>> Jorge Dávila

Ilusionismo Biométrico, Máscaras Digitales e Identificación

A veces las cosas solo cambian de nombre mientras subyacen a nuestro alrededor. Esto es lo que pasa con la verificación de identidades o Identidad Digital como algunos quieren llamarla. Desde 1961 seguimos utilizando las contraseñas, y han sido muchas las propuestas que se han hecho y no han triunfado. Sigue habiendo intentos de resolver el problema de la identidad digital y su autenticación, pero ahora algunos proponen el uso de la biometría para poder desenganchar definitivamente la generación de identidades de la verificación física y presencial, lo cual puede abrir paso a nuevas formas de falsificación con impacto directo en la economía y los derechos en la dimensión digital. Es buen momento para echar un vistazo a cómo ha evolucionado este escenario que pretende darnos entrada definitiva en la realidad digital.

Eslogan (del inglés *Slogan*): 1. m. Fórmula breve y original, utilizada para publicidad, propaganda política, etc. El pasado 15 de octubre pude participar en la segunda de las Jornadas de la sexta edición de **Identi::SIC**, y allí descubrí el nuevo titulillo que se repite tenazmente en la comercialización TIC de nuestros días. El lema en cuestión es "*La Identidad Digital es el nuevo perímetro*". De ello entiendo que ya deben haber aceptado todos eso de que el perímetro[1] no existe y no sé entonces ¿qué es lo que van a hacer los vendedores de *firewalls* y demás 'ferramenta' de nuestro oficio? Me temo que ese lema es solo otra ocurrencia de *marketing* con la que establecer algún tipo de continuidad derivable entre lo que han estado vendiendo todos estos años pasados (perímetro y más perímetro) y lo que esperan vender a partir de ahora (la identidad y más identidad).

Identidades hay muchas, entre otras la Legal. La Digital será un avatar, un representante digital de nosotros, como entes analógicos, en cualquier escenario digital, una mera transcripción de nuestra Identidad Legal al mundo digital.

Cuando uno presta atención a lo que llaman identidad se encuentra con la gestión clásica de cuentas y contraseñas a las que se les puede haber añadido los certificados digitales de alguna PKI vigorizada. Según parece, la nueva identidad digital no es realmente nueva sino la metamorfosis de lo que anteriormente se llamó "Single Sign On" (SSO). Por lo que se ve, en el mundo TIC sigue reinando el dueto usuario-contraseña dado que es el mecanismo de acceso que provee la inmensa mayoría de aplicaciones que componen la actual digitalización de nuestra sociedad y nuestras vidas. Han pasado 32 años desde la invención de los Certificados Digitales x509v3, y es ahora cuando empiezan a proponerse como elemento básico de la identificación y autenticación de usuarios, servicios y dispositivos.

Cerraduras para puertas sin marcos ni paredes

Lo curioso es que dicen que "el perímetro ha muerto" y lo que están vendiendo son cerraduras para unas puertas sin marcos ni paredes (perímetro) a las que anclarse. Está claro que la racionalidad va por un sitio y el *marketing* y las ventas va por otro completamente distinto.

Un aspecto al que se le dio importancia en las mencionadas jornadas es el de la Gestión de Cuentas Privilegiadas (PAM en inglés), y que son todas aquellas que controlan toda la infraestructura sobre la que se desarrollan las actividades TIC (servidores, bases de datos, sistemas de configuración, *routers*, *firewalls*, etc.). En este escenario, el uso de contraseñas estáticas es demasiado arriesgado y ahora se aboga por el uso de servicios que representen a las identidades en lo que a la autenticación dinámica ante la máquina o servicio se refiere. Esencialmente, esta aproximación lo que hace es transportar un nivel más arriba el problema de autenticación, ya que el usuario legítimo y autorizado tendrá que autenticarse de algún modo ante el servicio PAM, que gestiona las contraseñas dinámicas de la infraestructura. Además, el propio sistema PAM se convierte en un punto de ataque y fallo muy interesante dado la concentración de poder que en él se da.

Aunque todavía estemos tan lejos de encontrar un modo racional y razonable de afrontar el problema de que, realmente, el perímetro lo han destruido las externalizaciones ventajosas y las evaporaciones a la nube del mundo empresarial, cualquier perímetro, incluso el que pretenden atribuir a la "nueva" Identidad Digital, es una quimera. Hoy en día, los atacantes están y ocupan el mismo espacio digital que el que tienen utilizado por los usuarios legítimos. En esta nueva realidad, la identidad y su verificación son los elementos más esenciales de todo el escenario digital.

