecnológicas y los nuevos participantes del mercado innovan los productos y servicios ofrecidos actualmente por la industria de los servicios financieros tradicional”.

El informe de la consultora concluye contundentemente diciendo que “como fuente de innovación” las instituciones financieras nacionales están aceptando el potencial de los nuevos desarrollos tecnológicos.

Las *Fintech* buscan ofrecer productos y servicios altamente especializados, enfocados en los clientes. Buscan satisfacer necesidades específicas personalizando sus servicios y buscando la mayor eficiencia. No solamente es un concepto que hace referencia a la aplicación de la tecnología en las finanzas, actualmente conforma un modelo de negocios, organizaciones con una identidad propia que se diferencia de los servicios tradicionales que incluso aplican la tecnología en sus esquemas de negocios.

Podemos definir entonces a las empresas *Fintech* como “aquellas que a través de la utilización de las tecnologías de información crean modelos de negocios innovadores en la industria financiera, ya sea, ofreciendo productos o prestando servicios de intermediación financiera o desintermediación, es decir, directamente al cliente, o bien, brindando servicios de soportes a instituciones financieras tradicionales”.

Podemos decir que la mayoría de las empresas Fintech no tienen la habilitación de los entes reguladores para operar como bancos.

V. CLASIFICACIÓN.

Según Venture Scanner (empresa de investigación que proporciona informes y datos sobre nuevas empresas y tecnologías emergentes) aborda el tema de las Fintech desde una clasificación exhaustiva e intenta abarcar la mayor cantidad posible:

Crowdfunding: se refiere a la forma de conseguir financiación diferente al capital y la deuda. Pueden ser plataformas de *crowdfunding* para productos y servicios, proyectos sociales o creativos. En Argentina, un ejemplo es *idea.me* una plataforma de *crowdfunding* para financiar proyectos creativos. Las personas que buscan financiamiento se registran, seleccionan un método de recaudación, cargan su proyecto y en cuanto se aprueba los colaboradores ya pueden aportar. En el caso de los colaboradores, reciben una recompensa por hacer el aporte.

Financiación de capital: incluye la forma de obtener financiación a través del capital, es decir, obtenerlo a cambio de acciones (participación en empresas privadas) y, para los inversores particulares, medios para obtener participación en empresas privadas (empresas no cotizadas en bolsa). Este segmento hace referencia a las plataformas de *equity crowdfunding*. En Argentina podemos encontrar la Fintech *sesocio.com* que, entre otros, nos permite invertir en empresas sin límite mínimo.

Inversión institucional: soluciones para gestionar el portafolio de inversión de las empresas, destinada a los gestores de patrimonio para ayudarlos a optimizar los rendimientos. Son herramientas para el análisis de sentimiento de valores (proviene del término en inglés *stock sentiment analysis* y hace referencia a las *Fintech* que predicen comportamientos de mercado a partir del análisis de datos en tiempo real, generalmente, proveniente de las redes sociales). Ayudan a los inversores a tomar decisiones en base a las opiniones del mercado., plataformas alternativas de inversión y las métricas de análisis del trading.

Investigación y datos financieros: son *Fintech* que se encargan de proporcionar información para la toma de decisiones financieras. Esto facilita a los inversores dicho proceso. • **Transferencias de dinero internacionales (envío de dinero):** aglomera a las *Fintech* que se encargan de ofrecer servicios de envío de dinero al exterior con costos bajos. Un caso emblemático es el de *Nubi*, plataforma de transferencias internacionales que trabaja junto con *PayPal*.

Infraestructura bancaria: aportan herramientas que le permiten a las instituciones financieras mejorar sus operaciones. Abarca las *Fintech* que ofrecen aplicativos de integración con los bancos, herramientas móviles o de banca en línea de marca blanca, es decir, para que los bancos lo utilicen bajo su identidad y también ofrecen herramientas de análisis de bases de datos.

Seguridad de las transacciones financieras: en esta categoría se incluyen a las empresas que ofrecen servicios de autenticación de identidad para garantizar transacciones financieras seguras y evitar estafas o fraude. Ofrecen análisis de bases de datos para detectar comportamientos sospechosos y algoritmos de detección de fraude.

Finanzas personales: ofrece medios innovadores para que las personas puedan administrar sus finanzas. Entre otros, herramientas de control de gastos, gestión de presupuesto y planificación financiera.

TPV's (Terminal Punto de Venta): son organizaciones centrada en torno a los consumidores que ofrecen soluciones de pagos en el punto de venta para empresas. Entre ellas las TPVs móviles (sistema mPOS) y otras herramientas innovadoras como el pago mediante código QR o escáneres en el punto de venta. Un caso muy famoso recientemente de este tipo de servicios es *MOD0* que es una billetera que les presta servicios a todos los bancos tradicionales. También podría entrar en la categoría de infraestructura bancaria.

Pagos de particulares: se refiere a las empresas de pago que apuntan tanto a productores como consumidores. En esta categoría encontramos a las *Fintech* que ofrecen herramientas que dan soluciones para el manejo de dinero como billeteras móviles (*mobile wallet*), innovaciones en tarjetas de prepago y los pagos

P2P. En esta categoría se encuentra Ualá, caso que desarrollaremos completamente en el próximo capítulo. También Pim, Yacaré, Todopago, entre otras.

Herramientas para pymes: en esta categoría ingresan aquellas empresas que proveen de servicios de gestión de finanzas para las micro, pequeñas y medianas empresas. Son las Fintech que ofrecen herramientas para la gestión de impuestos, de liquidación de sueldos, facturación y contabilidad.

Préstamos a particulares: se refiere a soluciones en préstamos de tipo personal que además ofrecen un servicio de evaluación de riesgo de crédito. Aglomera a las Fintech que ofrecen soluciones en crédito como los préstamos peer-to-peer, crowdfunding, análisis de bases de datos (big data) y servicios de calificación y medición de riesgo crediticio.

Préstamos a pymes: de la misma manera que para los particulares, existen las soluciones de financiación para las PyMES también complementadas con evaluación de riesgo crediticio. Son Fintech que ofrecen plataformas de préstamos P2P, créditos que tienen respaldo en activos (prendario e hipotecario), crowdfunding y análisis de bases de datos para gestión del riesgo.

Entonces, incluiremos en una determinada clasificación a las organizaciones dependiendo de su actividad principal y la que caracterice su forma de hacer negocios.

Por ejemplo, Mercado Pago puede ser considerada en las categorías de préstamos a particulares (Mercado Crédito), Finanzas personales, pagos de particulares y herramientas para pymes.

A esta clasificación, corresponde adicionar una categoría especial, que es el área de las “Criptodivisas y Blockchain”, dado que en el último tiempo ha adquirido una relevancia tal como para convertirse en una categoría que merece ser analizada individualmente.

El 50% de las empresas *Fintech* de Argentina están en el área de los pagos digitales y préstamos. Según el informe de la Cámara *Fintech*, en 2018 el primer puesto pertenecía a las empresas de 41 préstamos, pero hacia la actualidad eso se revirtió pasando a liderar los pagos digitales. Esta evolución tiene que ver, en primer lugar, con la contracción del crédito y la suba en las tasas de interés y, en segundo lugar, el creciente uso de medios digitales de pago y de comercio. Destacamos avances en las formas de pago como las transferencias inmediatas, débitos inmediatos (DEBIN) y la creación de CVU (Clave Virtual Uniforme).

