5. Biometría del comportamiento: un paso más para la identificación digital en los servicios financieros

Uso creciente de la biometría en el sector bancario

A medida que el mundo se vuelve más digital, las entidades financieras se ven obligadas a adaptarse rápidamente a las necesidades de los consumidores. El uso de la biometría en banca ha ido ganando fuerza gracias a la introducción en el mercado de dispositivos que ya incluyen lectores biométricos y a la expansión de la banca móvil. Dado el incremento en la magnitud y frecuencia de los ciberataques, la seguridad en la identificación ya no puede depender únicamente de medios basados en elementos biométricos estáticos, que pueden verse comprometidos. La biometría del comportamiento podría representar una solución en la lucha contra el fraude y el robo de identidades.

Contraseñas *versus* biometría

Debido a una deficiente experiencia de usuario, al aumento de los costes[20] y a las brechas de seguridad asociadas al uso de contraseñas, **los bancos están migrando a nuevos sistemas de identificación digital que cumplan con el doble objetivo de garantizar una identificación segura y mejorar la experiencia del usuario.**

La biometría no es un territorio desconocido para el sector financiero: los bancos han explorado opciones como el escaneo de huellas digitales durante décadas, pero es la expansión en el uso del móvil lo que está permitiendo que prácticamente cualquier persona que disponga de un *smartphone* pueda utilizar sus datos biométricos para realizar pagos.[21] Según la consultora Goode Inteligence[22], **en el año 2020 habrá unos 120 millones de clientes que utilizarán la biometría a través del móvil a diario para sus transacciones financieras.**

Usos de la Biometría

Existen dos tipos principales de identificadores biométricos: **i)** las características fisiológicas o estáticas, que se basan en la forma o composición del cuerpo (huellas dactilares, iris, venas de la palma, cara) y **ii)** las características de comportamiento, basadas en la forma de actuar de una persona (pulsaciones del teclado, movimientos del ratón, coordinación de manos y movimiento de los ojos, temblores en las manos, la forma en la que los dedos se desplazan, etc.)

Aunque las entidades financieras han introducido todo tipo de elementos biométricos estáticos con fines de identificación, **en la actualidad, el más utilizado es el sistema de reconocimiento de huellas dactilares.** Estudios realizados por Deloitte[23] afirman que, para finales de 2017 en el mercado habrá mil millones de teléfonos inteligentes

20: Una encuesta reciente entre empresas estadounidenses constató que cada empleado pierde, en promedio, unos 420 dólares al año al tener que vérselas con tantas contraseñas.
21: Fuente: Biometrics: the future of Mobile Payments. Nathaniel Karp, BBVA Research, julio de 2015.
22: Fuente: Mobile Biometrics for Financial Services; Market & Technology Analysis, Adoption Strategies & Forecasts 2015-2020, Julio 2015
23: Fuente: A world beyond passwords: Improving security, efficiency, and user experience in digital transformation. Goode Intelligence. Diciembre de 2015.

con lectores de huellas digitales, rivalizando para 2018 con el iris y el reconocimiento facial. El Banco BBVA, por ejemplo, ha empezado a utilizar recientemente la biometría para la apertura remota de cuentas en España, mediante la verificación de la identidad del cliente a través de un proceso de reconocimiento facial. En la India, el proyecto Aadhaar ha recopilado datos gráficos y biométricos de mil millones de habitantes, en el mayor proyecto de identidad digital basado en biometrías desarrollado en el mundo.

Problemas de seguridad

A pesar de que los bancos se esfuerzan en proteger sus sistemas, los *hackers* han encontrado la forma de replicar los medios tradicionales de autenticación (códigos SMS, tokens). Aunque la biometría estática es relativamente segura debido a que los atributos físicos son únicos, no es menos cierto que las características físicas son **públicas, no podemos ocultarlas y, por lo tanto, son fáciles de reproducir y reutilizar.** Recientemente, hemos visto en las noticias que varios hackers habían engañado a los sistemas de reconocimiento facial con fotos extraídas de Facebook. En Japón, el Instituto Nacional de Informática (NII) está advirtiendo al público de que la tecnología de reconocimiento de huellas dactilares permite a los delincuentes informáticos copiar patrones a partir de imágenes de personas que hacen el signo de la paz en las fotos. Hay que resaltar que las consecuencias de un falso positivo son muy graves y resulta evidente que cuando nuestros datos biométricos estáticos se ven comprometidos, no se pueden utilizar de nuevo y el daño es permanente, porque, obviamente, **no podemos modificar nuestra huella dactilar o el iris de nuestros ojos.**

Adopción de la biometría del comportamiento

La tecnología biométrica del comportamiento es capaz de aprender los patrones de actuación de los usuarios con el fin de construir un modelo de identificación. El software analiza la forma en la que los usuarios interactúan con los diferentes dispositivos (teléfono, PC, tabletas): cómo sujetan el ratón, cómo teclean, la rapidez con la que se mueven, la presión con la que sostienen el teléfono, etc. Con el tiempo, estos datos biométricos se interpolan a través de algoritmos y permiten definir un patrón único de cada usuario con el fin de establecer su identidad de una manera cierta e inequívoca.

