PONTIFICIA UNIVERSIDAD CATÓLICA MADRE Y MAESTRA
DECANATO DE POSTGRADO
MAESTRÍA EN DERECHO DE LOS MERCADOS FINANCIEROS

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL E IDENTIDAD DIGITAL DEL USUARIO DE SERVICIOS FINANCIEROS EN LA REPÚBLICA DOMINICANA

Informe profesional final para optar por el título de
Magíster en Derecho de los Mercados Financieros

Sustentado por:
Suiden De Jesús 2001-1321

Asesor:
Enmanuel Cedeño Brea, Ph.D.

Santiago de los Caballeros
República Dominicana
Marzo, 2022

Pontificia Universidad Católica Madre y Maestra
Vicerrectoría Académica
Decanato de Postgrado

Formulario de Cesión Derechos de Autor al Repositorio Institucional Investigare

Este documento establece los derechos que usted otorga relacionados a la publicación de su trabajo académico, mediante su inclusión en el ***repositorio del sistema de biblioteca de esta institución (PUCMM)***. No habrá ningún pago para usted por esta publicación y por el otorgamiento de los derechos de esta.

Usted confirma que

Este trabajo académico es original propio que no infringe los derechos de autor de otros; en caso de no ser un trabajo completamente original, declara que tiene los permisos necesarios por escrito de este otorgamiento por parte de demás autores.
El contenido de este trabajo académico no contiene ningún material que sea difamatorio, viole los derechos de privacidad, o revele la información confidencial.
Este trabajo académico no se ha publicado en parte o en su totalidad, y usted no publicara este trabajo académico en ningún otro lugar sin el consentimiento del repositorio institucional.
Este trabajo académico se ha conducido respetando los principios éticos establecidos por la institución.

Usted otorga los derechos de autor de este trabajo académico al repositorio institucional (PUCMM), a nivel mundial, de manera perpetua y sin pagos; y en la medida requerida por los términos de este acuerdo. Conservara en todo momento el derecho a ser reconocido como el autor del trabajo académico. Además, acepta que el repositorio de la PUCMM tiene el derecho de tratar este trabajo académico como se considere oportuno (por ejemplo, derecho a imprimir, publicar, comercializar, comunicar y distribuir en todos los medios, editar la forma del trabajo, registrar los derechos de autor, cumplir con la política editorial establecida por el repositorio, entre otros).

He leído, entiendo y acepto los términos anteriores.

Nombre del Programa: ***Maestría en Derecho de los Mercados Financieros***

Título del Trabajo: ***Protección de datos de carácter personal e identidad digital del usuario de servicios financieros en la República Dominicana***.

Nombre (s) y Apellidos: ***Suiden Eunice De Jesús Hilario***

Matrícula: ***2001-1321***

Cédula de Identidad y Electoral: ***056-0133079-7***
Fecha (día, mes, año): ***08 de junio,2022.***

Firma _____

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL E IDENTIDAD DIGITAL DEL USUARIO DE SERVICIOS FINANCIEROS EN LA REPÚBLICA DOMINICANA

HOJA DE CALIFICACIÓN

_____

Presidente del Jurado

_____

Miembro del Jurado

_____

Asesor

_____

Calificación

En la ciudad de Santiago de los Caballeros, provincia de Santiago, a los _____ (___) días del mes de _____ del año 2022.

TABLA DE CONTENIDO

PLAN BINARIO

PLAN BINARIO

"PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL E IDENTIDAD DIGITAL DEL USUARIO DE SERVICIOS FINANCIEROS EN LA REPÚBLICA DOMINICANA"

SECCIÓN I. LA IDENTIDAD DIGITAL EN EL *ONBOARDING* FINANCIERO

I. Nociones sobre la identidad digital
   A. Distinción del concepto de identidad en el ordenamiento jurídico actual
   B. Importancia y beneficios aportados por la adopción de la identidad digital

II. Transformación del sector financiero
   A. Situación actual del sector financiero en cuanto a la digitalización
   B. El rol de la identidad digital en el sector financiero: el futuro inmediato

SECCIÓN II. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LOS SERVICIOS FINANCIEROS

I. Manejo de los datos en el sistema financiero
   A. Los principios de la banca para la protección de datos
   B. Situación regulatoria de la identidad digital

II. Gestión de seguridad en el uso de la identidad digital
   A. Privacidad
   B. Ciberseguridad

SECCIÓN III. GOBERNANZA Y PREVENCIÓN DE LAVADO DE ACTIVOS EN EL ENTORNO DIGITAL

I. Agentes de protección de los usuarios de servicios financieros
   A. Rol de la Superintendencia de Bancos
   B. Identificación y verificación de los clientes en el *Onboarding*

II. Estándares internacionales en protección de datos
   A. Tendencias actuales en prevención de lavado de activos
   B. Casos de éxito en regulación de identidad digital

INTRODUCCIÓN

INTRODUCCIÓN

La identidad es una característica del comercio, pues se requiere rutinariamente para las transacciones, pero sus ventajas vienen acompañadas de inconvenientes que pueden acarrear serios problemas, como el robo de identidad, que suele ser objeto de noticias, informes de la industria y del gobierno, por eso la ciberseguridad, que se ha vuelto una prioridad máxima para todo tipo de industrias. De ahí, pues, que el uso masivo de la tecnología y su dependencia para el comercio en el mundo, así como el surgimiento de modalidades tan diversas para ofrecer bienes y servicios, han motivado que se cuestione el surgimiento de la identidad digital. Por lo tanto, particularmente en el sector financiero, la dimensión de su uso, la protección bajo la cual debe operar, y el tratamiento y disposición de los datos deben estar especialmente delimitados y provistos por un marco normativo donde estén debidamente regulados.

La identidad ha sido tradicionalmente una noción nebulosa y al referirse a la misma, gran parte de la literatura jurídica en esta área carece de precisión. Da la impresión de que la identidad es identidad mientras que la constitución, la función y la naturaleza de esta dependen del contexto que se utilice, por lo cual es importante diferenciar el concepto puramente legal, de otras concepciones no legales. La importancia de la identidad debe ser abordada desde su función y su naturaleza legal, para de esta forma poder aproximarnos a un concepto desde el cual partir[1].

Lo cierto es que en el mundo actual es vital contar con una identidad. De hecho, conforme los Objetivos de Desarrollo Sostenible, se tiene previsto que el año 2030, todos los ciudadanos deberán disponer de una identidad jurídica, lo que incluye el registro de nacimiento. Además, no se puede ignorar que tener una identidad digital tiene el potencial de crear una serie de ventajas que todo ciudadano debería aprovechar, al servir la misma

[1] SULLIVAN, Clare. *Digital Identity: an emergent legal concept*. Australia: University of Adelaide Press, 2011. ISBN 978-0-9807230-2-7

como la *puerta de acceso* a la cual llamar, para conectar el mundo actual que se mueve prácticamente en su totalidad por vía de acceso digital, y busca evitar que haya personas marginadas por ciertas situaciones que la tecnología moldea.

Para la implementación exitosa de técnicas y tecnologías de análisis de datos en el sistema financiero, es fundamental que el modelo de negocio sea sostenible y que se desarrolle de acuerdo con las necesidades específicas de los consumidores. También, debe contarse con la regulación, que permita crear y ofrecer productos financieros de forma provistos por medios digitales y que, como mecanismo a utilizar para conocer el cliente, se pueda aceptar su identidad digital, y con ello mantener un balance entre la nueva realidad que obliga adoptar nuevos requerimientos del mercado, la estabilidad del sistema y la protección a los consumidores[2].

En la medida en que se amplían los horizontes del concepto de la identidad digital, junto a su uso y su regulación, a las personas se les deben consagrar sus derechos fundamentales en cuanto a la protección de los datos personales y, aunque la normativa en materia de protección de datos de carácter personal es mucho más compleja y extensa, en la materia que nos compromete deben ser abordados los marcos normativos relacionados, para dejar consagradas las obligaciones que impone tanto al usuario de los datos como al propietario, así como su trato, manejo y disposición[3].

En el mundo contemporáneo, identificar a las personas adecuadamente forma parte de la debida diligencia para combatir el lavado de activos, el financiamiento del terrorismo y la proliferación de las armas de destrucción masiva. Este proceso es fundamental para

[2] ASOBANCARIA. La identidad digital: el camino para impulsar la inclusión financiera [en línea] *Semana Económica*, 2017. Edición 1096 [consulta: 3 enero 2022]. Disponible en: https://www.asobancaria.com/wp-content/uploads/2018/02/1096.pdf

[3] SANTAMARÍA RAMOS, Francisco J. Identidad y reputación digital. Visión española de un fenómeno global [en línea] *Ambiente Jurídico*, Núm.17, 2015 [consulta: 3 enero 2022]. Disponible en: https://revistasum.umanizales.edu.co/ojs/index.php/Ambientejuridico/article/view/1570

permitir relación entre una persona y una entidad, de manera tal que permita la relación de negocios de una forma segura y con las garantías legales de lugar.

En la República Dominicana el marco jurídico donde se aborde y se gestione adecuadamente esta situación es poco satisfactorio, por lo que resulta impostergable mirar qué están haciendo los demás países al respecto, así como lo que han consagrado en su normativa y qué ha resultado efectivo a los fines de disponer de los datos personales de las personas, observando a la vez cómo esto ha impactado su apertura a las tecnologías[4]. Igualmente, resulta pertinente evaluar cuáles sanciones son aplicables en los casos de inobservancia de los derechos de los propietarios de los datos[5], sobre todo porque los datos tienen utilización transfronteriza.

La brillante oportunidad que representa para el sistema financiero adoptar un sistema de identidad digital, trae consigo la transformación del sistema que actualmente conocemos. Aquí, será posible identificar todos los beneficios que de manera directa surgen de digitalizar los procesos existentes, así como los asociados al surgimiento de nuevos servicios. Los procesos de automatización, las facilidades y la autonomía que supone al usuario para sus transacciones ordinarias, así como la personalización de los servicios y monetización de los mismos, son algunas de las tendencias clave de las aplicaciones de la identidad digital[6] y, son precisamente estas acciones de transformación y cultura digital

[4] Unión Europea. 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) [en línea] Diario Oficial de la Unión Europea [consulta: 3 enero 2022]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[5] Unión Europea. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales; Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo; Samuel Parra, socio de e Privacidad y experto en protección de datos, privacidad, ciberseguridad y transparencia.; Diario de Sesiones del Congreso de los Diputados (20/05/2021); Comunicado del Tribunal de Justicia de la Unión Europea sobre la sanción a España

[6] PAREJA, Alejandro, et. al. La gestión de la identidad y su impacto en la economía digital. *Documento para Discusión núm. IDB-DP-529.* [en línea] Banco Interamericano de Desarrollo© [consulta: 4 enero 2022]. Disponible en: https://publications.iadb.org/publications/spanish/document/La-gesti%C3%B3n-de-la-identidad-y-su-impacto-en-la-econom%C3%ADa-digital.pdf

que se deben promover dentro de las instituciones, pues para lograr la modernización del ecosistema digital del país, la tecnología debe de acompañarse de un cambio de cultura.

Es muy común escuchar el dicho que *"la oportunidad llama, pero solo una vez"*. Esto refiere a que no deben desaprovecharse las situaciones, por fortuitas que parezcan, para alcanzar los objetivos que se desean. También se ha escuchado cómo replica a este dicho la frase que reza que, *si la oportunidad no llama, construye una puerta*, refiriéndose a que debemos construir nuestras propias oportunidades. La crisis sanitaria la podemos ver, en parte, como una puerta que ha sido construida y detrás de la cual se ha encontrado la magnífica oportunidad de acelerar la transformación digital a todos los niveles, en todos los sectores.

Para abundar sobre lo expuesto, hemos dividido este trabajo en tres secciones: la sección primera, donde se abordará el contexto en el cual podemos enmarcar la identidad digital en el *onboarding* financiero, que consiste en la vinculación no presencial o remota que es aplicable a nuevos clientes que sean personas físicas. Seguido, procederemos con el análisis del concepto de identidad digital en el ordenamiento jurídico nacional e internacional, los beneficios que aporta y lo importante que resulta la adopción de este mecanismo de identificación personal.

Revisaremos cuál es la situación actual de la transformación del sistema financiero, qué están haciendo los países en ese sentido y el rol que desempeña la identidad digital.

En la sección segunda, evaluaremos cómo se manejan los datos en el sector financiero, los principios que la banca observa a estos fines y la situación regulatoria actual. Para esto, debe ser analizada la gestión que se realiza con los datos personales, de cara a evaluar si son protegidos adecuadamente por un marco normativo nacional los datos de carácter personal de cara a la vulneración que exista sobre estos, cuando se accede a los mercados financieros. Con base en esto, se pretende proponer acciones de lugar para su correcto

tratamiento y, cuáles serían las medidas a implementar en la República Dominicana. En tal sentido, nos interesa evaluar la actual situación normativa de la nuestro País, sobre la protección de la identidad digital y de los datos de carácter personal, en el uso de servicios financieros y sus riesgos asociados a la ciberseguridad, así como la debida diligencia adecuada para la validación de una identidad digital, su manejo y el uso de los datos de las personas por parte de las entidades.

La última parte trata sobre la gobernanza y la prevención de lavados de activos en el entorno digital, analizando cuál es el papel que desempeñan los agentes de protección de los usuarios de los servicios financieros y, más puntualmente, para el caso de nuestro país, el rol de la superintendencia de bancos como organismo supervisor en este contexto.

Por último, se examinan los estándares internacionales sobre la protección de datos y cómo los demás países han incorporado a sus marcos legales las garantías necesarias para que el entorno digital esté provisto de las seguridades jurídicas necesarias.

Con este trabajo damos una mirada sobre este tema en particular, que ya no puede ser una realidad latente sino irrefrenable, por lo que debemos, como sociedad, colaborar con su pronta adopción y a su vez ofrecemos soluciones innovadoras con interés en promover la identidad digital y sus ventajas, otorgando una valiosa herramienta a los ciudadanos y mejorando así su calidad de vida.

SECCIÓN I

LA IDENTIDAD DIGITAL EN EL *ONBOARDING* FINANCIERO

SECCIÓN I
LA IDENTIDAD DIGITAL EN EL *ONBOARDING* FINANCIERO[7]

Hoy en día, las soluciones de identidad digital son basadas en colecciones de datos, los cual es realizado a menudo sin conocimiento del sujeto. Los datos se replican una y otra vez en diferentes sistemas. Los terceros usan identificadores universales, tales como números de documento de identidad, seguridad social, número de teléfonos, entre otros, y no siempre es con el consentimiento de su dueño. En los servicios financieros, actualmente la identidad digital tiene un rol determinante, ya que es un mecanismo que facilita acceder a productos y servicios ofrecidos por las Entidades de Intermediación Financiera.

La exposición que genera el compartimiento de los datos en ambiente digital genera un problema de privacidad, que debe ser tratado en un marco legal donde los mismos resulten protegidos. En ese sentido, resulta importante plantearnos: ¿Existe en la República Dominicana una protección integral de los datos de carácter personal que componen la identidad digital, con sus distintas aristas, y cuál es el derecho que tiene la persona para la privacidad de sus datos cuando utiliza los servicios financieros de forma virtual?

Mediante el uso masivo del internet y de las tecnologías de la información mediante dispositivos, hoy día podemos hablar de identidad digital, que lejos de ser una tendencia novedosa resulta en una realidad que todos debemos afrontar. En consonancia con esta nueva realidad, no podemos negar la transformación trascendente del mundo análogo hacia el mundo digital, y con ello la disposición y tratamiento de estos.

[7] *Onboarding* digital también se denomina "vinculación digital" o "abordaje digital". Es el mecanismo mediante el cual las EIF, intermediarios cambiarios y fiduciarias vinculan nuevos clientes (persona física) contractualmente, de forma temporal o permanente, sin la interacción presencial de este con el personal o agente designado. Se ha optado por utilizar el término original en inglés dado que es el tecnicismo más utilizado.

En este trabajo cuestionamos los siguientes temas: ¿Cómo se compone la identidad digital y cuales son los beneficios que esta supone para el sistema financiero? ¿Qué obligación tienen las entidades de intermediación financiera con relación al tratamiento de los datos obtenidos de sus clientes? ¿Cuáles son los retos y desafíos a superar en la adopción de una identidad digital y cúal es el rol del organismo supervisor de cara a esta nueva realidad?.

I. Nociones sobre la identidad digital

Sin una identidad las personas no existen. Quienes no existen no puede tener derechos ni prerrogativas. Por esto, disponer de una identidad legal y única es necesario para permitir que los individuos participen plenamente en la sociedad y la economía. También para el desarrollo pleno de su personalidad.

La capacidad de demostrar la propia identidad es esencial para el acceso a servicios básicos y derechos, desde la atención de servicios médicos hasta las pensiones y los subsidios agrícolas. Esto es especialmente cierto para los segmentos más vulnerables de la sociedad, como son las mujeres, los agricultores rurales pobres, los refugiados, y los servicios financieros como catalizador de la economía.

Uno de los principales obstáculos para acceder a los servicios financieros es la falta de documentación de cientos de personas no bancarizadas en los países con niveles de ingresos bajos. Más allá de extender la identificación legal para abordar estas brechas, la introducción de una identificación legal y digital podría aumentar potencialmente la adopción de servicios financieros, al mismo tiempo que se promueve la agenda de inclusión financiera y se apoyan los objetivos de desarrollo. La identificación digital reduce las barreras puesto que es un vehículo para: a) facilitar a los no bancarizados la apertura de una cuenta de transacción caracterizada por los requisitos simplificados de documentación, b) permitir una incorporación de clientes más rentable que se puede realizar de forma

remota y c) contribuir a la integración del sector financiero al apoyar la prestación de servicios adicionales al individuo.

En esta parte estaremos explorando el concepto de identidad y su importancia en el marco de los servicios prestados de forma digital, lo cual forma parte del paisaje del ecosistema digital donde la sociedad se desenvuelve actualmente. En la segunda parte, revisaremos los beneficios que supone a las personas, a los gobiernos y a los mercados el uso de las nuevas tecnologías, en la adopción de una identidad con la que todos puedan ser identificados.

A. Distinción del concepto de identidad digital en el ordenamiento jurídico actual.

En el mundo actual, todas las organizaciones e industrias están implementando planes de transformación digital y el sistema financiero no escapa a esto. Disponer de un medio para identificar a las personas en el plano digital es esencial para su funcionamiento, y esto lo constituye la identidad digital. Para examinar la identidad digital desde la perspectiva jurídica, es necesario que nos hagamos las siguientes preguntas: ¿Qué la constituye? ¿Cuál es exactamente su función y cuál es su naturaleza jurídica? ¿Debe existir una identidad digital única? ¿O pueden coexistir varias?

En la investigación, para dar respuesta a estas preguntas, hemos encontrado mucho más de lo que esperábamos. En primer lugar, aunque la identidad digital se usa comúnmente, rara vez se define, y sus funciones y roles legales han sido poco analizados previamente en un contexto jurídico.

En tal sentido, para poder entender la identidad digital necesitamos, de inicio, disponer de la definición de lo que es propiamente la identidad. Este concepto ha sido objeto de discusiones a través de los años, abordado temprano por los pensadores de la Grecia antigua hasta llegar a las distintas corrientes hoy día, tales como la sociología, la psicología, la

antropología. En tiempos modernos, este análisis se extiende transversalmente a las cuestiones de género y de derecho, entre otras.

Este abanico tan amplio de materias convergentes hace que dar con el significado literal de la palabra identidad presente una aporía, término que literalmente significa "sin camino", o "camino sin salida", por ser de dificultad insuperable, en su razonamiento o conclusión a un mismo entendimiento para los diversos campos del saber. Podemos decir que estas teorías van desde su exaltación como hecho fundamental de la vida humana, hasta la negación absoluta de la existencia misma, tal y como lo describe Stuart Hall:

> *En los últimos años ha habido una auténtica explosión discursiva alrededor del concepto de 'identidad', al tiempo que era sometido a una penetrante crítica. ¿Cómo se explica este desarrollo paradójico? ¿Y cómo nos ubica con respecto al concepto? La deconstrucción ha sido conducida dentro de una variedad de áreas disciplinarias, todas ellas de algún modo críticas a la noción de una identidad integral, originaria y unificada. El yo infinito y performativo ha sido propuesto en variantes celebratorias del posmodernismo. En medio de la crítica anti-esencialista de las concepciones étnicas, raciales y nacionales de la identidad cultural y de las 'políticas de locación', algunas aventuradas concepciones teóricas han esbozado sus formas más territorializadas. ¿Cuál, entonces, es la necesidad de un mayor debate acerca de la 'identidad'? ¿Quién la necesita?* [8].

Consideramos que presentar una revisión histórica o filosófica del concepto identidad y analizar las teorías que han sido desarrolladas en los distintos campos del conocimiento excede la construcción del concepto sobre el cual versa la presente investigación, por lo que proponemos partir de un concepto que nos acerque al punto neurálgico objeto de esta tesis, que es la identidad digital.

Para la Real Academia Española, la identidad es la conciencia que una persona tiene de ser ella misma y distinta a las demás[9]. El Diccionario Panhispánico del Español Jurídico, define la identidad como datos básicos que permiten identificar a una persona por su

[8] HALL, Stuart y DU GAY, Paul (eds.). Questions of cultural identity. Traducción de Natalia Fortuny. Londres: Sage Publications, 1996, p. 1

[9] *Identidad* [en línea] Real Academia Española [consulta: 3 enero 2022]. Disponible en https://dle.rae.es/identidad.

nombre, filiación, lugar de nacimiento y número de documento nacional de identidad[10]. Esta definición la complementamos con el hecho que la persona debe aceptar esos datos como suyos, aunque no siempre aplica en todos los casos. De todos modos, para nuestros fines, tomaremos la definición como punto de partida de este análisis.

Para realizar un análisis sobre la naturaleza jurídica de la identidad, debemos revisar las normas que a ella se refieran. Por tanto, necesitamos cuestionar lo que significa para el Derecho la identidad. A fin de dar respuesta a esta pregunta, es difícil encontrar una norma jurídica que se refiera a la identidad como tal.

Todo ser humano tiene derecho a una identidad. El derecho a la identidad permite a todo individuo ejercer su libertad y a ser tratado de igual manera ante la ley. En particular, la Declaración Universal de Derechos Humanos, aprobada por la Asamblea General de las Naciones Unidas en 1948, ha establecido el derecho que asiste a toda persona de ser reconocida de su personalidad jurídica. Estos marcos legales abordan ciertos elementos de la identidad de las personas que, en efecto, son fundamentales, pero no lo hacen de una forma integral.

El Pacto Internacional de los Derechos Civiles y Políticos de 1996[11], confiere a una persona desde su nacimiento la protección a una serie de prerrogativas que componen su identidad, descritas en el numeral 24, y reconociendo como un derecho el tener un nombre, una nacionalidad.

[10] *Identidad* [en línea] Diccionario Panhispánico del Español Jurídico [consulta: 3 enero 2022]. Disponible en: https://dpej.rae.es/lema/identidad.

[11] Pacto Internacional de Derechos Civiles y Políticos [en línea] Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), del 16 de diciembre de 1966. [consulta: 3 enero 2022]. Disponible en: https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/ccpr_SP.pdf

En la Convención Internacional de los Derechos del Niño[12], en el artículo 8 se consagra como una obligación del Estado la preservación de la identidad, refiriéndose a algunos elementos que la componen, tales como nombre, nacionalidad y vínculos familiares.

Por otro lado, la meta 16.9 de los Objetivos de Desarrollo Sostenible de las Naciones Unidas establece: "[p]ara 2030, proporcionar acceso a una identidad jurídica para todos, en particular mediante el registro de nacimientos".

La Constitución Dominicana, en su artículo 55, numeral 8[13], establece como un derecho fundamental que todas las personas les asiste el derecho desde que nacen de inscribirse en el registro civil o en el libro de extranjería, según corresponda, libre de costos, así como obtener los documentos públicos que comprueben su identidad, conforme establezca la ley.

La personalidad es una prerrogativa de la cual gozan todos los seres humanos aptos para ser sujetos de derechos y obligaciones y, en principio, toda persona tiene la capacidad de goce de los mismos, lo que significa que puede adquirir, conservar y disponer de derechos. En el Código Civil de la República Dominicana[14], el artículo 7 refiere a que el ejercicio de los derechos civiles es independiente a la cualidad de ciudadano y la misma debe ser tenida en conformidad a la disposición de la Constitución.

El principal requisito para la personalidad es su propio nacimiento. El artículo 55 del Código Civil dispone que se realice una declaración de todo nacimiento ocurrido en la República Dominicana por ante un oficial del Estado Civil. Esta práctica constituye una herencia recibida de los conquistadores, pues en la época colonial fue establecido un registro civil que emulaba el utilizado en ese entonces en España y que servía para ordenar la población creciente en relación con sus filiaciones, propiedades, identidades, es decir,

[12] Convención sobre los Derechos del Niño [en línea] unicef.es © 2006. [consulta: 4 enero 2022]. Disponible en: https://www.unicef.es/sites/unicef.es/files/comunicacion/ConvencionsobrelosDerechosdelNino_0.pdf
[13] República Dominicana. Constitución de la República. *Gaceta Oficial* No. 10805 del 10 de julio del 2015.
[14] República Dominicana. Código Civil de la República Dominicana. Santo Domingo, 2007.

documentando la vida común y habitual de las personas. La institución fue organizada siguiendo los lineamientos de su evolución y desarrollo en el derecho francés, hasta culminar con el sistema que establece la Ley 659, sobre Actos del Estado Civil, de fecha 17 de junio de 1944 y sus leyes complementarias.

En ausencia de un marco normativo específico que se haya establecido mediante ley orgánica para regular el Registro Civil de nuestro país, esta ley ha fungido como el estatuto básico para su funcionamiento, la cual al día de hoy mantiene su vigencia, robustecida por ciertas disposiciones de la Junta Central Electoral que suplen la falta de reglamentos para facilitar la operatividad y el funcionamiento del Registro Civil.

Luego de revisado lo anterior, podemos decir que la identidad como tal, es algo distintivo de cada ser humano y que hace a una persona única entre una colectividad, sin que pueda ser discriminada por motivos de su raza, color, sexo, idioma, religión, origen nacional o social, posición económica o nacimiento, por lo que configura un derecho humano, con unos caracteres que deben ser protegidos, y es algo que debe ser respetado. Es decir, el bien jurídico tutelado es la persona.

En la Constitución de la República Dominicana no existe un derecho individualizado llamado a proteger el bien tutelado que podemos llamar "Derecho a la Protección de Datos Personales", sino que se deslinda por la protección del "Derecho a la Intimidad y el Honor Personal" de donde se desprende el reconocimiento de que las personas tienen prerrogativas sobre las informaciones que les competen.

En el artículo 44 de la carta magna dominicana se destaca que toda persona puede gozar de la no injerencia hacia su vida privada y familiar, su domicilio y su correspondencia, así como de disfrutar del derecho al honor, el buen nombre y la propia imagen. En el inciso 2 del mencionado artículo encontramos el reconocimiento del derecho que poseen todas las

personas de acceder a las informaciones que sobre ellas o sus bienes reposen en registros públicos o privados, igual que el de conocer el destino y uso que a estas se le asignen.

La ley dominicana sobre Protección de Datos Personales[15] en su artículo 1 especifica sus objetivos, distinguiendo que, entre otros asuntos, esta ley tiene la facultad de regular el tratamiento de los datos personales en los ámbitos públicos y privados. Para tales fines, define en el artículo 6 los datos especialmente protegidos, aquellos datos de carácter personal 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[16]. Es dato de carácter personal cualquier información en forma de números, letras, gráficos, fotografías, acústica o de cualquier otro tipo, relativa a personas físicas identificadas o identificables.

Así como nuestra ley es clara en su alcance, también lo es en los casos excepcionales. En ese sentido, la misma expresa que: *¨no se resguardarán los datos que: a) se utilicen para el ejercicio de actividades personales; b) que fueran empleados por los organismos de investigación y de inteligencia para la detección de delitos y crímenes; c) referidos a personas fallecidas; y d) que sean de personas jurídicas, en conjunto con los datos de las personas físicas que presten sus servicios en ellas, de modo que, no serán protegidos los nombres, apellidos, funciones o puestos, dirección postal o electrónica, teléfono, y número de fax profesionales¨*.

[15] República Dominicana. Ley Núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. *Gaceta Oficial*, del 15 de diciembre de 2013, Núm. 10737, pp. 44-84.

[16] Haciendo énfasis en el ejemplo de la Ley sobre VIF SIDA, que, por un asunto de evitar discriminaciones, que prohíben la divulgación de los resultados de los análisis de una persona que resulte positiva. De hecho, por ley, estos resultados se entregan de manera personal; no se pueden enviar por vía digital o por la App de los laboratorios.

A nuestro juicio, esta ley da unas definiciones un tanto ambiguas para poder establecer el alcance relativo a los componentes de la identidad, pero, de todos modos, llega a delinear una diferencia entre identidad y datos personales bastante clara. La identidad está compuesta por un universo de datos personales, los cuales debemos desglosar mas allá de lo recogido en la norma, a fin de entenderlos a cabalidad, para lo que proponemos agruparlos en tres clasificaciones: datos biométricos, datos atribuidos por el Estado, y datos generados por la persona. A continuación, una descripción de estos tres grupos.

a. Datos biométricos: según la definición del Reglamento General de Protección de Datos (RGPD) de la Unión Europea[17], los datos biométricos son aquellos datos personales referidos a las características fisiológicas, físicas o de conducta relacionadas a una persona, que hagan posible o asegure su identificación única, es decir, corresponden al universo de datos que surgen de la condición del ser humano como ente.
b. Datos atribuidos por el Estado: estos son datos que el Estado atribuye a las personas. Este tipo de datos tienen orígen en una ley, decreto, acto administrativo, sentencia judicial, o cualquier tipo de documento emanado de una entidad gubernamental. A modo de ejemplos sobre el particular podemos citar el estado civil de la persona o el número de la cédula de identidad y electoral, para el caso dominicano.
c. Datos generados por la persona: en esta clasificación de datos enmarcamos loque que la persona por su voluntad puede ser atribuidos o modificados en forma activa. En otras palabras, se forma a partir de ciertas elecciones que una persona realiza a lo largo de su vida. En este tipo de datos podemos enumerar las profesiones u oficios, los gustos en general, y todos aquellos que solo dependen de la voluntad de su titular.

[17] Unión Europea. 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. *Ob. Cit.*

El conjunto de datos de los dos primeros grupos son considerados con cierta complejidad para su modificación, o sea, resultan rígidos, mientras que el tercero es de fácil cambio ya que solo dependen de la determinación de la propia persona. Prueba de esto es que una persona a lo largo de su vida puede realizar cambios en esos datos y no por ello van a tener menor validez que el resto, ya que los mismos participan de forma activa en la conformación de la identidad de la persona. Sin embargo, el certificado de nacimiento es el que funciona como documento de identidad primario en la mayoría de los países y es el documento de identidad más permanente.

Definimos el concepto de identidad humana como el conjunto de rasgos que hace a una persona ser quien es y la distingue de los otros, al mismo tiempo que le permite interactuar con su entorno. La construcción de la identidad de un individuo se conforma de propiedades que le son inherentes, las cuales lo distinguen como un individuo particular que lo hace ser único. Ciertos psicólogos y filósofos angloparlantes han adoptado la palabra *self*, traducida al castellano como "sí mismo" para referirse a la suma de esas características que la persona sabe que posee y que la hacen diferenciable del resto de los congéneres[18].

El proceso de formación de la identidad incia su configuración partiendo de ciertas condiciones propias de la persona, que se encuentran a partir del nacimiento y, posteriormente, continúa su evolución de acuerdo a los hechos y las experiencias que vive en el transcurso de su existencia. Es de esta forma que la identidad humana es configurada, partiendo de su interacción con el medio y el funcionamiento individual propio del sujeto, lo que forma entre estas partes una tensión dinámica que marca la configuración de la identidad hacia una dirección determinada.

[18] DE LA PUENTE, Carlos. La identidad ¿Por qué es importante en el mundo de hoy? [en línea] Universidad del Pacífico© [consulta: 29 enero 2022]. Disponible en http://www.saberescompartidos.pe/wpcontent/uploads/2012/07/la_identidad_por_que_es_importante_en_el_mundo_de_hoy.pdf

La identidad es el elemento que hace posible la interacción del individuo con otros, así como con el gobierno, con las instituciones públicas y privada, y con la sociedad en su conjunto. Es mediante esta que se posibilita reconocer a las personas, para que el sistema pueda ofrecer seguridad jurídica, o bien que los particulares puedan realizar negocios de forma privada. Históricamente la identidad ha sido fundamental para que las personas construyan su forma de vida y los valores democráticos que sostienen el estado de bienestar.

El incremento exponencial que ha tenido el uso de las nuevas tecnologías se ha ido extendiendo a todos los ámbitos de la vida humana, sobre todo el de internet, mediante la web, las redes sociales, las compras, sistemas financieros, entre otros. El salto tecnológico que se ha producido en aproximadamente 15 años, ha impactado de manera medular el comercio, los medios de comunicación, la forma de consumir, el entrenimiento, la gestión, que ha evolucionado las herramientas de productividad. Es previsible que los próximos años continuarán evolucionando las industrias que conocemos actualmente, y tambien surgirán otros tipos de industrias digitales de mayor complejidad, tales como la biotecnología, sistemas de salud, educación, viajes y turismo, tecnología aplicada para cambio climático, servicios financieros globalizados, entre otras.

Todas estas industrias están en transformación y tendrán un efecto multiplicador que continuará impactando nuestra realidad actual. También ha repercutido en la manera como las personas interactúan, pues se ha hecho necesario aportar una serie de informaciones personales, privadas, para acceder al uso de los servicios a través de los medios digitales.

El proceso para poder ser parte de esta transformación y disponer de un mundo manejado digitalmente, debe realizarse de una manera en que resulte fácil vincular la persona al servicio digital. El conjunto de datos personales que se asocia a una persona en un marco

digital, es conocido por algunos como "identidad digital"[19]. La identidad digital es el homólogo en ambiente electrónico de la identidad oficial analógica, la cual se corresponde con los documentos de identidad físicos que expiden y son administradas por los Estados. Consiste en identificadores y atributos de personas que le otorgan a la misma una singularidad, es decir es lo que la hace única entre la población o en un contexto en particular, y es reconocida por los Estados con un propósito regulatorio u otras finalidades oficiales. Este concepto ya ha sido reconocido y desarrollado en Europa por el reglamento eIDAS (910/2014), en vigor desde julio de 2016[20].