Muchas identidades

Identidades hay muchas. Por una parte, está la **identidad esencial** o **identidad forense**, que tiene que ver con esa carga genética (ADN) y secuencia de desarrollo (fenotipo) que siga cualquier sistema vivo a lo largo de toda su vida. También hay que incluir aquí los efectos, las modificaciones irreversibles que imprimen hechos o acontecimientos concretos sobre dichos organismos (su historia). Por otra parte, está la **Identidad Legal**, que es la que a cada uno de nosotros nos otorgan los distintos sistemas judiciales que nos afectan. Esa identidad está plasmada en documentos y a ella se refiere todas nuestras posesiones, derechos y obligaciones. Cada día más, aumenta la preponderancia de la que podríamos llamar **Identidad Social**, que es aquella nacida de la reputación individual y colectiva, y de lo que de cada uno de nosotros se dice independientemente de si es verdad o no. En un ámbito más interior está la **Identidad Subjetiva** que es aquella que incluye cómo nos vemos nosotros a nosotros mismos (ego, autoestima, creencias, ética, estética, sexualidad, género, etc.). Suele ser la identidad menos apoyada por la realidad pero es la que con mano más férrea guía nuestro comportamiento y expectativas.

[1] **Perímetro** (del lat. perimĕtros, y este del gr. περίμετρος perímetros): 1. m. Contorno de una superficie. 2. m. Geom. Contorno de una figura. 3. m. Geom. Medida del contorno de una figura.

Identidad legal digital y biometría

Ninguna de las anteriores tiene nada que ver con la dimensión digital que está tomando nuestra realidad y por ello ahora se empieza a hablar de una necesaria Identidad Digital. Está **Identidad Digital** será un avatar, un representante digital de nosotros, como entes analógicos, en cualquier escenario digital. Esta Identidad Digital no es más que la mera transcripción de nuestra Identidad Legal al mundo digital. La Identidad digital es, esencialmente, necesaria para resolver legalmente conflictos que pudieran darse en la dimensión digital. De hecho, sin una identificación digital sólida, es imposible aplicar ningún código legal en el mundo digital.

Para poder construir una Identidad Digital que pueda llamarse así son necesarias tres características ineludibles: (1) Debe existir un **secreto único e irrepetible**, (2) de ese secreto **sólo puede existir una única copia** en todo momento, y (3) toda operación relacionada con ese secreto **sólo deberá poder operarla la voluntad de la entidad a la que representa**. Son tres condiciones sencillas de entender, pero no tan fáciles de implementar. De hecho, no tengo noticia de que exista ningún ejemplo concreto que satisfaga las tres condiciones simultáneamente. Las dificultades para satisfacer la anterior Trinidad, no han sido impedimento para que algunos vendan autenticación e identificación apoyándose en la Biometría.

La Biometría o Antropometría forense es una actividad antigua como la propia sociedad[2] pero la versión moderna la puso en pie Alphonse Bertillon[3] en la que se medían ciertas características físicas del sujeto para proceder a su identificación (es decir, distinguirlo inequívocamente de los demás). Su gran aportación fue lo importante de la forma de la nariz para el reconocimiento facial y de ahí, la tradición policial de hacer fotos de frente y perfil de los fichados. Hoy se miden aspectos estáticos (huellas dactilares, fondo de ojo, iris ocular, la voz, patrones faciales, distribución de las venas en la palma de la mano, geometría de está, etc.) y dinámicos (firma manuscrita, andares, el paso, las habilidades mecanográficas) y todos ellos se han propuesto para la autenticación de usuarios humanos.

La biometría no se debe utilizar para establecer un sistema de Identidad Digital, ya que (1) no es secreta, (2) existe un único original, pero no es digital, por lo que siempre se trabaja con registros digitales de los cuales no se puede asegurar su unicidad y, en su versión digital, (3) no se puede asegurar que este bajo el control exclusivo de su titular o propietario. La biometría es idónea para la identificación forense de individuos físicos presentes (vivos o muertos, íntegros o en trozos), pero no funciona cuando se intenta trasladar a la dimensión digital y por ende, virtual.

La biometría no se debe utilizar para establecer un sistema de Identidad Digital, ya que (1) no es secreta, (2) existe un único original, pero no es digital, por lo que siempre se trabaja con registros digitales de los cuales no se puede asegurar su unicidad y, en su versión digital, (3) no se puede asegurar que este bajo el control exclusivo de su titular o propietario.

Cualquiera puede registrar, con la precisión que quiera, cualquiera de los aspectos biométricos antes mencionados y, como veremos más adelante, reproducirlos con la precisión que sea necesaria ante cualquier verificador/autenticador.

Por otra parte, la autenticación es algo diferente a la identificación (establecer la identidad de una persona o cosa). La autenticación es establecer si una afirmación es cierta o no, y es un proceso de verificación que tiene que realizarse con éxito **todas y cada una de las veces** que se precise saber con quién o qué se está tratando en el mundo digital. En lo que toca a los sistemas de Identidad Digital, lo realmente eficaz en los casos de **suplantación de identidad** es atacar al sistema de verificación y no tanto intentar reproducir exactamente el aspecto analógico de interés biométrico. Esos verificadores biométricos son complejos y tiene varios componentes, todos ellos atacables con alta probabilidad de éxito.

