La digitalización de personas físicas y jurídicas en el sector financiero

Alfonso Carcasona[13]

Resumen

El hombre es un ser social y, por lo tanto, la identidad es un elemento clave de su ADN. Desde el principio de los tiempos se nos ha dado una identidad con el objetivo de existir para los gobiernos, que en sus diferentes formas regulan nuestras relaciones con objetivos fiscales o militares. La evolución de las sociedades en Europa y Latinoamérica nos ha facilitado una manera particular de identificarnos, tanto en el mundo analógico como en el digital. Centrándonos en este último, en donde las relaciones no son cara a cara, sino de manera remota, facilitar identidades digitales de manera segura y cierta —no existe certeza al 100 %, pero se ha de tender a ella— es esencial. Para ello debemos apoyarnos en la tecnología, aunque no solamente en ella, para identificar correctamente a la persona, validar los documentos facilitados, y corroborar los datos y su comportamiento con información externa a la misma. Todo ello con el objetivo de poder firmar correctamente los documentos que se presenten para obligar económicamente a las personas.

13 Licenciado en derecho y ciencias empresariales. Máster con mención especial por el Instituto de Estudios Bursátiles. En la actualidad es CEO de AC Camerfirma, S.A., sociedad participada por las cámaras de comercio españolas y por el principal prestador cualificado de servicios de confianza digital, la italiana Infocert. Ha formado parte del comité ejecutivo de diversas instituciones y fundaciones, como Chambersign, Avalmadrid, el Parque Científico de la Comunidad de Madrid y de Ifema, del consejo social de la Universidad Autónoma y es tesorero del Comité Ejecutivo del Club Empresarial de Icade. En la actualidad, además es profesor asociado a la Facultad de Ciencias Económicas y Empresariales.

1. La identidad, elemento clave en las relaciones sociales

Según la Real Academia Española de la Lengua, identidad proviene del latín tardío *identĭtas*, *-ātis*, y este deriva del latín *idem* ‹el mismo›, ‹lo mismo›. Facilita cinco acepciones al respecto:

"1. Cualidad de idéntico.

2. Conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás.

3. Conciencia que una persona o colectividad tiene de ser ella misma y distinta a las demás.

4. Hecho de ser alguien o algo el mismo que se supone o se busca.

5. Matemáticas igualdad algebraica que se verifica siempre, cualquiera que sea el valor de sus variables".

Centrándonos en el concepto de identidad del ser humano —ya nos extenderemos en su consideración a personas jurídicas o incluso a las cosas—, observamos diferentes rasgos que conforman el concepto:

1. Son rasgos propios, individuales y únicos, que sirven para caracterizarnos, para diferenciarnos de los demás.

2. Se ha de tener una conciencia, una sapiencia de ser persona, única y distinta de los demás.

3. La identidad nos provee de existencia. No podemos ser sin identidad. El hombre es un ser social, que conjuga rasgos únicos que le definen frente a los demás seres únicos que le rodean, y le permiten relacionarse con ellos.

4. Resulta interesante la aproximación al concepto de la identidad desde la perspectiva matemática que,

> como por otra parte no puede ser de otra forma, confirma que la identidad debe ser siempre verificable, cualquiera que sea el valor de sus variables. O lo que es lo mismo, el conjunto de rasgos que conforman la identidad de una persona debe ser siempre verificable, aunque alguna de sus variables cambie de valor, ya que debe ser inmutable desde el punto de vista algebraico.

Observamos pues diferentes componentes a la hora de definir la identidad de una persona: rasgos únicos, propios, de los que se tiene consciencia, imprescindibles para que podamos existir como seres humanos, y que pueden ser verificables ya que, con independencia de que varíen en el tiempo, facilitan siempre el mismo resultado.

Desde Adán y Eva el ser humano ha tenido una identidad. En su caso, partían del nombre y género. No existían otros seres humanos, por lo que el nombre era suficiente para dotarles de identidad. Al nacer sus hijos se incorporaba un nuevo atributo ("hijo/a de") que, al extenderse en diferentes familias hizo necesario ir complicando el concepto, de manera que se adecuase correctamente a la definición que hemos intentado crear a partir de la de la RAE en párrafos *ut supra*.