Es mediante la identidad digital que resulta posible establecer relaciones electrónicas de confianza entre las personas, sean estas físicas o jurídicas y el Estado al momento de identificarse y manifestar su voluntad en acuerdos y contratos. Esta seguridad, cuando es gestionada presencialmente requiere de acreditación mediante el documento de identidad o pasaporte, lo que toma especial relevancia en el contexto actual, donde cada día mas las personas tienen un estilo de interacción cada vez más digital. La identidad digital va a complementar por un tiempo la identidad analógica que se usa de forma cotidiana en los canales digitales y, posteriormente, la sustituirá completamente en razón de la facilidad de uso que reviste la identidad digital en cualquier canal.

Las actividades realizadas por cada persona en ambiente web configura una parte importante de la identidad digital, ya que deja una huella fuerte y clara, de forma consciente o inconsciente[21]. La diferencia fundamental de la identidad digital con la identidad que comunmente conocemos, es que está compuesta por distintos grupos de datos los cuales según el usuario tenga o no la intención de revelarlos, da origen a la composición de una

[19] SULLIVAN, Clare Linda. Digital Identity - An Emergent Legal Concept. *Ob. Cit.*
[20] NABALÓN, Iván, PÉREZ, Jesús y VANDEVIVERE, Benoit. Identidad Digital: Desbloqueando un efecto multiplicador del PIB en España [en línea] Govtech for Policy Making. IE Public Tech Lab, 2020 ©. [consulta: 29 enero 2022]. Disponible en: https://publictechlab.ie.edu/es/publicaciones/.
[21] GAMERO, Ruth. La configuración de la identidad digital [en línea] Nota Enter-IE 131, junio 2009 [consulta: 29 enero 2022]. Disponible en: https://cursa.ihmc.us/rid=1H8FQCJ5D-R3NH13-47X/acerca_de_la_identidad_digital.pdf

identidad declarada, conformada de información que es revelada expresamente por la misma persona, lo que realiza de acuerdo a las acciones que lleve a cabo, y otra que deriva del análisis de las acciones que realiza la persona. El universo de esta información se puede utilizar para conformar una idea de quién es y qué le gusta a una persona determinada[22].

Resulta relevante preguntarnos ¿qué datos configuran la identidad digital? Tal y como previamente hicimos con la identidad análoga, este universo de datos los agruparemos en otras tres categorías; estas son:

a. Datos de individualización: se trata de información necesaria para identificar a la persona, tales como el nombre, el número de cédula de identidad, el número de la licencia de conducir, fecha de nacimiento, lugar de nacimiento, número de tarjeta de crédito, nombre de usuario a los sitios web donde accede, etc.
b. Datos de comportamiento: sobre transacciones, historial de navegación, datos de localización, historial de compra, accesos, etc.[23]
c. Datos creados: son datos que va creando de manera activa el propio usuario, los cuales son posibles de obtener a traves del completado de formularios en línea, información suministrada mediante las redes sociales o profesionales, puntuación de productos y opiniones en páginas web donde compra productos, entre otras.

[22] GEORGES, Fanny. Who are you doing? Declarative, Acting and Calculated Identity in web 2.0. [en línea] En *VRIC 2009, Laval Virtual, Virtual Reality International Conference, 22-26 Avril 2009*. 2009, pp. 1-6. [consulta: 29 enero 2022]. Disponible en https://archivesic.ccsd.cnrs.fr/sic_00496816.

[23] *Shadow data*. Traducido significa textualmente sombra de datos, y llamamos a esto el cuerpo colectivo de datos que se genera y registra automáticamente a medida que avanzamos en nuestras vidas en lugar de crearse intencionalmente. Las fuentes incluyen sensores, metadatos de comunicaciones y mecanismos de seguridad y autenticación, entre otras posibilidades. Sombra, en este contexto, significa seguir. Los datos relacionados con la vigilancia son un motor particular para los requisitos de capacidad de almacenamiento. Estos datos a menudo se registran y almacenan a largo plazo, proporcionando un registro persistente de las actividades en línea y en el mundo físico.

Resumiendo lo antes expuesto, entendemos que la identidad digital puede clasificarse en dos categorías[24], a saber:

a. **Identidad digital legal**: es la que necesita de una vinculación con la identidad legal de la persona, sea esta de naturaleza física o jurídica. A modo de ejemplo, podemos indicar que la misma se necesita para realizar cualquier tipo de transacción en una institución financiera, o con entidades gubernamentales[25].
b. **Identidad digital simple**: este tipo de identidades no son necesarias que se encuentren vinculadas con una identidad legal física. Este tipo de identidad puede ser utilizada para navegar en la web, o para utilizar redes sociales[26].

Aunque podría decirse que el concepto de identidad digital se ha estado desarrollando en la práctica comercial durante algunos años, la necesidad de disponer de un concepto legal de identidad digital ha surgido claramente como resultado impostergable de poner un nombre a la identificación que las personas utilizan y necesitan para realizar millones de interacciones en el ecosistema que desarrollamos hoy día, específicamente en un ambiente *online*. Como hemos visto, la identidad digital de un individuo consiste en un conjunto de información almacenada en forma digital. Este conjunto de información figura en el registro de identidad, en bases de datos accesibles para identificar el individuo[27] que se propone realizar una operación.

[24] PAREJA, Alejandro, et. al. La gestión de la identidad y su impacto en la economía digital. *Documento para Discusión núm. IDB-DP-529. Ob. Cit.,* p. 7.
[25] *Ibidem.*
[26] *Ibídem*.
[27] DE OLLOQUI, Fernando; ANDRADE, Gabriela; HERRERA, Diego. Inclusión financiera en América Latina y el Caribe. [en línea] *Documento para discusión Nº IDB-DP- 385,* 2015, p. 12 [consulta: 29 enero 2022]. Disponible en: https://publications.iadb.org/publications/spanish/document/Inclusi%C3%B3n-financiera-en-Am%C3%A9rica-Latina-y-el-Caribe-Coyuntura-actual-y-desaf%C3%ADos-para-los-pr%C3%B3ximos-a%C3%B1os.pdf

B. Importancia y beneficios aportados por la adopción de la identidad digital

Los avances alcanzados con las nuevas tecnologías traen una gran oportunidad para que muchas personas puedan acceder y utilizar los servicios financieros y demostrar su identidad digital es trascendental para integrarse al desarrollo económico, financiero y social. Por tanto, se necesita de una forma de identidad válida habilitadora para distintos tipos de servicios, mercados, estándares y tecnologías. Tanto las entidades privadas, como los gobiernos y los reguladores han estado en la búsqueda de soluciones integrales que faculten los clientes y ciudadanos a identificarse *online*. De ahí ha surgido una situación particular, debido a que son muchas las personas que han quedado en un estatus de exclusión financiera a nivel mundial.

En el sector público, los problemas recurrentes planteados por los gobiernos se destacan por el hecho de que no existe un mecanismo que permita la identificación digital de los ciudadanos, ya que es de suma dificultad conciliar con el 100% de la población, incluidas las personas cuyas condiciones de vida son de vulnerabilidad. Es así como la adopción de un sistema que permita realizar la identificación digital adquiere una mayor importancia.

Contar con una identidad digital estándar, posibilita acceder a los servicios tanto públicos como privados de manera inclusiva y transparente. Si esta fuera provista por el mismo Estado beneficiaría los ciudadanos en su gran mayoría, pues mediante la misma se puede conseguir la simplificación de trámites, burocracia cero, expansión de la economía digital, conectividad, entre otros.

Asimismo, la identidad digital cada vez más encuentra su posición como una herramienta esencial en el sector bancario, especialmente en el caso que nos ocupa, para las entidades de intermediación financiera, ya que permite realizar operaciones críticas con una precisión mayor, entre ellas la de identificar y autenticar a sus usuarios, mejorar el conocimiento

sobre sus clientes, hacer más simple el proceso de vinculación y brindar una mejor experiencia en tiempo real, desde cualquier parte del mundo.

El hecho de contar con una identidad digital abre la puerta a un tema ampliamente trabajado por el Banco Mundial, que es la inclusión financiera de todas las personas. Según una encuesta de la referida entidad, presentada en el 2014, alrededor de 18% de los adultos excluidos económicamente no tienen acceso a los servicios financieros (ya sea a través de un banco o proveedores de servicios financieros móviles), porque carecen de los documentos necesarios para probar su identidad. En todo el mundo, por lo menos 1.500 millones de personas carecen de documentos de identificación oficial y la mayoría de estas personas viven en África, Asia y América Latina[28].

Lo expuesto hace considerar que ya es una realidad la evolución que ha tenido la identidad análoga hasta llegar a convertirse en identidad digital. La información que contienen los documentos de identidad o pasaportes son la fuente principal de información fiable en los procesos de *onboarding* a la hora de precisar la identidad de las personas y comenzar cualquier modelo de identidad digital de una forma segura y confiable.

En los países donde se han adoptado modelos de identidad digital para industrias reguladas, las identidades expedidas por estas suelen ser la fuente mas auténtica y fidedigna a la hora de responder quién es quién. Con esto se crea un entorno de confianza en la realización de transacciones de carácter público o privado, ayudando a construir la evolución del entorno digital en el que nos desenvolvemos. Hoy se viaja, se pagan impuestos, se accede a un sistema de salud y de educación, se tiene una relación laboral o se puede contratar un producto bancario o financiero en gran medida sobre la base de dicha identidad de carácter legal que gestionan los países[29].

[28] ASOBANCARIA. La identidad digital: el camino para impulsar la inclusión financiera. *Ob. Cit.*, p. 1.
[29] NABALÓN Iván, HERRERA, Diego, VADILLO, Sonia. *Onboarding* Digital [en línea] Banco Interamericano de Desarrollo© 2021, p.7. [consulta: 29 enero 2022]. Disponible en: https://publications.iadb.org/publications/spanish/document/Onboarding-digital.pdf

Un ejemplo de industrias reguladas es el sector financiero, donde el responsable de los datos de la identidad de los ciudadanos es el propio prestador de servicios. En este orden, el prestador de servicios asume el costo de la puesta en marcha de proyectos o compra de herramientas tecnológicas que le permitan conocer a sus clientes y realizar transacciones de forma segura y confiable.

El *onboarding* digital es un proceso electrónico que permite la identificación de los consumidores financieros en su interacción con una entidad financiera, cuyos resultados generan una confianza equivalente al proceso que normalmente se realiza de modo presencial. Para su efectividad, es requerida una confianza que equivale a la que ofrecen los canales directos; es decir, a la identificación realizada históricamente por parte de las entidades financieras en las oficinas comerciales. Es un proceso que se realiza de forma totalmente remota y exclusivamente mediante el canal en línea.

El *onboarding* digital mejora el acceso a los servicios financieros, incrementando el nivel de inclusión financiera. Habilita además a los bancos y prestadores de servicios financieros a mantener relaciones digitales de inicio a fin, lo que se traduce en una mejor competitividad y en la posibilidad de ofrecer mayor variedad de servicios.

La identidad de una persona física se basa comúnmente en una serie de atributos extraídos del proceso de verificación de su identidad legal, tales como nombre, dirección, país de residencia, fecha de nacimiento. Es importante enfatizar que el identificador único utilizado por las instituciones financieras suele representarse con el número del documento de identidad expedido por el Gobierno o identificadores únicos expedidos por la administración, como norma habitual y siempre que el país cuente con ellos.

Como elementos complementarios al identificador único, también existen una serie de atributos pertenecientes a la identidad legal de la persona que podrían diferir entre países,

como podría ser el género, la ocupación, el lugar de nacimiento, correo electrónico o número telefónico. Los últimos suelen ser datos de obligatorio suministro y confirmados en los procesos de *onboarding* porque sirven de punto de contacto y comunicación en toda la relación[30].

Es prácticamente unánime la identificación de los principales beneficios del proceso por parte de los grupos de expertos[31] y dentro de ellos podemos señalar los siguientes: a) genera eficiencia en la contratación. b) Favorece la inclusión financiera al lograr incrementar la penetración de los servicios en lugares remotos. c) Favorece el desarrollo y perfeccionamiento de los mercados, permitiendo un acceso abierto y eficiente de contratación de productos y servicios. d) Incrementa la conveniencia para el usuario y abre la posibilidad de nuevos canales (dispositivos móviles) así como su disponibilidad, por ejemplo, las 24 horas, los siete días de la semana. e) Disminuye costos de transacciones para el usuario.

La digitalización del proceso de abordaje de los clientes tiene numerosas ventajas para las instituciones financieras: simplificación de los procesos operativos, reducción de errores humanos en procesos manuales de control, ahorro de costos, y mejoramiento del monitoreo de las transacciones, al tiempo que facilita el acceso a una base de clientes más amplia, lo que ayuda con la inclusión financiera de los sectores poco favorecidos de la población. Para los consumidores financieros es indudable que la digitalización puede reportar enormes ventajas, al permitir el acceso a servicios financieros en cualquier momento, desde cualquier lugar[32].

---

[30] *Ibídem*, p. 46.

[31] Las instituciones expertas que han realizado sus aportes formales al estudio son las siguientes: Banco Central de Reserva y Superintendencia y Sistema Financiero del Gobierno (El Salvador); Secretaría de Hacienda y Crédito Público y Comisión Nacional Bancaria y de Valores (México); y gremios o asociaciones transnacionales como Federación Latinoamericana de Bancos (FELABAN), Federación Iberoamericana de Bolsas (FIAB), Alianza Fintech Iberoamérica (AFI), y American Business Dialogue (ABD).

[32] NABALÓN, Iván. La identificación electrónica: redefiniendo las reglas del sector financiero [en línea] *Papeles de Economía Española,* No. 162, 2019, pp. 162-176. [consulta: 29 enero 2022]. Disponible en: https://www.funcas.es/wp-content/uploads/Migracion/Articulos/FUNCAS_PEE/162art13.pdf

Por otra parte, desde el punto de vista económico, pueden ser consideradas dos tipos de ventajas relacionadas con el uso de la identidad digital: i) beneficios que surgen de forma directa de la digitalización de los procesos que ya existían y que antes solamente estaban disponibles si la persona se presentaba de forma presencial (por ejemplo, la verificación de identidad), y ii) beneficios asociados con el nacimiento de nuevos servicios y actividades económicas a través del uso de una identidad digital.

El avance hacia una digitalización de la economía es hoy una necesidad y el sector financiero no es ajeno a ello. El *onboarding* digital puede ser una solución que incentive el avance en la inclusión financiera de la población, al tiempo que facilite el acceso a nuevos productos y servicios financieros digitales de manera más eficiente. Los gobiernos y los encargados de elaborar las políticas pueden contribuir en este sentido mediante la adopción de políticas que posibiliten y promuevan el uso de las tecnologías, dentro de un marco ordenado, con garantías suficientes que salvaguarden de forma adecuada los derechos de los consumidores financieros.

Un excelente ejemplo de esto es el caso de Estonia, un país líder en adopción de identidad digital, que inició en el año 1996 el proceso de autenticación para la banca en línea[33]. Desde entonces, ha habido un desarrollo continuo y en 2014 inició la emisión de la identidad digital para extranjeros que querían formar parte de la comunidad de residentes digitales de Estonia (*Estonia e-residency*)[34]. Actualmente, el 98% de los Estonios tiene un documento de identidad que sirve como *token* para utilizar la identidad digital.

En este caso, solamente el Estado tiene la responsabilidad de identificar a las personas y cada persona debe tener solo una identidad legal, donde el vínculo entre el documento

[33] *Esta es la historia de la sociedad digital más avanzada del mundo* [en línea] e-Estonia © [consulta: 11 enero 2022]. Disponible en: https://e-estonia.com/story/

[34] *Estonia lleva otorgadas 12.000 residencias digitales* [en línea] e-Estonia © [consulta: 11 enero 2022]. Disponible en: https://e-estonia.com/e-residents/about/.

físico y el certificado digital es inequívoco y verificable públicamente a través del código de identificación personal (PIC, por su sigla en inglés), contentivo de 11 números que contienen información personal (incluyendo género y fecha de nacimiento), a diferencia de otros países donde el número de identidad están ordenados de forma secuencial y, no contienen información personal alguna. El PIC es asignado en el momento que la persona se inscribe en el Registro de Población puesto en vigencia en 1992[35].

Fue entre los años 2002 y 2006 cuando se puso en marcha el uso del documento de identidad digital, y desde entonces se ha conservado alrededor de 1.1 millones de documentos activos[36]. A partir de ahí, todo el desarrollo de servicios ha cambiado radicalmente para de esta forma dar paso al mundo digital. Los diferentes sistemas de administración que son utilizados reciben datos de las personas y también sirven como una fuente de datos. El registro de población se actualiza constantemente con los hechos del del estado civil y otras áreas, entre los cuales consta el registro del domicilio, el censo poblacional, los listados de votación, del proceso de emisión de documentos de identidad, de los sistemas de registro civil y del registro de residencia; es decir, que los datos para el registro de población son recopilados por el sector público al prestar diferentes tipos de servicios.

En octubre de 2010 comenzaron a emitirse tarjetas de identificación exclusivamente digitales (DigiID). Solo contiene la función digital del documento de identidad principal y por lo tanto no se puede utilizar para identificar físicamente a una persona. La tarjeta de identidad estonia es multifuncional y se utiliza en todas las áreas de los servicios que son provistos públicamente. Entonces, por ejemplo, en Estonia no tienen una tarjeta de seguridad social separada y no necesitan de llevar la licencia de conducir y los documentos del vehículo de forma separada, ya que la policía de tránsito puede consultar las respectivas

[35] PAREJA, Alejandro, et al. La gestión de la identidad y su impacto en la economía digital. *Ob. Cit.,* p.14.
[36] *La población total de Estonia para el año 2020 es de 1.331.057* [en línea] Banco Mundial © [consulta: 1 febrero 2022]. Disponible en: https://datos.bancomundial.org/indicador/SP.POP.TOTL?locations=EE.

bases de datos en tiempo real a partir de la identificación que contiene el documento de identidad[37].

La experiencia de Estonia muestra que no es necesario el uso de la biometría para crear un ecosistema seguro en un país digitalmente avanzado, es decir, que el mismo se encuente alfabetizado digitalmente. Cuando se preparó la adquisición de documentos de identidad de próxima generación a finales de 2014 y fueron realizadas consultas con expertos en materias de seguridad cibernética y protección de datos, no mostrando apoyo la medida de incluir biometría en el documento de identidad porque lo ven como una solución insegura.

En Estonia la formación en temas relacionados con la transformación digital es continua, sobre todo con los adultos mayores, y abarca capacitaciones de comportamiento seguro en Internet y utilización segura de dispositivos inteligentes, así como actividades formativas para jóvenes a quienes les interese estudiar ciencias de la tecnología.

Otro ejemplo que vale la pena revisar es el de la estrategia de gobierno digital de Canadá, la cual inició en el año 1999 con gran fuerza. Tenía como su norte convertirse en el principal país con mejor conectividad del mundo, cuyos servicios se centren en el cliente. La experiencia canadiense para identidad digital se basa en la lógica de *BYOI (bring your own identity)*[38], es decir, use la identificación que prefiera, para el uso de sus obligaciones tributarias, para el acceso al sistema financiero, y otra dependencia donde es necesario contar con la identificación personal, siempre que la credencial utilizada cumpla con los estándares mínimos requeridos por el Consejo de Identificación y Autenticación Digital de Canadá, conocido como DIACC[39], cuya compilación fue realizada en el 2015.

---

[37] *El e-Estonia Briefing Center está a su servicio* [en línea] e-Estonia© [consulta: 20 marzo 2022]. Disponible en: https://e-estonia.com/briefing-centre/about-us/.

[38] BARROS, Alejandro. ¡Identidad Digital- Canadá, un modelo que me gusta! [en línea] Blog eL ABC © [consulta: 2 febrero 2022]. Disponible en: https://www.alejandrobarros.com/identidad-digital-canada-un-modelo-que-me-gusta/

[39] *Identificación digital para canadiense* [en línea] Consejo de Identificación y autenticación digital de Canadá © [consulta 2 febrero 2022] Disponible en: https://diacc.ca/the-diacc/

El sistema utilizado en Canadá ha sido desarrollado por visionarios que entendieron la importancia de estar conectados, uniendo todo el país en una economía digital robusta, abierta al mundo, uniendo gobiernos y ciudadanos, ciudadanos entre sí, y comercios privados con los clientes. Desde el año 2015, un ciudadano cualquiera puede abrir una cuenta bancaria desde cualquier parte, interactuando en un ambiente diseñado con la seguridad y privacidad necesaria.

La identificación digital equivale electrónicamente a la identidad en formato físico, como medio de probar la correcta identificación personal y de este modo acceder a cualquier tipo de servicio en línea. Para ello hace falta agotar un proceso de autenticación necesario, el cual es realizado probando qué tipo de identidad tiene la persona, número de pasaporte, número de seguridad social, huella digital o escaneo de iris. Esta validación es posible realizarla combinando dos o más identificadores admisibles.

Cabe señalar que en el esquema desarrollado por Canadá, la verificación de identidad es un proceso separado de la validación de identidad y puede emplear diferentes métodos, así como utilizar información personal que no está relacionada con la identidad. Se puede acudir a diferentes métodos, tanto por separado o en combinación, tales como: confirmación basada en el conocimiento (por ejemplo, preguntas de desafío-respuesta), confirmación biológica o de comportamiento (por ejemplo, uso de huellas dactilares), confirmación de árbitro confiable (por ejemplo, confirmación de identidad basada en información en poder de una agencia gubernamental), confirmación de posesión física (por ejemplo, posesión de un *token* o dispositivo específico).

Este es un ingrediente clave para garantizar que la representación digital de una persona se cree correctamente, se use exclusivamente para representar a esa misma persona y sirva para llevar a cabo transacciones con confianza.

Se puede concluir que Canadá, por su temprana inserción en la economía digital, su intensivo uso de las TIC, y la combinación de las buenas relaciones públicas y privadas, han obtenido como resultado un gran éxito en su *e-gobierno*. Su éxito ha sido tal que ocupó los primeros lugares en *rankings* internacionales de economía digital, e incluso en algunos ámbitos y tiempos ha ocupado el primer lugar, reconocido por gobiernos de todo el mundo[40].

Casos de éxito probado como son los de Estonia y Canadá demuestran que los esfuerzos unificados entre los sectores público y privado son determinante para alcanzar el desarrollo de sistemas de identidad digital sólidos. Otros países están realizando sus esfuerzos en integrar estas bondades en su gobierno, para lo cual debe tenerse en cuenta, sobre todo, el rol del sistema financiero como principal consumidor de servicios de identificación y autenticación de la economía. Disponer de un plan unificado entre los sectores públicos, privados y el financiero no solamente genera ahorros, sino que posibilita su adopción por parte de la población.

En América Latina el panorama es muy distinto, pues existen marcadas diferencias en los niveles de madurez y gobernanza de los sistemas de identidad que son utilizados. Recientemente, los países de la región han tomado la iniciativa para fortalecer sus sistemas de identidad, que van desde la adecuación de sus marcos legales hasta la mejora de equipos para la emisión de tarjetas de identificación con tecnología avanzada[41]; sin embargo, son casi nulos los sistemas puramente digitales.

[40] GIL – GARCÍA, J. Ramón y ALDAMA, Armando. Gobierno electrónico en Canadá: Antecedentes, objetivos, estrategias y resultados [en línea] Cide.edu, 2010. Número 248. [consulta: 20 enero 2022] Disponible en: https://cide.repositorioinstitucional.mx/jspui/bitstream/1011/252/1/000103323_documento.pdf.

[41] Se puede mencionar a países como Argentina, Costa Rica, Ecuador y Uruguay, que han promovido el uso de la firma digital a partir de la reformulación de sus marcos legales. Así también Perú, Bolivia y Uruguay están emitiendo documentos de identidad que incluyen chips, lo cual facilitará la validación y autenticación de la información del ciudadano.

Las mejoras introducidas han contribuido a una mayor seguridad de los documentos, interconectando sistemas, permitiendo la autenticación de la identidad entre entidades y mejorando la calidad de la prestación de servicios. Sin embargo, en muchos países se requieren inversiones de mucha envergadura para implementar sistemas de identidad digital que puedan brindar un servicio confiable, seguro, accesible y con cobertura universal. Más aún, la promesa de mejores servicios vinculados al sistema de identidad requiere a su vez de inversiones adicionales en plataformas de conectividad e interconexión.

De acuerdo con el estudio realizado por *World Economic Forum* en 2016[42], para las instituciones financieras las grandes ventajas que supone la implementación de la identidad digital son múltiples y los mismos han aumentado a medida que la necesidad de virtualizar todos los procesos aumenta. Estos beneficios se pueden categorizar en seis reglones, a saber:

1. Mejora en los productos y servicios. Las Entidades Financieras (en lo adelante, también EF), han aumentado el acceso a información detallada y fiable para los usuarios que les permita adaptar mejor los procesos, productos y servicios, tales como: calificación de riesgos para productos de financieros, asesoramiento financiero, gestión de activos, calificación crediticia, entre otros. Las EF podrían comenzar a recurrir a información fiable, con consentimiento, para gestionar y evaluar mejor el riesgo; los protocolos de identidad digital seguros y la transferencia de atributos digitales mejorarían la experiencia del usuario y ampliarían el número de servicios que las EF podrían proporcionar de forma segura en línea.

[42] MCWATERS, R. J., et al. *A blueprint for digital identity the role of financial institutions in building digital identity.* [en línea] World Economic Forum, Future of Financial Services Series. 2016, pp. 1-108. [consulta: 2 febrero 2022] Disponible en: https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/WEF_A_Blueprint_for_Digital_Identity_0.pdf

2. Eficiencia operacional. Se podría acceder a la información de los usuarios de forma digital, consolidada mediante consultas en la red de identidad digital. Tener atributos en una forma digital consolidada proporcionaría una visión única del mismo y permitiría a las entidades agilizar las operaciones orientadas al cliente, como la incorporación, igual que muchos procesos de *back office*[43].

3. Disminución del fraude. La información del usuario solo estaría en manos de entidades que sigan los estándares en torno a la protección de datos; esto reduciría el fraude (como las transacciones de tarjeta no presente realizadas utilizando información de envío y facturación robada en diversas modalidades de violación de datos a gran escala u de otra manera). Los métodos de autenticación digital reducirían el fraude resultante de cuentas de usuario pirateadas o comprometidas.

4. Cumplimiento mejorado. La identidad digital daría a las entidades acceso a información de atributos confiable y actualizada para los usuarios, mejorando la precisión de los procesos de conozca su cliente. La transferencia y almacenamiento de información digital permitirían completar los procesos de cumplimiento de manera más rápida y fácil, lo que haría posible un procesamiento más rápido y reduciría el tiempo dedicado a la corrección de la información y de errores humanos. Los procesos de cumplimiento podrían automatizarse y ejecutarse en ciclos más regulares. Habría mejor visibilidad de las estructuras de propiedad corporativa y la identidad de los directores corporativos para mejorar los procesos corporativos de conocimiento de sus clientes.

5. Crecimiento de los ingresos. Las instituciones podrán monetizar la identidad como servicio a través de modelos de negocio, como tarifas de suscripción o servicios de

[43] El *back office* es el conjunto de tareas, actividades, puestos y procedimientos encaminados a dar apoyo y soporte a la empresa en la gestión de la misma.

tarifa por transacción para operaciones de identidad de alta seguridad, que incluyen: autenticación, firmas digitales, la finalización de transacciones de identidad, como sería la de proporcionar información de atributos (por ejemplo, proporcionar información de envío a comerciantes) o proporcionar información sobre atributos (por ejemplo, certificar a un comerciante que un usuario es mayor de cierta edad en función de fecha de nacimiento).

6. Mejor experiencia de usuario y posicionamiento competitivo. Al colaborar con gobiernos, entidades del sector público y otras entidades del sector privado, las EF pasarían a formar parte de un ecosistema confiable que trabaja en el desarrollo de la economía digital. Como salvaguardas confiables de la información de los usuarios, las instituciones aumentarían la fortaleza de sus relaciones con los usuarios.

Como vemos, estos avances, particularmente cuando se combinan con tecnologías digitales relacionadas, como los sistemas de pagos en línea y móviles, tienen el potencial de superar las ineficiencias de los sistemas de identificación basados en papel. Al mismo tiempo, la identificación digital plantea muchos desafíos relativos a la protección de datos y la privacidad, sostenibilidad fiscal y elección y el uso de diferentes opciones tecnológicas, pero la misma constituye la llave que abre la puerta de la transformación del sistema financiero, mudándolo de lo análogo al mundo virtual.

II. Transformación del sector financiero

El rápido desarrollo de la tecnología trae como consecuencia que el cambio que sufrimos sea altamente disruptivo[44]. No solamente es la magnitud de este cambio, sino

[44] Utilizado por primera vez en el artículo titulado 'Disruptive technologies: catching the wave' (de Joseph L. Bower y Clayton M. Christensen, 1995), el término disrupción tecnológica da nombre al fenómeno que se produce cuando la aparición de una nueva innovación o tecnología modifica por completo la manera de operar e interactuar de las personas, del conjunto de la sociedad e incluso de los mercados nacionales e

especialmente su rapidez es la que hace que sea particular en el caso de los servicios financieros.

Desde la banca tradicional hasta la banca digital, han incidido dos factores esenciales para que tenga lugar la digitalización, que son el desarrollo tecnológico y su aceptación en la vida de las personas. Hasta hace relativamente poco tiempo, era inconcebible abrir una cuenta de ahorros desde la conveniencia que presta la sala de casa simplemente con un *selfie* o foto de perfil.

En esta parte A estaremos abordando cómo ha irrumpido la transformación del sistema iniciando con la digitalización de los procesos fundamentales para el desarrollo de las actividades propias de la banca. En la parte B revisaremos como la identidad digital resulta ser el elemento clave que amalgama los servicios digitales provistos por las EF y las personas que quieren hacer uso no de las bondades que la atencion no presencial les brinda.

A. Situación actual del sector financiero en cuanto a la digitalización

La digitalización, según la definición que encontramos en la RAE es la acción y efecto de digitalizar, o codificar en números, dígitos, datos o informaciones de carácter continuo, como una imagen fotográfica, un documento o un libro. Por lo tanto, está claro que la digitalización es la traducción real de la información de la coordinación real a la coordinación digital, lo que hace información móvil y se puede procesar. La digitalización es, por tanto, una consecuencia de todo el avance que la tecnología ha tenido en los últimos años.

internacionales. Hoy en día, la disrupción tecnológica ha de entenderse como una revolución digital que engloba múltiples ámbitos. Ahondando en el núcleo de este concepto, hablar de disrupción tecnológica supone indagar en los cambios que están aún por venir, poder anticiparlos a través de análisis e investigaciones, para terminar, convirtiéndolos en realidades que contribuyan a facilitar la vida de los seres humanos.

En el sector financiero, la digitalización va más allá de lo de lo definido por la RAE. Es el proceso por el cual los bancos transforman su oferta de productos y la forma de proveer sus servicios ofreciéndolos al cliente mediante soluciones digitales y el acceso a todo esto ocurre vía dispositivos electrónicos, de la mano con una transformación completa en sus operaciones internas.

Las primeras evidencias de transformación en la banca, incluyendo procesos digitales, tienen lugar en el primer tercio del siglo pasado, correspondiendo a los alemanes el liderazgo en este proceso. En la década de los años 30, los germanos introdujeron en su estructura bancaria diversas innovaciones informáticas. Su primera gran innovación fue en un principio el télex, que permitía enviar mensajes a los bancos internacionales a través de una red de comunicaciones de alcance mundial, transmitiéndose así los textos oficiales y comerciales por parte de las entidades.

Ya en el año 1946 se sustituye la tecnología electromecánica por la electrónica, perfeccionándose el primer ordenador y creándose el *Electronic Numerical Integrator Computer*[45], una herramienta que significó un verdadero punto de inflexión para el posterior desarrollo de las tecnologías de la información en materia de servicios financieros.

Para el año 2017, Alemania era el país de Europa con menos bancos sin iniciar el proceso de digitalización, con tan solo un 4% de las instituciones financieras encuestadas con rezago en la materia, mientras que la media del estudio se sitúa en un 10%[46].

[45] ENIAC, acrónimo de Electronic Numerical Integrator And Computer. Fue el dispositivo de cálculo más potente construido hasta la fecha y el primer ordenador digital electrónico programable de propósito general. Al igual que el motor analítico de Charles Babbage (del siglo XIX) y el coloso informático británico de la Segunda Guerra Mundial, tenía ramificación condicional, es decir, podía ejecutar diferentes instrucciones o alterar el orden de ejecución de las instrucciones en función del valor de algunos datos.

[46] *La digitalización de la banca, in proceso pensando en el cliente* [en línea] bbva.com© [consulta: 10 febrero 2022]. Disponible en https://www.bbva.com/es/digitalizacion-banca-proceso-pensando-cliente/

Otra gran innovación en materia bancaria tuvo lugar en la década de los 70, cuando aparecen los primeros cajeros automáticos[47]. Inicialmente se limitaban a operaciones de efectivo, pero al cabo de los años ya se podían ejecutar diversas operaciones como transferencias y visualización de saldos. A su vez, la *Society of Worldwide Interbank Financial Telecommunication* (red SWIFT[48]) se instala como una versión mejorada del Télex alemán. En 1973, en un total de 15 países, 239 bancos compartían información y se comunicaban a través de la red SWIFT. Para la década del 90, al disponer de un sistema bancario más desarrollado que el resto del mundo, Japón instauró el concepto web móvil, permitiendo a los clientes acceder desde sus dispositivos a la web de su banco[49]. Esta práctica es una de las innovaciones de la banca que ha perdurado por mayor tiempo prácticamente en todo el mundo.

Actualmente, la tendencia de digitalización es cada vez más fuerte. Tanto es así que para el año 2025 se espera que la banca digital genere unos 8,646 millones de dólares, y que traiga consigo una Tasa de Crecimiento Anual Compuesto (CAGR) de alrededor del 3,8% entre 2019 y 2025.

Esto requiere que los bancos se preparen de forma eficiente para ser capaces de proveer soluciones comparables a las que son ofrecidas por otros proveedores de servicios

[47] Un cajero automático es una mñaquina. Expendedora de. Dinero que. Se usa con una tarjeta de plastico, con banda magnetica o chip sin necesidad de un personal del banco.

