Desafíos legales de las identidades digitales en la industria fintech

Por Andrés Chomczyk

1. Introducción

En términos generales, para la gran mayoría de los actos comerciales sencillos y cotidianos no se nos exige acreditar nuestra identidad. Sin embargo, existen actos para los cuales la otra parte con la cual estamos tratando nos exigirá algún documento o tipo de documento identificatorio para validar nuestra identidad.

Esto suele responder a dos grandes motivos: (i) contar con datos concretos sobre la contraparte para evitar medidas probatorias preliminares tendientes a la identificación del potencial demandado; y (ii) cumplir con alguna carga normativa, como por ejemplo aquella relativa a la prevención de lavado de dinero y financiamiento del terrorismo. Tal como se señala en un informe del World Economic Forum: "*La identidad resulta fundacional para muchas de las transacciones que ocurren en la sociedad actual. En cualquier negocio con requisitos acerca de las partes contratantes -como que sean de cierta edad o que residan en una determina jurisdicción- deben existir algunas estructuras para permitirles a estas conocer cierta información sobre la otra, así como también para tener confianza en que esa información es cierta*"[1].

Ahora bien, estas cuestiones están, en mayor o menor medida, resultas cuando se trata del comercio tradicional o físico. En esos casos existen formas certeras de lograr la identificación de las partes: la exhibición de un documento estatal de identificación, una comprobación de identidad por parte de funcionario público, una certificación de firma notarial o bancaria, etc. Sin embargo, al llevar la problemática de la identidad al mundo digital nos encontramos con algunas barreras propias de este ámbito que obstaculizan la identificación de las personas. Se han intentado desplegar ciertas soluciones que llevaban algunas de las herramientas del mundo físico al digital pero su éxito ha sido relativo: desde identidades digitales estatales con serios

[1] WORLD ECONOMIC FORUM, *A Blueprint for Digital Identity – The Role of Financial Institutions in Building Digital Identity*, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf, pág. 32. (Fecha de consulta 19 de febrero de 2019). La traducción es propia.

problemas de seguridad informática[2] hasta el uso de esquemas firmas digitales con cadenas legales de autenticación.

El mundo financiero también ha recibido el impacto de la tecnología bajo el nombre de tecnología financiera -o *financial technology*, en inglés, y abreviado como *fintech*. Esto implica la posibilidad de ofrecer productos y servicios financieros sin la necesidad que el cliente concurra físicamente a un banco; de allí la necesidad de contar con formas de identificación digital robustas[3].

En este marco es que se considera necesario hacer un breve análisis sobre que es lo que se entiende por identidad digital y los desafíos que representa en la operatoria digital de las compañías *fintech* este cambio de paradigma.

2. ¿Qué es la identidad digital y como se encuentra regulada?

Siguiendo el concepto expuesto en el artículo del World Economic Forum antes mencionado, la identidad no es un concepto integrado por un único elemento sino que es el producto de la

[2] En tal sentido, Estonia y España han tenido serios problemas de seguridad informática sobre las identidades digitales emitidas por esos países. Para más información se recomienda la lectura de los siguientes enlaces: (i) https://e-estonia.com/card-security-risk/ (Fecha de consulta 19 de febrero de 2019); (ii) MARDISTE, David, "Estonia orders online ID lock-down to fix security flaw", *Reuters*, 03.11.2017, https://www.reuters.com/article/us-estonia-cyber/estonia-orders-online-id-lock-down-to-fix-security-flaw-idUSKBN1D312Q (Fecha de consulta 19 de febrero de 2019); (iii) AASMAE, Kalev, "Estonia's ID card crisis: How e-state's poster child got into and out of trouble", *ZDNet*, 13.11.2017, https://www.zdnet.com/article/estonias-id-card-scrisis-how-e-states-poster-child-got-into-and-out-of-trouble/ (Fecha de consulta 19 de febrero de 2019); (iv) MEYER, David, "ID card security: Spain is facing chaos over chip crypto flaws", *ZDNet*, https://www.zdnet.com/article/id-card-security-spain-is-facing-chaos-over-chip-crypto-flaws/ (Fecha de consulta 19 de febrero de 2019); y (v) GARCIA, Jose Antonio – PERALES, Julio, "La seguridad del DNIe, otra oportunidad perdida", *Suplemento Cinco Días*, *El País*, https://cincodias.elpais.com/cincodias/2017/11/13/midinero/1510576751_274226.html (Fecha de consulta 19 de febrero de 2019).