VI. MEJORES FINTECH DE PAGOS Y TRANSFERENCIAS EN ARGENTINA

Dentro del conjunto de *Fintech* en Argentina se las puede segmentar como las mejores *Fintech* de pagos y transferencias en Argentina, entre las que se pueden encontrar las siguientes: Naranja X, Mercado Pago, Ualá, TodoPago, Nubi, SocialPOS, Apperto, Smiletechnologies, VeriTran, Olpays, YaPago, Pagos360, PagosPyme, Mobbex.

Más allá de los números y rankings, el ecosistema de startups *Fintech* en Argentina es de los principales en la región por nivel de crecimiento e inversión, lo que es todo un logro si se considera dificultades propias del país como tipo de cambio, impuestos, dificultades para iniciar un negocio e invertir, el contexto económico-social y de la pandemia, y a pesar de todo esto, si se considera el período entre los años 2018 al 2020, se llegaron a identificar unas 135 *Startups Fintech* nuevas en todo el país, tal como refleja un informe del Banco Interamericano de Desarrollo (BID) y de la Cámara de Fintech Argentina.

VII. ¿CUÁLES SON LOS BENEFICIOS DE LAS FINTECH?

La tecnología aplicada a servicios financieros gozó de una excelente recepción (lo cual se traduce en confianza) por parte del mercado. Sin embargo, las *Fintech* han logrado dar un paso más en lo que respecta a innovación y acceso al financiamiento tanto para la cartera minorista y mayorista en comparación con las entidades financieras tradicionales.

Entre los grandes beneficios que las Fintech otorgan a sus clientes se encuentran:

- 1) Acreditación de dinero en el momento sin necesidad de un vínculo previo.
- 2) Masificación del acceso al servicio financiero en zonas geográficas de difícil acceso.
- 3) Posibilidad de contar con liquidez sin necesidad de trasladarse físicamente.
- 4) Realizar operaciones de compraventa de monedas no soberanas (criptomonedas).
- 5) Facilidad para financiarse en masa a bajo costo sin intermediarios. (crowdfunding).
- 6) Generación de empleo en la misma industria y en los proyectos que ella financie.
- 7) Posibilidad de adquirir bienes y servicios sin necesidad de contar con dinero físico.
- 8) Productos financieros completamente en línea. Ofrecen productos (y servicios) de forma remota, realizando los trámites a distancia y por plataformas en línea brindando comodidad al cliente.
- 9) Brindan soluciones de manera eficiente a través de tecnologías innovadoras, con procedimientos ágiles y con una estructura flexible.
- 10) Apuntan a brindar servicios de forma personalizada y en tiempo real, adoptando un enfoque centrado en el cliente. De esta forma, buscan agregar valor a los servicios financieros actuales
- 11) El modelo de negocio se caracteriza por no utilizar intermediarios y buscando satisfacer una necesidad específica en la que se centran y desarrollan su idea.
- 12) Demuestran compromiso con la sociedad, logrando como consecuencia la fidelización de los clientes, al aumentar notablemente la inclusión financiera de individuos que están fuera del sistema bancario.
- 13) Finalmente, ofrecen productos y servicios promoviendo la transparencia.
- 14) Reducen notablemente los costos que representan los servicios financieros tradicionales, es decir, son eficientes en su prestación.

VIII. LOS SECTORES QUE POSEEN MAYOR PRESENCIA EN NUESTRO PAÍS

De acuerdo a un estudio realizado los sectores con mayor presencia en la Argentina serían los siguientes:

VIII.1. Préstamos

Los préstamos comprenden una de las categorías en las que estas empresas han tenido un gran crecimiento, sobre todo de la competitividad de los bancos tradicionales en esta materia, es decir, las dificultades que se le presentan a quienes buscan acceder al crédito.

Las *Fintech* ofrecen una forma más eficiente de acceder a los préstamos y, de ingresar al sistema a usuarios no bancarizados.

Como no tienen autorización para funcionar como entidad financiera, no puede realizar intermediación, por lo tanto, actúan como agentes entre los deudores y los prestamistas, es decir, operan por comisión.

Los tipos de préstamos más comunes son: personales, hipotecarios y a empresas. Desde que se desencadenó la crisis, las *Fintech* de préstamos han tenido un gran crecimiento, debido a que ofrecen una mejor experiencia al usuario permitiendo los trámites online, además la percepción que tienen las personas del sistema bancario se ha deteriorado y permiten la inclusión de usuarios que hasta el momento no tenían la posibilidad de bancarizarse.

Por otra parte, esta nueva forma de acceder al crédito les ha permitido a inversores pequeños colocar sus ahorros y generar un rédito de ellos, lo que les permite, en el largo plazo, conservar su riqueza y no verse

afectado por las consecuencias negativas de la inflación y devaluación sobre el dinero inmovilizado.

VIII.2. Pagos

En esta área está el mayor desarrollo de las Fintech. Ofrece específicamente cuatro servicios destacados:

Billetera virtual: permiten a través de aplicativos móviles realizar diversas transacciones como transferencias, usar códigos QR, pagar con tarjetas, pagar servicios o extraer efectivo de cajeros automáticos.

Ofrece una plataforma en la que se puede tener una cuenta virtual, una tarjeta prepaga y realizar transacciones por cuenta propia.

Remesas: herramienta que nos permite enviar dinero al exterior. Brinda una gran posibilidad a personas que tengan familia fuera del país y también a empresas que quieran ampliar sus fronteras.

Facilitadores de pago: permiten a los comercios, ya sea físicos o electrónicos, aceptar más medios de pago, sobre todo, el pago con tarjeta.

Gateway de pago: herramienta que permite enviar de forma segura los datos de pago de clientes de comercios electrónicos hacia las entidades emisoras de los medios de pago para que sean aprobados.

Mediante las herramientas de pago mencionadas se persigue el objetivo de dar acceso rápido y a menor costo a transacciones digitales, por ejemplo, para que un comercio pueda vender con tarjeta, o bien, para que un cliente pueda comprar en un comercio con tarjeta.

VIII.3. Inversiones

En esta área se encuentran las empresas que prestan servicios de inversiones en mercados regulados y *over the counter* (OTC), compraventa de instrumentos financieros y otras operaciones financieras a través de plataformas digitales.

VIII.4. Blockchain y criptoactivos

La cadena de bloques o *Blockchain* es un libro digital donde quedan registradas todas las transacciones que se realizan, en el caso de los contratos inteligentes, son acuerdos que quedan guardados y validados en ese espacio virtual.

En la *Blockchain* cada movimiento deja su marca digital. En los contratos inteligentes se estipulan las cláusulas y la red certifica si se cumplieron. También queda registrado qué pasos seguir en caso de incumplimiento (reparto de bienes, devoluciones o lo que corresponda).

La *Blockchain* (o “cadena de bloques”) constituye una de las tecnologías más disruptivas de este siglo y plantea una revolución no solo en nuestra economía, sino en todo tipo de ámbitos.

Aún no existe una norma jurídica que defina el concepto de *Blockchain* debido a lo novedoso de esta tecnología. Por lo tanto, y como se ha realizado con otros conceptos, recurriremos a la doctrina para su definición. Siguiendo a Andreas Antonopoulos, *Blockchain* es una forma de estructurar una base de datos.