[48] La Red SWIFT, es la Sociedad para las Comunicaciones Interbancarias y Financieras Mundiales es una gran red global a través de la cual el dinero electrónico viaja de un lugar a otro del mundo. Esta organización que tiene a su cargo una red internacional de comunicaciones financieras entre bancos y otras entidades, a lo largo y ancho del mundo, que funciona en más de 200 países ininterrumpidamente las 24 horas del día y los siete días de la semana. Creó un sistema de procesamiento de datos compartidos y una red de telecomunicaciones a nivel mundial, los procedimientos de operación fundamentales, las reglas para definir responsabilidades, etc., es decir, una especie de idioma común que entiendan todas las entidades financieras del mundo, no importa el lugar donde estén asentadas.

[49] CAMILO, Constantino, et. al. Digitalización del sector financiero español: impacto en la eficiencia y casos de estudio. [en línea] Trabajo fin de máster. Madrid: Colegio Universitario de Estudios Financieros [consulta: 12 febrero 2022]. Disponible en: https://biblioteca.cunef.edu/files/documentos/TFM_Camilo_Constantino,_Eva_Martinez,_Claudia_Rabal,_Zheng_Zhang.pdf.

financieros, aunque estos sean competencia o no de la banca tradicional, como es el caso de las *Fintech*[50]. Actualmente los bancos no son el único canal a través del cual muchos clientes reciben servicios financieros, también existen muchos prestadores de servicios no financieros que educan al cliente respecto de lo que resulta en una forma eficiente de prestar servicios. En efecto, cada día, las *Bigtech*[51] y las ya referidas *fintech* se interrelacionan con los usuarios de los servicios financieros, quienes encuentran ahí los nuevos métodos y modelos de hacer las cosas, a la vez que conocen la oferta disponible de soluciones financieras adaptadas a lo que mandan los tiempos, es decir, *Custom Made*.

Actualmente, la transformación hacia lo digital o digitalización que es llevada a cabo de forma colectiva por ciudadanos, entidades y por instituciones de todos los sectores, está caracterizada por ser un fenómeno veloz, el cual no está limitado a sustituir las herramientas o los procedimientos de actuación, sino que cambia la mentalidad de la sociedad en su conjunto y el modo en que esta lo percibe. La nueva generación es más hábil con la tecnología y son abanderados de la comodidad.

La omnicanalidad[52], como estrategia para gestionar el cliente, la necesidad de ofrecerle experiencias más que productos y servicios, vinculándolos, por ejemplo, en su diseño, o bien la interoperabilidad, la sostenibilidad. Su disponibilidad constante se ha vuelto fundamental para conectar los individuos y las organizaciones actualmente[53].

---

[50] Fintech es la contracción de las palabras inglesas 'finance' y 'technology', las cuales engloban a los servicios de las empresas del sector financiero las cuales utilizan las nuevas tecnologías para crear productos financieros innovadores.

[51] *Bigtech* hace referencia a grandes empresas tecnológicas que cuentan con una vasta red de operaciones. Debido a su alcance y capital, estas compañías pueden usar sus plataformas para ofrecer servicios financieros al público.

[52] *Omnichannel* es un acrónimo de neologismo que describe una estrategia comercial. Según Frost & Sullivan, omnicanal se define como "experiencias de cliente de alta calidad, fluidas y sin esfuerzo que ocurren dentro y entre los canales de contacto". La omnicanalidad es una estrategia que utiliza todos los canales de comunicación de una empresa de forma integrada y sincrónica. Tiene como objetivo fortalecer la relación cliente-empresa y, para ello, busca ofrecer una experiencia consistente en todos los canales. Disponible en: https://www.zendesk.com.mx/blog/omnicanalidad-que-es/

[53] MARTÍN, Bartolomé. La fiebre de lo Digital [en línea]. KPMG Tendencias ©. [consulta: 10 febrero 2022]. Disponible en: https://www.tendencias.kpmg.es/2019/04/fiebre-digital-juridico/

Los reguladores de todo el mundo están sumergidos en procesos de revisiones y modificaciones, así como estableciendo criterios, y en ello han evidenciado sus diferencias. Algunos pocos, son más lanzados y audaces, al darse cuenta de que una actitud positiva hacia la innovación tecnológica puede significar una ventaja competitiva para sus mercados financieros, y, en última instancia beneficiar por igual a los consumidores. Esto es lo que aparenta haber sucedido con el Reino Unido.

El país anglosajón lleva bandera ganadora en cuanto a lo que digitalización e innovación financiera se refiere, pues en el año 2013 creó la PSR[54] o Regulador de Sistemas de Pagos, dos años antes de que salieran los primeros borradores de la Directiva Europea relativa a este tema. Mediante la PSR se buscó la innovación del sistema bancario, actuando esta entidad como subsidiaria del *Financial Conduct Authority* (FCA), que es el Regulador Financiero con mandato de promover la confianza, transparencia y competencia en los servicios ofrecidos por el sistema financiero de Reino Unido, hasta ese momento poco flexible y con la infraestructura de los pagos tecnológicamente poco desarrollada.

Con esta nueva regulación, el Tesoro de Reino Unido estaría en capacidad de contribuir al fortalecimiento del sistema de pagos, sobre todo para minoristas, de modo que funcionaría efectivamente para todos los usuarios, incluidos los finales. Esto así, en razón de que este país tiene el criterio, desde hace tiempo, de que los dueños de las cuentas deben tener el poder de sus datos y el sector financiero debe estar abierto a la innovación, dentro de un marco de seguridad jurídica.

Gracias a este enorme avance, tuvo paso en el sistema financiero la Banca Abierta, que básicamente trata del acceso libre a los datos de los clientes en otras entidades, siempre que se tenga autorización explícita por parte del titular. Se conformó en el año 2015 el

[54] Siglas de *Payment Sistem Regulator,* Regulador del Sistema de Pago.

grupo de trabajo de banca abierta, *Open Banking Working Group*[55], cuya función es la creación los requisitos obligatorios de cumplimiento en la relación entre las entidades bancarias y las nacientes *fintech*, para lo cual se han emitido los estándares que indican cómo deben ser generados y compartidos los datos financieros y la forma en que se debe tener acceso a estos, para dictar la relación y operación entre ellas[56]. Se ha dado un importante paso para crea una guía que funge como un directorio con las *fintech* con licencia para operar en el territorio inglés.

El modelo "*open banking*", exigido al sector bancario por el regulador, significa que las Entidades Financieras deben construir *API* (interfaces que permiten el intercambio de información en condiciones seguras) que siguen un estricto proceso de estandarización, para que formen parte de un ecosistema de proveedores de servicios a los clientes bancarios[57]. La decisión permite que los proveedores de servicios de pagos (PSP) no bancarios dependan en menor medida de los sistemas de los cuatro grandes bancos británicos[58] para el proceso de las solicitudes de los clientes.

Las nuevas regulaciones que entraron en vigor gradualmente desde enero del 2018 hasta septiembre del 2019 incluyen cambios fundamentales en la industria, pues sirven de orientación a terceros sobre como acceder a la infraestructura bancaria. Las regulaciones relevantes están en vigencia y se aplican en países, tales como Reino Unido, EUA, Brasil, India y Australia.

[55] *Grupo de Trabajo de Banca Abierta* [en línea] Euro Banking Association © [consulta: 8 febrero 2022]. Disponible en: https://www.abe-eba.eu/thought-leadership-innovation/open-banking-working-group/.
[56] *The Open Banking Standard: la hoja de ruta de la banca abierta* [en línea] BBVA.com© [consulta: 11 febrero 2022]. Disponible en: https://www.bbva.com/es/the-open-banking-standard-la-hoja-de-ruta-de-la-banca-abierta/
[57] *Banco de Inglaterra pone más fácil a las 'startups fintech'* [en línea] BBVA.com© [consulta: 11 febrero 2022]. Disponible en: https://www.bbva.com/es/banco-inglaterra-pone-mas-facil-startups-fintech/
[58] Estos grandes bancos son identificados como Barclays, HSBC, Lloyds y RBS.

En esta transformación digital y en este continuo desarrollo de la tecnología, les corresponde a las empresas y a las entidades del sector financiero mantenerse actualizados, y simultáneamente contar con herramientas de punta, que mejoren y aumenten en la eficacia de los procesos, en la búsqueda de lograr así una mayor margen de ganancias, mejora en la calidad del servicio y en la forma de proveerlo.

La digitalización ofrece muchos beneficios a las entidades del sector financiero y puntualizarlos es muy importante en el marco de esta investigación, ya que mediante este proceso los bancos están transformando sus productos y servicios para ofrecer al cliente soluciones digitales y acceso a todos estos a través de dispositivos electrónicos, a la par que operan una transformación integral internamente en su operatividad. Con su efectiva y extendida implementación, la transformación digital es la base de las nuevas oportunidades de estrategia de negocios que surgen gracias a la aparición de las tecnologías. Asimismo, este cambio no se trata solamente de tecnología, sino que también implica nuevas habilidades tanto en los individuos como en la reinvención de organizaciones que influyen en los mercados globales tradicionales.

Según KPMG, un 88% de los directores ejecutivos (*CEO*, por sus siglas en inglés) en el sector financiero están listos para transformar fundamentalmente sus negocios para seguir siendo competitivos. La transformación digital es vital para sobrevivir en este nuevo mercado tecnológico, lo cual ya es casi natural. Con un cliente que exige soluciones digitales y un nuevo mercado competitivo de modelos capaces de ofrecerlo de manera más eficiente que cualquier banco tradicional, es un fenómeno frente al cual se debe de reaccionar, pues dudar de ello sería prácticamente sentenciar el fin del banco[59].

[59] URÍA, Francisco. El sector financiero español ante el reto de la transformación digital [en línea] KPMG Tendencias [consulta: 12 febrero 2022]. Disponible en: https://www.tendencias.kpmg.es/2018/08/el-sector-financiero-espanol-ante-el-reto-de-la-transformacion-digital/

Es tanto así, que de acuerdo con el *World Retail Banking Report*, hoy día los clientes están demandando servicios personalizados, los cuales los bancos no son capaces de ofrecer, mientras que este nuevo formato de negocios, gracias a las herramientas digitales desarrolladas a estos fines, sí lo permiten.

Dentro de los beneficios que podemos destacar en la digitalización del sector financiero, las opiniones generalizadas de los expertos en la materia coinciden en las siguientes ventajas, recogidas en un artículo publicado por la Liga de Asociaciones de Ahorros y Préstamos referente a la transformación digital[60], a saber:

1. Experiencia de usuario mejorada: la digitalización ha mejorado sustancialmente la experiencia general del usuario, moviéndose hacia un modelo centrado en el cliente, el cual proporciona soluciones de tecnología de análisis que permiten entregar a cada cliente productos y servicios personalizados.
2. Incremento en el número de clientes: A pesar de que algunas personas ya no confian tanto en la banca tradicional, las instituciones financieras han aumentado su base de nuevos clientes, gracias al crecimiento y la facilidad del uso de aplicaciones bancarias y banca en línea. Pero con la llegada de las *fintech*, está claro que los bancos deberán de cambiar la metodología con la que hacen negocios para así evitar la fuga de clientes.
3. Operaciones más eficientes: Gracias a esta transformación digital, las entidades bancarias pretenden mejorar sus operaciones realizadas manualmente y hacerlas más eficientes, con la finalidad de reducir el error humano en la gestión de sus clientes. Una solución digital que permite recopilar correctamente todos los datos y firmas desde el primer contacto, lo que beneficia enormemente sus operaciones.

[60] 5 ventajas de la digitalización en el sector bancario [en línea]. LIDAAPI. Transformación Digital 2019 [consulta: 24 marzo 2022]. Disponible en: https://lidaapi.org.do/2019/09/24/5-ventajas-de-la-digitalizacion-en-el-sector-bancario/

4. Reducción de costes: Una de las mayores ventajas que aporta la digitalización al sector bancario es la reducción de costes tanto para los clientes como para las instituciones, gracias al uso de transacciones sin efectivo y nuevos medios de pago. Un ejemplo de esto son los *Neobanks*, que no cuentan con sucursales físicas y que tienen licencia bancaria para ofrecer productos financieros, de ahorro y tarjetas de crédito, de la manera similar que lo hacen los bancos tradicionales, pero operan al 100% de manera digital.
5. Decisiones basadas en datos: La digitalización ha permitido que los datos se conviertan en uno de los activos más importantes. Esto permite tomar decisiones dinámicas, en base a la información que tienen los bancos.

Para los clientes, algunas de las ventajas destacables son el ahorro de tiempo, el acceso a más información sobre productos y servicios, con más seguridad en las transacciones y operaciones bancarias o un servicio de atención al usuario 24 horas al día, 7 días a la semana. En 2023, más de la mitad de la economía global será digital, por lo que se acelerarán aún más las inversiones a realizar en modelos operativos, para lograr hipervelocidad, hiperescala e hiperconexión, según predijo al final de 2019 la consultora IDC[61].

Como podemos ver, resulta de mayor conveniencia para los clientes disponer de todo lo que necesitan en sus dispositivos electrónicos y, honestamente, para los bancos también.

La pandemia ha sido un gran impulsor de la digitalización de la banca. La nueva normalidad implica banca digital. Si hay algo que aprendió la industria financiera en estos últimos meses es que, si los canales digitales no están listos para funcionar, el negocio

[61] *Digitalización, ¿cómo está cambiando la industria bancaria?* [en línea] elEconomista.es ©. [consulta: 10 febrero 2022]. Disponible en: https://marcas.eleconomista.es/hablemos-de-futuro/noticias/10824077/10/20/Digitalizacion-como-esta-cambiando-la-industria-bancaria.html.

pierde competitividad. Quedó claro que, para afrontar la nueva normalidad, lo virtual seguirá creciendo sobre lo físico.

A pesar de que los bancos tienen un peso muy importante en el sistema financiero, y que las plataformas tecnológicas nuevas, tales como las *fintech* anteriormente mencionadas, aún no son relevantes en tamaño, es cierto de que cada día estas ganan más espacio en la preferencia de las personas, y los inversores están apostando al futuro de las finanzas digitales, lo que constituye un gran reto al sistema tradicional de gestionar los servicios financieros.

En los últimos años se ha avanzado mucho, pero la transformación digital no se detiene. Uno de los grandes desafíos para la industria financiera es expandir y diversificar la provisión de productos, servicios y canales simples, económicos y personalizados para los usuarios, a la par que aprovecha la creciente digitalización para cerrar las brechas de inclusión financiera existentes especialmente en los países Latinoamericanos y África.

Como bien se ha explicado, y continuaremos analizando a lo largo de este trabajo, la identidad digital permite a las personas evitar las limitaciones del mundo análogo, a la vez que posibilita la conexión confiable a nivel global, como transacciones y recepción de servicios digitales en un mundo que se está volviendo cada día más digital. Contar con sistemas de gestión de identidad robustos, es necesario para permitir la identificación y autentificación electrónica, de manera que podamos saber con quién estamos interactuando, así como que los usuarios controlen personalmente sus datos, pudiendo decidir en todo momento con quién, cómo y con qué fin son compartidos.

En este contexto, la identidad digital agrega valor promoviendo la inclusión y la digitalización. Por ejemplo, si cuentan con una identidad digital, 1700 millones de personas pudieran tener acceso a servicios financieros, se reduciría potencialmente el 90% de los

costes de incorporación de clientes, y con la identificación digital llegaría a generarse un valor económico entre el 3 y el 13% del PBI para el 2030[62].

B. El rol de la identidad digital en el sector financiero: el futuro inmediato

Como acabamos de exponer, uno de los retos de mayor transcendencia actualmente para el sector financiero es la transformación digital en su más amplio sentido, ya que representa el presente como base para el futuro de las entidades.

A modo de ejemplo de lo anterior, durante el 2020, a causa de la movilidad restringida por la crisis sanitaria provocada por el COVID-19, las entidades bancarias han animado a sus clientes al uso de la banca digital, para facilitar a los usuarios realizar cualquier operación 24/7 y tener acceso permanente a toda su información financiera en tiempo real, pues tenían horario reducido en atención presencial, de modo que se afectaba la calidad de atención.

Sin embargo, y aunque los datos de uso de la banca *online* se incrementaron significativamente, de conformidad con las cifras manejadas por un estudio de la empresa Mitek[63], un 40% de consumidores europeos no pudieron acceder a los servicios bancarios durante el cierre por la pandemia, ya que las oficinas de las sucursales estaban cerradas y el *onboarding* digital no era fácil. Así, el reto no es solo conseguir que los usuarios confíen en los canales digitales y adopten plenamente su uso, sino mejorar el proceso de *onboarding* para facilitar al máximo la operatividad.

La atención eficiente de esos nuevos canales de demanda y que cada vez se pueda comercializar a través de estos con la seguridad pertinente es mandatorio para el sector. La

[62] *Infografía: ¿Qué es una buena identidad digital?* [en línea] McKinsey Digital © [consulta: 13 febrero 2022]. Disponible en https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/infographic-what-is-good-digital-id#.

[63] Mitek Systems, Inc. (NASDAQ: MITK) es líder mundial en captura móvil y verificación de identidad digital basada en los últimos avances en visión artificial e inteligencia artificial.

llave que enciende el motor de la transformación digital realizada por las entidades financieras es la identidad digital, ya analizada en páginas previas el usuario de los servicios financieros debe obligatoriamente contar con mecanismos que le permitan hacer uso de esta, ya que es donde inicia el acceso al mundo digital y lo que este ofrece. En el sector financiero, así como muchos otros, verificar y autenticar la identidad de sus clientes sigue siendo un reto.

En la mayor parte de los países del mundo, los gobiernos son responsables de proporcionarnos nuestro primer identificador de identidad, y una credencial asociada: el certificado de nacimiento. Posteriormente, se van incorporando otras tipologías de datos que dan forma a la identidad de la persona, que por lo general está contenida en un papel, luego en un plástico, y más recientemente en un chip[64].

Como ampliación del concepto de identidad, podemos establecer como definición de la identidad digital el conjunto finito de atributos que posibilita a una persona, animal, cosa o proceso ser identificado como único y probar su identidad frente a terceros electrónicamente. La persona digital está compuesta de varias identidades digitales, las que a su vez están representadas por una serie de identificadores y de atributos únicos en un contexto específico.

Impulsar la implementación de la identidad digital constituye un beneficio enorme no solo para inclusión financiera, sino, también socialmente. De acuerdo con investigación realizada para el BID, en el *paper* Identidad Digital Auto-Gestionada, se comenta que:

> *Poder disponer de billeteras de identidad portables en posesión de los individuos permitiría a los gobiernos desarrollar programas en los que los representantes que actúen como notarios o certificadores oficiales de nacimientos puedan viajar a zonas rurales y poblaciones vulnerables para emitir certificados de identidad digital que se manejarían con estas billeteras. Si bien puede pensarse que de este modo no se garantizan los niveles*

[64] Cédula de identidad y electoral, DNI, RUT, Pasaporte, entre otros, que varían en sus composiciones de acuerdo con los países emisores.

> *más altos de garantía en la identificación, sería más que suficiente para identificar a las personas de estas poblaciones rurales y/o vulnerables con un grado mínimo de precisión que permitiese proporcionarles todo tipo de servicios, como educación o atención médica*[65].

Los registros actualmente se almacenan de forma física, y los mismos pueden resultar dañados en caso de desastres naturales o accidentes, lo cual representa una amenaza para la información esencial de las personas o entidades. Con la digitalización y posterior implementación del uso de la identidad digital, se minimiza la exposición de pérdida de información. Actualmente, existen muchos sistemas sofisticados de almacenamiento, con los cuales, si bien los archivos digitales pueden estar expuestos a pérdidas, un repositorio virtual facilita su recuperación.

En 2015, la Agencia Federal para el Manejo de Emergencias (FEMA) de EE. UU. comenzó una iniciativa para transformar la forma en la que administraban las subvenciones y ayudas en casos de desastre natural. Afirmaron que:

> *además de la validación de activos, FEMA puede usar la gestión de identidad de blockchain para emitir identidades electrónicas a personas que buscan ayuda y asistencia. Una identidad electrónica de blockchain puede ayudar a garantizar que FEMA tenga un registro único de cada persona y emitir pagos de alivio de manera segura y transparente*[66].

La educación también es un sector que resultaría grandemente beneficiado de la adopción de la identidad en modalidad digital. Según un estudio del BID[67], los niños no registrados en los países de Latinoamérica tienen hasta 17.7% menos de posibilidades de inscribirse en la escuela que aquellos que sí están documentados. Esto hace que tengan hasta un 25.3% menos de opciones de tener acceso a la educación primaria y hasta un 19.5% menos de

[65] ALLENDE LÓPEZ, Marcos. Identidad digital auto - gestionada: El futuro de la identidad digital: auto-gestión, billeteras digitales y blockchain [en línea] BID ©, p. 41 [consulta: 13 febrero 2022] Disponible en: https://publications.iadb.org/publications/spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf

[66] *Ibídem*.

[67] BRITO, Steve, et al. El registro de nacimientos: La llave para la inclusión social en América Latina y el Caribe. [en línea] BID © 2013 [consulta: 14 febrero 2022]. Disponible en: https://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=37787072&pubDetail

tener acceso a la educación secundaria. Si contaran con un mecanismo de acceso más fácil para disponer de una identidad y una gestión más fácil de su identificación se podrían reducir considerablemente estos números y cerrar la brecha del analfabetismo, pues con esto se dota de mejores oportunidades a esos niños.

La cereza del pastel, y lo que motiva este análisis, es cómo impacta la identidad digital en la inclusión financiera. Según informes del BID[68], en 2015 solo en América Latina alrededor de 185 millones de personas no tenían acceso a servicios financieros. En países como Honduras, El Salvador, Nicaragua, Bolivia, Perú, Panamá, México y Colombia el acceso a estos servicios desde poblaciones en zonas rurales es inferior al 40%, debido en parte a que el desarrollo de plataformas digitales sostenibles y escalables ha sido escaso. En 2015, a pesar de que había 37 servicios de dinero móvil en 19 países de América Latina y el Caribe, estos solo representaban alrededor de 15 millones de cuentas con un 60% de inactividad.

De lo anterior se desprende que los gobiernos están llamados a implementar una identidad digital estandarizada, mediante la cual se permita una digitalización y bancarización más fácil, ágil y barata, que proporcione información más confiable para los procesos *KYC*[69] y *AML*[70].

Además, disponer de identidad digital no sólo contribuye a la inclusión financiera directamente, sino que también lo hace de manera indirecta, pues al habilitar la prestación de diversos servicios digitales se generan incentivos para que las personas utilicen servicios financieros electrónicos y generen así un historial crediticio. Según una encuesta realizada por *Federal Deposit Insurance Corporation* (FDIC)[71], distribuida en el año 2017 a la

[68] DE OLLOQUI, Fernando; ANDRADE, Gabriela; HERRERA, Diego. Inclusión financiera en América Latina y el Caribe. *Ob. Cit.*
[69] Conozca su cliente, por sus siglas en inglés (Know Your Costumer).
[70] Prácticas Anti-Lavado, por sus siglas en inglés Anti-Money Laundering (AML).
[71] *How America Banks: Household use of Banking and Financial Service* [en línea] Federal Deposite Insurace Corporation. 2017 [consulta: 14 febrero 2022]. Disponible en: https://www.fdic.gov/householdsurvey

población estadounidense que no tiene cuentas bancarias, el 30.2% argumenta que no confía en los bancos, el 28.2% dice que les preocupa su privacidad y el 13.1% reconoce que no tiene interés en los servicios prestados. Es muy probable que similares respuestas se obtengan y también en la población de América Latina y el Caribe como en el resto del mundo y podrían mitigarse con las soluciones que propone la identidad digital.

Otro de los beneficios que se consiguen, en términos de bancarización e inclusión financiera, es que este nuevo modelo de identidad tiene potencial para facilitar las transferencias y reducir el precio de las remesas. Combinado con la tecnología *blockchain*, permitiría transferir dinero digital de una identidad digital a otra en tiempo real, reduciendo los tiempos y los costes de las remesas, puesto que, por un lado, se facilita la bancarización y se fomenta la inclusión financiera de personas en situaciones de pobreza y, por otro, lado se reduce el número de entidades financieras intermediarias necesarias para pagos trasfronterizos.

El implementar este mecanismo, como tiene sus luces, también tiene sus sombras. Por ejemplo, la verificación de la identidad digital supone ciertos retos, tal como es la integración de un método estándar para realizar todo tipo de transacciones, sean públicas o privadas. Sin embargo, al mismo tiempo ofrece unas ventajas importantes pues nos facilita el acceso a los servicios digitales globales de toda clase, lo cual abre una gran oferta de posibilidades, muchas de ellas en materia de inclusión.

A modo de ejemplo de experiencia de usuario, cada vez existen más cosas que pueden realizarse con la biometría, voz, *selfie*, y todo esto genera cierta reticencia en cuanto a que sea un sistema seguro, porque estamos acostumbrados a utilizar contraseñas, o una tarjeta de coordenadas, es decir, elementos del conocimiento o de la posesión para acreditar nuestra identidad. Sin embargo, la biometría nos permite identificarnos por ser quienes somos, usando la cara, la voz, la huella dactilar, por nuestras características inherentes,

pasando de presunción a la certeza; ser quienes decimos ser, solo presentando un dedo. Y todo esto es la maravilla que trae contar con una identidad digital.

Conforme se incorporan nuevas tecnologías, los reguladores toman una mejor comprensión del entorno digital. Los gobiernos, las entidades privadas, sobre todo las EF, encuentran mejores formas de interactuar electrónicamente, y los usuarios se sienten más seguros con el uso de internet para todo tipo de transacciones, y también se van proponiendo y adoptando soluciones mejores y más robustas de identidad digital. Sin embargo, actualmente aún se presentan diversos problemas que dificultan el camino a la adopción de la identidad digital para los usuarios de servicios financieros, los cuales pueden organizarse en tres categorías: regulación, tecnología, y seguridad.

No podemos aseverar que exista un mecanismo de adopción de identidad digital para los procesos bancarios, que resulte mejor que otra, pues no existe una forma absoluta y definitiva para validar la identidad de una persona[72], sino que este proceso consistirá en una evolución y adaptación constantes a los nuevos retos, las nuevas necesidades y, por supuesto, a tecnologías que puedan surgir en un futuro inmediato o lejano. Será una búsqueda constante del equilibrio entre seguridad y experiencia de usuario.

En materia de regulación, hoy día no existe una norma sobre lo que conforma legalmente la identidad digital. Es por esto, y tomando en cuenta la rapidez con la que las personas se interrelacionan gracias al uso de esta, es una razón obligatoria para los abogados, jueces y autoridades de todo el mundo, sugerir soluciones creativas mediante el uso de elementos existentes en la actualidad, para encontrar un estándar normativo adaptado a esta nueva realidad.

[72] Validación de identidad. Es el proceso mediante el cual una persona es capaz de probar que la identidad que presenta corresponde con la que se encuentra registrada en los sistemas.

Es por esto por lo que una comprensión clara de la tecnología por parte de los reguladores es necesaria para que el marco legal normativo se vaya actualizando al ritmo que la tecnología avanza. En este punto, es vital resaltar que resulta prioritario poder contar con leyes de protección de datos más estrictas y modernas, garantistas de los derechos de privacidad en el tratamiento digital de la información.

Debemos mencionar el reto tecnológico de adaptación de la infraestructura de sistemas de uso actual, pues entendemos que se necesita de una transición para asimilar los modelos de datos digitales, y permitir el acceso a los servicios que son provistos bajo esta modalidad. Igualmente, deben crearse los estándares globales y protocolos necesarios para diseñar y desarrollar soluciones de creación de identidad digital. Christopher Allen[73] enumera los 10 principios que rigen en materia de técnica para la identidad digital soberana (SSI por sus siglas en inglés) en su detallado artículo "*The Path to Self-Sovereign Identity*", los cuales se resumen en tres categorías: seguridad, control y portabilidad para la identidad de las personas. También es importante destacar como oportunidad tecnológica el uso de la biometría[74] para la prueba de identidad y la autenticación, lo cual tiene un enorme potencial y requiere ser explorado en profundidad.

En vista de que no somos expertos en materia de tecnología de la información, estas opiniones se esbozan solo a modo enunciativo, sin la profundidad de la comprensión del detalle que amerita, lo cual sería objeto de otro trabajo investigativo.

En cuanto a la seguridad, en ambiente digital se le denomina como ciberseguridad y constituye un aspecto crítico en este esquema. Las entidades financieras deben estar

[73] ALLEN, Christopher. El camino hacia la identidad autosoberana [en línea] Blog sobre software social. Abril, 25, 2016 [consulta: 26 enero 2002]. Disponible en http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

[74] Consiste en la medición estandarizada de los seres vivos o de los procesos biológicos. Por ejemplo, las mediciones biométricas se pueden basar en el color de los ojos, la lectura del iris, los rasgos faciales, la forma en que se camina o los latidos del corazón.

preparadas para recibir ataques no vistos con anterioridad que buscan extraer sus recursos económicos y los de sus clientes y también cada vez más, información sobre estos últimos, lo que, sin duda alguna, es una amenaza económica y reputacional. Los supervisores y el Banco Central Europeo en particular han prestado mucha atención a este tema, pues reconocen del gran potencial desestabilizador que representa para el sector en su conjunto. En nuestro país también han sido realizados esfuerzos en ese sentido, con la publicación por parte de la Junta Monetaria del Reglamento de Seguridad Cibernética y de la Información[75] y el Reglamento de Sistema de Pagos, el cual provee seguridad y certeza jurídica a la forma de prestar servicios relativos a los sistemas de pago, mitiga los riesgos asociados a los referidos servicios y ofrece protección a los usuarios[76].

Otro gran desafío en esta área la supone la privacidad y la gestión de los datos de carácter muy sensible. Dado el gran valor y el volumen que representan, poder extraer la información sin incurrir en intrusión con el cliente es un reto.

Existe una nueva corriente que se refiere a la identidad autosoberana, donde el experto en esta materia, Christopher Allen[77], al referirse a la historia de los sistemas de identidad que han sido creados para su uso en el mundo digital, nos cuenta que han atravesado por varias etapas en materia de identificación en internet, y él es de opinión que se está iniciando a una cuarta. Esos sistemas son: (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 Auth; y, más recientemente, (iv)

[75] República Dominicana. Junta Monetaria [en línea] Segunda Resolución de fecha 01 de noviembre de 2018 que autoriza la publicación del Reglamento de Seguridad Cibernética y de la Información. [consulta: 7 marzo 2022]. Disponible en: https://sb.gob.do/sites/default/files/nuevosdocumentos/20181101_Segunda%20Resolucion_Reglamento_seguridad_cibernetica_de_la_informacion.pdf

[76] República Dominicana. Junta Monetaria [en línea] Segunda Resolución de fecha 29 de enero del 2021 que aprueba la modificación integral al Reglamento de Sistemas de Pago [consulta: 7 marzo 2022]. Disponible en: https://sb.gob.do/sites/default/files/nuevosdocumentos/20210129_Segunda-Reglamento-de-Sistemas-de-Pago.pdf

[77] ALLEN, Christopher. El camino hacia la identidad autosoberana. *Ob. Cit.*

sistemas de identidad autosoberana[78]. A la fecha no hay ninguna implementación concreta de este último tipo de sistema en los países.

Todos los sistemas de identificación desplegados hasta el momento presentan el inconveniente común de depender de una entidad centralizada y, en consecuencia, quitar el foco del usuario. En otras palabras, todos estos sistemas siguen un esquema donde una entidad decide sobre los datos personales, con algunas intervenciones menores del usuario que generan una falsa sensación de control sobre los datos integrantes de la identidad. Allen es de opinión que el único camino de generar identidad digital soberana es dando autonomía al usuario, y con ello hacerlo soberano sobre sus datos, como el término lo dice.

En todos existe la misma problemática, pues no existen normas donde la identificación pueda descansar en sistemas autosoberanos, sino que están basadas en las relaciones entre el usuario y el proveedor. En consecuencia, nos llevan a pensar cómo se debería interpretar la norma para acomodar estos sistemas.

Un buen sistema de identidad digital no solo aumenta el desempeño de los gobiernos y las empresas, sino que también beneficia y protege al público[79] y, de hecho, aparecen algunos patrones que reflejan el contexto local. A pesar de que algunos países tienen que empezar con un sistema básico de identificación para que todos puedan acreditar su identidad oficial, otros como son Australia, Canadá y Francia, han iniciado la creación de ecosistemas de identidad digital que permiten a las personas elegir entre proveedores de identidad tanto públicos como privados. Indistintamente del mecanismo adoptado, esos sistemas son urgentemente necesarios y debe existir un mecanismo para que las identificaciones sean válidas independientemente del país donde se utilice.

78 CHOMCZYK, Andrés. Regulación de blockchain e identidad digital en América Latina [en línea] BID© 2020 [consulta: 15 febrero 2022]. Disponible en http://dx.doi.org/10.18235/0002935

79 JIMÉNEZ, Pedro Manuel. Manejo de datos y privacidad. Identidad soberana: camino hacia una red segura [en línea] digitalbiz magazine. 2019 [consulta: 27 enero 2022]. Disponible en: https://www.digitalbizmagazine.com/manejo-de-datos-y-privacidad/

Con la crisis sanitaria fue probada la capacidad de los gobiernos y su madurez digital, cuando surgieron los programas de ayuda financiera, programas sociales y de los ministerios de trabajo, entre otros, para personas vulnerables. En ciertos países, mediante los sistemas de identidad digital fue posible que las autoridades gubernamentales identificaran de manera confiable y no presencial a personas con situaciones vulnerables, trabajadores informales, inmigrantes, habitantes de áreas remotas, entre otros.

A modo de ejemplo, citaremos algunos casos de *onboarding* y el uso de la identidad digital en países de todos los continentes.

Chile, a través de su sistema de identidad digital logró ubicar y crear en sus bases de datos a miles beneficiarios nuevos en asistencia social de una manera muy rápida. Las personas podían consultar en línea en qué situación se encontraban y, en algunos casos, solicitar la realización del cambio que aplicara.

En Tailandia, más de 28 millones de personas solicitaron beneficios para los trabajadores informales afectados por la pandemia, y el gobierno tuvo la posibilidad de identificar quiénes recibían asistencia a través de otros planes que se encontraban vigentes.

En la India, más de 200 millones de mujeres lograron efectuar pagos rápidamente, gracias a mejoras en procesos que incluyen la vinculación de las cuentas de cada individuo con su identificación digital[80]. El Banco de la Reserva de la India ha permitido a las entidades reguladas aceptar el número de identificación de *Aadhaar*[81] que es emitido por el Gobierno Indio como prueba de identidad, así como la dirección, para cumplir con los requisitos

[80] *G20 Digital Identity Onboarding* [en línea] The World Bank Group ©2018 [consulta: 15 febrero 2022]. Disponible en: https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

[81] UID Aadhaar [en línea] udyamregistration.gov.in © [consulta: 15 febrero 2022]. Disponible en http://udyogaadhaar.gov.in/UA/

reglamentarios existentes en lo relativo a la apertura de cuentas, incluyendo las cuentas de ahorro básicas llamadas *Jan-Dhan*.