Durante miles de años, los seres humanos nos hemos ido dotando de mecanismos para facilitarnos la identidad en entornos cambiantes.

2. La aparición de los imperios/Estados

Con la cada vez más compleja organización de las sociedades primitivas aparece el concepto del Estado, y la necesidad administrativa de tener controlados a los súbditos, con un doble objetivo inicial:

i. Fiscal: poder establecer los tributos e impuestos y poder cobrarlos, ya que el gobernante (en cualquiera de sus formas rey/tirano, artitócratas/oligarcas, demócratas/demagogos) necesita dotarse de una estructura administrativa, a la que hay que pagar.

ii. Guerrear: es necesario conocer con qué y con quién contaban para expandir o defender sus dominios.

Los sistemas de gobernanza desembocan en el concepto de "Estado", como organización política constituida por un conjunto de instituciones burocráticas estables, a través de las cuales ejerce el monopolio del uso de la fuerza (soberanía) aplicada a una población dentro de unos límites territoriales establecidos. Y para ello es imprescindible el concepto de identidad del individuo, ya no solo como persona, sino como súbdito o, en los Estados modernos, ciudadano, dotado de unos derechos y obligaciones para con sus semejantes, instituidos en esa "organización política".

Durante los últimos siglos la forma de dotar de identidad de los ciudadanos ha ido sufriendo diferentes variaciones, según el país y el momento. Las sociedades anglosajonas han intentado proteger la libertad del individuo frente al Estado, al menos desde el punto de vista nominal, lo que desembocaba en la inexistencia de documentos de identidad expedidos por el Estado, frente a las sociedades europeas (y por extensión latinoamericanas), cuyo esquema de identificación se basa en el Código Civil napoleónico de 1804, inspirado en el *ius commune* romano y en diferentes costumbres francesas de la época. El *ius commune* anglosajón o romano marcará, pues, cómo identificar a los ciudadanos, y con ello las relaciones que mantendrán entre ellos y con el Estado.

En el ámbito de las relaciones con entidades financieras se hace fundamental una correcta identificación no solo de la persona, física o jurídica, con la que se tiene relación, sino también de la propia entidad financiera, de sus trabajadores y en la era digital, de sus máquinas, correos electrónicos y páginas web, a través de las cuales se mantienen las relaciones que antes se realizaban de manera presencial.

3. La sociedad analógica versus la sociedad digital

Centrándonos en nuestra forma de hacer, los europeos y los latinoamericanos nos hemos dotado de códigos civiles que han regulado la forma en la que el Estado nos reconocía como ciudadanos y, basados en esa identidad, acometíamos las diferentes relaciones, tanto con el Estado como con nuestros conciudadanos. Diferentes acuerdos internacionales facilitaban incluso nuevas formas de identificación, a través de los pasaportes emitidos por cada Estado y reconocidos mutuamente por los demás Estados (con independencia en este caso de que nuestra identificación se realizase conforme al derecho común anglosajón o al derecho civil napoleónico).

De esta forma hemos sido dotados de identidad a través de nuestros Estados. Llegados a una edad se nos ha facilitado el Documento Nacional de Identidad (en sus diferentes acepciones), que nos permitía identificarnos ante la Administración Pública, instituciones locales, organizaciones públicas o privadas, con especial atención a las instituciones financieras que custodiaban nuestro dinero, y ante nuestros conciudadanos. Estos documentos nacionales de identidad (DNI) se emitían en papel, una vez realizadas por el Estado las comprobaciones pertinentes de manera física. Contenían datos básicos, como nuestro nombre, el de nuestros padres y el lugar de nacimiento, junto con un número asignado por el Estado que resumía dichos datos. Ese número certificaba nuestra

unicidad, nadie más lo podía utilizar para ser reconocido como ciudadano de nuestro país y, por extensión, nos permitía identificarnos en las relaciones contractuales de nuestra sociedad civil. Dichos documentos solo servían para nuestra identificación, ya que el resto de atributos que la conforman, por ejemplo, la formación académica, pertenecían a organizaciones, instituciones; solvencia financiera, datos sobre la salud, eran facilitados también en formato de papel por los organismos que los conocían, previa petición del dueño de dichas acreditaciones. Y eran válidos en cuanto eran reconocidos por las partes, o al menos por la parte solicitante de dicha identificación.