La función criptográfica *hash*, conocida también como función de resumen, es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija, con el objetivo de asegurar que no se ha modificado un archivo, hacer ilegible una contraseña, o firmar digitalmente un documento, entre otras.

Una *Blockchain* es como una red de computadoras conectadas a través de internet de manera descentralizada (en donde el poder está distribuido) y que permite a cada una tener una copia de estos contratos, haciendo que sea imposible adulterarlos, sino que también sean resistentes a la censura y la confiscación.

Utilizando una analogía bien clara de la vida cotidiana, sería como cuando uno intenta borrar un mensaje antiguo en una conversación grupal de *Whatsapp* para ocultar cierta información. Esto no se podría hacer en la *Blockchain*, ya que contiene el historial completo de todas las transacciones que se han efectuado en

la red. Por ello se cree que la *Blockchain* revolucionará toda la estructura de gestión administrativa de los gobiernos y los servicios financieros del futuro.

VIII.5. Servicios b2b

El B2B es un modelo de negocio que consiste en los servicios que una compañía entrega a otra con el objetivo de mejorar las ventas de los productos y bienes que ofrece. Es decir, una transacción comercial entre empresas.

A diferencia del negocio a consumidor—*Business-to-Consumer* (B2C)— cuyas acciones se encaminan hacia el cliente final, el B2B se enfila hacia el proveedor de bienes o parte media de la cadena de comercialización, la cual tiene una importancia suprema a la hora de garantizar la efectividad de un negocio.

Un ejemplo de negocio B2B es un proveedor de contenidos web para otras empresas —bien sea mediante entradas de blog, redes sociales o páginas web— que busca posicionar a las marcas a través de internet.

En nuestro país, quienes más demandan este tipo de servicios son las entidades financieras. Entre los más solicitados se encuentran asesoramiento y mejoras de software especializados para bancos, validación de identidad, evaluación de riesgo crediticio (scoring no tradicional) y facturación digital.

VIII.6. Financiamiento colectivo. *Crowdfunding*

Comprar entre muchas o varias personas algo para repartírselo obteniendo una ganancia, sacándolo más barato o simplemente llegando a concretar en conjunto algo que de manera individual no hubiese sido posible, no es una idea nueva y existe desde hace siglos.

Pero en la era digital de la globalización y las comunicaciones instantáneas, se hizo más fácil encontrar personas con quien juntarse para concretar estas inversiones colectivas mediante *crowdfunding*.

En el mundo digital surgieron plataformas de *crowdfunding* como GOFUNDME en donde se suben proyectos para que las personas inviertan en ellos a cambio de acceder a una primera versión de un producto y servicio, por ejemplo, fondeando así emprendimientos que van desde libros a edificios o nuevas empresas enteras.

Por eso, el financiamiento colectivo es una herramienta cada vez más utilizada y de fácil uso por los emprendedores para captar dinero de forma masiva directamente del público, sin necesidad de recurrir a una sola fuente de financiamiento, para poder realizar proyectos, productos, innovaciones o expansiones del negocio, que de otra forma no se podrían lograr.

Se considera que el *crowdfunding* es una herramienta efectiva porque se le solicita a un público masivo que aporte pequeñas cantidades de dinero por cada persona, para que luego, con el monto que se reúne en conjunto, se logre llegar al dinero necesario.

Cuando se comenzó a implementar, era sinónimo de ‘micromecenazgo’ y estaba muy vinculado a las causas sociales o innovaciones que atraían a grupos determinados. Sin embargo, los emprendedores vieron cada vez más atractivo a este instrumento para obtener el capital necesario.

Es decir, “crowd” se vincula a mucha gente, y “funding” en relación a “financiamiento”.

Su crecimiento es tan importante que no sólo hay firmas locales y mundiales que se dedican a gestionar y reunir financiamiento colectivo para determinado proyecto, sino que también distintos gobiernos y entidades públicas se suman al *crowdfunding*.

VIII.7. Seguridad de las transacciones

Las empresas que pertenecen al sector *Fintech*, es decir, que ofrecen productos y servicios financieros basados en la tecnología, también deben incluir dentro de su estrategia de negocio la seguridad y protección de sus activos de información.

Hacerlo les permite, por ejemplo, garantizar un manejo seguro y confiable de los datos e información confidencial de sus clientes y usuarios, así mismo, contar con una seguridad informática sólida sirve para prevenir la materialización de riesgos y ataques cibernéticos como *phishing* o secuestro y robo de datos, que no solo afectan la operación de la empresa sino también su economía, reputación y credibilidad.

VIII.7.1. Importancia de la seguridad de la información en las *Fintech*

Para entender por qué es importante la seguridad de la información en las *Fintech*, primero hay que tener claridad sobre lo que esta significa. En general, la seguridad de la información se refiere al conjunto de medidas preventivas para salvaguardar y proteger la información y los sistemas informáticos, tanto de las organizaciones como de las personas.

Así mismo, de acuerdo con la Norma ISO 27001, la seguridad de la información tiene como prioridad preservar la confidencialidad, integridad y disponibilidad de los datos que son almacenados en los servidores y activos de información de la empresa.

Teniendo esto claro, entonces, ¿por qué es importante que las *Fintech* garanticen la seguridad de su información?

Al igual que cualquier otra empresa, las *Fintech* deben proteger todos sus activos de información y gestionar los riesgos a los que estos están expuestos, hacerlo les permite proteger todos los datos confidenciales de su negocio, incluidos datos personales e información financiera de sus clientes. Datos que en manos de ciberdelincuentes pueden causar grandes impactos y daños, tanto para la *Fintech* como para sus usuarios.

Por eso, es fundamental contar con un área de seguridad de la información o con el apoyo y acompañamiento de especialistas que puedan implementar estrategias para asegurar las tres propiedades claves de la información (confidencialidad, integridad y disponibilidad), así como una buena administración de esta, es decir, la identificación y gestión de:

- Todos los activos de información con los que cuenta la empresa.

- Los riesgos y ciberamenazas que se pueden materializar, por ejemplo, filtraciones de datos, *ransomware*, suplantación de identidad, fraudes, robo de información, entre otros.

- Los controles por implementar para mitigar la probabilidad o el impacto de los riesgos identificados.

- Los incidentes que se presentan.

- Los planes de acción a seguir.

Igualmente, quien esté a cargo de la seguridad de la información en la empresa *Fintech* debe ser consciente de que contar con buenas estrategias para salvaguardar la información no la exime de ser víctima, en cualquier momento, de un ataque por parte de ciberdelincuentes, que como se ha visto cada vez utilizan técnicas más novedosas y sofisticadas para atacar y lograr sus propósitos.

IX. FINTECH O BANCA TRADICIONAL

La pregunta es, ¿será *Fintech* vs bancos tradicionales? ¿O pueden unir fuerzas para desarrollar los servicios financieros que buscan los consumidores?

La tecnología *Fintech* ayuda a los propietarios de negocios, empresas y consumidores a administrar fácilmente sus finanzas y procesos comerciales de forma digital. Por lo general, se puede acceder a través de un ordenador u otros dispositivos, como un smartphone o una tableta.