En Pakistán, las tarjetas de identificación nacionales *NADRA*[82] permitieron abrir cuentas bancarias y hacer cumplir de manera confiable los límites de transacción, lo que, junto con el crecimiento de los agentes bancarios sin sucursales, contribuyó a un aumento en la inclusión financiera. Por cierto, los agentes también fueron aprovechados para registrar todas las tarjetas SIM de teléfonos celulares como parte de una iniciativa de seguridad nacional.

En Singapur[83] el gobierno cuenta con un ecosistema digital avanzado, mediante el cual se les permite a las personas acceso a servicios gubernamentales y empresariales totalmente en línea. De este modo la interrupción generada por la pandemia no afectó el desarrollo normal de las actividades económicas ordinarias.

En Noruega, en 2004 se creó BankID[84], como una identificación digital única principalmente para transacciones financieras, a través de una colaboración entre el gobierno noruego y un grupo de bancos cooperativos. Más de 7,5 millones de noruegos (75 por ciento de la población adulta) ahora usan BankID para probar su identidad y completar transacciones en línea. El acceso a la banca por Internet y la firma digital de documentos financieros son los servicios más usados por los clientes. El sistema es fácil de usar, ya que apenas requiere que los usuarios ingresen su número de identificación personal, su contraseña personal elegida y una contraseña de un solo uso de su token de código físico. A finales de 2014, el tan esperado proyecto BankID 2.0 libre de Java fue completado e implementado por la mayoría de los bancos.

---

[82] Buró de información Crediticia (eCIB) [en línea] State Bank of Pakistan ©. [consulta: 15 febrero 2022]. Disponible en http://www.sbp.org.pk/ecib/index.htm.

[83] Singpass 2018. [en línea] Government of Singapor. [consulta: 15 febrero 2022]. Disponible en: https://www.singpass.gov.sg/spauth/login/loginpage?URL=%2F&TAM_OP=login.

[84] Bank-ID Privat, 2018 [en línea] bankid.no© [consulta: 15 febrero 2022]. Disponible en: https://www.bankid.no/ en/about-us/

En México, los recientes ajustes regulatorios han contribuido a alcanzar un avance significativo en materia de inclusión. El gobierno ha creado la Clave Única de Registro Nacional de Población (CURP), que consiste en una clave asociada de manera única a cada individuo en el país, incluidos los no ciudadanos y es emitido por el Registro Nacional de Población (RENAPO). Sin embargo, una persona puede tener más de una CURP emitida por el sistema. Los certificados de nacimiento y la CURP sirven como identificaciones principales que habilitan las personas para obtener identificaciones funcionales que se utilizan para votar y acceder a programas de seguridad social y servicios de atención médica pública. Las personas de bajos ingresos puede que carezcan de los documentos estándar para satisfacer los requisitos de *Know Your Client* (KYC) y *Anti money laundry* (AML / CFT, por sus siglas en inglés, respectivamente), que le permiten abrir una cuenta u obtener un préstamo.

Para abordar esta preocupación, en 2009 se crearon cuentas de niveles de riesgo con requisitos de *KYC* en niveles relacionados. Independientemente de la identificación presentada para abrir una cuenta u obtener un préstamo, las instituciones financieras deben validar que la información que recopilan, incluido el informe de las personas de la CURP, coincida con los registros de RENAPO, de modo que representa una ayuda para reducir el fraude. Además, en 2017, se introdujeron ajustes regulatorios al proceso de identificación. Estos incluían exigir a las instituciones financieras que recopilaran y verificaran datos biométricos para abrir cuentas de mayor riesgo y para obtener préstamos, o para realizar transacciones de alto valor en sucursales bancarias. Estos ajustes regulatorios ayudan a reducir el robo de identidad y mitigar aún más el fraude[85].

El esquema nacional de identificación electrónica del Reino Unido, *GOV.UK Verify*, ha estado en funcionamiento desde mayo de 2016 y actualmente tiene más de 2,2 millones de usuarios con una identidad verificada. Actualmente hay 17 servicios del sector público que

[85] *G20 Digital Identity Onboarding*. *Ob. Cit.*, p. 57

están utilizando estas identidades para permitir a los ciudadanos acceder a servicios digitales que van desde impuestos y transacciones de pensiones hasta beneficios, licencias de conducir y reclamos de redundancia. El programa se está ampliando actualmente a diversos servicios sociales y de salud, así como al sector privado. *GOV.UK Verify* es un sistema de identidad federada administrado por la Oficina del Gabinete del Gobierno del Reino Unido.

El marco de confianza dentro del cual operan los proveedores y servicios sigue las reglas definidas por el Gobierno del Reino Unido, tales como sus conocidos estándares de prueba de identidad, verificación y autenticación[86], todos los cuales están disponibles abiertamente. La prueba de identidad, la verificación y la autenticación son proporcionadas por un grupo de organizaciones comerciales certificadas para operar según los estándares del Reino Unido y sujetas a contratos comerciales derivados de un marco de adquisiciones de la Oficina del Gabinete para la garantía de identidad. Actualmente siete (7) proveedores están certificados para operar bajo este marco y proporcionar cuentas de identidad a los ciudadanos.

En República Dominicana la historia resulta distinta. Si bien fueron creados planes sociales, al existir tantas personas en situación de vulnerabilidad sin identificación, el acceso a las ayudas no les pudo llegar de manera proporcionada a todas las personas. En nuestro país no existe un gobierno digital de registro civil que pueda ser utilizado para los fines que antes hemos expuesto.

Tal como la creación de los caminos y las vías de ferrocarril fueron un potente impulsor de la economía para el siglo XX, las identificaciones digitales, los pagos digitales y la gobernanza de datos lo son hoy día. Estas nuevas creaciones son muy importantes en sí mismas y juntas constituyen un poderoso bien común.

[86] *Prueba de identidad y autenticación* [en línea] Gov. UK ©. [consulta: 15 febrero 2022]. Disponible en: https://www.gov.uk/government/collections/identity-assurance-enabling-trusted-transactions

Los sistemas de identidad digital deben diseñarse considerando la inclusión de personas que estén poco alfabetizadas y con acceso limitado a la tecnología, a la vez que genere confianza en la integridad del sistema, la privacidad y los derechos individuales.

La directora de políticas de Desarrollo y Alianza del Banco Mundial, Mari Elka Pangestu[87], argumenta que la pandemia ha resaltado la necesidad urgente de crear sistemas de identidad digital que permitan a los gobiernos brindar apoyo social y financiero a las familias y las empresas de manera más rápida y eficiente. Para estimular la búsqueda de soluciones innovadoras, la ID4D[88] lanzó su segundo desafío de la Misión Mil Millones, que persigue encontrar métodos alternativos que permitieran a las personas con situaciones de vulnerabilidad en los países registrarse para la obtención y uso de identificación digital de forma segura.

Independientemente de la forma que adopten, estos sistemas son esenciales y, cualquiera que fuere el modelo elegido, los gobiernos pueden cambiar la vida de personas por el mundo entero mediante la creación de una identidad digital diseñada para maximizar la inclusión, la confianza y sobre todo, la privacidad.

[87] PANGESTU, Mari. El Poder de la identidad Digital [en línea] Project Syndicate© [consulta: 15 febrero 2022] Disponible en: https://www.project-syndicate.org/commentary/digital-identification-systems-promote-inclusive-economic-growth-by-mari-pangestu-2020-08/spanish

[88] Siglas de identificación del proyecto Iniciativa Identificación para el Desarrollo del Banco Mundial.

SECCIÓN II.
PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LOS SERVICIOS FINANCIEROS.

SECCIÓN II.
PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LOS SERVICIOS FINANCIEROS

I. Manejo de los datos en el sistema financiero

La protección de los datos personales ha tomado cada vez mayor relevancia en las últimas décadas, principalmente debido al desarrollo de la tecnología, que ha tenido como resultado el almacenamiento de la información por un mayor periodo de tiempo, y a la vez que se permite su uso en cualquier momento y para múltiples fines. Incluso, se da el caso que la finalidad para la que se obtuvo originalmente el dato se haya modificado para darle otra distinta, ya que gracias a las telecomunicaciones y al desarrollo de sistemas informáticos avanzados se pueden procesar en milésimas de segundos grandes cantidades de información y, dependiendo del nivel del proceso, la posibilidad de afectar el derecho de a la privacidad de las personas pueden verse afectado en mayor o menor escala.

Para todo proveedor de servicios financieros, es mandatorio el manejo de los datos de una forma ética, transparente y de forma eficaz para su gestión.

Las instituciones recopilan, almacenan, tratan con datos de las personas y son comunicadoras de información, por lo que se constituyen en un agente de relevancia en el sistema de información. De modo general, las funciones descritas no son conocidas para el cliente del banco quien, además, por lo general no está familiarizado con los medios para protegerse en caso de datos falsos o con error, desactualizados o utilizados para propósitos no autorizados, a qué entidades y bajo qué circunstancias deben de ser comunicados sus datos o si bien ha sido realizado conforme a la normativa.

A propósito del tema objeto de nuestra investigación, al proponer el uso de identidad digital para el usuario de servicios financieros nos asiste revisar la importancia relacionada con la

protección de los datos que son suministrados por los usuarios. Es vital la existencia de un marco legal que, al efecto, establezca un procedimiento de gobernanza sólido, incluidos los sistemas de gestión de datos, y que este se mantenga y actualice de manera consistente dentro de un esquema de seguridad y privacidad. Es responsabilidad del gobierno definir las políticas de protección de datos, incluidas las reglas sobre la recopilación, el uso, la gestión y la divulgación de los datos digitales de las personas, lo que, conforme analizaremos, es de poca mención en la legislación actual.

La protección de la confidencialidad y la integridad de los datos debe ser responsabilidad primordial del recopilador de datos; aunque el procesador de datos y otras personas involucradas en el acceso, almacenamiento y uso de datos personales también tienen un papel que desempeñar. Ante todo, deben existir mecanismos adecuados para garantizar que se obtenga el consentimiento de las personas que abarquen la base sobre la que se recopilarán, mantendrán, utilizarán y divulgarán los datos. Las personas deben estar conscientes de quién posee y puede acceder a sus datos personales, además de tener la oportunidad de inspeccionar los datos que se conservan sobre ellos y solicitar correcciones por cualquier error o datos desactualizados.

Por lo tanto, es muy importante analizar la forma en la que las entidades financieras procesan hoy en día los datos personales de sus clientes y los sistemas de información económica que intervienen en sus procesos, para luego examinar las carencias que actualmente tienen los referidos sistemas y de esta manera proponer una correcta protección de los datos.

Si bien cada país tiene sus reglas particulares para la protección de los datos de las personas, a continuación, nos proponemos revisar cuáles son los datos que se entienden como personales, de qué manera pueden ser apropiadamente utilizados por los bancos, cómo impacta esto en relación con nuestra propuesta de identidad digital y cuál es la situación de nuestro país y otros de la región sobre el particular.

A. Los principios de la banca para la protección de datos

A raíz de las crisis financieras de escala mundial que han ocurrido en las últimas décadas, se han robustecidos los esfuerzos tanto a nivel internacional como nacional, con el objetivo de fortalecer la protección del consumidor de servicios financieros. La finalidad perseguida con estas acciones consiste en impulsar la prestación de servicios financieros adecuadamente, y que esta resulte compatible con la estabilidad financiera. En tal sentido, existe un reconocimiento marcado de que la protección del consumidor y la estabilidad financiera, que se han visto tradicionalmente como objetivos asociados de forma indirecta o incluso en algún momento considerados opuestos, resultan complementarios en gran medida.

Actualmente, los datos personales son recursos fundamentales de la sociedad de la información. La naturaleza central de los datos personales tiene aspectos positivos, debido a que posibilita la oferta de servicios nuevos y mejores. Sin embargo, también tiene sus sombras, pues la información sobre individuos se multiplica de manera exponencial, al ser más accesible por más intervinientes y cada vez más se facilita el procesamiento mientras que se dificulta controlar el destino y utilización que la misma tendrá, principalmente como resultado un crecimiento en el flujo multinacional de los datos personales como causa directa del funcionamiento de la globalización del mercado.

Los usuarios de servicios financieros ocupan posición doble en el mercado financiero, pues por un lado son inversionistas o ahorrantes, mientras por el otro son deudores de las EF y muchas veces las posiciones coinciden en la misma persona.

En el Derecho de los Mercados Financieros, la protección de los ahorrantes se basa en la transparencia informativa de las características de los instrumentos financieros y de la solvencia de sus emisores, al mismo tiempo que se desarrolla una normativa protectora

para los usuarios, orientada a protegerlos y prevenirlos frente a los conflictos que pudieran existir entre ellos como clientes y su intermediario de servicios financieros.
La finalidad del principio de transparencia es la protección del ahorrador frente a la asimetría de información, y con ello evita que el sistema financiero sea lastrado por la oferta de productos financieros denominados 'limones'. Es por esto que dentro de las obligaciones de las EF encontramos el deber de poner a disposición de sus clientes en todo momento toda la información relacionada con el catálogo de productos que ofrecen y los mecanismos con los que cuentan en caso de no entregar lo ofertado o caer en la vulneración a algún derecho estipulado[89].

Este esquema es prácticamente el mismo para todos los países. Al respecto, resulta importante resaltar en este punto que, si bien las normas del sector forman parte integral del derecho al consumidor, se estaría protegiendo al consumidor en calidad de ahorrante, frente a la entidad, cuando la entidad es su representante y defensora de sus intereses. Está claro, pues, que la normativa del sector contribuye a la protección de los usuarios; sin embargo, su fin último es garantizar el correcto funcionamiento del mercado financiero[90].

En principio son estas reglas de carácter administrativo las que han fijado criterios por los cuales deben orientarse las relaciones entre EF y sus clientes, los medios con los que deben contar en el ejercicio de sus actividades y el alcance del secreto profesional.

En el ordenamiento jurídico de la República Dominicana, el deber de secreto profesional aplicable al ámbito bancario y financiero está estipulado en la Ley 183-02 Monetaria y Financiera, artículo 56, literal b, donde refiere que:

[89] AKERLOF, George A. The market for "lemons": Quality uncertainty and the market mechanism. En *Uncertainty in economics*. Academic Press, 1978. p. 235-251
[90] ZUNZUNEGUI, Fernando. *Derecho del mercado financiero*. Madrid-Barcelona: Marcial Pons, 2005, pp. 30-31.

> *Además de las obligaciones de confidencialidad derivadas de las buenas prácticas y usos bancarios, las entidades de intermediación financiera tienen la obligación legal de guardar secreto sobre las captaciones que reciban del público en forma desagregada que revele la identidad de la persona. Solo podrán proporcionarse antecedentes personalizados sobre dichas operaciones a su titular o a la persona que este autorice expresamente por cualesquiera de los medios fehacientes admitidos en Derecho. Lo dispuesto en este Artículo se entiende, sin perjuicio de la información que deba suministrarse en virtud de normas legales a la autoridad tributaria y a los órganos jurisdiccionales, o en cumplimiento de las disposiciones reguladoras de la prevención del lavado de activos. Las informaciones que deban suministrar las entidades sujetas a regulación, tanto a la Administración Tributaria como a los órganos encargados del cumplimiento de la prevención del lavado de activos y a los tribunales penales de la República, deberán ser hechas caso por caso por intermedio de la Superintendencia de Bancos, tanto en lo que respecta al recibo de la solicitud de información como para el envío de la misma y siempre y cuando se soliciten mediante el cumplimiento de los procedimientos legales en la sustanciación de asuntos que se ventilen en la justicia. La obligación de secreto bancario no impedirá la remisión de la información que precisen la Superintendencia de Bancos y el Banco Central, en la forma que reglamentariamente se determine. La violación del secreto bancario en los términos del presente Artículo será castigada conforme a las disposiciones de los Artículos 377 y 378 del Código Penal*[91].

De esto podemos extraer, como información central, que el secreto bancario es la facultad legal que tienen las EF de no divulgar informaciones privadas de sus clientes. Esta información se extiende a toda la información que la entidad posee sobre los clientes, así como las acciones derivadas de su actividad con estos. Por ello, los bancos solamente pueden proveer información de sus captaciones sin revelar la identidad del cliente. El secreto bancario les impone la obligación de proporcionar solo los antecedentes personalizados sobre operaciones financieras a su titular o a su representante autorizado, so pena de sanciones penales.

Ante una situación de seguridad personal del usuario como tal, el secreto bancario tiene un importante componente de naturaleza constitucional[92], ya que se enmarca en el derecho de

[91] República Dominicana. Ley 183-02 Monetaria y Financiera. *Gaceta Oficial*, de 21 de noviembre 2002.

[92] Los tribunales del país se han pronunciado en ese sentido, mediante fallos emitidos por el Tribunal Constitucional, donde dan aquiescencia a la negativa en la entrega de información solicitada fuera del marco respecto de las cuales el artículo 8 de la Ley núm. 183-02, Código Monetario y Financiero, del 21 de noviembre de 2002, establece la confidencialidad de las informaciones recogidas por los técnicos y funcionarios de la Superintendencia de Bancos. Ver: Sentencia TC/0123/14. Expediente TC-05-2013-0099, relativo al recurso de revisión constitucional en materia de amparo incoado por la señora Ana Martina Torres

la privacidad e intimidad que tienen las personas. Su importancia radica en que los datos personales estarán protegidos adecuadamente, constituyendo, además, un incentivo para los usuarios confiar en que sus operaciones financieras no serán divulgadas públicamente.

Los datos bancarios de una persona se consideran datos de carácter personal, en cuanto permitan la identificación de ésta a través de ellos. Conforme definición del Diccionario Panhispánico del Español Jurídico se define como datos de carácter personal:

> *Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de otro tipo concerniente a personas físicas identificadas o identificables. El objeto del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales*[93].

La confidencialidad de los datos bancarios consagrada en el artículo 8 de la LMF se refiere al secreto bancario, el cual constituye un mecanismo para que las entidades y otras organizaciones financieras protegen la información relativa a los productos que mantienen sus clientes con total discreción. Las negociaciones y transacciones realizadas por los intermediarios financieros no deben ser divulgadas a terceros, con excepción de los casos en que se estipule lo contrario, por interés de la administración de la justicia, y con previa autorización judicial.

En otras palabras, es una especie de secreto profesional que asegura que las EF no compartan con terceros la información de sus clientes, tales como son los números de cuenta, transferencias, saldo, depósitos, y que de realizarse sea siempre dentro de los límites y obligaciones que establece la ley y la colaboración con la justicia.

---

contra la Sentencia núm. 170-2013, dictada por la Primera Sala del Tribunal Superior Administrativo el seis (6) de junio de dos mil trece (2013).

[93] *Dato de carácter personal* [en línea] Diccionario Panhispánico del Español Jurídico [consulta: 25 febrero 2022]. Disponible en: https://dpej.rae.es/lema/dato-de-carácter-personal

cabe señalar que la seguridad y la confidencialidad de los datos bancarios incluye a todo tipo de clientes, es decir tanto personas físicas como personas jurídicas, mientras que la ley de datos personales en bancos solo se aplica a personas físicas. En este sentido, podemos decir que la confidencialidad de estos datos bancarios forma parte de nuestro derecho a la privacidad, el cual se reconoce en nuestro ordenamiento jurídico como un derecho fundamental.

En concreto, dentro de nuestro ordenamiento jurídico, los datos bancarios pertenecen a información crediticia. Por lo tanto, están dentro de la categoría de datos generales, es decir, los datos bancarios no son considerados como datos sensibles, por lo que su tratamiento está permitido, dentro del marco provisto por la Ley 172-13, observando las limitaciones que esta dispone[94].

Los datos o información en sí mismos tienen un valor intrínseco, que varía según la finalidad para la que se proporciona. Este valor aumenta aún más cuando la información es recolectada, almacenada y analizada, e acuerdo con los objetivos del propio recolector, quien puede utilizar esta información para beneficio personal o para comunicar la información a terceros. La información se puede recopilar de distintas maneras y con diferentes fines. A modo de ejemplo, un centro de salud puede obtener datos de una persona directamente de su titular, con el objetivo de usarlos en el historial clínico privado entre el personal médico y el paciente, de modo que estos datos siempre serán privados para los terceros. En este sentido es importante señalar que, en todo caso, el permiso que una persona concede para que traten sus datos personales nunca se debe interpretar o considerar como un cheque en blanco para todo lo relativo a estos[95].

[94] República Dominicana. Ley No. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. G. O. No. 10737 del 15 de diciembre de 2013.
[95] CARNÉ M, Guillermo. La evolución y digitalización del sector bancario. Abril 2020, pp. 44-51.

En el caso de las entidades financieras, pueden capturar muchos tipos de información, pero sobre todo recopilan datos sobre la vida patrimonial de un individuo, convirtiéndose así en un repositorio de información y almacenaje de grandes cantidades de datos. En este tipo de instituciones no solamente se recoge y se almacena la información, también se realiza el tratamiento de dichos datos, lo que les permite, entre otros temas, realizar un análisis de los posibles clientes con el propósito de establecer relaciones comerciales confiables.

En la economía digital es necesario identificar a las personas de forma remota, es decir, sin interacción física, y en la mayoría de los casos, sin conocimiento previo de la otra parte, muchas veces utilizando una computadora responsable del proceso. Como resultado, la gestión de la identidad incluye nuevos riesgos relacionados a la privacidad, protección de datos y exponenciales riesgos de fraude y, por el otro lado, la necesidad de revisar y ajustar planes de gobernanza, marcos legales y las tecnologías que puedan quedar desactualizadas[96].

Una de las grandes preocupaciones de la era digital en la que vivimos es la protección de datos personales para las EF, tanto o más que para las personas, ya que su responsabilidad en el tratamiento y disposición de estos es sin duda muy alta. No en vano, los datos son toda una fuente de valor para empresas del sector financiero. Una entidad que no proteja sus datos se expone a diversos tipos de riesgos: operacionales, económicos, reputacionales, entre otros, y los impactos de este tipo de riesgos pueden llevar incluso a la quiebra.

Es muy importante, pues, disponer de las herramientas y los recursos necesarios para la protección de datos personales e identidad digital. Cualquier vulnerabilidad tratará de ser explotada por los ciberdelincuentes que, cada vez, cuentan con medios más sofisticados para realizar los ataques informáticos.

[96] URIARTE, Mikel. El tratamiento de datos personales en la determinación del riesgo. [en línea] En foco 134. ISSN 0717-9987, p. 12 [consulta: 1 marzo 2022]. Disponible en: http://www.expansiva.cl/media/en_foco/documentos/15042009150104.pdf

El registro y la gestión de identidad son herramientas esenciales para la inclusión, ya que reducen los costos transaccionales en toda la economía y que mejoran la calidad de los servicios para los sectores público y privado. Estos procesos deben superar una serie de desafíos; por ejemplo, la privacidad, por un lado, y el potencial fraude, por el otro. Los desafíos de desarrollo actuales solo pueden ser sostenibles si el sector privado es parte de la solución[97].

Conforme pasa el tiempo, en los presupuestos anuales de las entidades financieras se consagran partidas para inversión destinada a robustecer y modernizar sus sistemas de seguridad a fin de evitar que los fraudes que afecten a los clientes. Desarrollan estrategias para proteger los datos personales de los clientes y de esta forma cuidar su patrimonio. A veces en estas estrategias interviene el gobierno. La protección de datos personales es una herramienta esencial para los clientes bancarios porque les facilita adoptar hábitos que mantienen su vigilancia, fortalecen las medidas de cuidado financiero personal y bloquean los accesos de sus recursos económicos a los defraudadores de manera efectiva [98].

El amplio interés por proteger los datos personales es una realidad. Según un estudio realizado en la Unión Europea (UE), el 88 % de los encuestados manifestaron que les interesa ser notificados si los personales de su propiedad en poder de terceros fueran robados o alterados de cualquier. Esta preocupación crece con la aparición de incidentes como son las intrusiones en los sistemas de información de las empresas, muy común en las noticias diariamente[99].

[97] PAREJA, Alejandro, et al. La gestión de la identidad y su impacto en la economía digital. *Ob. Cit.*
[98] Protección de Datos Personales, el mejor candado de seguridad para tus finanzas. [en línea] BBVA Podcast [consulta: 26 febrero 2022]. Disponible en: https://www.bbva.com/es/mx/podcast-proteccion-de-datos-personales-el-mejor-candado-de-seguridad-para-tus-finanzas/
[99] "What they know" [en línea] The Wall Street Journal. [consulta: 26 febrero 2022]. Disponible en http://online.wsj.com/public/page/what-they-know-digital-privacy.html.

Las identidades de los usuarios en internet consisten en muchos tipos de informaciones, distribuidas en una gran cantidad de sistemas, empresas, organizaciones e instituciones. Dependiendo de la naturaleza de estos datos varía la forma de los usuarios percibir qué tan seguros son esos datos. Por tal razón, es posible que nos encontremos información de los usuarios no considerada como datos altamente privados y que sean conocidos por terceras partes o empresas no lo consideran como negativo, hasta datos que son considerados con alta sensibilidad y, por esto, no son pasibles de transmitirse o ser utilizados fuera de su entorno original.

Dentro de los datos que los usuarios consideran altamente confidenciales se encuentra la información financiera y la información relativa a la salud, consideradas por el 75% y 74% de los europeos, respectivamente, como información personal y, por lo tanto, no debe ser referenciada directamente por terceros. Mientras tanto, en el otro lado, están datos como son la fecha de nacimiento, lugar de nacimiento, los sitios *web* visitados o las actividades que se realizan en internet, con un 25% de usuarios que son de opinión que estos datos pueden considerarse como información personal[100].

A lo largo de la historia, la banca ha superado a otras industrias en lo relativo a la protección de datos. La industria financiera ha actuado como custodio, no solamente de los fondos depositados de sus clientes, sino de toda la información generada en torno a la transferencia y procesamiento de activos financieros, como son sus datos personales. De acuerdo con un artículo publicado en la página web de BBVA Research, se afirma que: "*A medida que el paisaje de la gestión y el uso de datos financieros está cambiando rápidamente, una constante es que los bancos siempre han estado comprometidos con elevados estándares en esta área*", afirma el informe[101].

[100] *Identidad Digital: El nuevo usuario en el mundo digital* [en línea] © Fundación Telefónica, 2013. [consulta: 26 febrero 2022]. Disponible en: http://www.educando.edu.do/files/9513/9281/6433/identidad_digital.pdf

[101] ALAMEDA, Teresa y ÁLVAREZ, Carmen. Más allá de la norma: el compromiso de la banca con la seguridad de los datos [en línea] BBVA.com. 2018 [consulta: 25 febrero 2022] Disponible en: https://www.bbva.com/es/mas-alla-norma-compromiso-banca-seguridad-datos/

La citada web, refiere que es primordial que todos los participantes, nuevos y viejos, en el ecosistema financiero imiten los principios bancarios cuando se trata de gestionar y proteger adecuadamente los datos de los usuarios. Los referidos principios deberían ser requisitos esenciales para cualquier otra organización que quiera procesar datos de clientes. Esto es especialmente importante con la llegada de la banca abierta, conocida por el anglicismo *open banking*, que permite a terceras entidades el acceso a los datos de los clientes, por lo general a través de APIs[102].

A modo de ejemplo de lo anterior, podemos referir el ejemplo de la Ley *Aadhaar,* ley india que siguió el principio de incorporar la privacidad por diseño, un concepto que establece que los proyectos de Tecnologías de Información (TI) deben diseñarse teniendo en cuenta la privacidad. La recopilación de datos biométricos a menudo se ha citado como uno de los medios para violar la privacidad y la biometría es esencial para garantizar la singularidad, un requisito clave para este proyecto. Además, estos datos biométricos se pueden utilizar para la autenticación de transacciones financieras, la obtención de tarjetas SIM móviles y varios otros servicios utilizando *KYC* electrónico (*eKYC*).

A medida que UIDAI[103] estaba creando una infraestructura de identidad, se decidió como principio de privacidad que solo se recopilara un conjunto mínimo de datos, lo suficiente para establecer la identidad de los residentes. Este conjunto irreductible contenía solo cuatro elementos: nombre, sexo, edad y dirección de comunicación del residente. Otro principio de diseño era emitir números aleatorios sin inteligencia, lo cual asegura que no se pueda hacer ningún perfil, ya que el número no revela nada sobre la persona. La Ley *Aadhaar* tiene restricciones claras sobre el intercambio de datos en cuanto a que no se

[102] Acrónimo de Application Programming Interface.
[103] La Autoridad de Identificación. Ünica de la India (UIDAI) es una autoridad creada para registrar y asignar todos los residentes de la India un número único de identificación basado en sus datos biométricos y demográficos. Este numero único está compuesto de 12 números.

permite la descarga de datos, no se permite la búsqueda y la única respuesta que UIDAI da a una solicitud de autenticación es 'sí' o 'no', pues no se divulga información personal[104].

Hay tres razones principales para explicar el rigor con el que los bancos manejan la información de sus clientes en el pasado y continúan con esta práctica en el presente: una regulación estricta y altos estándares de la industria, supervisión activa y continua que se tiene en este sector, así como también la necesidad del mismo sistema financiero de conservar la confianza de sus clientes lo que es considerado como el mayor activo con el que cuenta[105].

Los bancos han articulado una serie de principios en su actividad, los cuales han estado fuertemente arraigados en las instituciones, y sobre ellos trata la referida investigación de BBVA[106] se refiere con el siguiente alcance:

> *"**Seguridad:** las entidades financieras dedican grandes cantidades de recursos a mantener y la actualizar los sistemas tecnológicos para garantizar que cumplan con las crecientes demandas digitales de los servicios financieros.*
> ***Confidencialidad:** los bancos protegen no solamente la información personal de sus clientes, sino también todo tipo de datos financieros.*
> ***Integridad del mercado**: la gestión de información sensible es un pilar fundamental de la operativa bancaria. Es responsabilidad de las instituciones financieras asegurarse de que ninguna persona o entidad obtenga algún tipo de ventaja indebida a través de la información privilegiada.*
> ***Transparencia:** mantener la confianza de los clientes también significa informarles de manera concisa, comprensible y accesible sobre cómo se manejan sus datos".*

Mas allá de requerimientos de corte normativo, el sector bancario ha incorporado en su práctica cotidiana mecanismos para poder materializar los referidos principios al momento de gestionar en el día a día la información de sus clientes. Esto, aunado a una robusta

[104] ABRAHAM, Sunil. ¿Es Aadhaar una violación de la privacidad? [en línea] The Hindu ©. [consulta: 26 febrero 2022]. Disponible en https://www.thehindu.com/opinion/op-ed/is-aadhaar-a-breach-of-privacy/article62113418.ece.
[105] ALAMEDA, Teresa y ÁLVAREZ, Carmen. Más allá de la norma: el compromiso de la banca con la seguridad de los datos. *Ob. Cit.*
[106] *Ibídem.*

regulación es lo que permite que los usuarios puedan sentir la tranquilidad de que sus datos, como un preciado activo, están custodiados adecuadamente.

Este mismo es el sentimiento que se necesita de cara a la implementación de la identidad digital para los usuarios que quieran hacer uso de esta. Por ello, en el próximo apartado estaremos revisando el estado actual de la regulación, tanto para nuestro país como para otros, cuyo ejemplo es un referente en esta materia.

B. Situación regulatoria de la identidad digital

Uno de los grandes retos que presenta la implementación de la identidad digital en el entorno actual, reside en el marco normativo sobre el cual descansa la práctica bancaria en los países. Como ya hemos revisado, así como no hay una definición legal completa de identidad, y, por ende, tampoco hay una definición normativa sobre la noción de identidad digital en nuestro sistema normativo. Eso nos obliga necesariamente a analizar cómo se pudieran proteger los datos que son parte de esta. Según se verá más adelante, la situación principal que presenta dificultades es que todas las normativas analizadas sobre protección de datos personales y sistemas de identificación están basadas en relaciones de usuario-proveedor de servicios. Por tanto, esto nos lleva a pensar cómo se deberían interpretar las normas para acomodarnos a esta realidad.

De acuerdo con lo planteado por Zunzunegui, cada una de las normas que conforman la red de seguridad financiera tiene de manera indirecta un efecto de protección al usuario, ya que la finalidad de estas normas no es la protección al usuario, sino garantizar el correcto funcionamiento del mercado financiero[107].

En nuestro país, contamos con una serie de normas que rigen la protección al usuario de los servicios financieros, diseminadas en varios textos legales. Iniciamos revisando La

[107] ZUNZUNEGUI, Fernando. *Derecho del mercado financiero. Ob. Cit*. p. 31.

Constitución de la República Dominicana, que en su artículo 44, donde consagra el Derecho a la Intimidad y el Honor Personal, en el numeral 2, refiere lo siguiente:

> *Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos; (...)*[108].

La Ley Monetaria y Financiera[109], en sus artículos 52 y 53, se refiere a la obligación de transparencia financiera, la información al público y sobre la protección al usuario; sin embargo, en los mismos solo abarcan la contratación ordinaria de productos financieros. Por tanto, a los efectos de disponer de una ley especial para los usuarios de servicios financieros, se dictó en el año 2015 la actualización del Reglamento de Protección al Usuario de los Productos y Servicios Financieros[110], cuyo objeto es establecer los principios y criterios en la búsqueda de una efectiva protección de los derechos de los usuarios de los productos y servicios financieros[111].

La Ley 172-13[112] tiene dos objetos centrales, el primero, la protección de datos personales asentados en registros, archivos y bancos de datos, y el segundo, la constitución, organización, funcionamiento y extinción de las sociedades de información crediticia. Se aplica a los datos de carácter personal que se encuentren registrados en bancos de datos que los haga objeto de tratamiento, y a toda modalidad de uso posterior de estos datos en los ámbitos tanto público como privado. Los pilares de la protección de los datos están

[108] República Dominicana. Constitución de la República. *Ob. Cit.,* art. 44.
[109] República Dominicana. Ley 183-02 Monetaria y Financiera. *Ob. Cit.,* arts. 52 y 53.
[110] República Dominicana. Reglamento de Protección al Usuario de los Productos y Servicios Financieros, dictado por Junta Monetaria mediante Primera Resolución de fecha 5 de febrero 2015 y sus modificaciones.
[111] A fin de complementar el contenido de este marco normativo, el mismo debía ser acompañado de un Instructivo de aplicación, el cual nunca fue dictado.
[112] República Dominicana. Ley Núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. *Ob. Cit.*

compilados en el artículo 5, donde se desglosan las obligaciones para los que tratan los datos; sin embargo, esta norma refiere a los datos bancarios como información crediticia, dejándolos fuera de la tipología de datos sensibles y con tal enfoque, la identidad digital que se plantea utilizar para el acceso a los servicios financieros no encuentra su protección total.