[3] A modo de ejemplo, durante el año 2018 el Banco Central de la República Argentina (el "BCRA") ha continuado con su impulso de mesas de innovación financiera poniendo el foco de una de ellas sobre esta temática y el uso de nuevas tecnologías para hacer frente a este desafío. Tal es así que como resultado se ha presentado una solución de pasaporte financiero basado en tecnología blockchain por parte de dos compañías del sector (la red de procesamiento de transacciones Link y la empresa de firma electrónica Signatura). Para mayor información se recomienda la lectura de los siguientes enlaces: (i) http://web2.bcra.gob.ar/SistemasFinancierosYdePagos/Innovacion_financiera.asp (Fecha de consulta 19 de febrero de 2019); y (ii) MANFREDI, Melina, "El Central quiere que los clientes sean dueños de sus datos bancarios", *El Cronista Comercial*, 09.11.2018, https://www.cronista.com/finanzasmercados/El-Central-quiere-que-los-clientes-sean-duenos-de-sus-datos-bancarios-20181109-0036.html (Fecha de consulta 19 de febrero de 2019).

conjunción de diferentes aristas sobre una misma persona[4]. En este sentido, la identidad estaría dada por tres tipos de atributos: (i) inherentes; (ii) acumulados; y (iii) asignados[5].

Todos estos elementos que forman parte de la identidad de las personas pueden ser clasificados como datos personales[6]. Esto no es una cuestión menor porque implica que toda la problemática de la identidad digital debe ser abordada desde la óptica del régimen legal de la protección de los datos personales, como por ejemplo la Ley Argentina de Protección de Datos Personales o el RGPD, junto con la normativa propia del sector, en este caso la regulación de la industria fintech.

Todo sistema de identidad, en mayor o medida, funciona con terceros de confianza que validan ciertos atributos de la identidad de las personas; cuando estas tienen que demostrar su identidad, recurren a esos terceros de confianza y bien les solicitarán que validen la información presentada o se les pedirá confirmación de información ya validada. En líneas generales, según el World Economic Forum, los sistemas de identificación funcionan con cuatro roles (usuarios, proveedores de identidad, receptores de información y entidades de control) y todos contribuyen a que las entidades que necesitan acreditar su identidad puedan hacerlo gracias a las validaciones de los proveedores de identidad, bajo el control de una entidad que fija las reglas de procedimiento y los estándares a seguir[7].

[4] Cfr. WORLD ECONOMIC FORUM, Idem, Pág. 41.

[5] Los primeros son aquellos forman parte esencial de la persona y responden principalmente a sus características biológicas inalterables. Los segundos son las características que se van obteniendo o desarrollando a lo largo de la vida, como el comportamiento, el conocimiento, entre otros. Por último, los atributos asignados son aquellos que la entidad adquiere a partir de sus relaciones con otras entidades, como por ejemplo un número de identificación estatal, un título obtenido de una institución educativa, un número de teléfono, etc.

[6] En este sentido, el art. 2 de la Ley 25.326 (la "Ley Argentina de Protección de Datos Personales") define a los datos personales como "información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables"; inclusive, parte de estos elementos de la identidad pueden ser calificados como datos sensibles, los cuales son "datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual". La definición brindada por la normativa argentina esta en línea con las disposiciones en materia de protección de datos de casi todo el mundo, como por ejemplo las definiciones brindadas por el artículo 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (el "RGPD").

[7] Cfr. WORLD ECONOMIC FORUM, pág. 47. Según el World Economic Forum, en la actualidad se pueden distinguir cinco tipos de sistemas de identidad: (i) sistemas de gestión de identidad internos; (ii) sistema de autentición externa; (iii) sistemas centralizados de identidad; (iv) sistemas de autenticación federados; y (v) sistemas distribuidos de identidad.