El sector comenzó su desarrollo a finales de los años 1990, cuando surgieron las empresas de comercio electrónico e Internet. En el siglo XXI, esta tecnología se integró a los sistemas de *backend* de las instituciones financieras para digitalizar la banca.

Desde entonces, el *Fintech* ha cambiado su enfoque hacia los servicios orientados al consumidor. Ahora se utiliza en varios sectores, incluida la banca minorista, la gestión de inversiones, la recaudación de fondos y organizaciones sin fines de lucro, la educación y los servicios financieros para particulares. Las criptomonedas como bitcoin también son parte del desarrollo del *Fintech*.

Ambos tienen como objetivo brindar servicios financieros integrales a los consumidores, esa es realmente la única similitud.

Las empresas *Fintech* se consideran los mayores competidores de los bancos. El sistema financiero en el que se basan los bancos hoy en día se compone de algunas prácticas y procedimientos muy tradicionales y anticuados. A menudo le falta velocidad y agilidad. A medida que las exigencias de los consumidores aumentan en este sentido, van buscando soluciones financieras que satisfagan mejor sus necesidades.

Cuando se trata de innovación y avances, los bancos tradicionales se están quedando atrás y las empresas *Fintech* están dando un paso al frente. Quizás controlen por ahora una pequeña parte del sistema bancario mundial, pero los consumidores optan cada vez más por utilizarlas como sustituto de los bancos.

Las diferencias entre *Fintech* y banca tradicional se pueden dividir en cuatro categorías:

La manera de hacer negocio

- 1 - Las regulaciones
- 2 - El potencial de crecimiento
- 3 - Los factores de riesgo

- Las fintech están más avanzadas tecnológicamente; por eso utilizan principalmente plataformas digitales para prestar sus servicios. También tiene una distribución de mercado muy amplia, al poder trasladar el mismo servicio fácilmente de un país a otro.
- Por otro lado, los bancos tradicionales trabajan con una distribución de mercado limitada, más basada en el conocimiento específico de una zona (región, país) y apoyada por un modelo de atención personal.

La base de nuestro mundo es la tecnología. Poco a poco, el sistema bancario tradicional se está volviendo cada vez más dependiente también de las plataformas digitales para poder llevar a cabo su negocio.

Estas *Fintech* están desempeñando un papel muy importante para remodelar por completo el sistema bancario. Debido a que **la tecnología es cada vez más popular y accesible (casi todo el mundo tiene ya un smartphone)** los consumidores reclaman servicios sin complicaciones, cómodos y fáciles. Por eso, una mayor cantidad de personas optan por las *Fintech* para sus finanzas.

X. SOBRE LA REGULACIÓN DE LAS FINTECH

Al haber comprobado la existencia de un vacío legal en el ordenamiento jurídico nacional es necesario recurrir al derecho comparado con el fin de observar el tratamiento y entidad que los distintos sistemas jurídicos a nivel mundial le otorgan a nuestro objeto de estudio.

- 1) Las Fintech en la órbita del B.C.R.A como órgano de contralor.

Al igual que en la amplia mayoría de las legislaciones, concluiremos en que el B.C.R.A. debe ser el órgano de contralor de las empresas *Fintech*.

Desde el punto de vista técnico, la justificación se encontraría en el inciso h del Artículo 4° de la Carta Orgánica del B.C.R.A, la cual establece que es función del Banco “Proveer la protección de los derechos de los usuarios de servicios financieros y a la defensa de la competencia, coordinando su actuación con las autoridades públicas competentes en estas cuestiones”.

Actualmente, el B.C.R.A. ha tomado intervención junto con el Ministerio de Modernización encabezando jornadas de discusión en conjunto con abogados, contadores, entidades financieras y emprendedores denominadas “Mesas de Innovación Financiera”. Las primeras tres jornadas se celebraron en relación a tecnología, medios de pagos y servicios financieros. De esta forma, tanto emprendedores, entidades financieras, profesionales en la materia y funcionarios públicos trabajan en conjunto con el fin de sancionar una norma que permita desarrollar servicios financieros más sustentables y accesibles que garanticen la interoperabilidad. Al día de hoy, las conclusiones de la primera ronda de discusión se encuentran siendo analizadas por el B.C.R.A con el fin de emitir un dictamen que permita adoptar conclusiones firmes. Es de destacar que, desde el último cambio de administración, el B.C.R.A. ha buscado regular la utilización de tecnología por parte de las entidades financieras tradicionales mediante la apertura de caja de ahorros a distancia (Comunicación “A” 6059), el depósito electrónico de cheques (Comunicación “A” 6071 y “A” 6112) y la creación de plataformas para la realización de pagos móviles (Comunicación “A” 6043).

Pese a esto y tal como expresó su vicepresidente Lucas Llach, la entidad no tiene pensado regular las Fintech en el corto plazo.

2) La creación de *Sandboxes* que analicen cada unidad de negocio en particular.

Una solución extremadamente novedosa adoptada en Londres por la *Financial Conduct Authority* (FCA) y replicada en países como Australia y Singapur son los “*Sandboxes*”, es decir, bancos de prueba regulatorios que permiten evaluar el impacto que tiene una determinada regulación en un negocio particular llevado adelante por una empresa Fintech.

La utilidad de los *Sandboxes* radica en que gran parte de la regulación vigente en materia contractual y bancaria no se encuentra preparada o adaptada para la llegada de nuevas tecnologías, la dispensa del formato papel y el reemplazo de la firma ológrafa. De esta forma, los *Sandbox* podrán, mediante un método inductivo (desde lo particular a lo general) encontrar las bases de la futura regulación Fintech evitando que el mercado siga operando en un vacío legal.

Una posible solución sería que este “prueba y error regulatorio” sea paulatinamente incorporado al ordenamiento jurídico nacional creando a tal efecto un tipo exclusivo de Comunicación del B.C.R.A, por ejemplo, utilizando la letra “F” delante de la misma (Eg. Comunicación “F” 6789).

XI. POSTURA DE LAS ENTIDADES FINANCIERAS

La irrupción de las Fintech, trajo como consecuencia que las entidades bancarias tradicionales comenzaran a reclamar la fiscalización estatal permanente de las Fintech bajo la órbita del B.C.R.A esgrimiendo una violación por parte de éstas últimas de los incisos e) y m) del Artículo 2° de la Ley 25.156 como consecuencia de la potencial competencia desleal que supone la intervención en el mercado financiero de sociedades cuyos costos operativos y requisitos legales son significativamente menores a los de sus competidores por no estar sometidas al mismo régimen de fiscalización.

Este pedido por parte de las entidades financieras se magnificaría si tenemos en cuenta la inseguridad jurídica que bajo la regulación actual supone el esquema de acuerdo de voluntades que proponen las Fintech instrumentado únicamente por intermedio de *clicks* y sin verificación de firma alguna.