La indicada ley consagra, además, que cuando se recaben datos personales es indispensable requerir el consentimiento del titular de los datos. A fin de tratar adecuadamente dichos datos o que los mismos puedan ser cedidos luego de obtener ese consentimiento, se debe informar previamente, i) el propósito para el cual serán destinados, quien puede ser su destinatario y sus clases; ii) la existencia del archivo, registro, banco de datos o de cualquier otro tipo y la identidad y domicilio de su responsable, y; iii) la posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos. Es decir, que el tratamiento y la cesión de datos personales son ilícitos cuando el titular de los datos no hubiere prestado su consentimiento libre, expreso y consciente, lo cual debe de constar de forma escrita.

Están exentos de los requisitos de consentimiento antes citados todas las entidades de investigación e inteligencia del Estado, los encargados de prevenir, perseguir y castigar de los crímenes y delitos, siempre que conste la autorización previa de la autoridad judicial que corresponda.

La principal crítica por realizar a esta norma es que no abarca integralmente el tema de Protección de Datos Personales. Tiene por objeto regular la constitución, organización, funcionamiento y extinción de las Sociedades de Información Crediticia (SIC). Su objetivo es regular únicamente a las entidades de intermediación financiera y crediticia, a la vez que le reconoce a la Superintendencia de Bancos las más amplias facultades para la vigilancia de protección de datos en los mercados. Por tanto, esto no es suficiente, ya que no se disponen de los parámetros adecuados para el tratamiento, uso, recopilación,

almacenamiento, transferencia, y eliminación de datos que, si bien no pertenecen al sector financiero, son necesarios para el desarrollo de la vida económica de las personas.

Estos dos textos legales abarcan lo que tiene que ver con intimidad, honor personal, el buen nombre, correspondencia del individuo, la protección integral de los datos personales almacenados en archivos, repositorios públicos, bases de datos u otros medios técnicos de tratamiento de datos para la elaboración de informes, ya sean públicos o privados. Sin embargo, en opinión de Omar Victoria y Eduardo Jorge[113], en la República Dominicana, la puesta en práctica de las normas sobre protección de los consumidores y usuarios ha tenido un lento desarrollo, del cual no ha escapado el sistema financiero. En materia de protección al consumidor, el avance ha sido de lo particular a lo general, esto es, la adopción de normas especiales relativas a áreas específicas, complementadas posteriormente con normas generales de adopción más reciente.

Respecto al dueño de los datos según normativa, la Ley Dominicana de Protección de Datos Personales no menciona expresamente la titularidad de los mismos, pero una lectura sistemática de la norma nos lleva a concluir que, dadas las facultades reconocidas al titular de los datos, la persona física es la dueña de estos. Las entidades que los gestionan únicamente pueden hacerlo en respeto de esas facultades.

Desde el punto de vista de Estado, existe una necesidad de reformular las normas en ese sentido, ya que no dispone de una regulación adecuada puede prestarse para vulneraciones de los derechos constitucionales de privacidad, de intimidad, de honor personal, y, en el caso de empresas grandes, de abusos de posición dominante, lo cual impacta a los intereses personales y colectivos que de ninguna manera pueden ser inobservados. De modo que está en poder de los legisladores de nuestro país como tarea urgente la de promover la reforma del marco regulatorio correspondiente en procura de que exista el espacio de creación de

[113] PRATS, Eduardo Jorge; CONTRERAS, Omar Victoria. *Derecho de la regulación monetaria y financiera*. Santo Domingo: Ius Novum, 2012, pp.271-272. ISBN 978-9945-8648-6-1

la identidad digital de las personas y la regulación de su uso para que nuestros derechos sean correctamente protegidos.

Es oportuno indicar que en nuestro ordenamiento jurídico se han realizado tempranos esfuerzos por incluir el ámbito digital en el escenario comercial, iniciando en el año 2002 con la Ley sobre Comercio Electrónico, Documentos y Firma Digital[114] que, si bien no ha podido tener el impacto que se buscaba, constituyó un importante hito para dar espacio a una nueva modalidad de contratación. Igualmente se han estado tomando acciones desde la Superintendencia de Bancos, pues han establecido que para las personas ser admitidas como clientes, relacionados o beneficiarios de una EF deben obligatoriamente acreditar su identidad mediante el suministro de información al momento de iniciar la relación, utilizando documentos, datos e información confiable y de una fuente independiente.

Ya se han dado pasos para incorporar a este mundo digital algunas técnicas de soporte para empezar a transitarlo; por ejemplo, en la última modificación del instructivo sobre debida diligencia, se incorpora la novedad que las EF tienen obligaciones especificas cuando el caso del servicio a prestar sea no presencial y se debe contar con herramientas tecnológicas apropiadas, con miras a prevenir la suplantación o hurto de identidad, entre otras posibilidades, para que el proceso de vinculación digital sea fiable[115], como veremos en detalle más adelante.

En el ámbito internacional, las normativas latinoamericanas siguen la estructura de las normas europeas de protección de datos personales y presentan definiciones muy similares a las de las entidades que están involucradas en el tratamiento de datos personales. En los países de América Latina donde existen normas de protección de datos

[114] República Dominicana. Ley núm. 126-02 sobre el Comercio Electrónico, Documentos y Firmas Digitales. *Gaceta Oficinal* No. 10172 de 4 de septiembre del 2002.
[115] *Instructivo de Debida Diligencia. SB 05-2022* [en línea]. Superintendencia de Bancos© [consulta: 22 febrero 2022]. Disponible en: https://www.sb.gob.do/sites/default/files/20220302_Circular_SB_Num_005-22_Instructivo_sobre_debida_diligencia_tercera_version.pdf

personales, estas reconocen la existencia de los siguientes sujetos: (i) el titular de los datos; (ii) el responsable del tratamiento; y (iii) el encargado del tratamiento. A estos sujetos se sumarán aquí los conceptos de importador y exportador de datos, dado que podría ocurrir que exista un flujo transfronterizo de datos personales y haya que atender a estos roles. Al respecto, es menester señalar que estas consideraciones se realizan sobre el proceso de creación de la identidad.

Chile fue el primer país Latinoamericano en aprobar algún marco normativo sobre protección a la privacidad que contiene algunos principios básicos relativos a la protección de datos personales. La Ley Chilena 19628, sobre la protección de la vida privada, establece en su artículo 4 que los datos personales solo pueden ser tratados si esta ley u otras disposiciones legales así lo permitan o con el consentimiento expreso por parte del titular. Además, el mismo debe estar informado correctamente con relación al propósito del almacenamiento de los datos personales propios y su posible difusión al público[116].

Hasta el momento de la investigación de este trabajo, México no cuenta con un estándar normativo para la protección a la vida privada, pero a través del artículo 76 bis de la Ley Federal de Protección al Consumidor, es ampliado el alcance de la Ley en transacciones realizadas mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología y la utilización de los datos aportados de manera adecuada.

La Ley Mexicana fue la primera en Latinoamérica que se refirió a la protección de datos personales en sistemas y servicios en línea, sin embargo, solamente regula estos tipos de transacciones. Por otra parte, adquiere un enfoque basado en la protección al consumidor, cuando existan situaciones en las que la recopilación y tratamiento de información no sea

[116] Chile. Ley19628 Sobre Protección de la Vida Privada o Protección de Datos de Carácter Personal. [en línea] Publicada en el Diario Oficial de 28 de agosto de 1999, p. 4. [consulta: 21 febrero 2022]. Disponible en: http://www.informatica-juridica.com/anexos/anexo137.asp

resultado de la relación directa con el consumidor. Debido a esta razón, existe un vacío normativo que persiste[117].

Perú no tiene una norma general de protección a la vida privada, pero su Código Civil puntualiza lo siguiente:

> *Artículo 16.- Confidencialidad de la correspondencia y demás comunicaciones. La correspondencia epistolar, las comunicaciones de cualquier género o las grabaciones de la voz, cuando tengan carácter confidencial o se refieran a la intimidad de la vida personal y familiar, no pueden ser interceptadas o divulgadas sin el asentimiento del autor y, en su caso, del destinatario. La publicación de las memorias personales o familiares, en iguales circunstancias, requiere la autorización del autor*[118].

Es posible considerar que la recopilación de los datos en el marco de las contrataciones por medios electrónicos constituye una comunicación y, por lo tanto, quedan amparados por el Código Civil.

Colombia tiene la protección al consumidor como una tarea pendiente. Con la Ley 1328 de 2009 es creado el régimen de protección al consumidor financiero y a partir de esa reforma quedan establecidas las disposiciones relativas a los aspectos propios de la relación comercial, como son la debida diligencia, que es la obligación de suministrar la información orientada a satisfacer las necesidades del consumidor. La información debe ser clara y transparente al consumidor con la finalidad de que este disponga totalmente del conocimiento sobre sus derechos y sus obligaciones en el uso de los canales electrónicos[119]. Esta norma aparentemente no resulta suficiente de cara a su realidad.

---

[117] PALAZZI, Pablo Andrés. La transmisión internacional de datos personales y la protección de la privacidad. Buenos Aires: AD-HOC, 2002. ISBN: 950-894-318-1

[118] Perú. Código Civil. Decreto Legislativo 295. [en línea] Publicado 25 de julio de 1984. [consulta: 8 febrero 2022]. Disponible en: http://www.osce.gob.pe/consucode/userfiles/image/CodigoCivil.pdf

[119] BLANCO BARÓN, Constanza. La información como instrumento de protección de los consumidores, los consumidores financieros y los inversionistas consumidores [en línea] Opinión Jurídica, 2012. 11(21); 135-152 [consulta: 27 febrero 2022] Disponible en: https://revistas.udem.edu.co/index.php/opinion/article/view/532/481

En los Estados Unidos no existe una ley general que regule la protección de datos personales, pero sí existen regulaciones concretas para ciertos sectores y temas. El *Fair Reporting Act*[120] fue aprobado en el 1970, y su objeto es la protección al cliente de las entidades de crédito en contra la violación a su privacidad por parte de las agencias de información. Posteriormente en el 974 fue sancionada la *Privacy Act*[121], que otorga a todos los ciudadanos el derecho a la protección de su vida privada y esta aplicación se extiende a las informaciones con este carácter que refieran a personas físicas y estén disponibles en los registros del gobierno federal. En ese sentido, la aprobación por parte del interesado debe ser clara y expresa a fin de poder difundir los datos personales registrados.

Como hemos visto, existe cada vez una orientación políticamente más marcada, tendente a tener presentes las prerrogativas que asisten a los usuarios de servicios financieros.

En el ámbito europeo, tuvo lugar la promulgación del Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y del Consejo del 06 de abril de 2016. El Reglamento reemplaza la Directiva de Protección de Datos 95/46/EC y fue diseñado para armonizar las leyes de privacidad de datos en toda Europa para la protección de las personas con respecto al procesamiento de datos personales y la libre circulación de dichos datos. Este reglamento se considera una medida fundamental para potenciar y fortalecer los derechos básicos de toda persona en la era digital y viabilizar las actividades económicas, ya que aclara las normas que se aplican a las empresas y los organismos públicos en el mercado único digital. Además, contar con un estándar único pondría fin a

[120] La Ley de Información Crediticia Justa (FCRA) es una ley federal que regula la recopilación de información crediticia de los consumidores y el acceso a sus informes de crédito. Fue aprobado en 1970 para abordar la equidad, exactitud y privacidad de la información personal contenida en los archivos de las agencias y de informes de créditos. Disponible en: https://www.investopedia.com/terms/f/fair-credit-reporting-act-fcra.asp.

[121] La *Privacy Act* o Ley de Privacidad de 1974, en su forma enmendada, 5 U.S.C. § 552a, establece un código de prácticas justas de información que rige la recopilación, mantenimiento, uso y difusión de información sobre personas que las agencias federales mantienen en sistemas de registros.

la fragmentación en los diferentes sistemas nacionales y a las cargas administrativas que no sean necesarias, todo lo cual obstaculiza el intercambio y la fluidez de información.

En nuestro ordenamiento jurídico, en el ámbito de la protección de datos para los usuarios de servicios financieros, existe una gran oportunidad a nivel normativo, donde se pueda incluir el uso y adaptación de las nuevas tecnologías a un marco adecuado, más semejante a la norma incorporada en la Unión Europea. Todas las regulaciones en América Latina consideran a la persona como el titular de los datos y como la única que debería estar en condiciones de determinar cómo serán tratados. Esto se alinea con el espíritu de los proyectos de identidad digital, en tanto proponen construir una identidad digital que certifique y valide datos sociales, cívicos y económicos, a través de la emisión de credenciales verificables.

Las conclusiones del estudio sobre regulación de *blockchain* e identidad[122,] proponen ciertos principios para una posible regulación en materia de identidad digital, los cuales somos de opinión que resultaría interesante adoptar en un marco legal nuestro, a saber:

1. Todo sistema de identidad digital basado en tecnología *blockchain* o de registros distribuidos debería anteponer los intereses del dueño de los datos personales sobre los intereses que los terceros pudieran tener sobre ellos.
2. La participación en sistemas de identidad digital debe ser voluntaria, no obligatoria: en cualquier momento, el usuario debería ser capaz de eliminar todo su perfil. De lo contrario, se vulneran los cimientos sobre los que se construye la idea de identidad digital.
3. La base legal para cualquier tipo de tratamiento de datos que se realice a partir de la información que forme parte del perfil de un usuario debe disponer del consentimiento expreso e informado, tal y como dispone la normativa vigente aplicable de protección de datos personales.

[122] CHOMCZYK, Andrés. Regulación de blockchain e identidad digital en América Latina. *Ob. Cit*., p.124.

4. La utilización de los datos de la persona por parte de terceros debe tener términos claros y simples sobre los datos que se pretenden usar, como serán utilizados y qué terceros tendrán acceso a ellos.
5. La información y solicitud de consentimiento deberían hacerse de forma que no resulte en un agotamiento de la atención del usuario, debiendo, antes que todo, hacer un ejercicio de minimización de los datos que pretenden usarse antes de la efectiva recolección.
6. Todo marco regulatorio en torno a estos desarrollos debería ser tecnológicamente neutro, para permitir el desarrollo de soluciones usando tecnologías presentes y futuras.

II. Gestión de la Seguridad en el uso de la identidad digital

En sentido general, los usuarios de servicios financieros se preocupan por el tratamiento de su información, pues el intensivo intercambio de datos y la incorporación de medios digitales como nuevas herramientas para proveer los servicios que de forma cotidiana antes se limitaban a papel escrito, plantean un cambio radical en el modo como se trata la seguridad. Mirando hacia atrás, muchas empresas han sido sancionadas por no gestionar adecuadamente la seguridad de la información de sus usuarios.

Sin embargo, a nivel bancario, con la rígida regulación para el sector, el nivel de seguridad con el que se deben tratar los datos debe ser muy alto. En este apartado, revisaremos cuál es el alcance de la privacidad en este tema, y cómo las instituciones deben actuar en materia de ciberseguridad.

A. Privacidad

En un mundo cada vez más digital y sin fronteras, la privacidad y la seguridad no se pueden garantizar mediante la construcción de muros alrededor de la información confidencial. La

identidad es la nueva frontera de la privacidad y la seguridad, donde la naturaleza misma de las entidades es lo que les permite completar algunas transacciones.

La gestión de la identidad digital tiene muchas facetas, pues abarcan temas técnicos, económicos, sociales y culturales, de modo que la misma es compleja de entender y abordar holísticamente. La gestión de la identidad digital es esencial para que el ecosistema digital funcione como una plataforma para el desarrollo económico y el progreso social, pero todo esto debe ser realizado en un ambiente donde tener el marco de la seguridad y la privacidad bien definido es obligatorio. Es deber en el análisis de este trabajo plantear la cuestión de la incorporación de la privacidad como un requisito previo para la interacción en el mundo digital.

Actualmente, hemos visto que los sistemas que en general son utilizados como medios de identificación digital, plantean problemas de privacidad porque recopilan datos personales. A modo de comentario sobre las buenas prácticas y principios existentes de los estándares que internacionalmente se observan en materia de Protección de Datos y Privacidad, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE)[123] establece un estándar internacional de buenas prácticas para la protección de datos y la privacidad, y el mismo se constituye como la norma estrella, a emular por el resto de los países, aunque el mismo no es de obligatorio cumplimiento.

En los sistemas de identificación, la privacidad de los datos no significa necesariamente que todos los datos se mantengan en secreto en todo momento. Más bien significa que los datos solo deben ser accedidos, procesados o compartidos por y con usuarios autorizados para fines especificados que se hayan acordado de antemano. La protección de datos, que incluye los métodos y controles legales, operativos y técnicos para proteger la información

[123] Unión Europea. Reglamentos (EU) 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 el 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). *Ob. Cit.*

y hacer cumplir las reglas sobre el acceso y el uso, es, por lo tanto, fundamental para garantizar la privacidad de los datos, sabiendo que no todos los datos merecen el mismo nivel de protección y que los datos personales se refieren a cualquier información relacionada con una persona física que pueda ser identificada, como define el artículo 4 del RGPD. Una persona física que pueda ser identificada es un "sujeto de datos" y se define como una persona física

> *que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, datos de ubicación, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona física*[124].

Cualquier actividad que recopile, almacene o procese datos personales plantea ciertos riesgos, dentro de los cuales podemos listar algunos, tales como: violaciones de seguridad, ataques físicos o cibernéticos a datos; divulgación no autorizada, cuando se hace transferencia inapropiada de datos a terceros; exposición de información personal confidencial, con la divulgación de datos, como, por ejemplo, biometría, religión, etnia, género, historiales médicos, para fines no autorizados; intercambio de datos que traspasa los límites de los fines para los que se dio el consentimiento; robo de identidad, que puede llevar a consecuencias tan graves como las del mundo físico real, y que, dada la naturaleza global y descentralizada de Internet, puede generar daños que a menudo son más difíciles de reparar.

La suplantación de identidad puede ser realizada por casi cualquier persona. Igualmente, la capacidad de correlacionar la información de identificación entre bases de datos (por ejemplo, a través del reconocimiento facial) aumenta los riesgos de vigilancia, particularmente cuando se trata de biometría. También pueden surgir inconvenientes por discriminación o persecución, pues los atributos de identidad se prestan para discriminar o perseguir a personas o grupos particulares, ocasionando tratamiento injusto o errores.

[124] *Ibídem*, art. 4.

Por otra parte, al tiempo que la digitalización de los sistemas de identificación crea o aumenta los riesgos inherentes a su utilización, es cierto que también presenta nuevas oportunidades y medios tecnológicos para una mayor protección. Específicamente, los sistemas de identificación digital pueden ofrecer identificación y autenticación más precisas. A medida que los sistemas de identificación digital aprovechan el procesamiento informático y las tecnologías avanzadas, pueden ofrecer un mayor nivel de seguridad y precisión que los procesos de autenticación manuales basados en papel, que están sujetos a errores humanos e indiscreción. Hacerlo aumenta la confianza, reduce los costos y respalda sistemas sostenibles y flexibles, además de que mejora la integridad de los datos. Aunque los sistemas de identificación digital presentan nuevos riesgos de seguridad, pueden, al adoptar las medidas de protección de datos descritas anteriormente, garantizar mejor la integridad y el uso de los datos recopilados en comparación con los sistemas de registros en papel que pueden destruirse, dañarse o alterarse fácilmente.

La tecnología digital permite nuevas características de mejora de la privacidad que antes no eran posibles. En los sistemas que utilizan credenciales no digitales, la transacción generalmente implica presentar una tarjeta de identificación física a un proveedor de servicios y, por lo tanto, revelar toda la información mostrada. A modo de ejemplo, presentar una credencial física como prueba de edad revela información adicional, como nombre completo, fecha de nacimiento y, a menudo, dirección.

También, las nuevas tecnologías y estrategias de diseño ofrecen a las personas más control sobre sus datos personales, incluidos los portales de acceso que facilitan a los usuarios verificar la precisión de sus datos y monitorear su uso, incluyendo que automatizan las notificaciones, de modo que se puede controlar la violación de datos. Además, los ecosistemas emergentes de identificación digital brindan a los usuarios una mayor variedad de proveedores de identificación.

En los últimos años, como acabamos de revisar más arriba, varios países han promulgado leyes, regulaciones y políticas para la proteger la privacidad y los datos personales como un derecho humano fundamental, en consonancia con otras herramientas regionales e internacionales de protección de datos. Brasil, Colombia, Costa Rica, República Dominicana, Ecuador, México, Nicaragua, Perú y Uruguay son algunos de los países de Latinoamericanos que cuentan con normativa y regulación vigente en esta materia. Solo en México el enfoque de regulación proactivo ha evolucionado para incluir el uso y la implementación de autorregulación vinculante referente a la protección de datos e impone restricciones regulatorias a los flujos de datos transfronterizos para viabilizar la comercialización internacional, así como el intercambio de datos con otros países, además de motivar la innovación tecnológica[125].

Sin embargo, muchos de los países Latinoamericanos todavía deben enfrentar un sin número de desafíos, tales como:

i. Mejorar los programas de gestión de la privacidad que incluyen la obligatoriedad de dar respuesta, notificar y brindar acciones correctivas a los dueños de los datos en caso de vulneración de la seguridad que afecte su información personal.
ii. Colaborar a través de controles en las fronteras entre países para proteger adecuadamente la privacidad y autoridades y, de manera similar mejorar la interoperabilidad con otros marcos de privacidad y protección de datos tanto regionales como nacionales.

[125] Broadband policies for Latin America and the Caribbean. [en línea] OECDiLibrary © [consulta: 1 marzo 2022]. Disponible en: https://www.oecd-ilibrary.org/science-and-technology/broadband-policies-for-latin-america-and-the-caribbean/summary/spanish_091f56bb-es;jsessionid=fu7ytQ-Mg8nJFs8P5Jf6jXCa.ip-10-240-5-172

En ese sentido, la OCDE[126] ha venido desempeñando un papel importante en la promoción del respeto a la privacidad, toda vez que el mismo es un valor fundamental y la misma constituye una condición *sine qua non* para el libre flujo de los datos personales. Sus directrices de privacidad son la piedra angular en esa materia, al estar reconocidas como el estándar mínimo global para la privacidad y protección de datos. La segunda revisión de la Guía para la Privacidad realizada por la OCDE, es tenida a nivel mundial como una referencia internacional sobre los estándares mínimos que deben observarse para la privacidad y la protección de datos personales. Esta refuerza las medidas políticas que pueden ser adaptadas en ese sentido.

Los principios básicos promovidos por la OCDE se resumen en los referidos a continuación[127]:

> ***Principio de limitación de la recolección***. *Debe existir restricciones en la recopilación de los datos personales y dichos datos deben ser recopilados por medios legales y justos y, cuando corresponda debe realizarse con el conocimiento o consentimiento del titular.*
> ***Principio de calidad de los datos***. *Los datos personales deben ser apropiados para los fines que se utilizan, y en la medida necesaria para esos fines, deben ser exactos, completos y actualizados de forma permanente.*
> ***Principio de especificación del propósito***. *Los fines para los cuales se recopilan los datos personales se determinarán a más tardar en el momento de la recopilación de los datos y su uso posterior se limitará a lograr estos u otros fines incompatibles con los fines de recopilación de datos. Debe especificarse en cada ocasión que haya un cambio de propósito.*
> ***Principio de limitación de uso***. *Los datos personales no pueden ser divulgados, proporcionados o utilizados de un modo distinto al especificado, con excepción de: a) con el consentimiento del titular, o b) según lo permita la ley.*
> ***Principio de salvaguardia de seguridad***. *Los datos personales estarán protegidos por garantías de seguridad razonables contra riesgos como son pérdidas o acceso no autorizado, la destrucción, su utilización, la modificación o la divulgación de datos.*
> ***Principio de apertura***. *Debe existir una política común con respecto al desarrollo, prácticas y políticas relacionadas a los datos personales. Debe disponerse de los medios*

[126] Las Siglas de *OECD: Organization for Economic Co-operation and Development*, corresponden a Organización para la Cooperación y el Desarrollo Económicos (OCDE) es una organización internacional que trabaja para construir mejores políticas.
[127] *The evolving privacy landscape: 30 years after the OECD Privacy Guidelines* [en línea] OECD Publishing. 2013. [consulta: 1 marzo 2022] Disponible en: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

> *para establecer la existencia y naturaleza de los datos personales, así como las finalidades principales de su uso, la identidad y la residencia habitual del responsable del tratamiento.*
> ***Principio de participación individual**. Las personas deben tener derecho: a) a obtener de un controlador de datos, o de otra manera, confirmar si el controlador de datos dispone o no de datos relacionados con ellos; b) que le sean comunicados los datos relativos a ellos, dentro de un plazo razonable; con los costos asociados accesibles a cualquier persona, si lo hubiere, y en una forma que sea de fácil comprensión para estos; c) que les sea explicada la razón en caso de ser denegada una solicitud formulada en virtud de los apartados a) y b), y tener la facultad de impugnar dicha denegación; y d) impugnar los datos relativos a ellos y, si la impugnación tiene éxito, solicitar que los datos sean borrados, rectificados, completados o modificados.*
> ***Principio de rendición de cuentas**. Un controlador de datos que sea responsable de velar por el cumplimiento de las medidas que dan efecto a los principios establecidos anteriormente.*

Enmarcado en un lenguaje conciso y tecnológicamente neutro, el enfoque basado en principios de las Directrices de Privacidad es ampliamente reconocido no solo como una base sólida para construir una protección y confianza efectivas para las personas, sino también para desarrollar enfoques internacionales comunes respecto a los flujos de datos transfronterizos.

Entre las buenas prácticas regulatorias relativas a la protección de la privacidad, la promoción de la gestión de riesgos de privacidad por parte de los que tienen a su cargo las políticas de los países de América Latina y el Caribe se destaca como una forma útil para que los encargados del tratamiento de datos protejan la privacidad. Este quizás sea uno de los desafíos más importantes de la región, porque es un concepto nuevo y todos son de opinión que "*hacen falta esfuerzos para entender las aplicaciones e implicaciones prácticas de la gestión de riesgos de privacidad"*[128].

En ese sentido, en las estrategias de privacidad que deben ser incorporadas, deben contemplarse cada una de las políticas contenidas en el principio 19, parte quinta de las Directrices de Privacidad de la OCDE revisadas[129], las cuales esbozamos a continuación:

[128] *Ibídem*, p.120.
[129] *Ibídem.*

i. *Desarrollar estrategias nacionales de privacidad que reflejen un enfoque coordinado entre organismos gubernamentales.*
ii. *Establecer y mantener autoridades de protección de datos que dispongan de recursos y conocimientos técnicos para ejercer sus facultades de forma efectiva y adoptar decisiones coherentes, objetivas e imparciales.*
iii. *Fomentar y apoyar la autorregulación, ya sea en forma de códigos de conducta o de otro tipo.*
iv. *Establecer mecanismos razonables para que las personas ejerzan sus derechos.*
v. *Prever las oportunas sanciones y soluciones en caso de incumplimiento de las leyes que protegen la privacidad.*
vi. *Contemplar la adopción de medidas complementarias, como el incremento de la educación y concienciación, el desarrollo de competencias, y la promoción de medidas técnicas que contribuyan a proteger la privacidad.*
vii. *Tener en cuenta el papel de otros actores distintos de los responsables del tratamiento de datos, en una manera adecuada a su función individual.*
viii. *Garantizar la no existencia de discriminación de manera injusta en contra de los titulares de los datos.*

En este contexto es de vital importancia aplicar el principio de responsabilidad. Los encargados del tratamiento de datos y los ejecutores dentro de sus controles y acciones deberían de realizar las siguientes, propuestas igualmente por la OCDE[130]:

i. *Establecer un programa de gestión de la privacidad que refleje estos principios en todos los datos personales bajo su control, adaptable a la estructura, escala, volumen y sensibilidad de las operaciones, que ofrezca garantías adecuadas basadas en la evaluación de riesgos de privacidad, integrado en su estructura de gobernanza y que establezca mecanismos internos de supervisión, conteniendo un plan definido para responder a las consultas e incidentes, actualizable en función del seguimiento continuo y su examen periódico.*
ii. *Estar preparado para demostrar la idoneidad del programa de gestión de la privacidad, especialmente cuando sea requerido por una autoridad de protección de datos competente u otra organización responsable de promover la observación y cumplimiento de un código de conducta o semejante que confiera efecto vinculante a estas Directrices.*
iii. *Notificar a las autoridades de protección de datos competentes sobre cualquier violación importante de la seguridad que afecte a los datos personales. Cuando la violación tenga repercusiones negativas sobre los titulares de los datos, el responsable del tratamiento deberá informar a los afectados.*

[130] *Ibídem*.

Esperamos, en un futuro no tan lejano, que estas recomendaciones queden a nivel de marcos legales en cada país, con miras a hablar un solo idioma en materia de privacidad de datos, y que la identidad digital tenga las brechas de riesgo a nivel de privacidad y seguridad disminuidas a su mínima expresión.

B. Ciberseguridad

La ciberseguridad es un conjunto de procedimientos y herramientas implementadas para la protección de la información que se genera y procesada mediante el uso de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.

Conforme a la opinión de expertos de *Information Systems Audit and Control Association* (ISACA)[131], la ciberseguridad es definida como "*una capa de protección para los archivos de información*". Igualmente, en referencia a la ciberseguridad, es utilizado el término seguridad informática o seguridad de la información electrónica[132].

El objetivo de la ciberseguridad es crear confianza entre clientes, proveedores y el mercado en su conjunto. En un mundo altamente conectado donde la mayoría de nuestras actividades son realizadas a través redes y dispositivos electrónicos, la seguridad de las operaciones es una necesidad fundamental.

La ciberseguridad, o seguridad cibernética, es el campo de la tecnología de la información que se ocupa de asegurar de los sistemas informáticos y proteger de datos contra ataques

[131] Asociación Internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

[132] Ciberseguridad una guia completa del concepto, tipos, amenazas y estrategias. [en línea] INFOSECURITY México© [consulta: 1 marzo 2022]. Disponible en https://www.infosecuritymexico.com/es/ciberseguridad.html.

maliciosos o informáticos en el mundo digital. Esto incluye las amenazas contra hardware, cuidado de información confidencial, cuidado de *software* y datos de las computadoras, incluidos robo, piratería, virus, ataques a bases de datos o incluso nuevas tecnologías. El campo de la seguridad informática ha crecido exponencialmente conforme se van habilitando más dispositivos para Internet y más servicios están disponibles en línea. Términos como el cifrado de la información o la criptografía son cada vez más comunes y son utilizados para combatir el cibercrimen, así como las distintas amenazas cibernéticas y al tiempo que protegen los sistemas de seguridad[133].

Conforme la economía se expande, los ataques cibernéticos son cada vez más comunes, y los antivirus no resultan suficientes, pues con frecuencia es notable que los cibercriminales se valen de ingeniería social, los emails con *phishing*[134] realizan ataques a millones de correos electrónicos a diario, los *hackers*[135] también quieren incorporar *software* malicioso en los sitios web. Es por esto la necesidad imperante para las instituciones financieras de implementar soluciones de protección de la información.

La ciberseguridad es la primera barrera para proteger los recursos de las empresas o individuos. Para las instituciones financieras, la ciberseguridad es un mecanismo para mantener sus activos protegidos contra violaciones en sus sistemas de información, datos personales, dispositivos móviles, sistemas electrónicos, información personal, copias de seguridad, entre otros, así como de cualquier ataque cibernético que atente en contra de la

[133] Curso de Ciberseguridad [en línea] EDX© [consulta: 1 marzo 2022]. Disponible en: https://www.edx.org/es/aprende/ciberseguridad

[134] *Phishing* es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo revelar información confidencial o hacer click en un enlace). Disponible en https://www.osi.es/es/banca-electronica

[135] Hacker es un experto de las tecnologías de comunicación e información que utiliza sus conocimientos técnicos en computación y programación para superar un problema, normalmente asociado a la seguridad. Habitualmente se les llama así a técnicos e ingenieros informáticos con conocimientos en seguridad y con la capacidad de detectar errores o fallos en sistemas informáticos para luego informar los fallos a los desarrolladores del software encontrado vulnerable o a todo el público. Disponible en: http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/hackers.aspx

seguridad de la información. La ciberseguridad se trata del establecimiento de parámetros de seguridad para los activos de información y en contra de agentes maliciosos tales como son, por ejemplo, los virus informáticos[136].

Es cierto que tradicionalmente la ciberseguridad se encarga de la protección integral de la integridad, disponibilidad de los sistemas y la confidencialidad, igualmente de las redes y la información que discurre por Internet, pero la aparición de la digitalización exige defender la reputación y los derechos de quienes hacen uso de la identidad digital, la cual se desarrolla, por un lado, asociando la protección de derechos como la privacidad, el olvido o el anonimato, a la de otros derechos fundamentales mediante la regulación y la jurisprudencia y, por otro, se desarrollan mecanismos de identificación y autenticación que faciliten un uso seguro de Internet y el aprovechamiento de las posibilidades y nuevos modelos de negocio que ofrece la economía digital.

Las amenazas a la ciberseguridad son un problema global y requieren de una solución integral que incluya a todas las partes involucradas, incluyendo una responsabilidad compartida de parte de la sociedad civil, el sector privado y del Gobierno.

En el ordenamiento jurídico de la República Dominicana, contamos con una amplia gama de fuentes normativas, que han ido evolucionando a través del tiempo, con las cuales se regula lo referente a las TIC/Ciberseguridad de una forma holística, a saber: Ley General de Telecomunicaciones No. 153-98, Ley sobre Comercio Electrónico, Documentos y Firma Digital No. 126-02, Ley de Crímenes y Delitos de Alta Tecnología No. 53-07, Decreto 229-07 que ratifica la OPTIC y ámbitos de desarrollo del Gobierno Electrónico, Ley No. 267-08 sobre Terrorismo, que crea el Comité Nacional Antiterrorista y la Dirección Nacional Antiterrorista, Decreto 258-16 sobre Programa República Digital, la Comisión Presidencial de República Digital y, muy especialmente aplicable a este tema, el

[136] Ibídem, p. 125.