El progreso, con la consecuente complejidad en las relaciones humanas, llega a finales del siglo XX a una nueva revolución: la sociedad digital.

En esta nueva sociedad las relaciones ya no son solo presenciales, sino que cada vez más se realizan de manera remota, con la intervención de máquinas (desde el teléfono, el fax, el ordenador, hasta los modernos servidores en la nube). Los modos de facilitar identidades, validarlas y corroborarlas cambian de manera dramática. Si antes del siglo XXI un empresario se acreditaba ante su contraparte de una manera determinada, mostrando sus documentos de identidad y en su caso su certificado de estar constituido como empresa, hoy es necesario construir dichas identidades de manera distinta, más eficaz y dotada de una seguridad jurídica superior a la que facilitaban los medios analógicos. Y los Estados buscan la manera de no perder dicho monopolio de identificación. Unida a la identificación de la persona como ciudadano aparecen nuevas necesidades de identificación, lo que conocemos como atributos de la persona. Estos atributos se refieren a las diferentes características del individuo derivadas, por ejemplo, de su formación, de su historia laboral, clínico o

médico —hablamos hoy del *greenpass* o pasaporte sanitario derivado del covid-19—, o de su situación financiera. Aparecen nuevos actores en el mercado: los prestadores de confianza, los terceros encargados de dotar de seguridad a las transacciones remotas, seguridad que comienza por la correcta identificación de los intervinientes en las relaciones —ya no solo como ciudadano, sino con los atributos que le acompañan y configuran su identidad—.

Para dotar de identidad digital a una persona, ya sea física o jurídica —en adelante, salvo que se exprese lo contrario, nos referiremos indistintamente a ambas—, debemos tener en cuenta tres fases diferenciadas:

1. La identificación propiamente dicha, es decir, la comprobación de que esa persona es quien dice ser.

2. La validación de la documentación aportada, de la veracidad de su documento de identidad o de los documentos de atributos —por ejemplo, en el caso de una persona jurídica, la representación que se manifiesta—.

3. La corroboración de la situación de la persona, así como otra información que contribuya a la segura identificación de la persona.

4. La identificación, instrumento básico en las relaciones contractuales

Tradicionalmente, para dotar a una persona de una identidad digital se exigía, como único medio de identificación, la acreditación presencial de la misma. Es decir, se debía acudir al emisor de la identidad para que uno de sus empleados o funcionarios, debidamente formado y homologado como Autoridad de Registro (AR), comprobase cara a cara que la persona a identificar era la misma que se presentaba ante él, y le facilitase la documentación

requerida para la emisión del certificado digital que le dotaba de identidad para realizar operaciones en remoto.

La rápida evolución de la necesidad de las personas de dotarse de identidades digitales hace que se tengan que aceptar medios de identificación que no requieran de la presencia física para la emisión de certificados digitales, como se denominan en Latinoamérica, o cualificados, en Europa. Estos certificados tienen la máxima seguridad jurídica, invierten la carga de la prueba y su eficacia se asemeja a la de la firma manuscrita. Por ello, es fundamental que exista una total certeza a la hora de emitirse, pero a la vez debe facilitarse que puedan ser emitidos de forma eficaz, combinando seguridad jurídica y usabilidad.

Algunas compañías tecnológicas han desarrollado determinados productos de identificación biométrica, basados en el reconocimiento facial, iris del ojo, la voz o la huella dactilar. Estos modelos están basados en el mayor porcentaje de reconocimiento efectivo, pero han de ser completados con los requerimientos exigidos por la legislación en cuanto al cumplimiento normativo. De poco sirve un reconocimiento biométrico muy preciso si no va acompañado de un proceso que asegure otros elementos necesarios para facilitar la identidad digital.