Por otro lado, los contratos bancarios en general difieren de una compraventa tradicional dado que requieren por parte del consumidor un conocimiento técnico superior a la media. Como consecuencia de esto y en virtud del artículo 1384 y siguientes del Código Civil y Comercial de la Nación (en adelante, “CCyC”), los contratos bancarios de carteras minoristas están encuadrados en el marco del derecho del consumo. El CCyC impone ciertas obligaciones respecto a la publicidad, información, forma y contenido de estos contratos con el fin de proteger al consumidor. De esta forma, resulta imperante analizar si el método de contratación utilizado por las Fintech debe o no cumplir con las disposiciones previstas en el Capítulo 12, Título IV, del Libro III del CCyC. Por su parte, el B.C.R.A también posee dentro de sus comunicaciones un texto ordenado actualizado al 7 de marzo de 2017 que regula la protección a los usuarios de servicios financieros. Lo que tanto el CCyC como las comunicaciones del B.C.R.A tienen en común es que ninguna contempla la posibilidad

de que estos servicios financieros sean prestados únicamente mediante la utilización de tecnología. En virtud de esto último, podemos concluir que prima facie las empresas Fintech no se encuentran obligadas a cumplir con estas previsiones.

Otra queja por parte de las entidades financieras tradicionales tiene que ver con el sistema de prevención de lavado de dinero y activos. Mientras que a nivel mundial éstas están siendo obligadas a una exhaustiva política de “Conozca a su Cliente” (“*Know Your Client*”) por ser sujetos obligados ante la Unidad de Información Financiera (UIF) en virtud de la Ley 25.246 - las Fintech no cuentan con ningún tipo de obligación en la materia.

Finalmente, el último inconveniente que las entidades bancarias alegan respecto de las Fintech es la falta de respaldo de una autoridad de contralor. La carta orgánica del B.C.R.A en su artículo 4° establece sus funciones, competencias y el rol que jugará la entidad en el sistema financiero argentino. Me gustaría detenerme sobre el inciso que transcribo a continuación:

“g) Regular, en la medida de sus facultades, los sistemas de pago, las cámaras liquidadoras y compensadoras, las remesadoras de fondos y las empresas transportadoras de caudales, así como toda otra actividad que guarde relación con la actividad financiera y cambiaria”.

Es por esto, que el objeto del análisis debe centrarse en si el B.C.R.A efectivamente cuenta con facultades suficientes para controlar aquellos negocios bancarios que se presten bajo la modalidad Fintech. Es por esto que podemos inferir que si bien el B.C.R.A. posee atribuciones para regular este tipo de negocios, estos no han sido regulados por no contar la entidad con facultades suficientes (eg. falta de capacidad técnica para ejercer el control, desconocimiento respecto al funcionamiento de las mismas, etc.). Esta última afirmación nos permite concluir en que existe un vacío legal en la materia.

Luego de concluir en la necesidad de un marco regulatorio para las Fintech, arribamos a las siguientes conclusiones:

1) Las Fintech en la órbita del B.C.R.A como órgano de contralor: al igual que en la amplia mayoría de las legislaciones, podemos concluir que el B.C.R.A. debe ser el órgano de contralor de las empresas Fintech.

Desde el punto de vista técnico, la justificación se encontraría en el inciso h del Artículo 4° de la Carta Orgánica del B.C.R.A 13, la cual establece que es función del Banco “Proveer la protección de los derechos de los usuarios de servicios financieros y a la defensa de la competencia, coordinando su actuación con las autoridades públicas competentes en estas cuestiones”.

2) La creación de *Sandboxes* que analicen cada unidad de negocio en particular: Una solución extremadamente novedosa adoptada en Londres por la *Financial Conduct Authority* (FCA) y replicada en países como Australia y Singapur son los “*Sandboxes*”, es decir, bancos de prueba regulatorios que permiten evaluar el impacto que tiene una determinada regulación en un negocio particular llevado adelante por una empresa Fintech.

Los Sandbox podrán encontrar las bases de la futura regulación Fintech evitando que el mercado siga operando en un vacío legal.

3) La firma digital. El Artículo 288 del Código Civil y Comercial de la Nación.

La Ley 25.506, promulgada en diciembre de 2001, creó el marco jurídico de la firma digital para igualarla con el *status* de la firma ológrafa.

El Artículo 3° sienta como principio general que donde se requiera una firma ológrafa, se podrá utilizar una firma digital. Este principio es de vital importancia para el tema que nos compete dado que constituye una de las pocas referencias claras de nuestro ordenamiento jurídico a formas alternativas de operatoria comercial y de acuerdo de voluntades.

Sin embargo, como consecuencia de los sucesos de público conocimiento ocurridos en diciembre de 2001 y por no ser obligatorio contar con una firma digital, ni el sector público ni el sector privado se han acogido a los beneficios que esta ley otorga.

Por su parte, el artículo 288 menciona que únicamente serán válidos los documentos electrónicos que cuenten con firma digital.

En consecuencia, nos encontramos en un callejón sin salida: ante la necesidad de legislar no solo las Fintech sino también su metodología de contratación debemos optar entre: i) modificar la redacción del Artículo 288 del CCyC permitiendo nuevamente la utilización de medios alternativos, como pueden ser la firma electrónica, las *application programming interfaces* (APIs) y/o la grafometría digital; o ii) abaratar los costos de los entes certificantes para que las personas físicas en general puedan ser obligadas a contar con una firma digital con la misma facilidad con la que hoy pueden contar con una clave de *home banking*.

Es de destacar que contar con estos métodos de contratación no solo dinamizaría el comercio, sino que también mejoraría la competitividad de nuestro país frente a otras economías facilitando así la llegada de inversores extranjeros.

XII. SIETE ÁREAS ESTRATÉGICAS DEL FUTURO FINTECH

El número de *startups Fintech* se ha duplicado en los dos últimos años. A finales de 2021 se contabilizaron cerca de 26.000 nuevas empresas, con un valor de financiación de 20.400 millones de dólares. Estos datos evidencian la buena salud por la que atraviesa el sector.

Según el informe *2022 Fintech Market Ecosystem*, su futuro pasa ahora por potenciar siete grandes áreas estratégicas. Los expertos hablan de la nueva banca, los sistemas de pagos, la financiación alternativa, la inversión, la regulación, el riesgo y el *Blockchain*.

New banking

El *new banking* abarca nuevas modalidades bancarias que dejan atrás el modelo tradicional apoyándose en el uso de nuevas tecnologías y modelos abiertos», afirman los autores del informe. La nueva banca centrará su actividad en cuatro grandes vertientes: venta de productos propios del banco; la construcción de un ecosistema enfocado en la distribución; vender las capacidades del banco como servicio y la creación de nuevas ofertas a través de la paquetización.

Pagos digitales

Los pagos a través de los canales sociales o las plataformas de mensajería crecerán con fuerza. «Las compañías financieras, y de otros sectores, que mantengan estructuras de pago tradicionales tendrán que adaptarse e innovar al ritmo demandado por el mercado: la modernización de la infraestructura de pago actual y tradicional es una premisa “sine qua non” para el avance en este segmento», aseguran los autores del estudio.

Finanzas alternativas

El *Equity Crowdfunding* se posiciona como una de las principales tendencias del futuro Fintech. Y no solo para financiar a empresas emergentes. Las compañías ya establecidas también entrarán en su radio de acción.

WealthTech

El *WealthTech* es una de las tendencias con más posibilidades de desarrollo por el interés que generan actividades como: las *Autonomous Finance* y los distintos tipos de *Robo Advisors*. Eso sí, el sector depende de los avances que se produzcan en Big Data y en la analítica de datos para poder desarrollar sus funciones básicas.

RegTech

Los datos, la privacidad y los sistemas de seguridad mantendrán la importancia que han adquirido en los últimos años. Su futuro está marcado por el enfoque ESG (es decir, criterios ambientales, sociales y de gobierno corporativo).