Decreto 230-18 sobre Estrategia Nacional de Ciberseguridad y el Reglamento de Seguridad Cibernética y de la Información emitido por la Junta Monetaria.

Además de las Leyes Monetaria y Financiera, de Protección de Datos Personales y sobre Crímenes y Delitos de Alta Tecnología, al marco legal de la ciberseguridad del país se agrega el Centro Sectorial de Respuesta a Incidentes de Ciberseguridad para el Sistema Financiero y de Pagos (SPRICS), el cual tiene una gran relevancia en la transformación digital hacia la que se encamina el país, con el objetivo principal de fortalecer la capacidad de gestión de la ciberseguridad de los participantes del sistema financiero y de pago, a fin de contribuir con la reducción de los riesgos que por su naturaleza soportan.

También debemos mencionar que en el país contamos con la ratificación de tratados internacionales, tales como el Convenio sobre Ciberdelincuencia del Consejo de Europa. Igualmente, han sido creados oficinas gubernamentales especializadas en la persecución y enjuiciamiento de estos delitos, entre ellos: la Dirección de Investigación de Crímenes y Delitos de Alta Tecnología de la Policía Nacional (DICAT) y la Procuraduría Especializada en Delitos de Alta Tecnología (PEDATEC).

Recientemente, nuestros congresistas conocieron un Proyecto de Ley sobre gestión de la Ciberdelincuencia en República Dominicana, que viene a fortalecer el rol y las facultades pertinentes, constituyéndose como entidad de derecho público con autonomía. El mismo hacía años ya era una necesidad y se estaba esperando para que completara, aunque no exclusivamente o de manera limitativa, el marco jurídico en dicha materia y de esta forma disponer de los mecanismos apropiados a fin de realizar las investigaciones con el conocimiento y la estructuración de los expedientes a ser juzgados, así como la tipificación de las sanciones correspondientes[137].

[137] FIGUEREO, Julia. Senadores concluyen estudios del proyecto de Ley sobre Gestión de Ciberseguridad [en línea] Senado de la República© [consulta: 1 marzo 2022] Disponible en https://www.senadord.gob.do/senadores-concluyen-estudio-del-proyecto-de-ley-sobre-gestion-de-ciberseguridad/

Nuestro país ocupa la posición 66 en la tercera edición del informe sobre el "Índice Global de Ciberseguridad (GCI)" que realizó en 2020 un ranking mundial en el que participan 186 países, donde se mide el nivel de desarrollo o compromiso de cada país en base a cinco pilares: "(*i) Medidas legales, (ii) Medidas técnicas, (iii) Medidas organizativas, (iv) Desarrollo de capacidades, y (v) Cooperación, gracias a las acciones implementadas y desarrolladas por el Centro Nacional de Ciberseguridad y los diferentes actores del sector público y privado*" [138].

Esto es una clara representación del avance que ha logrado en los últimos años el país en lo relativo a ciberseguridad, gracias al notable esfuerzo y coordinación del Centro Nacional de Ciberseguridad, quienes han dado su soporte a los sectores públicos y privados en general, así como a la población en general.

El Centro Nacional de Ciberseguridad está dedicado al desarrollo de la ciberseguridad, al fortalecimiento de la confianza digital de los usuarios de la República Dominicana, así como a la protección de la infraestructura crítica y tecnológica del Estado dominicano. Quedó establecido mediante Decreto 230-18 en el marco de la estrategia nacional de ciberseguridad 2018-202, como dependencia del Ministerio de la Presidencia de la República dominicana.

A pesar de que la ciberseguridad constituye un reto mayor para los servicios financieros que son gestionados por medios digitales y, por ende, mediante uso de la identidad digital, entendemos que en materia de Ciberseguridad, el país se encuentra en una muy buena posición, con muchas fortalezas de carácter regulatorio y normativo, pues ha demostrado una evolución y madurez que nos permitiría implementar el uso de la identidad digital a

[138] República Dominicana escala 26 posiciones índice Global de Ciberseguridad [en línea] Portal de la Presidencia de la República Dominicana [consulta: 1 marzo 2022] Disponible en: https://presidencia.gob.do/noticias/republica-dominicana-escala-26-posiciones-indice-global-de-ciberseguridad.

nivel nacional, en los sectores públicos y privados, de una manera satisfactoria para todos los involucrados.

SECCIÓN III.
GOBERNANZA Y PREVENCIÓN DE LAVADO DE ACTIVOS EN EL ENTORNO DIGITAL

SECCIÓN III.
GOBERNANZA Y PREVENCIÓN DE LAVADO DE ACTIVOS EN EL ENTORNO DIGITAL

La creciente digitalización en el ámbito de servicios financieros se ha servido de las tecnologías para hacer la transición de lo análogo a lo digital. La transformación digital financiera ha transcurrido en paralelo con las respuestas regulatorias avanzadas para encarar la más reciente crisis económica global en el año 2008[139]. La transformación digital ha venido como un propulsor, sin detenimiento del crecimiento sostenible, aprovechando la digitalización para una recuperación económica que pretende ser resiliente, fuerte y sostenible.

También, ha traído consigo grandes oportunidades de inclusión, un objetivo de mucha relevancia, y de la mano también trae grandes retos a nivel normativo, ya que los riesgos inherentes del cambio de modelo motivan a cuestionarse si el panorama regulatorio actual resulta suficiente o necesita ajustarse para ir a la par del tiempo en el que vivimos.

Un modelo de gobernanza establece principios, políticas, terminología, estándares y responsabilidades. Como ejemplo metafórico, los marcos de confianza establecen los acuerdos y las reglas del juego, mientras que los modelos de gobernanza definen los roles y responsabilidades de los jugadores. Para la incorporación del uso de la identidad digital, la gobernanza corresponde a los gobiernos, con la emisión de políticas, directrices, normas o instrucciones, y están encargadas de su aplicación las entidades supervisoras en materia financiera.

En vista de que la presencialidad será cada vez menos común, el uso de la identidad digital continúa tomando fuerza en cada jurisdicción, con sus propias características. Por esto, los

[139] GURREA-MARTÍNEZ, Aurelio, REMOLINA LEÓN, Nydia. Fintech, regtech and legaltech: Fundamentos y desafíos regulatorios. Valencia: Colección Esfera todo el Derecho 2020, p. 208.

países deben implementar un correcto tratamiento de los datos obtenidos, así como identificar, evaluar y entender los riesgos de lavado de activos y financiamiento del terrorismo al que están expuestos. En igual sentido, dentro de las acciones que se deben iniciar están la designación de una autoridad o mecanismo para coordinar esfuerzos orientados en la evaluación de los riesgos y aplicar recursos encaminados a asegurar la mitigación eficaz de dichos riesgos.

La identidad digital debe ser provista por el Estado y esa práctica cada vez se ha replicado en distintos países. Hemos visto cómo se han ido ajustando los marcos legales y la disposición normativa de acuerdo con lo necesario para su incorporación está bastante desarrollada en algunos países y en camino de fortalecerse más en otros. Existe cierto miedo aún, relativos al tratamiento de la protección de los datos del consumidor de servicios financieros, de que toda la información personal que es utilizada virtualmente sea almacenada y tratada posteriormente por el tercero a quien se ceden; sin embargo, contamos con bastante regulación al respecto en todas las latitudes. Revisar las opiniones, directrices y casos de éxito, permite que implementar nuevas prácticas se pueda realizar con una mayor confianza.

Una traba que existe es la de asociar la identidad digital a un control gubernamental indiscriminado, como una especie de ¨Gran Hermano¨, que de forma arbitraria pueda seguir la actividad de los ciudadanos, para luego utilizar esa información en su beneficio. No obstante, como se analizará, el papel del supervisor, de la mano con los lineamientos establecidos para nuestro país, no da mucho espacio a que la exposición de información pueda resultar en un exceso que perjudique a la persona.

En este apartado estaremos revisando cuál es el rol del supervisor en materia de protección de los datos y privacidad junto a otras disposiciones similares insertadas en los distintos esquemas en materia de supervisión que han adoptado los países, de acuerdo con su necesidad de incorporar la identidad digital en el nuevo modelo de negocios.

También revisaremos las novedades propuestas por las entidades líderes en materia financiera, sus recomendaciones, y ejemplos de mejores prácticas, algunas ya implementadas por países cuyos ejemplos esbozaremos brevemente.

I. Agentes de protección de los usuarios de servicios financieros

La autoridad de supervisión bancaria desempeña una función vital en la protección del consumidor. Hasta la fecha, la orientación regulatoria internacional no ha prestado suficiente atención a las oportunidades y los desafíos específicos a los que se enfrentan estas autoridades al asumir la supervisión de la protección del consumidor. En algunos casos tienen la doble responsabilidad de promover la estabilidad y promover la inclusión financiera.

La supervisión financiera es un componente esencial que garantiza el buen funcionamiento del sistema financiero y, por ende, de la economía. Lo experimentado por ciertos países muestra que una supervisión deficiente imposibilita descubrir malas prácticas o riesgos que podrán generar problemas de solvencia para alguna entidad o para el sistema en su conjunto.

Después de transcurridos años de desregulación y la crisis financiera posterior, surgió un interés legítimo en que los reguladores de servicios financieros adoptaran una postura más intervencionista. Si bien la primera directiva europea trata sobre el crédito y busca garantizar un nivel mínimo de protección para los préstamos hipotecarios, recientemente impuso normas más estrictas acerca de la concesión responsable a los Principios de Alto Nivel del G20 y la OCDE respecto a la Protección del Consumidor de Servicios Financieros[140].

[140] G20 Digital Identity Onboarding. *Ob. Cit.*

Por ello, los líderes del G20 han acordado la creación de la Alianza Global para la Inclusión Financiera (GPFI por sus siglas en inglés)[141], con el objetivo de identificar y aplicar enfoques innovadores para mejorar el acceso a los servicios financieros, así como el desarrollo de normas de acceso financiero, educación financiera y protección del consumidor de servicios financieros. Como consecuencia de esto, para las autoridades de regulación y supervisión en materia financiera, los temas de protección al usuario han adquirido prioridad en la agenda normativa, impulsada por la adecuación de las prestaciones de servicios a financieros y el mejoramiento de los estándares y marcos normativos en los que se desenvuelve este sector.

Las entidades financieras como prestadoras de servicios y ser representantes de las mejores prácticas, están llamadas a fomentar una cultura de protección. En este contexto, las entidades financieras deben priorizar las políticas y prácticas corporativas relacionadas con la protección al consumidor, y promover una cultura de confianza y protección al consumidor en sus operaciones. Deben contar con recursos y procedimientos especiales diseñados específicamente para proteger al cliente financiero, responder proactivamente a las recomendaciones y orientaciones de los supervisores y otras autoridades en materias relacionadas a proteger a los consumidores de servicios financieros.

La responsabilidad de la entidad financiera con sus clientes es permanente, tanto en el manejo de los servicios y la seguridad de las operaciones, como en la atención oportuna y eficiente de los reclamos que reciben. Por su parte, los consumidores comparten la responsabilidad de una buena relación con las instituciones al comprender sus derechos y obligaciones, asumiendo su deber de cumplir con estos.

Como mecanismo de control para el ejercicio de esta responsabilidad, existen distintos modelos de supervisión, donde el esquema utilizado por los países para atender las

[141] TIMERMANN, B. and GMEHLING, Philipp. Financial inclusion and the G20 agenda. R*egional S*, 2017, pp. 197-200.

necesidades de los usuarios depende de factores que condicionan el alcance de las responsabilidades y facultades del supervisor. Sin importar cuál sea el modelo adoptado, el supervisor tiene bajo su responsabilidad prestar atención a los temas relativos a la protección al consumidor, directa o indirectamente, inclusive en coordinación con otras autoridades.

La supervisión de la integridad del mercado o normas de conducta esta comprometida con la protección del consumidor e inversor, a la vez que asegura la adecuada actuación de los agentes del mercado y promoviendo la transparencia. Algunas veces incluyen por igual el control del blanqueo de capitales[142]. A esta última le queremos dedicar especial atención en los próximos párrafos.

A continuación, nos proponemos analizar el modelo que se ocupa de la supervisión en la República Dominicana, el cual vela por que sean protegidos adecuadamente los usuarios del sistema financiero y dicta las pautas que deben ser observadas por las EF.

A. Rol de la Superintendencia de Bancos

Como efecto de las crisis, el sistema financiero ha tenido que ser ajustado regulatoria e institucionalmente con miras, entre otras cosas, a mantener la estabilidad financiera de la mano de un crecimiento sostenido. En ese sentido, la protección al usuario de servicios financieros tomó una gran relevancia convirtiéndose en uno de los compromisos de la banca para mejorar su seguridad.

La integración de un sistema de protección al consumidor requiere de una serie de acciones a ser realizadas por parte de las entidades financieras, así como por las autoridades gubernamentales. De esta forma se proporcionará un marco regulatorio con instituciones

[142] VILLARROYA, Joaquín Maudos. Observatorio sobre la Integración Financiera en Europa: análisis del caso español 2009. En Observatorio sobre la reforma de los mercados financieros europeos (2010). Madrid: Fundación de Estudios Financieros, 2011. p. 204.

que mejoren el entorno de protección al consumidor financiero y, al mismo tiempo, proporcionen información suficiente, que utilicen contratos transparentes y equilibrados y seguridad en todas las operaciones. Estos factores no solo colaboran con la demostración de compromiso por parte de las instituciones financieras con el usuario, sino que también proporcionan beneficios a las mismas, con lo cual se genera la confianza de todos los involucrados.

El consumidor de servicios financieros es el destinatario de todas las actividades que son realizadas por las EF, por lo que es fundamental que su relación se base en la transparencia, buen trato, protección en sus políticas y que ese sentido esté asumido por parte de la cultura de los directivos, la alta gerencia y los accionistas como un valor de su organización.

Con el propósito de que los clientes financieros cuenten con la debida protección debe contarse con regulación orientada en ese sentido que sea de fácil comprensión y que trate activamente la relación con el consumidor. De esta forma se garantiza una relación de doble vía que fluye armoniosamente.

Parte de la responsabilidad de la autoridad de supervisión es la protección de la estabilidad financiera. A pesar de no tener como mandato la atención de los reclamos de los usuarios, es también su deber fundamental supervisar las condiciones de gobernanza, robustez operativa y gestión de riesgos que relacionados de manera directa en la relación con los consumidores de sus servicios.

Para el supervisor, la prestación de servicios de forma no adecuada puede causar un daño a su reputación, sumando a que compromete la credibilidad de la entidad y genera inconvenientes incluso de carácter financiero.

El modelo de supervisión varía de acuerdo con la necesidad de cada país, influido por una serie de factores como son estrategia, políticas públicas, la existencia de pluralidad de autoridades competentes en la materia, entre otros.

De conformidad con la disposición institucional, se determina la responsabilidad y el alcance legal frente a los clientes financieros. Según la tradición que tenga cada país, se condiciona de manera relevante el entendimiento de los roles que deben tener las instituciones, comprendiendo la participación de sus integrantes: regulador, supervisor, agencia especializada en protección al consumidor, defensoría de protección al consumidor, entre otros similares.

En República Dominicana, con la promulgación de la Ley Monetaria y Financiera no. 183-02 (LMF), se transformó el sistema financiero del país, pasando de un modelo de banca especializada hacia el modelo de banca múltiple, basado en lineamientos internacionales de un mercado financiero global. Con esta norma se inició el proceso de modernización y robustecimiento de la regulación que aplica a las entidades de intermediación financiera, que tiene por objeto velar por el correcto funcionamiento del sistema de acuerdo con los estándares internacionales conocidos como mejores prácticas, incluyendo disposiciones que fomentan la protección de los usuarios del sistema financiero como precedente.

El artículo 19 de la LMF refiere sobre las funciones que tiene la Superintendencia de Bancos que: *debe supervisar las Entidades de Intermediación Financiera (EIF), con el objeto de verificar el cumplimiento por parte de dichas entidades de las disposiciones de la Ley, Reglamentos, Instructivos y Circulares*. Este artículo le otorga *potestad reglamentaria subordinada para desarrollar a través de instructivos y reglamentos relativos a las materias propias de su competencia*.

En la Sección V, sobre transparencia financiera, el artículo 53 sobre la protección al usuario indica que: “Reglamentariamente, la Junta Monetaria determinará los supuestos de

contratos abusivos en relación con los derechos de los consumidores y usuarios de servicios de entidades de intermediación financiera. Las infracciones a las disposiciones de dicho Reglamento serán objeto de sanción administrativa, sin perjuicio de las acciones civiles que correspondan a la parte perjudicada".

El Tercer Pilar de Basilea II, relacionado con la disciplina de mercado, propone una serie de requisitos de divulgación que permitiría a los participantes del mercado evaluar el perfil de riesgo de cada banco y su nivel de capitalización. En relación con esta dirección, la Superintendencia de Bancos ha ampliado los requisitos para la divulgación al público, proporcionando información consolidadas y de entidades individualizadas para brindar más transparencia al Sistema Financiero.

Igualmente, es importante resaltar que la Superintendencia de Bancos (SB) "ha suscrito 19 acuerdos de cooperación internacional, con 17 países del continente americano y con 2 Organismos Multilaterales, que favorecen la cooperación, el intercambio de información y la supervisión de temas prudenciales y de prevención del lavado de activos, como país anfitrión o país de destino, preservando la confidencialidad de la información, de conformidad con las regulaciones impuestas por el marco normativo de cada país suscribiente"[143].

La voluntad de las autoridades en materia monetaria y financiera ha sido conferir a la SB la supervisión de la protección al consumidor, ya que se ha concebido dicha función como actividad que potencia la estabilidad integral del sistema financiero y como un axioma fundamental para mantener el equilibrio de la relación contractual con adecuada prestación de los servicios, transparencia, el suministro de la información y la atención de los reclamos individuales.

[143] ASUNCIÓN ÁLVAREZ, Luis Armando. Evolución de la Supervisión Bancaria en el Sistema Financiero Dominicano. En: *52º Asamblea Anual de la Federación Latinoamericana de Bancos (FELABAN)*. [en línea] República Dominica: Superintendencia de Bancos. 2018 [consulta: 5 de marzo del 2022]. Disponible en: http://felaban.s3-website-us-west-2.amazonaws.com/memorias/archivo20181122180170PM.pdf

En ese sentido, se ha creado la Oficina de Servicios y Protección de los Usuarios Financieros (PROUSUARIO), instituida mediante el Reglamento de Protección al Usuario de los Productos y Servicios Financieros, dictado por la Junta Monetaria el 05 de febrero de 2015 y modificado en 30 de septiembre de 2015[144]. PROUSUARIO es una oficina habilitada permanentemente, como dependencia de la Superintendencia de Bancos que tiene dentro de sus principales obligaciones, atribuidas por la Junta Monetaria, la atención a consultas, denuncias y reclamaciones presentadas por los usuarios en relación con los servicios prestados por las entidades reguladas y supervisadas por la SB. Su misión es "velar por el respeto de los derechos de los usuarios financieros e impulsar su empoderamiento, procurando una relación equitativa y armoniosa entre los usuarios y sus prestadores de servicios financieros".

En el objeto del citado Reglamento quedan establecidos los principios y normas para la protección efectiva de los derechos de los usuarios de los productos y servicios financieros, a través de mecanismos de transparencia, las condiciones de contratación de los productos y servicios financieros, así como los procedimientos para la atención de las reclamaciones de manera oportuna, y las consultas de informaciones financieras, con base en lo dispuesto en los Artículos 30, 52 y 53 de la Ley No.183-02 Monetaria y Financiera, de fecha 21 de noviembre del 2002[145].

Dentro de los derechos que garantiza la protección de PROUSUARIO está el derecho la aplicación de las leyes y que las EF cumplan sus obligaciones con el usuario, donde, entre otras cosas, se puede exigir la protección de la información personal; que los datos que reposen en los registros sean ciertos, exactos y actualizados cuando corresponda; que los

[144] República Dominicana. Junta Monetaria. [en línea] Cuarta Resolución de fecha 30 de septiembre del 2015 emitida por la Junta Monetaria. [consulta: 7 marzo 2022]. Disponible en https://sb.gob.do/sites/default/files/nuevosdocumentos/Proteccion_Al_Usuario_Servicios_Financieros_modificacion.pdf

[145] República Dominicana. Reglamento de Protección al Usuario de los Productos y Servicios Financieros, dictado por Junta Monetaria mediante Primera Resolución de fecha 5 de febrero 2015 y sus modificaciones.

datos total o parcialmente incorrectos sean suprimidos y sustituidos, o, en su caso, completados, y que los datos no sean tratados y divulgados sin autorización de su titular, con excepción de lo que la ley establece como tal[146].

Como medidas tomadas por la autoridad monetaria y financiera para fortalecer la regulación y supervisión, en nuestro país se ha asignado la supervisión a una entidad especializada con capacidad de prestar estos servicios de forma permanente, lo cual le facilita la adopción desde sus funciones de correctivos que correspondan cuando observe inclinaciones que revelen fallas en la gestión o en la infraestructura de las instituciones. En este enfoque, el desempeño operativo en el servicio al cliente se convierte en un insumo esencial para la estrategia supervisora, identificando acciones que los lleven al logro de soluciones mejoradas.

No obstante, cuando se requiere que el supervisor sea responsable de atender quejas y reclamos, se hace evidente que se deben dedicar importantes recursos humanos y técnicos para cumplir con esta función. En este modelo, es importante no comprometer la función principal del supervisor, que es la de garantizar la adecuada administración de los riesgos de las entidades y la estabilidad del sistema.

La Superintendencia de Bancos de República Dominicana ha desarrollado un régimen sancionatorio de carácter general aplicable a la protección del consumidor financiero, cuyo contenido se encuentra en el Reglamento de Sanciones de la Superintendencia de Bancos y en sus respectivas Modificaciones. La agencia encargada de aplicar el régimen es la Superintendencia y las sanciones pueden ser pecuniarias, suspensiones temporales o definitivas, según sea el caso[147].

[146] *Derecho a Protección*. [en línea] Superintendencia de Bancos© [consulta: 7 marzo 2022]. Disponible en: https://sb.gob.do/prousuario/derecho-a-proteccion

[147] República Dominicana. Reglamento de Sanciones, aprobado por la Quinta Resolución dictada por la Junta Monetaria en fecha 18 de diciembre del 2003.

Recientemente, en su calidad de agencia protectora de los datos de las personas, la SB emitió una norma orientada de manera particular al respeto del derecho que tiene el cliente de no ser contactado por las EF sin su consentimiento y, más aún, reconoce el derecho de la persona a revocar el mismo, respetando con ello el Derecho a la intimidad de los usuarios[148].

B. Identificación y verificación de los clientes en el *Onboarding*

Dentro de los retos principales que enfrentan las EF actualmente está la correcta identificación y verificación de los nuevos clientes, proveedores y relacionados que son vinculados de manera no presencial, ya que este proceso debe ser realizado con seguridad y cumpliendo con las normas que regulan el sector. Los supervisores en todo el mundo cada vez dan mayor peso a los controles y los procedimientos que las EF deben tener para conocer tanto a sus clientes existentes como a sus clientes potenciales. Ejercer una debida diligencia es parte fundamental de los controles a estos fines, ya que en caso contrario se corre el riesgo reputacional, operativo, legal y/o de concentración, que se traduciría en un coste financiero relevante.

En ese sentido, cabe preguntarnos: ¿existen riesgos de lavado de dinero o financiamiento del terrorismo que surgen del uso de sistemas de identidad digital para Debida Diligencia de los clientes? El proceso de identificación de clientes es realizado, naturalmente, al inicio de la relación y la EF debe asegurarse de obtener toda la información necesaria para establecer satisfactoriamente la identidad de sus nuevos clientes y la naturaleza de la relación, entre otras informaciones vitales para la permanencia en el tiempo del vínculo.

[148] Protocolo para la protección y uso adecuado de los datos personales de los usuarios. SB: 004-2022 [en línea] Superintendencia de Bancos© [consulta: 1 marzo 2022]. Disponible en: https://www.sb.gob.do/sites/default/files/20220207_Circular-SB-Num-004-22-Establecimiento-de-Protocolo-para-la-Proteccion-y-Uso-Adecuado-de-los-Datos-Personales-de-los-Usuarios.pdf.

Por tal razón, las EF deben realizar las actualizaciones periódicamente, con la finalidad de que sus registros se mantengan actualizados. Cuando el cliente no cuente con una identificación o el mismo insista en mantener el anonimato, no debe ser admitido como cliente, conforme lineamientos del Comité de Basilea sobre la Debida Diligencia con la clientela de los bancos.

La debida diligencia no presencial del cliente no necesariamente representa un mayor nivel de riesgo de lavado de activos, con relación a la debida diligencia presencial, siempre que tenga niveles adecuados de garantía. Nuevamente, la preocupación gira en torno a lo que se considera como adecuado, ya que en las regulaciones de muchos países no han sido incluidas las operaciones no presenciales como la nueva normalidad.

Adaptar las normas y procesos que tradicionalmente se requieren al ambiente virtual ha necesitado apoyarse de soluciones tecnológicas a fin de facilitar estas tareas. Algunas de estas tecnologías son utilizadas en materia de cumplimiento y monitoreo de transacciones para PLAFT[149]. Estas aplicaciones incluyen aspectos relacionados con la identificación de clientes de alto riesgo o individuos o entidades sancionadas internacionalmente. También incluyen sistemas de alertas automáticas y el uso de algoritmos e inteligencia artificial para continuamente evaluar y clasificar el riesgo de los clientes y sus transacciones e identificar actuaciones inusuales o sospechosas de cara al perfil de los clientes[150].

Dentro de los múltiples beneficios que trae la incorporación de estos sistemas podemos indicar que se fortalece la debida diligencia del cliente, ya que con los sistemas de identificación digital se pueden mejorar la confiabilidad, seguridad, privacidad y eficiencia en identificar a las personas. Se minimizan las debilidades en las medidas de control humano. El monitoreo de transacciones puede ser mejorado con ayuda de la identificación

[149] PLAFT son las siglas para Prevención de Lavado de Activos y Financiación del Terrorismo.
[150]GURREA-MARTÍNEZ, Aurelio, REMOLINA LEÓN, Nydia. Fintech, regtech and legaltech: Fundamentos y desafíos regulatorios. *Ob. Cit.* p..221.

de transacciones sospechosas. También favorece la inclusión financiera, ya que permite que las personas sin documento de identidad tradicional obtengan servicio de contar con una identidad digital. Los sistemas de identificación digital pueden llegar a los residentes de áreas remotas para respaldar la prueba o inscripción segura de identidad sin interacción personal o *face to face* para la identificación / verificación del cliente. Los sistemas de identidad digital pueden facilitar los pagos de gobierno a persona (G2P), la aplicación de nóminas salariales y pensiones del gobierno y la asistencia a personas en situaciones de vulnerabilidad, en contextos humanitarios[151].

No obstante, la evolución del sistema financiero ayudada de la implementación de estas nuevas herramientas debe ir aparejada de esquemas robustos de prevención de lavado de activos y financiación de terrorismo que acompañen el objetivo último, que es proteger a la vez que impulsa el sector financiero y la economía. Las vulnerabilidades por el uso no debido de estas herramientas digitales justifican la necesidad de que las transacciones realizadas a través de ellas estén bajo el ojo del regulador y el supervisor.

En algunos países se han incorporado tecnologías que cuentan con mecanismos que mejoran el proceso de identificación de los clientes, tales como implementación de documentos de identidad fehacientes con elementos electrónicos, biométricos y de firma digital, también desarrollo de biometría móvil y portátil, bases de datos biométricos centralizados, sistemas de reconocimiento facial, entre otros que favorecen ampliamente el proceso de *KYC*[152], el cual ha evolucionado, como es natural, al llevarlo de forma digital, para ser conocido ahora como *eKYC*[153].

[151] ¿Qué es la Identidad Digital (ID)? Mesa de Investigación de la Secretaría del GAFIC [en línea] cfatf-gfic.org © [consulta: 8 abril 2022]. Disponible en: https://www.cfatf-gafic.org/es/documentos/rinc%C3%B3n-de-investigaciones/17082-%C2%BFqu%C3%A9-es-la-identidad-digital-id-_nov_2021/file.

[152] *KYC* siglas en ingles de Conozca su Cliente

[153] *eKYC* es el conjunto de controles digitalizados de verificación de identidad de usuarios y clientes. En contraposición a su predecesor, este convierte todo el proceso en *paperless*, es capaz de remotizarlo y automatizar con bots inteligentes tareas que antes eran llevadas a cabo por agentes humanos.

Un ejemplo de estas modalidades que se está aplicando en el país lo tenemos con la novedad que trae ProUsuario Digital donde, por medio de la aplicación web y móvil, se ofrece acceder a la información de los productos financieros de cada persona y los servicios. Para acceder al portal, se debe utilizar el número de cédula de identidad y posteriormente se deben suministrar pruebas fehacientes de la identidad, tales como fotografía del documento de identidad introducido, foto de la persona y reconocimiento facial para acreditar al individuo que interactúa en el portal y al cual se le emiten las credenciales pertinentes que lo habilitan al uso del portal.

Por otra parte, también en el ámbito nacional, la última actualización del Instructivo sobre Debida Diligencia emitido por la SB, incluye la vinculación no presencial o remota en los lineamientos como una novedad normativa. En el numeral 8, da autorización a las entidades para implementar políticas y procedimientos a los fines de vincular los nuevos clientes que sean personas físicas, por medio de canales de distribución no presenciales, siempre que sean aplicados controles en proporción al alto riesgo que supone la modalidad a distancia, o no presencial, asegurando el cumplimiento a las disposiciones establecidas en el instructivo.

En el literal e del referido numeral 8, especifica que la vinculación de forma no presencial o remota debe estar apoyada de sistemas y tecnologías robustas, mediante las cuales se tomen como mínimo las siguientes pautas:

> *i. Facilidad de identificación y verificación de la identidad de los clientes personas físicas, cuando sean vinculados.*
> *ii. Fomenten un adecuado nivel de aseguramiento de autenticación basada en más de un factor e incluyan el uso de tecnología que garantice su efectividad continua.*
> *iii. Apoyen la realización de debida diligencia y monitoreo continuo, incluyendo la detección y evaluación de transacciones inusuales.*
> *iv. Faciliten que sean aplicadas medidas de debida diligencia basada en riesgos.*
> *v. Estén sujetos a revisiones independientes, para asegurar la adecuación y efectividad de los controles involucrados, así como de la efectividad del monitoreo, permanencia y conservación de la información.*

> *vi. Sean establecidos controles adecuados que garanticen que se minimicen los riesgos asociados, teniendo en cuenta la naturaleza, complejidad y perfil de riesgos de los productos y servicios ofrecidos y de los procedimientos asociados.*
> *vii. Fortalecer el aseguramiento de la autenticidad, vigencia, integridad, permanencia y trazabilidad de los documentos de identidad utilizados y la correspondencia del titular del documento con su cliente persona física objeto de la vinculación remota.*

La digitalización del proceso de *onboarding* permite potencialmente a una institución financiera aumentar su alcance en el mercado y cumplir con las regulaciones. Dependiendo del tipo de documento utilizado, la mayoría de los pasos del proceso no digital pueden ser reemplazados por un equivalente digital. La digitalización de los pasos de verificación y cobro representa una ventaja pues reducirá la carga para el funcionario de la institución financiera a cargo. Sin embargo, es importante garantizar el nivel pertinente de seguridad sobre la identidad y autenticidad reclamadas de los documentos proporcionados.

El éxito de cualquier proceso digital requiere la adopción por parte del usuario o del cliente. Un marco regulatorio claro respaldado por tecnología segura puede proporcionar este entorno de confianza. A modo de ejemplo, en abril 2018, la Comisión Europea publicó un estudio sobre documentos electrónicos de identidad (eID) y el establecimiento de relaciones financieras digitales dentro de la Unión Europea. Esta iniciativa lo que busca es promover la digitalización financiera sin que se sacrifique el cumplimiento de las regulaciones de PLAFT, pues en esa jurisdicción se considera que los productos nuevos y nuevas prácticas comerciales, incluyendo los mecanismos para entregar y utilizar las tecnologías nuevas o en vía de desarrollar para productos nuevos o ya existentes, son también factores de mayor riesgo de cara a la PLAFT en función del producto, servicio, transacción o canal utilizado[154]. De hecho, esa es la posición en relación con las transacciones y operaciones no presenciales. Como representan mayores niveles de riesgo requieren que se realice la debida diligencia ampliada, es decir, con otros requisitos y actuaciones según el nivel del riesgo que involucren.

[154] ¿Qué es la Identidad Digital (ID)? Mesa de Investigación de la Secretaría del GAFIC. *Ob. Cit.,* p. 224.

A todas luces, podemos notar la voluntad de los supervisores y reguladores en las distintas regiones, de continuar incorporando la adopción de las nuevas tecnologías para la identificación de los clientes nuevos de manera no presencial. Así se favorece favoreciendo la inclusión financiera y se aprovechan las ventajas que supone el disponer de información de los clientes para ofrecer servicios con una mejor calidad, provistos los mismos de manera ágil y a un costo menor. Los bancos tradicionales tienen que competir con las *Fintech*, cuyo desarrollo es totalmente digital, adaptando sus productos para que las exigencias de los consumidores sean satisfechas en un marco donde no se tenga que sacrificar la protección de los consumidores, de sus datos personales y las exigencias de PLAFT.

Como puede entenderse, la supervisión financiera es un elemento esencial para asegurar el buen funcionamiento del sistema financiero y, con él, de la economía.

El sistema financiero es una recopilación de elementos y agentes que funciona como lo hace un rompecabezas. Cuando una de sus piezas falta, todo el resto se ve afectado. El desafío para los países en general es mantenerse vigilantes en cuanto a las necesidades de su situación jurisdiccional y a la vez que avanzan hacia un esquema de prevención con las garantías de una correcta vigilancia del sistema, en la búsqueda de mitigar o evitar situaciones como las vividas en el pasado y las que pueden traer las nuevas tecnologías.

II. Estándares internacionales en protección de datos

El auge de la transformación digital de las organizaciones, tanto a nivel público como privado y en todos los sectores, tiene un factor crítico de cumplimiento en relación con el respeto a la privacidad de las personas, vinculado con la información personal que procesa su infraestructura, lo cual abarca información de sus clientes, usuarios, colaboradores y ejecutivos, entre otros.