Internet, por sus características, ha dado lugar a diferentes sistemas de identificación, los cuales, a criterio de Christopher Allen[8], han estado coexistiendo casi desde el mismo nacimiento de Internet. Este autor sostiene que todos los sistemas desplegados hasta el momento presentan, en mayor o menor medida, el problema de depender de una entidad centralizada y, en consecuencia, quitar el foco del usuario; es decir, todos estos sistemas siguen el esquema donde el responsable del tratamiento es quien decide sobre los datos personales, con algunas intervenciones del usuario que generan una falsa sensación de control sobre los datos integrantes de la identidad. Allen sostiene que la única forma de generar una identidad que ponga el foco en el usuario y no las entidades que validan la información es darle autonomía al usuario y hacerlo soberano de sus datos; estas conclusiones llegan también el Banco Mundial[9] así como también la iniciativa de Naciones Unidas, ID2020[10].

Algunas normas a nivel internacional, como el RGPD y toda la regulación inspirada en aquel como el anteproyecto de reforma a la Ley Argentina de Protección de Datos Personales junto con la Directiva (UE) 2015/2366[11] ("PSD2"), han hecho eco de estos desafíos y presenta herramientas para devolver el control de los datos personales a los titulares de estos con medidas como la privacidad por defecto y desde el diseño, la eliminación del consentimiento tácito como base legal para el tratamiento, el derecho a la información y a la oposición de elaboración de perfiles, el derecho a la portabilidad de los datos y la promoción de la competencia en la provisión de servicios accesorios al sistema financiero tradicional. Dada la novedad de estas nuevas normas, todavía queda camino a recorrer para ver si las mismas

[8] Cfr. ALLEN, Christopher, "The Path to Self-Sovereign Identity", *Life With Alacrity*, 25.04.2016, http://www.lifewithalacrity.com/previous/2016/04/index.html (Fecha de consulta 19 de febrero de 2019). Allen distingue que se hemos atravesado, hasta el momento, cuatro etapas en materia de sistemas de identificación en Internet: (i) sistemas centralizados, como ICANN para la asignación de nombres de dominio; (ii) sistemas federados, como Passport de Microsoft; (iii) sistemas centrados en el usuario, como las soluciones basadas en 0Auth; y (iv) sistemas de identidad auto soberana, de los cuales a la fecha no hay ninguna implementación concreta.

[9] Cfr. DAHAN, Mariana – EDGE, John, "The World Citizen: Transforming Statelessness into Global Citizenship", *Blog Information and Communications for Development (IC4D)*, 25.11.2015, http://blogs.worldbank.org/ic4d/world-citizen-transforming-statelessness-global-citizenship (Fecha de consulta 19 de febrero de 2019).

[10] Cfr. ID2020, "Why Digital Identity?", https://id2020.org/digital-identity-1/ (Fecha de consulta 19 de febrero de 2019).

[11] Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE

proporcionan las herramientas jurídicas apropiadas para lograr este propósito de hacer soberano al usuario de sus datos.

3. Principales desafíos relativos a la identidad para la industria *fintech*

Se puede considerar que las *fintechs* tienen tres grandes problemas en lo que hace a la identidad digital de sus clientes: (i) asegurarse que el usuario sea quien dice ser; (ii) prevenir el lavado de activos y financiamiento del terrorismo; y (iii) que todos estos datos recolectados sean tratados en conformidad con la normativa en materia de protección de datos personales.

a) Identidad del usuario

El análisis legal sobre este punto difiere si la empresa en cuestión se encuentra sometida o no a las normas del BCRA. En razón de ello, el análisis será separado entre las compañías fintech sometidas a la regulación general, principalmente el Código Civil y Comercial de la Nación (el "CCyCN") y la Ley Nº 24.240 y sus modificatorias (la "Ley Argentina de Defensa del Consumidor"), aún cuando parcialmente estén alcanzadas por alguna norma del BCRA, como las entidades proveedoras de crédito no financieras, frente a aquellas compañías sometidas de forma plena a la regulación del BCRA por ser entidades financieras bajo la Ley Nº 21.526 (la "Ley Argentina de Entidades Financieras").