Se permitirán, entonces, identificaciones basadas en videoconferencias sujetas a determinadas normas técnicas que garanticen la seguridad de las mismas y basadas en procesos perfectamente auditados. Estas videoconferencias pueden realizarse:

i. De manera síncrona, es decir, en una sesión de video de la persona que solicita dicha identidad y un operador (la AR a la que hacíamos referencia con anterioridad), grabada y custodiada por el tercero cualificado de confianza.

ii. De forma asíncrona, es decir, por un proceso guiado por una máquina, que nos va dando las instrucciones precisas para capturar la información necesaria para la emisión del certificado (de la identidad digital), que incluyen la toma de una foto y de un video, una prueba de vida y la sumisión de los documentos requeridos (documento de identidad, pasaporte). Este proceso ha de acabar con una comprobación física, es decir, de la AR del prestador, que compruebe que no hay fallos ni fraude en el archivo.

Otros medios de identificación no basados en la presencia física incluyen:

i. Emisión de un certificado basado en la identificación que previamente haya hecho otro prestador cualificado.

ii. Emisión de un certificado a través de la solicitud del envío de una transferencia bancaria (en este caso se confía en la previa identificación que ha realizado la entidad bancaria para facilitar la cuenta desde la que se hace la transferencia).

iii. Emisión del certificado basado en la información recogida por la entidad financiera para la prevención del riesgo de blanqueo de capitales (en Europa regulada por la Directiva del Parlamento 2005/60), y facilitada al prestador cualificado para la emisión de la identidad digital.

iv. Emisión de certificados basados en otros esquemas, notificados o no, en función del nivel de confianza que se busque conseguir.

v. Emisión de certificados basados en la extracción de datos de los documentos de identidad/pasaportes a través de tecnologías seguras, debidamente autorizadas,

como por ejemplo NFC (Near Field Communication, en español Comunicación de Campo Cercano).

En definitiva, la identificación es un elemento clave para facilitar la identidad digital, y los requisitos exigidos para su expedición dependerán del uso que se precise de ella. Incluyen elementos de biometría, junto con procesos auditados y certificados por la autoridad competente en cada uno de los países. Con ello nos habremos asegurado de que esa identidad existe en el mundo "real", y que se corresponde con la persona que está solicitando la identidad digital.

5. La validación, herramienta necesaria para cotejo de la identificación

Una vez nos hayamos asegurado de la identidad de la persona, es necesario que continuemos con la validación de la documentación necesaria para la emisión de la identidad digital. Entramos en el mundo del reconocimiento de datos aportados por el solicitante de la identidad digital.

Las principales tecnologías utilizadas para la extracción de datos de los documentos presentados son:

i. Optical Character Recognition (OCR) usada para la extracción de datos del documento de identidad presentado.

ii. Near Field Communication (NFC), ya analizado con anterioridad, permite en determinados casos la emisión de un certificado digital (Colombia) o cualificado (Europa).

iii. Machine Readable Zone (MRZ), es un formato de documento que contiene los datos del documento de manera que es legible de forma visual y codificado para el reconocimiento óptico de caracteres.

La validación realiza en tiempo real la verificación del documento presentado, para evitar el fraude de la presentación de un documento falso. Además de las tecnologías de reconocimiento, es necesario poderlos cotejar contra las bases de datos oficiales de los países (en Colombia, Registraduría Nacional del Estado Civil), confirmando la validez del documento basado en el reconocimiento biométrico de las fotografías capturadas y otros aspectos del documento.

Además de la validación del documento soporte, en el caso de personas jurídicas será necesario contrastar la información facilitada por el solicitante con los datos obrantes en el registro público correspondiente, normalmente el mercantil para el caso de representantes y apoderados. Será necesario cotejar que la información se halla debidamente registrada en el momento de la emisión del certificado, y será obligación de la persona jurídica comunicar al emisor del certificado la caducidad del mismo en el supuesto de que el representante o el apoderado deje la compañía.