Un elemento que diferencia la biometría del comportamiento de la estática en la verificación de la identidad es que **los datos se recogen de una manera pasiva y no se interrumpe la actividad del usuario, un elemento clave para mejorar la experiencia del cliente.**

Empresas como Google, con su proyecto Abacus, están utilizando el aprendizaje de máquinas para autenticar usuarios en función de múltiples factores de comportamiento. El uso de sensores, como cámaras, acelerómetros y las funciones de GPS, permite a los teléfonos inteligentes recopilar gran cantidad de información acerca de los usuarios, incluyendo sus geolocalizaciones habituales, y cómo escriben, caminan y hablan.

Algunos bancos ya han comenzado a adoptar la biometría del comportamiento como sustituto de las contraseñas en dispositivos móviles. Uno de ellos es el Leumi Bank, con sede en Israel, que utiliza el tamaño del dedo y la presión que ejerce el usuario sobre las teclas para habilitar la autenticación. Algunas *fintechs*, como Mobetize, también han esta tecnología para analizar los patrones de los usuarios y determinar si se trata de auténticos clientes, *bots* o *hackers.*

Regulación

Dado que la tecnología biométrica es tan reciente, hay **muy poca regulación específica sobre su uso y aplicación.** El mayor riesgo en la utilización de la biometría estática está relacionado con la privacidad, ya que los registros se almacenan a menudo en bases de datos que pueden verse comprometidas.

En Europa, los reguladores reconocen que estas tecnologías podrían mejorar la experiencia del usuario, pero también que podrían «conducir a una pérdida gradual de los niveles privacidad si no se aplican las garantías adecuadas»[24]**.** El nuevo Reglamento General de Protección de Datos establece que, para el tratamiento de «categorías especiales de datos personales», como la biometría**, se requiere un mayor nivel de permiso del usuario, un consentimiento «explícito».** Normas como la nueva Directiva de servicios de pago (PSD2) establecen la autenticación de dos factores para ciertos pagos y, de este modo, el uso de métodos de identificación biométrica que puede facilitar la aceptación de los pagos móviles. El Reglamento eIDAS prevé el uso opcional de la biometría como factor de autenticación en el uso de firma electrónica en toda la UE. Y en EE.UU., algunos estados han establecido normas para proteger la privacidad de los datos biométricos de las personas.

En el caso del almacenamiento de la biometría del comportamiento, dado que se recogen datos de interacciones, resulta más sencillo cumplir con las normas protección de datos.[25]

24: Fuente: Data protection working party, Opinion on developments in biometric technologies, abril 2012
25: Fuente: Biometrics: The Physical Attributes vs. Behavioral Patterns Privacy Debate

Conclusiones

Se espera que los bancos adopten de manera incremental estas tecnologías, ya que son muy precisas y fáciles de integrar en las aplicaciones móviles y de Internet. Es obvio que contar con un único método de autenticación aumenta la vulnerabilidad frente a los ataques y que es ahí donde se produce la mayor parte de los fraudes hoy en día. Por ello, **los bancos están introduciendo la biometría del comportamiento como una forma adicional de proteger el proceso de identificación.** Este enfoque permite la detección de anomalías en los patrones de uso de un cliente después de la autenticación. Es la llamada autenticación de múltiples factores. Al controlar los patrones de una manera continua dentro de una sesión**, la biometría del comportamiento ofrece una solución integral para evitar que las cuentas sean hackeadas por piratas informáticos.** El otro factor que hace que la biometría de comportamiento sea tan atractiva es la experiencia del usuario, ya que funciona sin interrumpir de ninguna forma la actividad diaria del cliente.

AVISO LEGAL

El presente documento, elaborado por el Departamento de BBVA Research, tiene carácter divulgativo y contiene datos, opiniones o estimaciones referidas a la fecha del mismo, de elaboración propia o procedentes o basadas en fuentes que consideramos fiables, sin que hayan sido objeto de verificación independiente por BBVA. BBVA, por tanto, no ofrece garantía, expresa o implícita, en cuanto a su precisión, integridad o corrección.