RiskTech

En los últimos años las inversiones en esta área se han dirigido a la analítica de datos, la IA y el Cloud. Pero los avances son limitados, de ahí que el 76% de los *players* del sector financiero estén planificando mejoras y nuevas acciones para los dos próximos años.

Blockchain

Esta tecnología ofrece información transparente sobre las transacciones y permite la verificación de los procesos y la autenticidad de los mismos. Proporcionar seguridad sobre las transacciones y mejora la sensación de confianza. El *Blockchain* es una herramienta con capacidad para liderar la transformación digital de cualquier empresa. De hecho, se espera que entre el 10% y el 15% de la infraestructura económica mundial la utilice de alguna manera en los próximos 10 años.

La irrupción de las Fintech trajo como consecuencia que las entidades bancarias tradicionales comenzaran a reclamar la fiscalización estatal permanente bajo la órbita del B.C.R.A. esgrimando una violación por parte de éstas últimas de los incisos e) y m) del Artículo 2° de la Ley 25.156 como consecuencia de la potencial competencia desleal que supone la intervención en el mercado financiero de sociedades cuyos costos operativos y requisitos legales son significativamente menores a los de sus competidores por no estar sometidas al mismo régimen de fiscalización.

Este pedido por parte de las entidades financieras se magnificaría si tenemos en cuenta la inseguridad jurídica que bajo la regulación actual supone el esquema de acuerdo de voluntades que proponen las Fintech instrumentado únicamente por intermedio de clicks y sin verificación de firma alguna.

XIII. ¿QUÉ ES EL CIBERCRIMEN?

El crecimiento del dinero digital y la bancarización, fenómeno que se profundizó a partir del surgimiento de la pandemia de Covid-19 en marzo de 2020, es una realidad en la Argentina que se viene desarrollando de la mano de nuevas propuestas financieras por parte de las *Fintech*, billeteras virtuales, la propia banca tradicional e incluso las iniciativas vinculadas a las criptomonedas. Sin embargo, acompañado de este crecimiento exponencial de la digitalización aumentó la ciberdelincuencia a nivel global y la Argentina no quedó exenta.

El fraude y estafa en cuentas bancarias, como el robo de claves de acceso a *homebanking* o de datos de tarjetas de crédito, fueron algunos de los delitos que más crecieron en la pandemia según la Unidad Fiscal Especializada en Ciberdelincuencia (Ufeci) dependiente de la Procuración General de la Nación.

Los ataques pueden darse a través de diferentes programas maliciosos (*malware*), como es el *ransomware*. Pero también pueden ocurrir a través de ataques de *phishing* o ingeniería social que no implica la instalación de un software dañino, sino que se da por el robo de datos confidenciales a través de diversos engaños.

Sin embargo, no todos los ciberdelitos se dan a través del uso de *malware*, también se pueden dar por medio de técnicas de ingeniería social. Esto alude a los métodos de engaño que usan los delincuentes para lograr que sean los propios usuarios quienes les brinden sus credenciales de acceso como la contraseña a cuentas bancarias, correos, perfiles en redes sociales y hasta WhatsApp.

Según la Unidad Fiscal Especializada en Ciberdelincuencia (Ufeci) en Argentina se registró sólo en 2020 “una suba del 70% de los delitos informáticos, lo que equivale a todos los delitos cometidos en los cinco años anteriores a la pandemia”. A modo de ejemplo señalaron en el organismo que “las estafas con compras electrónicas crecieron 106% y las denuncias de robo de identidad un 700 por ciento”.

Los casos más importantes reportados están relacionados a *phishing*, modificación no autorizada de la información y *spam*.

El cibercrimen es una actividad delictiva que se dirige a una computadora, una red informática o un

dispositivo en red, o bien que utiliza uno de estos elementos. La mayor parte del cibercrimen está cometido por cibercriminales o hackers que desean ganar dinero. Sin embargo, a veces el objetivo del cibercrimen es dañar computadoras o redes por motivos distintos a la obtención de dinero. Pueden ser motivos personales o políticos.

Las personas u organizaciones pueden cometer cibercrimen. Algunos cibercriminales están organizados, utilizan técnicas avanzadas y cuentan con grandes habilidades técnicas. Otros son hackers novatos.

El cibercrimen incluye una de las siguientes opciones o ambas:

- La actividad criminal *dirigida* a computadoras mediante virus y otros tipos de *malware*.
- La actividad criminal en la que se *usan* computadoras para cometer otros crímenes.

Es posible que los cibercriminales que *atacan* computadoras las infecten con *malware* para dañar los dispositivos o detener su funcionamiento. También puede suceder que usen *malware* para eliminar o robar datos. Por otro lado, los cibercriminales pueden evitar que los usuarios utilicen un sitio web o una red, o bien prevenir que una empresa provea un servicio de software a sus clientes, lo cual se denomina ataque de denegación de servicio (DoS, por su sigla en inglés).

El cibercrimen en el que se *utilizan* computadoras para cometer otros crímenes puede involucrar el uso de computadoras o redes para propagar *malware*, información ilegal o imágenes ilegales.

De acuerdo con un reporte publicado por *Cybersecurity Ventures*, los costos de los cibercrímenes pasaron de 3 trillones de dólares en 2015 (sí, trillones...) a 6 trillones en 2021, para 2025 el costo global será de 10.5 trillones de dólares. Estas proyecciones muestran un crecimiento exponencial que, de no existir las condiciones para su expansión, no serían tan elevadas, sin embargo, con la digitalización de prácticamente todos los procesos industriales, empresariales y de gobierno, el pastel no sólo se hizo más grande y rico, sino sumamente diverso.

XIV. ¿CUÁLES SON LOS CIBERDELITOS MÁS DENUNCIADOS EN LOS ÚLTIMOS AÑOS?

Más allá que los ciberdelitos vinculados a fraude disminuyeron en 2022, según un informe de la Asociación Argentina de Lucha Contra el Cibercrimen (AALCC) siguen representando un importante porcentaje.

Durante el año corriente, uno de los más denunciados fue el phishing a través de *Whatsapp*, redes sociales y correo electrónico. Aunque la mayoría quedó en grado de tentativa, muchos otros lograron concretar el robo de datos gracias a la inteligencia criminal y a técnicas de ingeniería social. En segundo lugar, y vinculado también a algunos casos de phishing, se encuentra fraude electrónico a través del robo de datos de tarjetas de crédito, la compra de productos en falsas tiendas digitales, como así también los fraudes bancarios.

En concordancia con el mismo estudio de la AALCC, los delitos que en general tienen fines económicos son:

- **Phishing.** Los *phishers* envían un correo electrónico fraudulento, haciéndose pasar por una entidad oficial, con el objetivo de obtener información personal y confidencial del destinatario.
- **Fraude electrónico.** *Phishing* bancario, *phishing* con tarjeta de crédito, compras en portales no validados, compras a través redes sociales y compras / validaciones de datos telefónicas.
- **Extorsión online.** Robo de contraseñas (*hackeo* o *phishing* previo), posterior a la práctica de Sexting (*sextorsión*), *ransomware* (encriptación por archivo malicioso) y posterior al robo de información.
- Usurpación o suplantación de identidad (en caso de robo y uso de información personal).
- Robo de datos financieros o de pagos con tarjeta.
- Robo y venta de datos corporativos.