6. La corroboración de datos, complemento fundamental para completar la identidad digital

La corroboración de atributos y metadatos es una actividad que complementa de modo esencial la identificación y validación de datos precedentes. Ofrece información sobre los hábitos de conducta del solicitante de la identidad digital y detecta posibles anomalías que puedan provocar dudas acerca de la veracidad de la operación de identificación. Si los sistemas detectan alguna anomalía emitirán un aviso y serán denegadas o enviadas a un "centro de corroboración" para un análisis más en profundidad.

Determinadas alertas de seguridad en el ámbito corroborativo pueden ser subsanadas por la petición del

prestatario al solicitante de que se persone físicamente en una AR para la comprobación física de la persona. Este es el caso de sesiones donde la calidad de la videoconferencia, de la fotografía o video grabado no sean suficientemente concluyentes y otorguen un nivel de fiabilidad por debajo de los porcentajes acordados.

Sin embargo, la corroboración es el módulo donde normalmente interviene la tecnología para detectar y analizar en tiempo real datos personales del consumidor (solicitante de la identidad digital) y cambios o modos extraños de actuación, utilizando herramientas de análisis de comportamiento y de *machine learning*. Hay que tener en cuenta que durante el proceso de video identificación remota tendremos al solicitante facilitando información y parte del análisis no se realizará solo sobre el contenido, sino sobre la forma para eliminar posibles incoherencias en el proceder que alerten sobre potenciales fraudes. Para ello se realizarán en tiempo real consultas tanto a bases de datos externas (listas negras, grises o blancas), como internas de la compañía con quien quiera contratar el solicitante. El objetivo es facilitar junto con la identidad digital el mayor nivel de conocimiento del cliente. Este módulo de validación de datos no facilitados por el cliente permite en tiempo real un *scoring* de riesgo acerca de la posibilidad de fraude por parte del solicitante. No solo se comprueba, por tanto, como en los módulos anteriormente analizados, la identidad y validez de los documentos, sino datos existentes en bases de datos que nos aseguren o minimicen el riesgo de emisión de la identidad o certificado digital.

Como podemos comprobar, facilitar una identidad digital es mucho más que simplemente la comprobación de ciertos rasgos biométricos. Al igual que en el mundo analógico, es imprescindible tener la mayor certeza

(nunca será al 100 %, ni en el mundo analógico ni en el digital) a la hora de emitir una identidad digital que vaya a permitir la firma de cualquier documento o archivo. Cuanta mayor trascendencia tenga la operación a realizar, más importante será el haber dotado al firmante de una identidad digital "fuerte", o más segura, lo que a veces redunda en una mayor dificultad a la hora de adquirirse, en una menor usabilidad del proceso. Insistimos en que en este punto es fundamental la referencia al cumplimiento normativo en cuanto al tipo de firma necesario, aspecto íntimamente ligado a la forma en que se ha adquirido y facilitado una identidad digital.

7. Relaciones contractuales en el ámbito financiero, firma y custodia de documentos

Hemos analizado en los anteriores apartados la importancia de la consecución de una identidad digital para las hoy más crecientes transacciones en remoto. De hecho, en la actualidad cada vez son menos las operaciones financieras que requieren de presencia física, salvo quizá en las de crédito al consumo. Pero incluso en esta categoría es imprescindible presentar identidades digitales, en este caso "fuertes" que permitan la identificación lo más segura posible de los acreditados.

Digitalizar procesos está asociado al concepto de eficiencia y ahorro de costes. Sin embargo, en el mundo financiero, además de conseguir esos objetivos, también puede generar nuevas formas de negocio. El ejemplo del crédito al consumo es bueno para comprobar cómo el acortamiento de tiempos en la aprobación de una operación incrementa el negocio. Si en el pasado podían transcurrir días entre el momento en que el potencial cliente adquiría un bien, solicitaba su financiación y le era concedido, con el potencial riesgo de desistir de la operación en ese espacio de tiempo, la posibilidad de que la financiación

se le pueda aprobar de manera inmediata elimina esta opción, y por lo tanto incrementa el negocio. Y todo ello se realiza de manera segura, otorgando al cliente una identidad digital cualificada, mediante un certificado digital emitido expresamente para esa operación y que caduca una vez utilizado. El cliente firma, por tanto, el contrato de préstamo con un certificado digital, no electrónico, en el que se invierte la carga de la prueba que, además, recae en el prestador de servicio de confianza, eximiendo por tanto a la entidad financiera de dicha responsabilidad.