Las estimaciones que este documento puede contener han sido realizadas conforme a metodologías generalmente aceptadas y deben tomarse como tales, es decir, como previsiones o proyecciones. La evolución histórica de las variables económicas (positiva o negativa) no garantiza una evolución equivalente en el futuro.

El contenido de este documento está sujeto a cambios sin previo aviso en función, por ejemplo, del contexto económico o las fluctuaciones del mercado. BBVA no asume compromiso alguno de actualizar dicho contenido o comunicar esos cambios.

BBVA no asume responsabilidad alguna por cualquier pérdida, directa o indirecta, que pudiera resultar del uso de este documento o de su contenido.

Ni el presente documento, ni su contenido, constituyen una oferta, invitación o solicitud para adquirir, desinvertir u obtener interés alguno en activos o instrumentos financieros, ni pueden servir de base para ningún contrato, compromiso o decisión de ningún tipo.

Especialmente en lo que se refiere a la inversión en activos financieros que pudieran estar relacionados con las variables económicas que este documento puede desarrollar, los lectores deben ser conscientes de que en ningún caso deben tomar este documento como base para tomar sus decisiones de inversión y que las personas o entidades que potencialmente les puedan ofrecer productos de inversión serán las obligadas legalmente a proporcionarles toda la información que necesiten para esta toma de decisión.

El contenido del presente documento está protegido por la legislación de propiedad intelectual. Queda expresamente prohibida su reproducción, transformación, distribución, comunicación pública, puesta a disposición, extracción, reutilización, reenvío o la utilización de cualquier naturaleza, por cualquier medio o procedimiento, salvo en los casos en que esté legalmente permitido o sea autorizado expresamente por BBVA.

BBVA | Research

Este informe ha sido elaborado por la unidad de Regulación Digital:

Economista Jefe de Regulación Digital
Álvaro Martín
alvaro.martin@bbva.com
+ 34 91 537 36 75

María Álvarez
maria.alvarez.caro@bbva.com

Vanesa Casadas
vanesa.casadas@bbva.com

Edward Corcoran
Edward.corcoran@bbva.com

Jesús Lozano
jesus.lozano@bbva.com

Alicia Sánchez
alicia.sanchezs@bbva.com

Javier Sebastián
jsebastian@bbva.com

Ana Isabel Segovia
ana.segovia@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

BBVA Research

Economista Jefe Grupo BBVA
Jorge Sicilia Serrano

Análisis Macroeconómico
Rafael Doménech
r.domenech@bbva.com

Escenarios Económicos Globales
Miguel Jiménez
mjimenezg@bbva.com

Mercados Financieros Globales
Sonsoles Castillo
s.castillo@bbva.com

Modelización y Análisis de Largo Plazo Global
Julián Cubero
juan.cubero@bbva.com

Innovación y Procesos
Oscar de las Peñas
oscar.delaspenas@bbva.com

Sistemas Financieros y Regulación
Santiago Fernández de Lis
sfernandezdelis@bbva.com

Coordinación entre Países
Olga Cerqueira
olga.gouveia@bbva.com

Regulación Digital
Álvaro Martín
alvaro.martin@bbva.com

Regulación
María Abascal
maria.abascal@bbva.com

Sistemas Financieros
Ana Rubio
arubiog@bbva.com

Inclusión Financiera
David Tuesta
david.tuesta@bbva.com

España y Portugal
Miguel Cardoso
miguel.cardoso@bbva.com

Estados Unidos
Nathaniel Karp
Nathaniel.Karp@bbva.com

México
Carlos Serrano
carlos.serranoh@bbva.com

Turquía, China y Geopolítica
Álvaro Ortiz
alvaro.ortiz@bbva.com

Turquía
Álvaro Ortiz
alvaro.ortiz@bbva.com

China
Le Xia
le.xia@bbva.com

América del Sur
Juan Manuel Ruiz
juan.ruiz@bbva.com

Argentina
Gloria Sorensen
gsorensen@bbva.com

Chile
Jorge Selaive
jselaive@bbva.com

Colombia
Juana Téllez
juana.tellez@bbva.com

Perú
Hugo Perea
hperea@bbva.com

Venezuela
Julio Pineda
juliocesar.pineda@bbva.com

INTERESADOS DIRIGIRSE A: BBVA Research: Calle Azul, 4. Edificio de la Vela - 4ª y 5ª plantas. 28050 Madrid (España). Tel.:+34 91 374 60 00 y +34 91 537 70 00 / Fax:+34 91 374 30 25 - bbvaresearch@bbva.com www.bbvaresearch.com