Este requerimiento ha cobrado relevancia en todo el mundo, avalado por leyes o reglamentos, especialmente en el ámbito internacional, relativas a la privacidad o protección de datos personales, obligando a las empresas y organizaciones a que tengan en cuenta lo anterior en sus operaciones, desarrollo e implementación de arquitectura e infraestructura empresarial u organizacional. En los últimos años, los reguladores han coincidido en la urgente necesidad de proteger los datos de carácter personal y la privacidad de los individuos en un mundo donde las fronteras cada vez están más desdibujadas, en particular por la virtualidad, como ya se ha comentado ampliamente en este trabajo, impulsada por la crisis sanitaria.

Para asegurar un alto nivel de protección de los derechos y libertades de las personas físicas, entre otras cosas, es necesario unificar la protección de su información personal, y que atienda a la necesitad y exigencia que actualmente existe a nivel global, con la finalidad de no limitar la libre circulación de los datos personales y, como consecuencia, favorecer las actividades comerciales entre los países.

Con el propósito de facilitar la comprensión y homologación de los conceptos base, las entidades internacionales han ido adoptando medidas relativas a gobernanza y ética en el tratamiento de los datos personales que contribuyan con la armónica relación necesaria para todos los sectores e industrias, muy especialmente para el ámbito financiero.

Un ejemplo de esto es la Organización Internacional de Estandarización (ISO[155]), organización internacional independiente que tiene su asiento en Ginebra, está conformada por 163 entidades nacionales, una por país, y la misma redacta las normas internacionales que son de carácter voluntario, que se basan en el consenso, que sean de relevancia para el mercado, las cuales suministran especificaciones para los productos, servicios y sistemas,

[155] ISO/TC68 es el Comité Técnico de ISO encargado de desarrollar y mantener las normas internacionales que cubren las áreas de banca, valores y otros servicios financieros.

con el propósito de garantizar la calidad, seguridad y eficacia, al mismo tiempo que colabora con las iniciativas de innovación. La ISO ha publicado una serie de estándares que tratan todos esos aspectos con la finalidad de viabilizar el comercio internacional, colaborando con las empresas y organizaciones en cuanto al cumplimiento normativo desde un enfoque técnico neutral y que pueda funcionar en todo tipo de empresas u organizaciones sin importar su tamaño o sector.

En materia de servicios financieros, existen varias entidades o grupos que se dedican a examinar el sector para de esta forma hacer las recomendaciones que entiendan pertinentes, de acuerdo con la realidad que se vive en cada jurisdicción. El Grupo de Acción Financiera Internacional (GAFI, en lo adelante), elaboró una guía de recomendaciones internacionales que nos permitiremos revisar a continuación. También enfocaremos cuál es el estado actual de los estándares que son observados en materia de protección de datos y cómo los países han sorteado la confluencia entre la normativa y la realidad del entorno digital.

A. Tendencias actuales en prevención de lavado

La regulación juega un papel importante en lo relativo a la gestión de los riesgos que tienen que ver con los servicios de identidad digital y es un factor clave para desarrollar correctamente la economía digital, sobre todo en lo referente a servicios financieros. La brecha entre la forma de interactuar del consumidor y el uso de datos personales por parte de la industria, define la necesidad de observar ciertos requisitos para la protección del consumidor más allá de los ámbitos del consentimiento. Por otro lado, la legislación sobre ese consentimiento se ve cada vez más socavada por las expectativas poco realistas puestas en el consumidor para comprender a qué está consintiendo.

A medida que se desarrolla esta tendencia, es necesario disponer de normas que definan la conducta entre los consumidores y las entidades que utilizan sus datos, establecer directrices sobre las mejores prácticas y promover su adopción.

En ese orden, también es necesario para las instituciones resguardar la sanidad del sistema, controlando el movimiento del dinero, tomando conocimiento sobre quién es la persona que pretende acceder a los servicios financieros, conocer el origen de los fondos que pretende manejar por intermediacion de las EIF y el destino de estos. Todo con miras a establecer un procedimiento de diligencia debida para cimentar la confianza que, según nos hemos referido, debe existir entre estas partes, al tiempo que se utilizan las nuevas tecnologías y sus bondades.

El mandato del Grupo de Acción Financiera Internacional[156] (GAFI, en lo adelante) es promover la aplicación efectiva de medidas jurídicas, reglamentarias y operacionales para combatir el blanqueo de dinero, la financiación del terrorismo y la financiación de su propagación, así como otras amenazas conexas a la integridad del sistema financiero internacional. Con la colaboración de otras partes interesadas internacionales, el GAFI también trabaja para identificar vulnerabilidades a nivel nacional que puedan afectar el sistema financiero internacional por uso indebido.

Comúnmente, frente a algo nuevo surgen ciertos miedos y resistencia al cambio por lo desconocido, pero el tiempo y la experiencia han dado paso al reconocimiento de los beneficios del mundo electrónico para la sociedad. El GAFI ha tenido que rectificar su posición, pasando de considerar hace años el entorno digital como un riesgo, a incorporarlo dentro de sus recomendaciones a la industria, al reconocer sus ventajas, motivado por las

[156] El Grupo de Acción Financiera Internacional, es una institución intergubernamental creada en el año 1989 por el entonces G8. El propósito de la GAFI es desarrollar políticas que ayuden a combatir el blanqueo de capitales y la financiación del terrorismo.

soluciones digitales que han masificado los servicios financieros y el volumen de transacciones no vistas antes.

En este sentido, fue elaborada una Guía[157] sobre Identidad Digital, la cual es informativa, no normativa, pues los estándares de GAFI actuales son tecnológicamente neutrales, pero la misma nos sirve para favorecer la implementación de los procesos digitales, sobre todo en el entendimiento de cómo funciona la identidad digital y cómo puede ser utilizada en el marco de normas globales, por parte de los sujetos obligados y los reguladores, para lograr un mejor entendimiento de cómo los individuos se identifican y se verifican en el mercado de servicios financieros digitales. Esta guía se apoya en el uso de las nuevas tecnologías y hace las recomendaciones de lugar.

La referida guía está enfocada en la implementación de la Recomendación 10 (Debida Diligencia del Cliente) para el uso de sistemas de identidad digital para la identificación/verificación en el momento de la aceptación como cliente de una persona bajo la Recomendación 10(a). También examina las capacidades de la identidad digital para respaldar la debida diligencia continua que se incluye en la supervisión de las transacciones, en virtud de la Recomendación 10(d). También se refiere a la aplicación de la Recomendación 17 (Dependencia en terceros) donde se abordan situaciones en las que los sujetos obligados utilizan sistemas de identidad digital para llevar a cabo la identificación/verificación de los clientes a otros sujetos obligados[158].

La guía está diseñada para ser aplicada a personas físicas, excluyendo de sus recomendaciones a los representantes legales de personas jurídicas, ya que para tal proceso deben ser tomadas en consideración otras particularidades que exceden el alcance de este trabajo.

---

[157] *Guidance on Digital Identity*, FATF, París [en línea] FATF©, 2020 [consulta: 1 marzo 2022] Disponible en: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf
[158] ¿Qué es la Identidad Digital (ID)? Mesa de Investigación de la Secretaría del GAFIC. *Ob. Cit*., p. 16.

Prueba de ello es la siguiente declaración que se encuentra en la referida guía de identidad digital, donde se afirma lo siguiente: "*la guía clarifica que la identificación de cliente y transacciones no presenciales que confíen en sistemas de identidad digital fiables, con una apropiada planificación de los riesgos, podrían presentar un nivel de riesgo estándar o incluso un riesgo menor*"[159].

Los siguientes beneficios han sido extraídos de la forma en que se indican en la guía de identidad digital del GAFI:

> *Los sistemas de identidad digital que se basen en alta tecnología y estándares de buen gobierno mantienen la gran promesa de mejorar la confianza, seguridad, privacidad y conveniencia de identificar personas físicas en una gran variedad de escenarios, tales como los servicios financieros, la salud y el gobierno electrónico en la economía global en la era digital. Estos sistemas de identidad digital se refieren a los que cuentan con altos niveles de seguridad*[160].

Con respecto a los estándares GAFI, el uso de sistemas de identidad digital independientes y confiables podrían:

i. Posibilitar la identificación y verificación en el onboarding del cliente. Soportar procesos de diligencia debida en curso y el escrutinio de transacciones a través del curso de las relaciones de negocio.
ii. Viabilizar otras medidas de diligencia debida de cliente.
iii. Apoyar la monitorización de transacciones, con el propósito de detectar y denunciar transacciones sospechosas, además de mejorar la gestión general del riesgo y los esfuerzos en la gestión del fraude.
iv. Los sistemas de identidad digital independientes y confiables contribuyen con la inclusión financiera, habilitando a personas que no han accedido a servicios para

[159] ¿Qué es la Identidad Digital (ID)? Mesa de Investigación de la Secretaría del GAFIC. *Ob. Cit.*
[160] *Guidance on Digital Identity*, FATF. *Ob. Cit.*, p. 13.

probar su identidad oficial en un rango amplio de circunstancias, incluso de forma remota, y así obtener servicios financieros regulados. Incorporar más personas dentro del sector financiero regulado refuerza la lucha en la Prevención de Blanqueo de Capitales y Financiación del Terrorismo (PBCFT).

v. Los sistemas reducir costos potencialmente e incrementan la eficiencia para las entidades reguladas, permitiendo reasignar recursos en otras funciones para la PBCFT.

Contar con estos lineamientos ayuda a realizar una debida diligencia apropiada, simplificando la labor a la hora de supervisar.

Otras recomendaciones extraídas de la guía, importantes de tomar en consideración y aplicar a la hora de implementar relaciones no presenciales con los clientes, son las siguientes[161]:

i. Desarrollar guías y regulaciones claras que permitan fortalecer el uso de sistemas de identidad de forma apropiada y gestionando el riesgo inherente de las mismas. Como punto de partida, entender los sistemas de identidad digital disponibles en cada jurisdicción y cómo pueden encajar en los requerimientos existentes para la identificación y verificación del cliente y procesos de diligencia debida.

ii. Evaluar si las regulaciones existentes son apropiadas en un contexto jurisdiccional y su ecosistema de identificación. Por ejemplo, las autoridades deben considerar que clarificar las relaciones no presenciales y el *onboarding* digital podría presentar un riesgo estándar o incluso menor para procesos de diligencia debida, cuando los sistemas de identidad digital, con niveles de aseguramiento apropiados, son usados para la identificación y verificación remota de clientes.

[161] ¿Qué es la Identidad Digital (ID)? Mesa de Investigación de la Secretaría del GAFIC. *Ob. Cit.* p. 5.

El aporte de mayor impacto que trae esta guía, en nuestra opinión, tiene que ver con el impulso de la incorporación de nuevas tecnologías en los procesos de verificación de identidad. Al ser neutra en el tipo de tecnología a utilizar, presenta lineamientos a ser ajustados en cada jurisdicción. Se destacan los conceptos de independencia y confianza como requerimientos mínimos en las fuentes que alimentan los sistemas de identificación digital, además de que contarse con mecanismos de seguridad robustos y con políticas de privacidad a la par de esta exigencia.

Con esta amplitud en el criterio, queda a discreción de cada regulador el identificar y regular, si lo requiere y de forma precisa, qué documentos son admitidos para este tipo de procesos por el derecho en vigor para esta clase de transacciones en su jurisdicción. En el país se han incoporado gran parte de las recomendaciones dadas en esta guía dentro del ya referido Instructivo de Debida Diligencia recién actualizado.

Revisando la situación que presenta la Unión Europea, para los países miembros el panorama sobre estándares y gobernanza de sus datos respecto a la implementación del uso de identidad digital está avanzando, ahora con la emisión del Reglamento eIDAS[162], el cual crea un marco jurídico transfronterizo para garantizar la interoperabilidad de los sistemas de identificación electrónica en todos los estados miembros de la UE. La meta perseguida es la eliminación de los obstáculos que surjan y que la identificación y sistemas de firmas electrónicas tengan validez tanto para personas físicas como jurídicas. Que estas puedan utilizar su identificación electrónica en cualquier país de la Unión Europea.

En el Reglamento eIDAS se definen estándares así como normas básicas y razonables para la identificación digital, la firma electrónica simple, la firma electrónica avanzada, la firma

[162] Unión Europea. Reglamento (UE) n ° 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 *OJ L 257, 28.8.2014, p. 73–114 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV).* [consulta: 8 marzo 2022]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32014R0910

electrónica cualificada, la emisión de certificados cualificados y los servicios de confianza online. De esta misma manera son reguladas las transacciones electrónicas.

La necesidad de presentarse de manera física en una institución era una condición *sine qua non* para validar la identidad de las personas y luego de esto iniciar con las relaciones comerciales con las garantías de lugar. Mediante la adopción de esta norma, se crea un entorno confiable con las máximas garantías y seguridad, lo cual abre la puerta a nuevos mecanismos para validar la identidad de las personas, en un ambiente digital. Esto, por la necesidad de crear ese entorno confiable dentro de las máximas garantías técnicas que revistan de seguridad este gran paso.

Con el reglamento eIDAS, se evita tener que ir presencialmente a una institución, y permite la actuación directa de manera remota, previo a la obtención de un certificado en una Entidad de Registro, tal y como lo establece el artículo 24, relacionado a los Medios de verificación. Recursos como la identificación por vídeo actúan como solución clave dentro de este marco[163].

Los Estados suscriptores del eIDAS pueden hacer uso de la identidad digital para tener acceso a los servicios en línea. Estos pueden decidir involucrarse con sector privado en el suministro de soluciones de identidad digital. Basados en el principio de reconocimiento mutuo, los Estados miembros están obligados a aceptar los medios de identidad digital notificados de otros Estados miembros siempre que este permitido el uso de la identidad digital para acceder en línea a los servicios públicos. El nivel de garantía de los medios notificados es igual o mayor al que se necesita para acceder al servicio. El Reglamento eIDAS define tres niveles de garantía diferentes (bajo, sustancial y alto) las cuales se clasifican en función del grado de confianza en la identidad declarada o afirmada del individuo.

[163] *Identificación electrónica y servicios de confianza* [en línea] EDICOM.com © [consulta: 8 marzo 2022] Disponible en: https://edicomgroup.es/centro-aprendizaje/reglamento-eidas

El uso de marcos comunes de garantía permite a los Estados miembros de la UE adaptarse a los diferentes requisitos nacionales, tales como la aceptación de diferentes requisitos de documentos y procesos de identidad oficial disponibles a nivel nacional, siempre que los resultados sean de conformidad con los requisitos del marco del eIDAS. Dependiendo del contexto en el que se deba verificar algún aspecto de la prueba de identidad, las fuentes autorizadas pueden tomar varias formas, incluidos registros, documentos y organismos relevantes, entre otras opciones. Las fuentes autorizadas pueden variar en los distintos Estados miembros de la UE incluso en un contexto similar, pero el marco eIDAS permite la armonización y el reconocimiento mutuo.

Es la primera vez en la historia que un reglamento introduce métodos de identificación digital que hace posible a las entidades no requerir la presencia física de sus clientes para operar en una oficina, comercio o instituciones financieras para, por ejemplo, abrir una cuenta bancaria.

De esta forma, sectores regulados como el financiero o el de telecomunicaciones tienen la posibilidad de adquirir clientes en línea en cualquier momento y desde cualquier parte del mundo. El reglamento eIDAS supone un marco de actuación totalmente nuevo en un lenguaje económico común para las operaciones entre empresas y usuarios.

Otro gran hito para el mercado europeo lo constituye la Directiva AML5[164], la cual es una norma comunitaria creada para prevenir el blanqueo de capitales y financiación del terrorismo, precisamente pensada sobre el eIDAS y con la identificación electrónica de base. Dicha Directiva hace un cambio total de este precepto, creando un espacio único digital para identificar los clientes en el sector financiero.

[164] Unión Europea. Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018 (DOUE-L-2018-81022). [consulta: 9 marzo 2022]. Disponible en: https://www.boe.es/doue/2018/156/L00043-00074.pdf

La Directiva AML5 conjuntamente al reglamento eIDAS, forman la creación de un Mercado Único Digital que permite la homogenización de la identificación electrónica en Europa, a la vez que adquiere clientes en línea de forma inmediata.

Con normativas como RGPD, AML5 y el eIDAS, Europa está siendo la primera región a nivel global en relación a la regulación financiera, lo que permite a los negocios aprovechar las oportunidades que trae consigo la innovación en el sistema financiero adoptando marco normativo nuevo en esta materia, que busca modernizar sus disposiciones y garantizar una mayor solidez y coherencia en la salvaguarda efectiva del derecho fundamental a la protección de datos personales en la Unión Europea, generando confianza en la sociedad en general y, facilitando el desarrollo de la economía digital, tanto en las relaciones globales como en las internas. El marco normativo logrado constituye un referente obligado que debe ser emulado por las distintas naciones de Latinoamérica en la elaboración de las legislaciones nacionales de protección de datos.

Las Américas, en ese sentido, están más rezagadas, aunque se reconoce lo importante que es adoptar estas las medidas preventivas que permitan implementar el uso de tecnologías para la identificación electrónica de las personas. Las autoridades de cada jurisdicción hacen uso de sus facultades discrecionales en la emisión de leyes, reglamentos y acuerdos que garanticen el uso de las mismas en sus latitudes, pero los mecanismos y procedimientos para esto difieren y no son aún reconocidos entre países.

Queda como gran tarea pendiente, emular el sistema normativo implementado por la Unión Europea, y quién sabe si en un futuro quizá no muy lejano puedan adoptarse estándares que se homogenicen con el resto de los países. Lo que se busca es hablar un mismo idioma, en el escenario de la economía financiera digital, que amplíe el mercado único digital para llevarlo fuera de Europa y, con ello, los clientes puedan libremente transitar por el sistema monetario que se ajuste a su necesidad, pero no a su conveniencia.

B. Casos de éxito en regulación de identidad digital[165]

En general, los países de América Latina no cuentan con un modelo sofisticado para incorporar un mercado de los servicios financieros único. Por ello, los proveedores y los consumidores deben llegar a ofrecer o comprar productos financieros a distancia y a través de las fronteras, respetando plenamente los requisitos de lucha contra el blanqueo de capitales, y con la seguridad que la protección de sus datos personales será resguardada apropiadamente.

Los cambios tecnológicos permiten la identificación remota a través de nuevas modalidades. Sin embargo, a menudo existen barreras causadas por normas o prácticas divergentes y porque deben tomarse nuevas iniciativas con respecto a la identificación a distancia para ayudarles a ofrecer servicios transfronterizos.

En vista que las prácticas actuales de supervisión y negocio varían mucho en todo el mundo, estaremos revisando cómo en algunos países han podido sortear las dificultades en materia de protección al usuario y debida diligencia, además de enfocarnos en ver cómo han podido incorporar el *Onboarding* digital con las garantías legales apropiadas.

En Argentina, el Estado ha desarrollado un Sistema de Identidad Digital (SID), una plataforma que permite verificar la identidad de forma remota y en tiempo real, mediante autenticación biométrica. Su objetivo primario es disponerla para que todos los ciudadanos

[165] Para la redacción de este apartado, fueron revisados los siguientes documentos: Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, *Study on eID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the EU: executive summary*, [en línea] Publications Office of the European Union, 2018 [consulta: 8 marzo 2022] Disponible en: https://op.europa.eu/en/publication-detail/-/publication/139abc5b-49c6-11e8-be1d01aa75ed71a1/language-en Red Iberoamericana de Protección de Datos. Estándares de Protección de Datos Personales para los Estados Iberoamericanos [en línea] Infoem.org.mx© 2017. [consulta: 8 marzo 2022]. Disponible en: https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf

puedan acceder a servicios y trámites desde cualquier tipo de dispositivo electrónico con conectividad[166].

En ese país, en materia a prevención y lavado de activos, la Unidad de Información Financiera[167] dictó el 26 de diciembre de 2018 la Resolución UIF Nº156/2018163 por medio de la cual fueron efectuadas las modificaciones y se aprobaron los textos ordenados de las Resoluciones UIF No. 30-E/2017, 21/2018 y 28/2018 donde se regulan las medidas de prevención de lavado de activos y financiación del terrorismo que deben implementar los Sujetos Obligados de los sectores financiero, mercado de capitales y seguros, respectivamente.

Esta normativa realizó una modificación de las Resoluciones UIF No. 50/2011 (actualización de datos de registración del Sujeto Obligado y del Oficial de Cumplimiento), 70/2011 (clientes que revisten carácter de Sujetos Obligados) y 67-E/2017 (revisores externos independientes). En consulta con la Comisión Nacional de Valores (CNV), se habilitó la implementación de plataformas tecnológicas a los sujetos obligados en el sector asegurador y de mercado de capitales, que faciliten realizar los trámites de manera remota sin presentación personal de los documentos, aplicando el enfoque basado en riesgos. Marzo de 2018 (28/2018 y 21/2018)[168].

En el caso de Colombia, el Gobierno lanzó en noviembre de 2020 la nueva cédula digital, y desde el 01 de diciembre los colombianos que quisieran utilizar este instrumento de

[166] SID- Sistema de Identidad Digital. Validación remota de identidad en tiempo real con el Renaper mediante factores de autenticación biométrica (reconocimiento facial) y fotografía del DNI. [en línea] Argentina.gob.ar [consulta: 9 marzo 2022] Disponible en: https://www.argentina.gob.ar/interior/renaper/sid-sistema-de-identidad-digital

[167] Organismo encargado del análisis, tratamiento y transmisión de información para prevenir e impedir el Lavado de Activos y la Financiación del Terrorismo.

168 Nueva Resolución UIF que actualiza el marco normativo en materia de PLA/FT [en línea] Argentina.gob.ar [consulta: 9 marzo 2022] Disponible en: https://www.argentina.gob.ar/noticias/nueva-resolucion-uif-que-actualiza-el-marco-normativo-en-materia-de-plaft

identificación nuevo lo pueden solicitar para después utilizarlo desde cualquier *smartphone*.

Se da prioridad a la protección de los datos, evitando que se suplante la identidad por medio de un método de encriptación de la información con cerca de 20 elementos de seguridad que garantizarán la fidelidad de esta nueva forma de identificarse, sin desplazar definitivamente el documento tradicional de identidad. Se prevé que más de 125 entidades nacionales se vincularán a este servicio[169].

En materia de PLAFT, fue emitida la Circular Externa 027 de septiembre de 2020 de la Superintendencia Financiera de Colombia que instruye con relación a la administración del riesgo de lavado de activos y la financiación del terrorismo. Quedó establecido que las entidades financieras puedan realizar procedimientos de conozca su cliente de manera presencial o no presencial a través del uso de canales digitales o electrónicos. La norma permite que las entidades puedan obtener la información necesaria para realizar los procedimientos de conocimiento del cliente utilizando datos e información de fuentes confiables e independientes[170].

México, pionero en la legislación sobre *Fintech* en América que allí fue emitida en 2018, ya había tardado en dotar de identidad digital a su población. Conscientes en el momento del aumento de los casos de robo de identidad en el país, las autoridades emitieron medidas para mitigar tales preocupaciones al tiempo que cumplían con las recomendaciones del GAFI para conocer a su cliente. Las medidas emitidas incluyeron las reglas detalladas con respecto al uso de la biometría, impulsando a las entidades reguladas a buscar soluciones

[169] Identidad digital en Colombia. [en línea] InLegis © 2020. [consulta: 9 marzo 2022] Disponible en: https://blog.inlegis.com.co/2020/11/30/identidad-digital-en-colombia/

[170] Superintendencia Financiera de Colombia. Circular Externa 027 de Septiembre 2020 [en línea] Deloitte.com © [consulta: 8 marzo 2022]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/legal/Legal/2020/octubre/primerasemana/Superintendencia%20de%20Sociedades%20-%20Circular%20Externa%20No.%20027%20del%202%20de%20septiembre%20de%202020%20(2).pdf

adecuadas en el mercado de identificación digital, que cumpla con los requisitos reglamentarios de Conozca a su Cliente.

Finalmente, en diciembre 2020 fue aprobada la modificación de la Ley General de Población, donde se crea la Cédula Única de Identidad Digital para los ciudadanos mexicanos, gratuita y expedida por la Secretaría de Gobernación, y constituye el documento de identificación oficial ante todas las autoridades para todo tipo de trámite o servicio[171].

Anteriormente, la Comisión Nacional Bancaria y de Valores (CNBV), emitió facilidades regulatorias en materia de identificación no presencial para instituciones de crédito, permitiendo la apertura de cuentas y el otorgamiento de créditos de forma no presencial. Para los no clientes refuerzan la identificación y permiten el *onboarding* digital a través de videoconferencia[172].

El Registro Nacional de Identificación y Estado Civil (RENIEC), es el utilizado en el Perú como sistema de identidad digital nacional. Brinda servicios de identidad digital a muchas entidades públicas y privadas de diferentes sectores, para facilitarle la agilización en la verificación y autenticación de la identidad de las personas, así como mejorar la prestación de servicios. En el sector financiero, el RENIEC actúa como sistema central para realizar la identificación/verificación de los clientes, en cumplimiento de los requisitos de Debida Diligencia para la plataforma de dinero electrónico y dinero móvil de Perú, Billetera Móvil (BiM), lanzada en febrero de 2016, y que proporciona servicios como son la entrada y

[171] México. Aprueba Cámara de Diputados expedir la Ley General de Población [en línea] Boletín No. 5513, diciembre 3, 2020. [consulta: 9 marzo 2022]. Disponible en: https://comunicacionnoticias.diputados.gob.mx/comunicacion/index.php/boletines/aprueba-camara-de-diputados-expedir-la-ley-general-de-poblacion#gsc.tab=0

[172] Comisión Nacional Bancaria y de Valores (CNBV). Facilidades regulatorias en materia de identificación no presencial para instituciones de crédito. [en línea] México: Secretaría de Hacienda y Crédito Público, 21 de junio 2020. [consulta: 8 marzo 2022]. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/558905/Comunicado_de_Prensa_045_Flexibilizaciones_Onboarding_Remoto_Bancos.pdf

salida de efectivo en los agentes, la comprobación de saldos, realización de pagos P2P y recargas de crédito a millones de clientes[173].

En el caso chileno, la Ley no.21.180 fomenta que el ciclo completo de los procedimientos administrativos los órganos de la Administración del Estado que estén sujetos a Ley de Bases de Procedimiento Administrativo sean realizados en formato electrónico. Esto permitirá una mayor certidumbre, seguridad y rapidez en la prestación de los servicios a las personas, junto con una mayor transparencia de los procesos y actuaciones del Estado en su relación con los ciudadanos. Los órganos de la Administración tendrán la obligación de disponer y hacer uso adecuado de plataformas electrónicas para los efectos de tener los expedientes en formato electrónicos, cumpliendo en todo momento con estándares de seguridad, interoperabilidad, interconexión y ciberseguridad[174].

[173] NABALÓN Iván, HERRERA, Diego, VADILLO, Sonia. Onboarding Digital. *Ob. Cit.* p.7.
[174] Chile. Reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en la Ley Nº 21.180 sobre transformación digital del estado. Diario Oficial de la República. Noviembre 2020. [consulta: 9 marzo 2022. Disponible en: https://www.diariooficial.interior.gob.cl/publicaciones/2021/12/11/43125/01/2055208.pdf

CONCLUSIÓN

CONCLUSIÓN

A lo largo de estas páginas, hemos recorrido parte de la evolución que han tenido los mercados financieros de cara a la incorporación de la tecnología como bastón para su mejora evolutiva. Cada vez que el sistema ha sufrido una disrupción, hemos visto cómo esto se traduce en un avance que ha servido de catapulta hacia el futuro.

Innegablemente, constituye toda una revolución el hecho de abandonar la analogía para migrar hacia lo digital, ante la necesidad de buscar constantemente canales alternativos, para accesos a servicios no presenciales que permitan a los consumidores disponer de las ventajas ofrecidas por la tecnología en cuanto a sistemas de pago, o en la obtención de todo tipo de productos y servicios financieros. Aquí surge una realidad vigorosa, pujante, que nos obliga a subirnos en el tren de la transformación digital de nuestra propia identidad: hacer el cambio desde el plástico hacia una identidad digital para acceder a los servicios financieros.

Los componentes que ayudan a configurar la identidad digital son los de identidad individual inherentes a la persona, los atribuidos por terceras partes y los que la propia persona va configurando para identificarse en un el ambiente digital. La construcción de la identidad digital hace la distinción entre la información revelada por la persona y las acciones que esta realiza. Nada distinto del mundo análogo, la diferencia reside en el potencial que esto otorga a la tecnología, generando cuestiones importantes sobre la privacidad y la seguridad, pues en este nuevo entorno para poder gestionar correctamente la identidad digital se deben gestionar estos dos temas. Toda la actividad de las personas en el mundo digital es susceptible de ir creando su propia identidad digital, de manera consciente o inconsciente.

Toda persona puede tener acceso a una identidad digital única e irrepetible, compuesta de su información y sus atributos personales, siempre que exista un mecamismo para dotarla de la misma.

Como hemos ampliamente revisado a lo largo de este trabajo, los sistemas de identidad digital suponen una grandes beneficios para el sistema financiero, pues tienen el potencial de mejorar la confiabilidad, la seguridad, la privacidad y la conveniencia. La digitalización del sistema financiero tiene numerosas ventajas para las instituciones financieras: simplificación de los procesos operativos, reducción de errores humanos en procesos manuales de control, ahorro de costos, y mejoramiento del monitoreo de las transacciones, al tiempo que facilita el acceso a una base de clientes más amplia, todo lo que contribuye directamente con la inclusión financiera de los sectores más vulnerables de la población. Para los consumidores financieros es indudable que la digitalización puede reportar enormes ventajas, permitiendo el acceso a servicios financieros en cualquier momento, desde cualquier lugar.

La migración de la identidad análoga a la identidad digital es hoy una necesidad imperiosa y los gobiernos no son ajenos a esto. Por consiguiente, muchos países han encaminado sus esfuerzos y ya están recogiendo frutos, tal y como revisamos en este trabajo. Para el caso que nos ocupa, hay que reconocer que nuestro país no se encuentra actualmente en condiciones de dar entrada a un proyecto de incorporación de identidad digital con el manejo ordinario que se lleva a cabo hoy día para dotar a la población de identificación, condicionante que se suma al panorama regulatorio que presentamos, por lo que es conveniente avanzar en estrategias adecuadas y oportunas para encaminar su desarrollo y posterior implementación.

La recomendación que a partir de lo explicado en este trabajo se propone, es que esta iniciativa esté impulsada desde los organismos del Estado pertinentes, y tal y como en otros países se ha tenido la experiencia, se logre dotar a toda la población de una identidad digital

única habilitadora para el desarrollo de la vida ordinaria en ambiente digital. Estas iniciativas deben estar orientadas a que todo ciudadano migre de una identidad análoga a la digital y, además, el que no tenga a la fecha una identidad, que pueda acceder a la misma. De hecho, disponer de una identidad sin tanta barrera debe ser parte de la meta de un proyecto como este.

Como posible estrategia, se propone, desde nuestra opinión, la realización de un levantamiento de toda la población del país, tanto del que tiene identidad como del que no la tiene, para que se trabaje en la inscripción de la persona en los registros nacionales a la par del interés de regularizar su situación, siempre que sean respetados los principios constitucionales bajo los cuales se rige nuestro país.

La identidad es un derecho fundamental de todo ser humano y en tal sentido este servicio debe ser prestado gratuitamente. Las instituciones proveedoras del servicio de identidad pueden ser financiadas combinando los recursos que provienen del presupuesto nacional y, por ejemplo, los obtenidos de la venta de servicios, como pueden ser los que se ofrecen en la actualidad a empresas del sector financiero y otras. También, pueden obtenerse destinando un porcentaje de las partidas que se cobran a servicios que son obligatorios para los ciudadanos como, por ejemplo, las tasas cobradas por la expedición de actas del estado civil.

Las políticas de inclusión financiera y educación constituyen una herramienta valiosa que promueve el crecimiento económico y la equidad social, lo que ha sido evaluado por los gobiernos a nivel mundial en el contexto de estabilidad financiera.

Un tema que no puede ser pasado por alto en este contexto es que nuestro país, como en otros de la región, el nivel de alfabetización digital es bajo, por lo que educar a la población en torno a la utilización de estos mecanismos nuevos y desconocidos resulta en una necesidad obligada. Es por esto precisamente que el mecanismo a utilizar debe ser

amigable al usuario. Un ejemplo de mecanismo de fácil uso implementado en otros países es la utilización de biometría en la comprobación de identidad, que en nuestro caso puede ser una opción viable. Esto último debe ser tomado en consideración para el diseño del documento mediante el cual se dotaría la población de su *eID*.

Instituciones como la Junta Central Electoral, el Banco Central y la Superintendencia de Bancos, desempeñan un papel fundamental en los programas de educación, tanto en lo referente a la identificación personal como en su uso en el sistema financiero, ya sea como miembros o como líderes de los comités organizadores de este proyecto. En la mayor parte de los países que revisamos en este trabajo, los bancos centrales son los principales promotores de los programas de educación financiera en la región. Para dichos fines, entre las características de estos programas, las entidades financieras hacen acuerdos de participación o coordinación con otros sectores para implementarlos con un nivel de desarrollo bastante diverso, ya que se han aplicado diversas metodologías de evaluación, además de contar con contenido y programas variados y numerosos. Para nuestro país sería vital que así se hiciera aquí también.

Difícilmente se pueden desarrollar actuaciones dirigidas a mejorar las habilidades digitales si previamente no se tiene la educación continuada que ayude a construir un uso adecuado y sostenido, además de contar con acceso a los recursos tecnológicos necesarios.

En este sentido, las campañas de concientización son esenciales para mantener informada a los ciudadanos con relación a lo que es y lo que se debería esperar de la identidad digital, explicando claramente los beneficios que supone y de qué forma se disfrutará de la misma. Estas campañas deben ser constantes y periódicas, compuestas por cursos de alfabetización digital, cuyo contenido tenga facilidad de comprensión para adultos mayores y persona con poca educación escolar; cursos de comportamiento seguro en Internet y uso seguro de dispositivos inteligentes; así como colaboración e incentivo de actividades

extracurriculares relativas a la informática para niños y jóvenes en edad escolar, quienes a su vez pueden replicar el conocimiento en sus entornos.

Otra propuesta es que se realice un análisis integral de toda la normativa dispersa, para robustecer una estructura legal que permita la entrada de la identidad digital y de esta forma desarrollar un proyecto de envergadura similar a los que hemos revisado, que comprenda también el método para su implementación. Por otra parte, debe crearse un paquete normativo especial para apoyar este tipo de iniciativas, aunque resultará más compleja esta parte, dado que se requiere para ello de regulación con alcance internacional, cuya aprobación y coordinación puede ser más difícil y tomar mayor tiempo.