La utilización de la identidad digital en el ámbito financiero es una obligación. No solo para las entidades "tradicionales", sino para las emergentes *fintechs*, en las que prácticamente el 100 % de sus relaciones son virtuales.

En la actualidad estamos asistiendo al nacimiento de modelos de negocio, dirigidos fundamentalmente a las franjas de edad más jóvenes, en donde la propuesta de valor física no existe. Apertura de cuentas, contratación de productos financieros, asesoramiento, en definitiva, virtualizar todas o casi todas las relaciones con el cliente, es la tendencia del mercado. No solo por ahorro de costes, que evidentemente también, sino por adecuarse a la cultura de los clientes que no valoran la presencia física en sucursales, sino la posibilidad de operar virtualmente. La captura de nuevos clientes y multiplicar la operativa de los mismos son retos tradicionales que, apoyados en identidad y firma digital se convierten en estrategias multiplicadoras del negocio actual.

Grande es el debate sobre la caducidad del modelo de negocio de las entidades financieras, abocadas en el mundo occidental a una restructuración de plantillas, cierre de sucursales y disminución de balance. Sin embargo, analizado desde la perspectiva de la transformación

digital, el mundo financiero es el paradigma de éxito basado en la adaptación a los nuevos tiempos. Partiendo de la identidad digital, combinando usabilidad con seguridad jurídica, multiplicando las transacciones a través de la firma digital, el sector financiero crecerá de manera sana y rentable en los próximos años.

Para finalizar, el proceso de transformación digital de las entidades financieras no puede acabar sin una referencia a la custodia documental. Y es que es evidente que la forma de hacer del pasado, en el que el soporte de todas las transacciones era el papel que se archivaba en almacenes, debe cambiar en el mundo digital. Problemas como certificar el contenido de un documento digital, su integridad y en su caso cifrado, su fecha de creación, la validez de las firmas a la hora de su archivo definitivo debe ser abordada de manera muy distinta a como se hacía en el mundo analógico del papel. Se trata de un servicio que requiere una legislación *ad hoc*, que regule desde el punto de vista técnico y legal cómo custodiar la inmensa documentación digital que se produce cada día, con las debidas garantías en cuanto a su cifrado, posibilidad de acceso, inviolabilidad del documento en el tiempo. Los documentos firmados digitalmente deben ser accesibles no solo ahora, sino en periodos largos (hasta veinte años), en los que pueden servir como prueba en procesos judiciales. Por ello, es necesario una verdadera concienciación acerca de su importancia en el diseño de la transformación digital de las entidades financieras en el mundo.

Conclusión

Asistimos en la actualidad a un intenso proceso de transformación digital de la sociedad, lo que es particularmente cierto en el ámbito financiero. Existen múltiples aspectos necesarios para transformar procesos

analógicos en digitales. Pero no existiría la digitalización sin que las personas, tanto físicas como jurídicas, se doten de una identidad digital que les permita ser reconocidas para la realización de cualquier transacción. En el ámbito financiero, donde las operaciones suponen la adquisición de obligaciones económicas, es esencial la correcta emisión de la identidad digital, lo que no se consigue solo con tecnología, ni solo con comprobaciones biométricas. La emisión de certificados digitales basados en identificaciones "fuertes" permite desde el punto de vista de la seguridad jurídica equiparar la firma digital a la manuscrita, invertir la carga de la prueba y delegar la responsabilidad de la identificación en el prestador de servicios de confianza digital, dedicándose la entidad financiera a su actividad principal.

Referencias

Documentación interna Camerfirma/Infocert.

Esquirol J. M. (2021). *Humano, más humano*. Editorial Acantilado.

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-EU-digital-ID-scheme-for-online-transactions-across-Europe/F2669106_en https://www.european-signature-dialog.eu/

Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.