Toda la operatoria de estas empresas es realizada de forma electrónica. Con lo cual, la celebración de los acuerdos con sus clientes también es ejecutada con medios electrónicos. En consecuencia, para la firma de los acuerdos existen dos alternativas según el Ley Nº 25.506 (la "Ley Argentina de Firma Digital"): (i) usar firmas electrónicas; o (ii) usar firmas digitales. Los efectos de ambas son diferentes, ya que las segundas gozan de ciertas presunciones legales (autoría e integridad del documento firmado) que las primeras no; sin embargo, la doctrina[12] es pacífica en cuanto al uso de firmas electrónicas para aquellos acuerdos que no tengan requisitos especiales en cuanto a la forma de su celebración. La gran mayoría de los acuerdos que son celebrados entre las empresas fintech y sus usuarios pueden, y en la práctica son,

[12] Para profundizar en la cuestión, se recomienda la lectura de los siguientes artículos: (i) MORA, Santiago: "Análisis de las disposiciones sobre firmas digitales, firmas electrónicas y documentos digitales en el acceso al crédito y la inclusión financiera. Varios aciertos y un desacierto", *La Ley Argentina*, *Suplemento Especial "Decreto de desburocratización y simplificación: Impacto en el mundo empresarial y en la gestión pública"*, pág. 214; y (ii) CHOMCZYK, Andrés, "Reflexiones sobre el incipiente marco legal de la industria fintech en Argentina", *RDYNT – Revista de Derecho y Nuevas Tecnologías*, Nº 1, 2017.

firmados con firmas electrónicas, generalmente mediante la adhesión a términos y condiciones generales[13].

En lo que hace a las entidades no financieras, estas no tienen ningún requisito legal que deban cumplir para acreditar la identidad de la contraparte, salvo que la operación en particular requiera algún tipo de verificación por aplicación de una norma especial que demande ello al momento de contratar; el mismo BCRA reconoce esta cuestión en un artículo publicado en uno de sus canales oficiales[14].

Es importante señalar que el hecho de basar toda la operatoria en firmas electrónicas, aún siendo ello posible, lleva la consecuencia que toda cuestión relativa a la identidad del firmante debe ser demostrada por quien alega la validez de la firma, si es que esta es desconocida, y por lo tanto de la identidad subyacente, mientras que si se usaran firmas digitales esto sería al revés. En todo caso, el desconocimiento de la firma pasará a ser una cuestión que deberá ser objeto de prueba en un proceso judicial y será de aplicación la previsión del artículo 319 del CCyCN que deja en manos del juez la ponderación sobre la validez de la firma, quien la analizará en función de los elementos de prueba que le sean aportados; de allí la importancia de generar todos los elementos probatorios posibles, y si es posible independientes entre sí, para que la compañía sea capaz de generar convicción en el juez.

Es decir, este tipo de empresas usan medios de identificación que logren acreditar de alguna forma fehaciente que quien dice ser el usuario es efectivamente esa persona; a tales efectos, se recurre a diversos medios como la carga de una foto de un documento de identidad -generalmente combinado con una foto de la persona sosteniendo el documento en cuestión al lado de su cara-, la revisión de ese documento contra una base de datos públicas[15], la

[13] Esta forma de operar ha sido admitida tanto por el BCRA, conforme he mencionado previamente, así como también por la Comisión Nacional de Valores al admitir la secutirización de créditos digitales generados por estas plataformas mediante la constitución de fideicomisos financieros cuyos activos subyacentes son los créditos en cuestión.

[14] Ver CANE, Marcos – HEFFES, Julieta – SANCHEZ, Sol, "Las Fintech y la oferta de créditos online: una aproximación a sus aspectos jurídicos", *Ideas de Peso*, 27.08.2018, https://ideasdepeso.com/2018/08/27/las-fintech-y-la-oferta-de-creditos-online-una-aproximacion-a-sus-aspectos-juridicos/ (Fecha de consulta 19 de febrero de 2019).

[15] Por ejemplo, en la República Argentina el Registro Nacional de las Personas ha lanzado el Sistema de Identidad Digital para realizar validaciones bajo demanda de datos biométricos contra aquellos registrados por esa entidad. Para más información, ver el siguiente enlace https://www.argentina.gob.ar/sid-sistema-de-identidad-digital (Fecha de consulta 19 de febrero de 2019).

vinculación con otros elementos de su identidad -como un número de móvil, una cuenta de correo electrónico, etc.-, la realización de preguntas sobre su historial crediticio, entre otras. Es importante señalar que toda esta prueba generada tiene como consecuencia la recolección de datos personales del usuario, siendo aplicable la Ley Argentina de Protección de Datos Personales, problemática que se verá más adelante. Por lo tanto, este tratamiento de los datos deberá ser realizado contando con una base legal para ello -la cual a mi criterio estará dada por el consentimiento del usuario así como también por la ejecución del contrato que une a las partes- y cumplir con el deber de información, así como también con el resto de las obligaciones propias del responsable del tratamiento.