En igual propósito, es recomendable dividir en etapas lo anterior: etapa de creación o construcción de la identidad y etapa de uso de la identidad. Cada etapa presenta sus particularidades y demanda diferentes esfuerzos dentro de los actuales marcos normativos y los pendientes de desarrollar. En atención prioritaria a la privacidad, en estos marcos debe garantizarse el control de la persona sobre sus datos y la libre disposición de la identidad digital en cualquier entorno, indistintamente se trate del sistema de salud, el sistema educativo o, en el caso que nos ocupa, el sistema financiero.

Tal como ha se demostrado con la pandemia, nos queda claro que la peor política es no tenerla, sobre todo en el caso del acceso a los servicios financieros, dado que, según la experiencia recién vivida, los bancos se vieron obligados a acelerar sus procesos de transformación digital, a veces forzando procedimientos a un contexto sin marco legal definido del cual no se tenía experiencia previa en cuanto a cómo resultaría, siendo este sector, con sus estrictas regulaciones, el más descubierto regulatoriamente en temas de innovación y uso de nuevas tecnologías, por lo ya explicado sobre las crisis y las vulnerabilidades que podía representar su incorporación.

Por último, es pertinente señalar los retos y desafíos que plantea la adopción de la identidad digital, pues los riesgos asociados a la incorporación de un sistema de identidad digital son innegables; sin embargo, pueden ser mitigados con las acciones orientadas en varios sentidos. Desde la perspectiva de los riesgos, hemos identificado cuatro grandes retos principales asociados a la adopción de la identidad digital como mecanismo habilitador de los servicios financieros provistos digitalmente.

Primero tenemos el normativo; segundo, el de protección de datos; tercero, el de seguridad de los sistemas o ciberseguridad y, por último, el de lavado de activos.

En el primer aspecto, las potenciales políticas deben ser neutras tecnológicamente, pues la rápida obsolescencia de las nuevas tecnologías haría que queden desfasadas pronto, quedándonos con un marco regulatorio no aplicable a la novedad que traerán los tiempos.

En segundo lugar, en relación con la protección de datos, las EF manejan diariamente una gran cantidad de datos personales de sus clientes, sujetos a requerimientos muy exigentes en materia de protección de datos, el manejo de su privacidad y la seguridad de la información. Aunque el uso de las tecnologías para el manejo, tratamiento y almacenamiento de la información representa la simplificación de los procesos, la obligación que tienen las EF en relación con el tratamiento de los datos obtenidos de sus clientes requiere que cuenten con sus políticas internas y controles robustos sobre tratamiento adecuado de manejo de datos en procura constante del cumplimiento de la normativa aplicable. Esto impone la necesidad de una regulación clara, que en muchos países aún no existe y en el nuestro es urgente su modificación, lo que representa otro desafío en términos de incorporación digital. En el caso de la prestación de servicios por parte de terceros, es necesario establecer procedimientos que permitan la supervisión de las tareas realizadas por ellos y atribuir de forma clara las responsabilidades de cada una de las partes. Este tipo de relaciones contractuales también debe definirse de manera simple en la regulación correspondiente.

Tercero, en cuanto a la ciberseguridad, es necesario que los procedimientos utilizados para el abordaje de los clientes sean cumplidos con altos estándares internacionales en términos de prevención frente a ciberataques, protección de la información y manejo de los datos de los clientes, de acuerdo con las respectivas legislaciones nacionales.

Cabe dimensionar aquí un tema importante para tener en cuenta en la estructuración de un marco para la identidad digital y es el principio de proporcionalidad ya que, comúnmente a mayor seguridad empleada en un mecanismo de identificación, más complejo resulta de utilizar. Por esto debe buscarse un punto de equilibrio entre la seguridad y la usabilidad donde el nivel de seguridad exigida sea el que corresponda adecuadamente a la naturaleza del servicio y de la información que se maneja.

Finalmente, en lo referente a lavado de activos, el rol del supervisor de cara a esta nueva realidad es mantenerse en la misma sintonía de los expertos en esta materia a nivel internacional, incorporando sus sugerencias y mejores prácticas a los procedimientos de debida diligencia de clientes para identificar al titular real y al beneficiario de las operaciones, aun en el mundo digital. Asimismo, los procesos a utilizar deben estar orientados a prevenir conductas fraudulentas o el uso de la relación comercial del cliente y el banco en el uso de fines delictivos.

¿Alguna vez se ha detenido a analizar la función mecánica de una puerta? A veces, por razones de facilidad en su utilización, abren hacia adentro, de modo tal que se logra dar una cálida bienvenida al visitante; otras, por temas de seguridad, cierran hacia afuera, para facilitar la salida, por ejemplo, en caso de incendios. Otras, más sofisticadas, pensando en la accesibilidad, abren y cierran de forma automática e inclusiva, pensando en personas con alguna discapacidad. De modo similar, también el sistema financiero se puede beneficiar de sistemas automatizados de apertura, junto a mecanismos de identificación

biométrica y sin contacto, garantizando estándares de bioseguridad, un aspecto muy preciado en la actualidad.

La identidad digital, en nuestra opinión, es la llave que abre con seguridad la puerta que permite el acceso a la inclusión hacia los servicios financieros digitales. Esperamos que en un futuro no muy lejano nuestro país pueda disponer de los mecanismos para su desarrollo y uso, para asumirlos como elementos necesarios en la construcción de un ecosistema financiero confiable, sostenible e inclusivo.

Nos queda la tarea pendiente de que, como ciudadanos, Estado, reguladores, instituciones financieras, sociedad, nos aseguremos de que, una vez alcanzado este nuevo hito en la historia evolutiva de los mercados financieros, quienes utilicen esa llave en mano lo hagan bajo la protección que brindarán los marcos normativos para, de esta forma, permanecer y prosperar financieramente.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

LIBROS Y SIMILARES

CARNÉ M, Guillermo. La evolución y digitalización del sector bancario. Abril 2020.

HALL, Stuart y DU GAY, Paul (eds.). Questions of cultural identity. Traducción de Natalia Fortuny. Londres: Sage Publications, 1996

MOLINA QUIROGA, Eduardo. Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material. *Id SAIJ: DACC030027*, 2003

OTEYZA, Alejandra Kindelán; DE MESA GÁRATE, Lara; MUÑOZ, María Vera. La supervisión financiera: funciones, modelos existentes y retos planteados por la crisis. La reforma europea. En *Observatorio sobre la reforma de los mercados financieros europeos (2009)*. Fundación de Estudios Financieros, 2010. ISBN 978-84-613-7661-2.

PALAZZI, Pablo Andrés. La transmisión internacional de datos personales y la protección de la privacidad. Buenos Aires: AD-HOC, 2002. ISBN: 950-894-318-1

PRATS, Eduardo Jorge; CONTRERAS, Omar Victoria. *Derecho de la regulación monetaria y financiera*. Santo Domingo: Ius Novum, 2012. *ISBN 978-9945-8648-6-1*.

SULLIVAN, Clare. *Digital Identity: an emergent legal concept*. Australia: University of Adelaide Press, 2011. ISBN 978-0-9807230-2-7. Disponible en: http://ssrn.com/abstract=1803920

VILLARROYA, Joaquín Maudos. Observatorio sobre la Integración Financiera en Europa: análisis del caso español 2009. En Observatorio sobre la reforma de los mercados financieros europeos (2010). Madrid: Fundación de Estudios Financieros, 2011.

ZUNZUNEGUI, Fernando. *Derecho del mercado financiero*. Madrid-Barcelona: Marcial Pons, 2005.

PUBLICACIONES SERIADAS EN LÍNEA

ALLENDE LÓPEZ, Marcos. Identidad digital auto - gestionada: El futuro de la identidad digital: auto-gestión, billeteras digitales y blockchain [en línea] BID© [consulta: 13 febrero 2022] Disponible en: https://publications.iadb.org/publications/spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf

ASOBANCARIA. La identidad digital: el camino para impulsar la inclusión financiera [en línea] *Semana Económica*, 2017. Edición 1096 [consulta: 3 enero 2022] Disponible en: https://www.asobancaria.com/wp-content/uploads/2018/02/1096.pdf

ASUNCIÓN ÁLVAREZ, Luis Armando. Evolución de la Supervisión Bancaria en el Sistema Financiero Dominicano. En: *52º Asamblea Anual de la Federación Latinoamericana de Bancos (FELABAN).* [en línea] República Dominica: Superintendencia de Bancos. 2018 [consulta: 5 de marzo del 2022]. Disponible en: http://felaban.s3-website-us-west-2.amazonaws.com/memorias/archivo20181122180170PM.pdf

BLANCO BARÓN, Constanza. La información como instrumento de protección de los consumidores, los consumidores financieros y los inversionistas consumidores [en línea] Opinión Jurídica, 2012. 11(21); 135-152 [consulta: 27 febrero 2022] Disponible en: https://revistas.udem.edu.co/index.php/opinion/article/view/532/481

BRITO, Steve, et al. El registro de nacimientos: La llave para la inclusión social en América Latina y el Caribe. [en línea] BID © 2013 [consulta: 14 febrero 2022] Disponible en: https://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=37787072&pubDetail

CAMILO, Constantino, et. al. Digitalización del sector financiero español: impacto en la eficiencia y casos de estudio. [en línea] Trabajo fin de máster. Madrid: Colegio Universitario de Estudios Financieros [consulta: 12 febrero 2022]. Disponible en: https://biblioteca.cunef.edu/files/documentos/TFM_Camilo_Constantino,_Eva_Martinez,_Claudia_Rabal,_Zheng_Zhang.pdf.

CHEN MOK, Susan. Privacidad y protección de datos: un análisis de legislación comparada. [en línea] *Diálogos Revista Electrónica de Historia*, 2010, vol. 11, no 1, p. 111-152. [consulta: 27 febrero 2022] Disponible en: https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1409-469X2010000100004

DE OLLOQUI, Fernando; ANDRADE, Gabriela; HERRERA, Diego. Inclusión financiera en América Latina y el Caribe. [en línea] *Documento para discusión Nº IDB-DP-385,* 2015 [consulta: 29 enero 2022] Disponible en: https://publications.iadb.org/publications/spanish/document/Inclusi%C3%B3n-financiera-en-Am%C3%A9rica-Latina-y-el-Caribe-Coyuntura-actual-y-desaf%C3%ADos-para-los-pr%C3%B3ximos-a%C3%B1os.pdf

GAMERO, Ruth. La configuración de la identidad digital [en línea] Nota Enter-IE 131, junio 2009 [consulta: 29 enero 2022] Disponible en: https://cursa.ihmc.us/rid=1H8FQCJ5D-R3NH13-47X/acerca_de_la_identidad_digital.pdf

GEORGES, Fanny. Who are you doing? Declarative, Acting and Calculated Identity in web 2.0. [en línea] En *VRIC 2009, Laval Virtual, Virtual Reality International Conference, 22-26 Avril 2009*. 2009, pp. 1-6. [consulta: 29 enero 2022]. Disponible en https://archivesic.ccsd.cnrs.fr/sic_00496816.

MCWATERS, R. J., et al. *A blueprint for digital identity the role of financial institutions in building digital identity.* [en línea] World Economic Forum, Future of Financial Services Series. 2016, pp. 1-108. [consulta: 2 febrero 2022] Disponible en: https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/WEF_A_Blueprint_for_Digital_Identity_0.pdf

NABALÓN, Iván. La identificación electrónica: redefiniendo las reglas del sector financiero [en línea] *Papeles de Economía Española,* No. 162, 2019, pp. 162-176. [consulta: 29 enero 2022] Disponible en: https://www.funcas.es/wp-content/uploads/Migracion/Articulos/FUNCAS_PEE/162art13.pdf

PAREJA, Alejandro, et. al. La gestión de la identidad y su impacto en la economía digital. *Documento para Discusión núm. IDB-DP-529.* [en línea] Banco Interamericano de Desarrollo © [consulta: 4 enero 2022] Disponible en: https://publications.iadb.org/publications/spanish/document/La-gesti%C3%B3n-de-la-identidad-y-su-impacto-en-la-econom%C3%ADa-digital.pdf

SANTAMARÍA RAMOS, Francisco J. Identidad y reputación digital. Visión española de un fenómeno global [en línea] *Ambiente Jurídico*, Núm.17, 2015 [consulta: 3 enero 2022] Disponible en: https://revistasum.umanizales.edu.co/ojs/index.php/Ambientejuridico/article/view/1570

TAYLOR, Michael. *"Twin Peaks": A Regulatory Structure for the New Century*. [en línea] London: Centre for the study of financial innovation, 1995. [consulta: 8 marzo 2022]. Disponible en: https://static1.squarespace.com/static/54d620fce4b049bf4cd5be9b/t/55241159e4b0c8f3afe1d11e/1428427097907/Twin+Peaks+A+regulatory+structure+for+the+new+century.pdf

URIARTE, Mikel. El tratamiento de datos personales en la determinación del riesgo. [en línea] En foco 134. ISSN 0717-9987, p. 12 [consulta: 1 marzo 2022]. Disponible en: http://www.expansiva.cl/media/en_foco/documentos/15042009150104.pdf

SITIOS WEB

ALAMEDA, Teresa y ÁLVAREZ, Carmen. Más allá de la norma: el compromiso de la banca con la seguridad de los datos [en línea] BBVA.com. 2018 [consulta: 25 febrero 2022] Disponible en: https://www.bbva.com/es/mas-alla-norma-compromiso-banca-seguridad-datos/

ALLEN, Christopher. El camino hacia la identidad autosoberana [en línea] Blog sobre software social. Abril, 25, 2016 [consulta: 26 enero 2002]. Disponible en http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Banco de Inglaterra pone más fácil a las 'startups fintech' [en línea] BBVA.com© [consulta: 11 febrero 2022]. Disponible en: https://www.bbva.com/es/banco-inglaterra-pone-mas-facil-startups-fintech/

CHOMCZYK, Andrés. Regulación de blockchain e identidad digital en América Latina [en línea] BID© 2020 [consulta: 15 febrero 2022]. Disponible en http://dx.doi.org/10.18235/0002935

Ciberseguridad una guía completa del concepto, tipos, amenazas y estrategias. [en línea] INFOSECURITY México© [consulta: 1 marzo 2022]. Disponible en https://www.infosecuritymexico.com/es/ciberseguridad.html.

Cinco Días. Un nuevo modelo de supervisión que no debería retrasarse sine die. [en línea] elpaís.com© [consulta: 8 marzo 2022] Disponible en: https://cincodias.elpais.com/cincodias/2020/12/04/opinion/1607113967_011149.html

Convención sobre los Derechos del Niño [en línea] unicef.es © 2006. [consulta: 4 enero 2022]. Disponible en: https://www.unicef.es/sites/unicef.es/files/comunicacion/ConvencionsobrelosDerechosdelNino_0.pdf

Curso de Ciberseguridad [en línea] EDX© [consulta: 1 marzo 2022]. Disponible en: https://www.edx.org/es/aprende/ciberseguridad

Dato de carácter personal [en línea] Diccionario Panhispánico del Español Jurídico [consulta: 25 febrero 2022]. Disponible en: https://dpej.rae.es/lema/dato-de-carácter-personal

DE LA PUENTE, Carlos. La identidad ¿Por qué es importante en el mundo de hoy? [en línea] Universidad del Pacifico © [consulta: 29 enero 2022]. Disponible en http://www.saberescompartidos.pe/wpcontent/uploads/2012/07/la_identidad_por_que_es_importante_en_el_mundo_de_hoy.pdf

Derecho a Protección. [en línea] Superintendencia de Bancos© [consulta: 7 marzo 2022]. Disponible en: https://sb.gob.do/prousuario/derecho-a-proteccion

Digitalización, ¿cómo está cambiando la industria bancaria? [en línea] elEconomista.es ©. [consulta: 10 febrero 2022] Disponible en: https://marcas.eleconomista.es/hablemos-de-futuro/noticias/10824077/10/20/Digitalizacion-como-esta-cambiando-la-industria-bancaria.html.

Esta es la historia de la sociedad digital más avanzada del mundo [en línea] e-Estonia © [consulta: 11 enero 2022] Disponible en: https://e-estonia.com/story/

Estonia lleva otorgadas 12.000 residencias digitales [en línea] e-Estonia © [consulta: 11 enero 2022. Disponible en: https://e-estonia.com/e-residents/about/.

FIGUEREO, Julia. Senadores concluyen estudios del proyecto de Ley sobre Gestión de Ciberseguridad [en línea] Senado de la República© [consulta: 1 marzo 2022] Disponible en https://www.senadord.gob.do/senadores-concluyen-estudio-del-proyecto-de-ley-sobre-gestion-de-ciberseguridad/

FORBES. «*Blueprint for a Modernizad Financial Regulatory Structure*». Tesoro de Estados Unidos, marzo 2008. [en línea] Forbes.com © [consulta: 8 marzo 2022]. Disponible en: https://www.forbes.com/2008/03/31/paulson-financial-regulation-oped-cx_0331paulsonspeechtext.html?sh=cd049de6321e

G20 Digital Identity Onboarding [en línea] The World Bank Group ©2018 [consulta: 15 febrero 2022] Disponible en: https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

Grupo de Trabajo de Banca Abierta [en línea] Euro Banking Association © [consulta: 8 febrero 2022]. Disponible en: https://www.abe-eba.eu/thought-leadership-innovation/open-banking-working-group/.

Guidance on Digital Identity, FATF, París [en línea] FATF©, 2020 [consulta: 1 marzo 2022] Disponible en: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf

How America Banks: Household use of Banking and Financial Service [en línea] Federal Deposite Insurace Corporation. 2017 [consulta: 14 febrero 2022] Disponible en: https://www.fdic.gov/householdsurvey

Identidad [en línea] Diccionario Panhispánico del Español Jurídico. [consulta: 3 enero 2022] Disponible en: https://dpej.rae.es/lema/identidad.

Identidad [en línea] Real Academia Española© [consulta: 3 enero 2022]. Disponible en https://dle.rae.es/identidad.

Identidad digital en Colombia. [en línea] InLegis © 2020. [consulta: 9 marzo 2022] Disponible en: https://blog.inlegis.com.co/2020/11/30/identidad-digital-en-colombia/

Identidad Digital: El nuevo usuario en el mundo digital [en línea] © Fundación Telefónica, 2013. [consulta: 26 febrero 2022]. Disponible en: http://www.educando.edu.do/files/9513/9281/6433/identidad_digital.pdf

Identificación digital para canadiense [en línea] Consejo de Identificación y autenticación digital de Canadá © [consulta 2 febrero 2022] Disponible en: https://diacc.ca/the-diacc/

Identificación electrónica y servicios de confianza. [en línea] EDICOM.com © [consulta: 8 marzo 2022] Disponible en: https://edicomgroup.es/centro-aprendizaje/reglamento-eidas

Infografía: ¿Qué es una buena identidad digital? [en línea] McKinsey Digital © [consulta: 13 febrero 2022] Disponible en https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/infographic-what-is-good-digital-id#.

JIMÉNEZ, Pedro Manuel. Manejo de datos y privacidad. Identidad soberana: camino hacia una red segura [en línea] digitalbiz magazine. 2019 [consulta: 27 enero 2022]. Disponible en: https://www.digitalbizmagazine.com/manejo-de-datos-y-privacidad/

La digitalización de la banca, in proceso pensando en el cliente [en línea] bbva.com© [consulta: 10 febrero 2022]. Disponible en https://www.bbva.com/es/digitalizacion-banca-proceso-pensando-cliente/

La población total de Estonia para el año 2020 es de 1.331.057 [en línea] Banco Mundial © [consulta: 1 febrero 2022] Disponible en: https://datos.bancomundial.org/indicador/SP.POP.TOTL?locations=EE.

MARTÍN, Bartolomé. La fiebre de lo Digital [en línea]. KPMG Tendencias ©. [consulta: 10 febrero 2022]. Disponible en: https://www.tendencias.kpmg.es/2019/04/fiebre-digital-juridico/

NABALÓN Iván, HERRERA, Diego, VADILLO, Sonia. *Onboarding* Digital [en línea] Banco Interamericano de Desarrollo © 2021, p.7. [consulta: 29 enero 2022]. Disponible en: https://publications.iadb.org/publications/spanish/document/Onboarding-digital.pdf

NABALÓN, Iván, PÉREZ, Jesús y VANDEVIVERE, Benoit. Identidad Digital: Desbloqueando un efecto multiplicador del PIB en España [en línea] Govtech for Policy Making. IE Public Tech Lab, 2020 ©. [consulta: 29 enero 2022] Disponible en: https://publictechlab.ie.edu/es/publicaciones/.

Nueva Resolución UIF que actualiza el marco normativo en materia de PLA/FT [en línea] Argentina.gob.ar [consulta: 9 marzo 2022] Disponible en: https://www.argentina.gob.ar/noticias/nueva-resolucion-uif-que-actualiza-el-marco-normativo-en-materia-de-plaft

PANGESTU, Mari. El Poder de la identidad Digital [en línea] Project Syndicate© [consulta: 15 febrero 2022] Disponible en: https://www.project-syndicate.org/commentary/digital-identification-systems-promote-inclusive-economic-growth-by-mari-pangestu-2020-08/spanish

Protección de Datos Personales, el mejor candado de seguridad para tus finanzas. [en línea] BBVA Podcast [consulta: 26 febrero 2022]. Disponible en: https://www.bbva.com/es/mx/podcast-proteccion-de-datos-personales-el-mejor-candado-de-seguridad-para-tus-finanzas/

Red Iberoamericana de Protección de Datos. Estándares de Protección de Datos Personales para los Estados Iberoamericanos [en línea] Infoem.org.mx© 2017. [consulta: 8 marzo 2022]. Disponible en: https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf

República Dominicana escala 26 posiciones índice Global de Ciberseguridad [en línea] Portal de la Presidencia de la República Dominicana [consulta: 1 marzo 2022] Disponible en: https://presidencia.gob.do/noticias/republica-dominicana-escala-26-posiciones-indice-global-de-ciberseguridad.

RODRÍGUEZ AZUERO, Sergio. Modelos Regulatorios para una supervisión efectiva. Foro Internacional Superintendencia de Banca Seguros y AFP del Perú. Marzo 2010. [en línea] Superintendencia de Banca, Seguros y AFP © [consulta: 8 marzo 2022]. Disponible en: https://www.sbs.gob.pe/Portals/0/jer/evnt_inter_for_inter_consu_present/Modelos%20Regulatorios%20para%20una%20Supervisi%C3%B3n%20Efectiva%20-%20Sergio%20Rodr%C3%ADguez%20Azuero.pdf

SID- Sistema de Identidad Digital. Validación remota de identidad en tiempo real con el Renaper mediante factores de autenticación biométrica (reconocimiento facial) y fotografía del DNI. [en línea] Argentina.gob.ar [consulta: 9 marzo 2022] Disponible en: https://www.argentina.gob.ar/interior/renaper/sid-sistema-de-identidad-digital

Study on eID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the EU: executive summary, [en línea] Publications Office of the European Union, 2018 [consulta: 8 marzo 2022] Disponible en: https://op.europa.eu/en/publication-detail/-/publication/139abc5b-49c6-11e8-be1d-01aa75ed71a1/language-en

Superintendencia Financiera de Colombia. Circular Externa 027 de septiembre 2020 [en línea] Deloitte.com © [consulta: 8 marzo 2022]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/legal/Legal/2020/octubre/primerasemana/Superintendencia%20de%20Sociedades%20-%20Circular%20Externa%20No.%20027%20del%202%20de%20septiembre%20de%202020%20(2).pdf

The evolving privacy landscape: 30 years after the OECD Privacy Guidelines [en línea] OECD Publishing. 2013. [consulta: 1 marzo 2022] Disponible en: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

The Open Banking Standard: la hoja de ruta de la banca abierta [en línea] BBVA.com© [consulta: 11 febrero 2022] Disponible en: https://www.bbva.com/es/the-open-banking-standard-la-hoja-de-ruta-de-la-banca-abierta/

URÍA, Francisco. El sector financiero español ante el reto de la transformación digital [en línea] KPMG Tendencias [consulta: 12 febrero 2022]. Disponible en: https://www.tendencias.kpmg.es/2018/08/el-sector-financiero-espanol-ante-el-reto-de-la-transformacion-digital/

LEGISLACIONES

Leyes

República Dominicana. Constitución de la República. *Gaceta Oficial* No. 10805 del 10 de julio del 2015.

República Dominicana. Ley 183-02 Monetaria y Financiera. *Gaceta Oficial*, de 21 de noviembre 2002.

República Dominicana. Ley Núm. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. Gaceta Oficial, del 15 de diciembre de 2013, Núm. 10737.

Internacionales

Chile. Ley19628 Sobre Protección de la Vida Privada o Protección de Datos de Carácter Personal. [en línea] Publicada en el Diario Oficial de 28 de agosto de 1999, p. 4. [consulta: 21 febrero 2022]. Disponible en: http://www.informatica-juridica.com/anexos/anexo137.asp

Perú. Código Civil. Decreto Legislativo 295. [en línea] Publicado 25 de julio de 1984. [consulta: 8 febrero 2022]. Disponible en: http://www.osce.gob.pe/consucode/userfiles/image/CodigoCivil.pdf

JURISPRUDENCIA

Nacionales

República Dominicana. Junta Monetaria. [en línea] Cuarta Resolución de fecha 30 de septiembre del 2015 emitida por la Junta Monetaria. [consulta: 7 marzo 2022]. Disponible en https://sb.gob.do/sites/default/files/nuevosdocumentos/Proteccion_Al_Usuario_Servicios_Financieros_modificacion.pdf

República Dominicana. Reglamento de Protección al Usuario de los Productos y Servicios Financieros, dictado por Junta Monetaria mediante Primera Resolución de fecha 5 de febrero 2015 y sus modificaciones.

República Dominicana. Reglamento de Sanciones, aprobado por la Quinta Resolución dictada por la Junta Monetaria en fecha 18 de diciembre del 2003.

Internacionales

Chile. Reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en la Ley Nº 21.180 sobre transformación digital del estado. Diario Oficial de la República. Noviembre 2020. [consulta: 9 marzo 2022. Disponible en: https://www.diariooficial.interior.gob.cl/publicaciones/2021/12/11/43125/01/2055208.pdf

Pacto Internacional de Derechos Civiles y Políticos [en línea] Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), del 16 de diciembre de 1966. [consulta: 3 enero 2022] Disponible en: https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/ccpr_SP.pdf

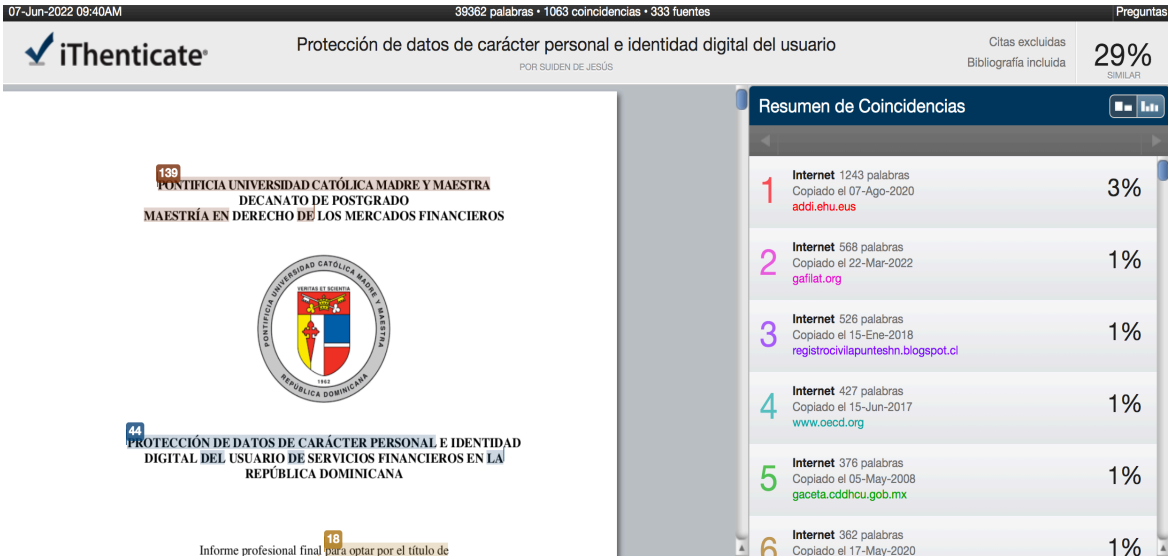
Unión Europea. Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018 (DOUE-L-2018-81022). [consulta: 9 marzo 2022]. Disponible en: https://www.boe.es/doue/2018/156/L00043-00074.pdf

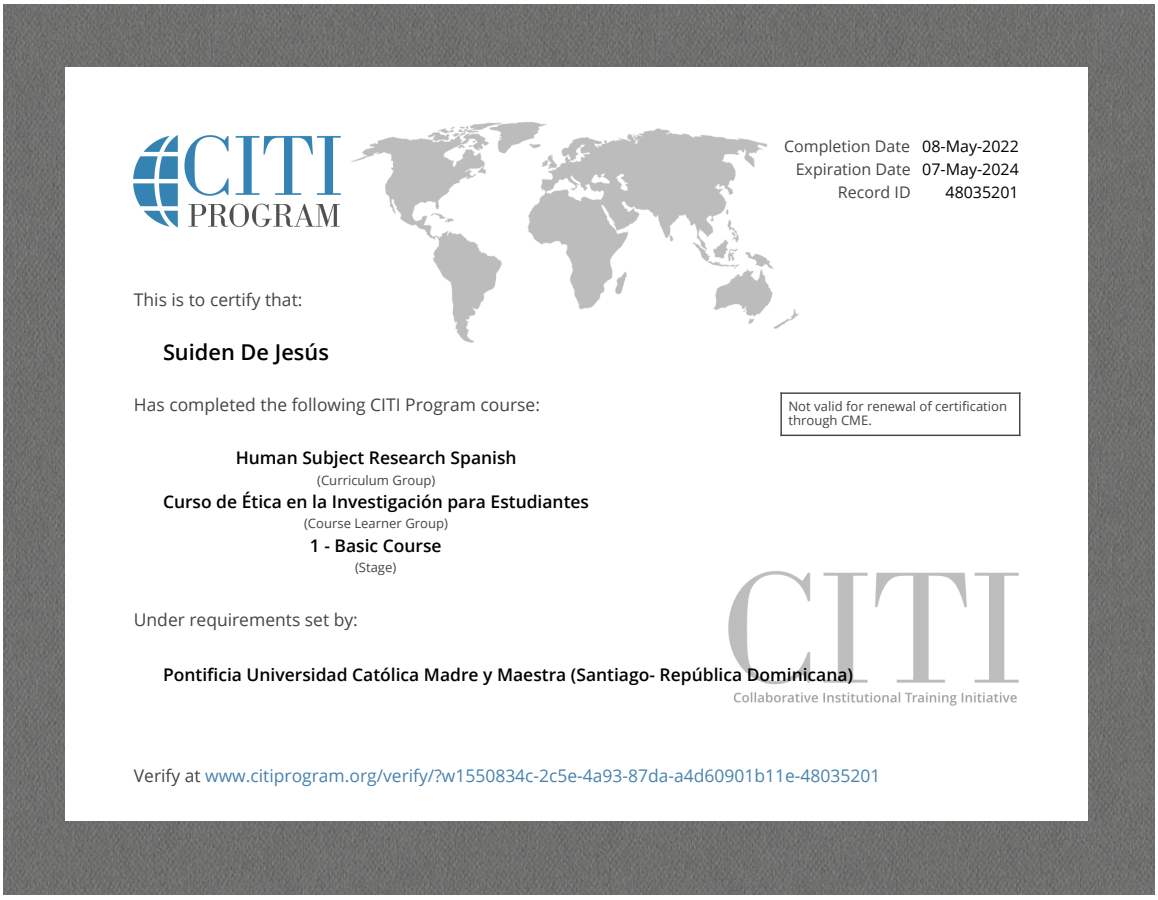
Unión Europea. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales; Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo; Samuel Parra, socio de e Privacidad y experto en protección de datos, privacidad, ciberseguridad y transparencia.; Diario de Sesiones del Congreso de los Diputados (20/05/2021); Comunicado del Tribunal de Justicia de la Unión Europea sobre la sanción a España

Unión Europea. 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) [en línea] Diario Oficial de la Unión Europea [consulta: 3 enero 2022] Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Unión Europea. 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). (Texto pertinente a efectos del EEE). 2021.

Unión Europea. Reglamento (UE) n ° 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 *OJ L 257, 28.8.2014, p. 73–114 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)*. [consulta: 8 marzo 2022]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32014R0910


07-Jun-2022 09:40AM
39362 palabras • 1063 coincidencias • 333 fuentes
Preguntas
iThenticate
Protección de datos de carácter personal e identidad digital del usuario
POR SUIDEN DE JESÚS
Citas excluidas
Bibliografía incluida
29%
SIMILAR
139
PONTIFICIA UNIVERSIDAD CATÓLICA MADRE Y MAESTRA
DECANATO DE POSTGRADO
MAESTRÍA EN DERECHO DE LOS MERCADOS FINANCIEROS
44
PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL E IDENTIDAD DIGITAL DEL USUARIO DE SERVICIOS FINANCIEROS EN LA REPÚBLICA DOMINICANA
18
Informe profesional final para optar por el título de
Resumen de Coincidencias
1 Internet 1243 palabras 3%
Copiado el 07-Ago-2020
addi.ehu.eus
2 Internet 568 palabras 1%
Copiado el 22-Mar-2022
gafilat.org
3 Internet 526 palabras 1%
Copiado el 15-Ene-2018
registrocivilapunteshn.blogspot.cl
4 Internet 427 palabras 1%
Copiado el 15-Jun-2017
www.oecd.org
5 Internet 376 palabras 1%
Copiado el 05-May-2008
gaceta.cddhcu.gob.mx
6 Internet 362 palabras 1%
Copiado el 17-May-2020



CITI PROGRAM

Completion Date 08-May-2022
Expiration Date 07-May-2024
Record ID 48035201

This is to certify that:

Suiden De Jesús

Has completed the following CITI Program course:

Not valid for renewal of certification through CME.

Human Subject Research Spanish
(Curriculum Group)
Curso de Ética en la Investigación para Estudiantes
(Course Learner Group)
1 - Basic Course
(Stage)

Under requirements set by:

Pontificia Universidad Católica Madre y Maestra (Santiago- República Dominicana)

CITI
Collaborative Institutional Training Initiative

Verify at www.citiprogram.org/verify/?w1550834c-2c5e-4a93-87da-a4d60901b11e-48035201