- Ciberextorsión (exigir dinero para evitar un ataque bajo amenaza).
- Ataques de *ransomware* (un tipo de ciberextorsión).
- *Cryptojacking* (por medio del cual los hackers realizan la minería de criptomonedas usando recursos que no son propios).
- Ciberespionaje (en el que los hackers acceden a los datos gubernamentales o empresariales).
- Interferencia con sistemas de manera que se compromete una red.
- Infracción de derechos de autor.
- Apuestas ilegales.
- Venta de artículos ilegales en línea.
- Solicitud, producción o posesión de pornografía infantil.

XV. ALGUNOS EJEMPLOS DE CIBERCRÍMENES

A continuación, se presentan algunos ejemplos conocidos de distintos tipos de ataques de cibercrimen usados por los ciberdelinquentes:

XV.1. Ataques de *malware*

Un ataque de *malware* es aquel en el que un sistema informático o una red se infectan con un virus informático u otro tipo de *malware*. Una computadora que se ve comprometida por un *malware* podría ser usada por ciberdelinquentes con distintos propósitos, como robar datos confidenciales, utilizar la computadora para llevar a cabo otros actos delictivos o dañar los datos.

Se trata de un tipo de virus que encripta información, secuestra esos datos y bloquea accesos a los sistemas, y su finalidad es extorsionar, pidiendo la devolución de esta información sensible, a cambio de altas sumas de dinero, o incluso criptomonedas”.

XV.2. *Carding*

Se trata de una forma de estafa online que consiste en acceder ilegalmente al número de una tarjeta bancaria y a través de un software generan de manera aleatoria la fecha de expiración y el código de seguridad. Con esta información en su poder, los estafadores realizan compras pequeñas que pueden pasar desapercibidas para el usuario de la tarjeta.

XV.3. *Phishing*

Una estrategia de estafas que intenta “pescar” despistado a los usuarios de servicios financieros. Los ciberdelinquentes envían un correo electrónico con carácter urgente con la intención de manipular a sus víctimas y forzarlos a revelar información confidencial, como claves de acceso y nombres de usuario. En el mensaje, se incluyen enlaces fraudulentos que redirigen a páginas webs o aplicaciones apócrifas. El usuario engañado, creyendo estar entrando su cuenta legítima, entrega a los dueños del sitio falso su tarjeta.

Los mensajes de las campañas de phishing pueden contener archivos adjuntos infectados o enlaces a sitios maliciosos, o pueden pedir al destinatario que responda con información confidencial.

Un ejemplo conocido de estafa de phishing sucedió en el Mundial de fútbol de 2018. Según nuestro informe, el Mundial del engaño, la estafa de *phishing* de este evento involucró correos electrónicos que se enviaron a los aficionados al fútbol. Mediante estos correos electrónicos de spam, se intentaba atraer a los aficionados con viajes gratuitos falsos a Moscú, donde se celebraba el Mundial. A las personas que abrieron los enlaces incluidos en estos correos electrónicos e hicieron clic en ellos les robaron los datos personales.

XV.4. *Jackpotting*

Por otro lado, el *jackpotting* es otro ataque de carácter masivo y peligroso que no solo involucra tarjetas de crédito y débito, sino que también cajeros automáticos y retiro de dinero físico.

El *jackpotting* es una técnica para robar dinero que consiste en instalar un malware en un cajero automático. Los ciberdelincuentes consiguen acceso físico al núcleo de la CPU del cajero automático y lo infectan con un *malware*.

Este virus toma control total del dispositivo y los ciberdelincuentes dispensan el dinero hasta dejar el cajero sin efectivo. Por último, eliminan el software para no dejar rastro del ataque.

XV.5. Ataques de DoS distribuidos

Los ataques de DoS distribuidos (DDoS) son un tipo de ataque de cibercrimen que utilizan los cibercriminales para inhabilitar un sistema o una red. A veces se utilizan dispositivos IoT (del inglés “*Internet of Things*”, Internet de las cosas) conectados para lanzar ataques de DDoS.

Un ataque de DDoS satura un sistema mediante el uso de uno de los protocolos de comunicación estándar que utiliza para enviar spam al sistema con solicitudes de conexión. Los cibercriminales que realizan la ciberextorsión pueden utilizar la amenaza de un ataque de DDoS para pedir dinero. También es posible que un ataque de DDoS se utilice como táctica de distracción mientras se comete otro tipo de cibercrimen.

Un ejemplo famoso de este tipo de ataque es el ataque de DDoS que se produjo en el sitio web de la lotería nacional del Reino Unido en 2017. El ataque hizo que el sitio web y la aplicación móvil de la lotería quedaran sin conexión, por lo que los ciudadanos del Reino Unido no podían jugar. El motivo del ataque aún no se conoce, sin embargo, se sospecha que fue un intento de extorsión a la lotería nacional.

XVI. IMPACTO DEL CIBERCRIMEN

En términos generales, el cibercrimen está en aumento. Según el informe Estado de Resiliencia en Ciberseguridad 2021 de Accenture, los ataques de seguridad aumentaron un 31 % de 2020 a 2021. La cantidad de ataques por empresa aumentó de 206 a 270 de un año al otro. Los ataques a las empresas también afectan a las personas, ya que muchas almacenan datos sensibles e información personal de los clientes.

Un solo ataque, ya sea de vulneración de datos, *malware*, *ransomware* o DDoS, les cuesta a las empresas de todos los tamaños un promedio de 200.000 dólares. Como consecuencia, muchas de las empresas afectadas quiebran en un plazo de seis meses desde el ataque, según la empresa de seguros Hiscox.

Javelin Strategy & Research publicó un estudio sobre el robo de identidad en 2021 en el que se reveló que las pérdidas por robo de identidad de ese año sumaban un total de 56 000 millones de dólares.

Tanto para las personas como para las empresas, el impacto del cibercrimen puede ser significativo, principalmente, por los perjuicios económicos, pero también por la pérdida de la confianza y el daño de la reputación.

XVII. ¿QUÉ MEDIDAS HA TOMADO EL SECTOR FINANCIERO PARA COMBATIR EL CIBERCRIMEN?

En septiembre de 2022, los principales actores del sector financiero en la Argentina se unieron para mejorar la seguridad de los usuarios por medio de un importante acuerdo de cooperación. El convenio fue firmado por la Asociación de Bancos de la Argentina (ABA), Asociación de Bancos Públicos y Privados de la República Argentina (ABAPRA), Asociación de la Banca Especializada (ABE), la Asociación de Bancos Argentinos (ADEBA), y la Cámara Argentina Fintech (Cámara Fintech).

El pacto apunta a “profundizar acciones preventivas y maximizar el control de transferencias sospechosas entre cuentas bancarias y virtuales a través de una comunicación integral entre las entidades adherentes.” Asimismo, facilitará sistematizar el seguimiento de casos y la protección de los usuarios y consumidores del ecosistema financiero. Las entidades firmantes destacan, además, el inicio de una nueva

etapa en el combate del delito, que se suma a las inversiones en tecnología y campañas de concientización, donde las entidades continuarán focalizando sus esfuerzos.