Por el otro lado, las entidades financieras sujetas a la Ley Argentina de Entidades Financieras, y aquellas entidades obligadas a seguir las prescripciones en materia de conocimiento de sus clientes dictadas por el BCRA, presentan mayores inconvenientes en torno a los criterios que deben adoptar.

Una lectura sistemática del marco normativo del BCRA lleva a considerar que únicamente cuando esta entidad autoriza el conocimiento a distancia de los clientes, ello sería posible. El principal motivo de ello es evitar un riesgo sistemático de desconocimiento de las operaciones y jaque al sistema financiero en su totalidad.

En este sentido, la Comunicación "A" 6059, junto con sus modificatorias, la cual introdujo la novedad para las entidades financieras de poder abrir cuentas bancarias -cajas de ahorro- a nuevos clientes de forma no presencial. Al respecto, la norma del BCRA adoptó un criterio amplio y tecnológicamente neutral al únicamente pedirles a las entidades financieras usen aquellos medios que les permitan dar cumplimiento con la normativa en materia de prevención de lavado de activos y financiamiento del terrorismo, cuestión que se verá en el siguiente punto, y que se cumpla con la normativa relativa a canales electrónicos así como aquella dictada en materia de conservación, integridad, autenticidad y confidencialidad de los instrumentos ejecutados por la entidad financiera con el cliente, la cual también fue actualizada al mismo tiempo mediante el dictado de la Comunicación "A" 6068 y 6072, junto con sus modificatorias. Es importante señalar que todo el proceso de identificación, aún realizado a distancia, debe contemplar y basarse en los documentos de identificación admitidos por el BCRA, en particular la Comunicación "A" 5717 y 5728 a la fecha de este artículo.

En función de ello, las entidades financieras en Argentina son capaces de interactuar con nuevos clientes de origen digital para la apertura de cajas de ahorro. Por lo tanto, todas las operaciones que puedan realizarse desde estas podrán ser realizadas por clientes que sean nativos digitales para la institución financiera. Sin embargo, para la oferta del resto de los productos y servicios bancarios a clientes que sean nativos digitales, las entidades sujetas a la Ley Argentina de Entidades Financieras deberán aguardar la autorización general del BCRA o bien solicitar una autorización especifica para ello, como están haciendo algunos bancos digitales que han salido al mercado en los últimos meses del 2018.

b) Prevención de lavado de activos y financiamiento del terrorismo

El segundo gran problema al que la industria fintech tiene que hacer frente es la prevención de lavado de activos y financiamiento del terrorismo generado por usuarios que no son conocidos de forma presencial. Tradicionalmente, este tipo de clientes era considerado más riesgoso, desde el punto de vista de la prevención de lavado de activos y financiamiento del terrorismo, que los clientes identificados en forma presencial. Sin embargo, esta posición esta siendo revisada actualmente por el Grupo de Acción Financiera Internacional[16] y, en cierta medida, ya ha sido receptada por la Unidad de Información Financiera (la "UIF") en Argentina al admitir expresamente la posibilidad de hacer el proceso de conocimiento del cliente a distancia con el dictado de varias resoluciones que recogen este principio.

Es importante remarcar que la gran mayoría de las *fintechs* no deben considerar esta normativa por no recibir fondos de sus clientes en custodia y que puedan provenir de origen delictivo; la gran mayoría de las *fintechs* en Argentina están volcadas a la vertical de préstamos. Asimismo, la recepción de fondos de los clientes para su custodia es una cuestión que las *fintechs* suelen evadir para evitar la aplicación del principio de intermediación financiera, consistente en la intermediación habitual entre la oferta y la demanda de recursos financieros y la sujeción, como consecuencia de la aplicación del giro final del artículo 2 de la Ley Argentina de Entidades Financieras, a la regulación de aquella normativa, la autoridad del BCRA y la aplicación de otras normas como aquellas dictadas por la UIF. Sin embargo, existen ciertos sectores, como las verticales de pagos, criptomonedas y dinero electrónico, que si toman fondos del público y

[16] FAFT, "Statements on Virtual Assets and Digital ID", 06.11.2018, https://fintech.mourant.com/articles/fatf-statements-on-virtual-assets-and-digital-id.aspx (Fecha de consulta 19 de febrero de 2019).

aplican medidas de prevención de lavado de activos y financiamiento del terrorismo, ya sea de forma voluntaria o obligatoria, según sea el caso.

La Ley Nº 25.246 (la "Ley Argentina de Prevención de Lavado de Activos y Financiamiento del Terrorismo") impone una serie de obligaciones a un conjunto de sujetos obligados a los fines que estos adopten medidas para prevenir las actividades que tengan por finalidad lavar fondos de origen delictivo o financiar al terrorismo por su situación en el sistema mundial de movimientos de dinero. Fuera de estos sujetos obligados, no hay deber de realizar las tareas exigidas por la normativa referenciada, salvo en lo indispensable para evitar la comisión de algún delito previsto en el Código Penal Argentino[17].

En tal sentido, la conclusión inmediata es que las compañías *fintech*, salvo que estuvieran expresamente incluidas entre los sujetos obligados, no tienen la obligación de conocer a su cliente con la rigurosidad que exige la Ley Argentina de Prevención de Lavado de Activos ni con la misma finalidad que exige esa norma. Los objetivos de conocimiento del cliente y determinación de la identidad de los usuarios digitales son únicamente aquellos señalados previamente en el capítulo anterior.

Ahora bien, es cierto que las compañías *fintech* forman parte del sistema financiero -inclusive, muchas veces se promocionan u operan bajo el lema de ser entidades que luchan por la inclusión financiera de las personas y como puente entre la desbancarización y el sistema financiero tradicional. Como consecuencia de ello, sucede que estas empresas son requeridas de brindar más información sobre algunas de sus operaciones con sus clientes por parte de los sujetos obligados. A modo de ejemplo, es común que las empresas que ofrecen servicios relacionados con criptomonedas sean requeridas de por ese motivo e, inclusive, en ocasiones se procede a cerrar sus cuentas[18]. Por lo tanto, estas entidades pasan a tener la necesidad de

[17] El presente artículo no tiene por finalidad indagar sobre esta variable pero, a mero modo de ejemplo los antecedentes jurisprudenciales en la materia no son alentadores e, inclusive, con graves fallos de interpretación en materia penal. En tal sentido, se sugiere la lectura el auto de procesamiento dictado en el marco del operativo "Bobinas Blancas", únicamente en lo que hace al imputado Emmanuel García. El mismo se encuentra disponible en la página web del Centro de Información Judicial en el artículo "Procesaron a diez imputados en el marco de la causa "Bobinas Blancas", https://www.cij.gov.ar/nota-26599-Procesaron-a-diez-imputados-en-el-marco-de-la-causa--Bobinas-Blancas--.html (Fecha de consulta 19 de febrero de 2019).

[18] Solo en América Latina, esta situación ha tenido lugar en Argentina, Brasil y Chile con diferentes resultados en cada una de estas jurisdicciones. Mientras en Argentina no se ha judicializado la cuestión quedando simplemente en cierre de cuentas bancarias a exchanges, en Brasil y Chile se ha llevado la cuestión a la Justicia usando

recolectar más información de sus clientes. La contracara de ello es que también sobre esa información pesan los deberes de la Ley Argentina de Protección de Datos Personales; es decir, por las decisiones arbitrarias de las entidades financieras, las compañías fintech se ven obligadas a asumir obligaciones que estas no querían asumir desde un primer momento y que no están obligadas por imperativo legal a hacerlo.