XVIII. OPINIÓN DEL GAFI

El Grupo de Acción Financiera Internacional (GAFI) reconoce que la adopción de nuevas tecnologías en pos de la prevención del lavado de dinero y financiamiento del terrorismo trae aparejado beneficios y desafíos para las empresas. Entre los primeros, destaca la reducción de costos y una mayor inclusión financiera, dentro de un sistema más transparente. Mientras que, por el otro lado, el GAFI ha identificado desafíos regulatorios (con especial énfasis en el apoyo necesario del regulador) y operacionales, asociados a la adaptación necesaria frente a la implementación de nuevas tecnologías.

XIX. ¿CÓMO PUEDEN ACTUAR LAS FINTECH PARA MEJORAR SUS SOLUCIONES TECNOLÓGICAS Y CUÁLES SON LOS DESAFÍOS DE CARA A LA POSPANDEMIA?

No obstante, de la mano de las técnicas de Aprendizaje Automático (*Machine Learning*), y con apoyo en el Aprendizaje Profundo (*Deep Learning*), se pueden crear modelos flexibles para la detección automática de fraude en tiempo real: estos modelos evalúan el comportamiento individual del cliente a medida que se produce. Analizan constantemente su actividad “normal”, por lo que cuando se detecta una anomalía pueden marcar o bloquear automáticamente un pago para que un analista lo revise. Y visibilizan patrones de fraude que no son aparentes al ojo humano.

Utilizar técnicas de *Machine Learning*, en este caso en particular, es como tener varios equipos de analistas al mismo tiempo que ejecutan cientos de miles de consultas y comparan todos los resultados para encontrar el óptimo. Esta compleja clasificación de perfiles críticos se realiza en tiempo real y solo requiere milisegundos.

Los principales beneficios de los sistemas de detección de fraude basados en datos, que recurren tanto a *Machine Learning* como *Deep Learning*, son:

- **Precisión:** aumenta el poder de detección al procesar grandes volúmenes de datos masivos y focalizan la búsqueda dentro de subconjuntos de datos detectados anómalos que poseen una mayor cantidad de fraudes que el promedio.
- **Eficiencia:** el volumen de datos organizacionales a ser analizados requiere la automatización de los procesos para poder explotar al máximo su potencial y acelerar el proceso para la organización, incrementando las probabilidades de identificación del delito cometido o de los perfiles fraudulentos.
- **Escalabilidad:** estos sistemas permiten aumentar el volumen de transacciones y mejoran con conjuntos de datos más grandes porque le proveen al sistema más ejemplos de clientes genuinos y fraudulentos. Esto significa que el modelo puede identificar las diferencias y similitudes entre los comportamientos más rápidamente y usar estos patrones para predecir el fraude en transacciones futuras.
- **Ahorro:** el costo humano de esa tarea sería inmenso, mientras que el costo actual se traduce en servidores en funcionamiento. A diferencia de los humanos, las máquinas pueden realizar tareas repetitivas y tediosas sin detener su trabajo (24/7), y escalan las decisiones a un humano cuando se necesita información específica.

XX. EL 2023 PARA LAS FINTECH, LO QUE SE VIENE

La perspectiva para los próximos años es que el cambio que introdujeron las Fintech al mundo financiero global continúe con más usuarios, más transacciones, más empleo y más inversiones.

Ninguno de estos factores parece sufrir síntomas de desaceleración. Por el contrario: el fenómeno digital ha penetrado hasta en los instrumentos financieros más tradicionales, como ser el cheque, que está siendo reemplazado velozmente por el *e-cheq* (de noviembre del 2020 a septiembre de 2022 pasó del 11,3 al 31,5% de participación de mercado, mientras que si se mide en montos consolidados pasó del 30,9% al 57,4%, según datos del BCRA).

Además, aún en contextos de incertidumbre económica, la cantidad de *Fintechs* en Argentina continuará en aumento, escenario que también se replicará en distintos países de Latinoamérica y Europa.

La transformación digital es un hecho. Los pagos digitales han logrado consolidarse como una alternativa de la forma en que los ciudadanos se relacionan con sus necesidades financieras.

XXI. CONCLUSIONES

En el escenario actual, la economía digital está obligada a incorporar esquemas para la detección de riesgos y elaborar políticas de prevención de lavado en forma permanente para evitar el avance de la ciberdelincuencia. Y este es un desafío que puede resultar complejo. Es allí donde irrumpe la tecnología otra vez como un aliado para las empresas, un eslabón clave que les permitirá cumplir con el marco normativo y, a su vez, moderar los costos.

Considero que la única solución para permitir el avance y el desarrollo de estas nuevas tecnologías no radica en legislar en contra de ellas, sino en generar regulaciones provisorias como el caso de Gran Bretaña que monitorean el desarrollo de las mismas sin afectar su bajo costo, es decir, su principal ventaja competitiva.

Es evidente que la mayor carga regulatoria es una tendencia que vino para quedarse. La regulación busca extender progresivamente su ámbito de aplicación, incluyendo así nuevos sujetos regulados.

Además, en este recorrido vimos cómo la innovación, a través de estas organizaciones, busca democratizar los servicios financieros y devolver al público la confianza en ellos.

Finalmente, considero que estamos ante el comienzo de una nueva era en materia de derecho financiero y bancario. Por lo tanto, sería un error pensar que los nuevos actores se limitarán a pensar esta nueva era con las mismas herramientas utilizadas durante los últimos tres siglos.

En consecuencia, sería errado aplicar por analogía la ley de cheque o los principios consagrados en ella. En mi opinión, no debemos pensar los nuevos avances como una evolución de las instituciones ya existentes, sino como herramientas absolutamente distintas que deben ser analizadas jurídicamente en forma independiente a lo ya conocido.

Las *Fintech* no pueden ser sólo innovadora en la forma en que celebran sus negocios, también deben serlo con la información que brindan, las medidas de seguridad que toman, la protección de los datos de sus clientes y al respeto de su privacidad.

BIBLIOGRAFÍA

Peralta, Gabriel Alberto. *Fintech: El Futuro de la Industria Financiera*. Universidad Nacional de Cuyo. Facultad de Ciencias Económicas.

Oltavares, Juan J. El Status jurídico de las empresas *Fintech* y el desafío que supone su regulación. *Revista Argentina de Derecho Comercial y de los Negocios*. Número 19. marzo 2018.

Damen, Alexis. Bancos Tradicionales vs *Fintech* ¿Competidores o Complementarios? 819.05.21.

Vaccarello, Miguel Otero. *Fintech vs. Banca Tradicional: la evolución del sector financiero*.

Liceda, Ernesto. *Fintech entre la inclusión financiera y el cibercrimen*. 06.08.20.

Giménez, Mónica María. ¿Qué es el Crowdfunding? Una nueva forma de financiar proyectos. Universo Crowdfunding.

Giménez, Mónica María. Seguridad de la información en las Fintech. 30.03.22.

Kaspersky. ¿Qué es el cibercrimen? Cómo protegerse del Cibercrimen.

García Alejandra. Las Fintech y su estrecha relación con la ciberseguridad. 30.07.21.

Blanco Gómez Daniel. Estafas virtuales. Cuáles son los delitos más comunes y cómo prevenirlos. 12.06.22.

Ciberdelitos en Bancos y Fintech. Panorama y soluciones. Equipo Nosis. 29.09.22.