Por otro lado, las entidades financieras, conforme el artículo 20 inciso 1, están sujetas al régimen de la Ley Argentina de Prevención de Lavado de Activos y Financiamiento del Terrorismo, junto con otras entidades que pueden formar parte del ecosistema *fintech*[19]. Al respecto, la Resolución Nº 30/2017 de la UIF (la "Resolución") ha introducido obligaciones específicas para el conocimiento no presencial del cliente de estas entidades. En tal sentido, la Resolución les permite a las entidades financieras conocer a sus clientes a distancia por dos métodos, dejando a su criterio cual de ellos van a adoptar. Es importante señalar que estos métodos de identificación a distancia son aplicables tanto a las personas humanas que actúan a titulo personal como a las personas humanas que actúan en representación de una persona jurídica; en este último caso, la identificación del cliente solo puede hacerse por el primer método establecido en la Resolución.

El primer método consiste en hacer la identificación del cliente por "*medios electrónicos sustitutivos de la presencia física con uso de técnicas biométricas rigurosas o métodos tecnológicos alternativos de igual rigurosidad, almacenables y no manipulables*", que deben ajustarse a los lineamientos funcionales fijados en la Resolución. En este sentido, se exige que el procedimiento contemple la presentación del DNI original de la persona usando algún medio técnico como una videollamada; alternativamente, se podrá usar el sistema de validación de identidad y DNI proporcionado por el Registro Nacional de las Personas de la República Argentina (el "ReNaPer").

diferentes argumentos (desde cuestiones de defensa de la competencia hasta argumentos de defensa al consumidor).

[19] En este sentido, se recuerda que también podrían formar del ecosistema fintech no solo las entidades financieras sino también las entidades dedicadas a las remesas de fondos y al mercado de cambios (inciso 2), aquellas relacionadas con el mercado de capitales (incisos 4 y 5) y las emisoras de tarjetas de crédito (inciso 9). Cada una de ellas cuenta con una regulación particular pero actualmente la UIF esta realizando un proceso de actualización normativa y la cuestión de la identificación de los clientes a distancia esta recibiendo un tratamiento similar para todos los sujetos obligados.

Como se deja en manos de la entidad la determinación del sistema que va a utilizar para identificar a sus clientes, es necesario que la misma realice un análisis de los riesgos que presenta el sistema implementado así como de la persona que estará abocado a esta tarea de conocer a los clientes de forma no presencial. El objetivo de esto es hacer que la entidad identifique posibles situaciones que deriven en violaciones a las obligaciones que el sujeto obligado tiene debido a la Ley Argentina de Prevención de Lavado de Activos y Financiamiento del Terrorismo y que podrían derivar en responsabilidad de aquella por los incumplimientos. A su vez, este procedimiento debe ser sometido a aprobación del revisor externo del sujeto obligado para refrendarlo.

Así como en los procesos de conocimiento del cliente en forma presencial es sencillo poder establecer un marco temporal en el cual el proceso tuvo lugar, lo mismo debe lograrse cuando el conocimiento del cliente se hace por medios técnicos. Tal es así, que, el uso de herramientas técnicas que permitan otorgar fecha cierta a los documentos digitales generados por el proceso es necesario; una solución técnica apropiada podrían ser los sellos de tiempos, tal como están reconocidos en la Ley Argentina de Firma Digital. Junto con ello, la norma exige que todos los elementos informáticos dispuestos sean capaces de asegurar la autenticidad, vigencia e integridad de los documentos de identificación así como su pertenencia al titular del documento presentado al mismo tiempo que se garantice la confidencialidad e inalterabilidad de todos los datos recolectados. Idealmente ello implicaría el uso de herramientas como las firmas digitales o firmas electrónicas cualificadas pero, por aplicación del art. 319 del CCyCN, también sería viable la aplicación de otras soluciones, como una firma electrónica avanzada, en la medida que todo el procedimiento pueda cumplir con la finalidad pretendida por la norma.

El segundo mecanismo autorizado por la norma para la identificación del cliente a distancia contenido en la Resolución consiste en la remisión por parte del cliente de los documentos exigidos para el conocimiento de personas físicas o jurídicas vía el sitio web del sujeto obligado u otro canal. Tras la remisión y revisión de esta, la entidad financiera entrega una contraseña con preguntas de seguridad para que el usuario pueda operar con la entidad, en caso de ser aprobado. Tras ello, queda en manos de la entidad la verificación en forma presencial concurriendo al domicilio declarado por el cliente; esto último puede hacerlo por sus propios medios o recurriendo a algún agente con facultades suficientes para ello.

c) Problemáticas en materia de datos personales

Todas las actividades analizadas previamente, así como cualquier otra relativa a las identidades digitales de los clientes de las *fintechs*, constituyen tratamientos de datos personales, conforme la definición proporcionada por la Ley Argentina de Protección de Datos Personales y otras normas como el RGPD; en particular, existen 2 cuestiones de impacto en el ecosistema *fintech* con los datos personales de los usuarios: (i) la formación de perfiles crediticios y la evaluación de los mismos para la toma de decisiones[20]; y (ii) la comunicación de los datos generados por la interacción de los usuarios con las empresas a bureaus de crédito.

Sobre la primera cuestión, cabe señalar que la Ley Argentina de Protección de Datos Personales aún no cuenta con normativa como el RGPD que se encarga de lidiar con la problemática de la formación de perfiles y la toma de decisiones con efectos jurídicos en consecuencia. Sin embargo, la cuestión puede resolverse aplicando los principios generales previsto en la norma, en particular el deber de información; si el consumidor no logra entender como sus datos fueron usados para el análisis crediticio, habrá un incumplimiento a este deber y la Agencia de Acceso a la Información Pública deberá tomar intervención para la sanción de la empresa *fintech*. Del otro lado, las entidades que pretendan hacer uso de datos de otras fuentes para la conformación de los perfiles deben reparar en si se encuentran habilitadas por la fuente a hacer uso de los datos en tal sentido; a modo de ejemplo, Facebook prohíbe ello en los términos y condiciones de sus APIs.

En segundo lugar, dado que las empresas *fintech* forman parte del ecosistema financiero, es importante que los datos sobre la situación crediticia de sus clientes sean reportados por los canales formales previstos a esos efectos. En este sentido, al ser el BCRA quien controla estos canales de comunicación y determina que, quien y como debe informar su cartera de clientes y la situación crediticia, solo cuando una entidad este obligada a informar, deberá cumplir con esa carga y comunicar su cartera mediante la Central de Deudores mantenida por el BCRA, fuente pública de donde los bureaus de crédito luego toman la información que comunican.

[20] En tal sentido, se sugiere la lectura de: (i) CREEMERS, Rogier, "China's Social Credit System: An Evolving Practice of Control", 9 de mayo de 2018, https://ssrn.com/abstract=3175792 (Fecha de consulta 19 de febrero de 2019); y (ii) WEI, Yanhao – YILDIRIM, Pinar – VAN DEN BULTE, Christophe – DELLAROCAS, Chrysanthos N., "Credit Scoring with Social Network Data", *Marketing Science*, 35(2), Págs.234-258, https://ssrn.com/abstract=2475265 (Fecha de consulta 19 de febrero de 2019).

Alternativamente, y conforme las facultades previstas en la Ley Argentina de Protección de Datos Personales en el artículo 26 inciso 2, las empresas *fintech* pueden proporcionar sus datos de deudas de las cuales sean acreedores a estos bureaus de crédito.

Estas cuestiones y otras, como la portabilidad de los datos, suelen estar contempladas además en normas que apuntan a fomentar la competencia en el ecosistema financiero, como hace la PSD2 en Europa o las iniciativas de *open banking* en el Reino Unido. Esto es consecuencia de reconocer que los datos de los clientes son, hoy en día, uno de los principales activos que puede tener una entidad financiera o una empresa *fintech*.

4. Conclusiones

Tal como ha sido reseñado brevemente en este artículo, la problemática de las identidades digitales representa un gran desafío para las empresas *fintech*. Este desafío afecta su forma de contratar con los clientes, el cumplimiento de deberes legales que pudieran tener como engranajes del ecosistema financiero así como también la manera en que deben dar cumplimiento a la normativa en materia de protección de datos personales puesto que toda gestión que se haga con los datos constituye un tratamiento por parte de estas empresas.

En todo caso, así como sucede con todo desarrollo tecnológico, la falta de una normativa clara y la aplicación de normas generales no debe constituir un obstáculo para el desarrollo de una nueva industria y es responsabilidad de los juristas dar soluciones concretas con las herramientas técnicas existentes en la práctica jurídica.