La autenticación es establecer si una afirmación es cierta o no, un proceso de verificación que tiene que realizarse con éxito todas y cada una de las veces que se precise saber con quién o qué se está tratando en el mundo digital. En lo que toca a los sistemas de Identidad Digital, lo realmente eficaz en los casos de suplantación de identidad es atacar al sistema de verificación y no tanto intentar reproducir exactamente el aspecto analógico de interés biométrico.

Realmente, la identidad y la autenticación no son, per se, lo que preocupa en el mundo digital. El escenario no se completa hasta que se incluye en él la **Autorización**. En una autorización se transfiere temporalmente y se reconoce en un determinado agente ciertas capacidades que son vinculadas a su identidad. Si puedes autenticarte como propietario de una identidad, obtienes automáticamente todas las autorizaciones y potestades que se hayan otorgado a dicha identidad. Aquí está la verdadera razón de querer poder suplantar identidades, ya que con ello les robas el alma digital, y probablemente la analógica también, a su titular.

Robo y suplantación

En realidad, a fecha de hoy, la suplantación y el robo de identidad están en la base casi todos los ciberdelitos que se comenten. En la mayoría de los casos se hace a través del **robo y posterior uso de credenciales válidas/auténticas** que se han conseguido robar (intercepción, sustracción física, cogeneración, etc.) más que a través de verificaciones fallidas por parte del sistema de autenticación. Cuando se lleguen a proteger correctamente las credenciales (los *tokens software*), los ataques tendrán que focalizarse en engañar al autenticador y, si el mecanismo de protección es biométrico, los atacantes podrán tener grandes éxitos. En el mundo comercial de las TIC todavía estamos bastante lejos de que se utilicen identidades y autorizaciones digitales seguras.

Además de robar identidades y suplantar todo lo que se mueva digitalmente, la creación de falsas identidades también puede ser un negocio muy lucrativo. El uso de "**dobles**"[4] ha sido una solución muy utilizada como medida contra los magnicidios. Todos los grandes líderes han tenido sus dobles para que fuesen ellos los que sufriesen los atentados.

En el mundo digital, la creación de iden-

[2] Ver el uso de la capacidad de decir correctamente la palabra "*Shibboleth*" en la Biblia, en concreto, consultar en Jueces 12.6

[3] Ver https://es.wikipedia.org/wiki/Alphonse_Bertillon

[4] Ver https://en.wikipedia.org/wiki/Political_decoy

tidades falsas es el pan nuestro de cada día en las Redes Sociales, y el centro del negocio[5] de entidades como **Cambridge Analytica**[6], donde los **Troles**[7] y los **Sock puppets**[8] son la munición más utilizada.

En el mundo analógico hay un personaje que está muy relacionado con los "dobles" de los mandatarios y son los **Testaferros**[9], que son personas que suplantan, encubren o aparentan legalmente ser algo, prestando para ello su nombre, identidad y firma a la persona que realmente le manda y controla. La capacidad de generar Identidades Digitales Falsas es sinónimo de poder crear **Testaferros Digitales** (***Fake Digital Persons***) que harían ininvestigable cualquier operación financiera u operación transaccional en general.

Por el momento, las identidades digitales que se emiten a través de PKIs, como las construidas sobre Autoridades de Certificación (CERES, etc.) o sobre *tokens* físicos (eDNI, Pasaporte, tarjetas bancarias EMVs, etc.) requieren en alguno de sus pasos, la personación física del titular y su correspondiente autenticación analógica fuera de Internet. Sin embargo, (1) la aparición de nuevos servicios (*carsharing*, bicicletas, patinetes, etc.), y (2) la decadencia bancaria en cuanto al número de sucursales abiertas al público, han vitalizado las propuestas de recurrir a **procesos de 'enrolamiento' completamente digitales**, sin personación física de nadie frente a un verificador analógico entrenado (*On Boarding* Digital).

Desarrollos como los de NVIDIA para la traducción video-to-video o el Proyecto Face2Face abren el melón de las Máscaras Digitales en las cuales, como en aquella canción de Radio Futura, una Historia de Play Back, "alguien dicta en la sombra y tú sólo mueves los labios". Gracias a estas tecnologías "sintéticas", cualquier posible "prueba de vida" de los sistemas de On Boarding Digital sería falsificable.

'Enrolamiento' digital

Todos los sistemas de ***On Boarding* Digital** propuestos utilizan el teléfono móvil del supuesto titular, y recurren a biometrías faciales y de voz para intentar relacionarlos con los documentos de identidad (generalmente analógicos) puesto en el sistema a través de fotos realizadas con el móvil (DNI, carnet de conducir, etc.). Al principio se contentaban con registros estáticos de los mismos, por lo que engañar al sistema era trivial. Los más avanzados incluyen "**pruebas de vida**" obtenidas a través de solicitar al titular que diga o haga algo indicado por el verificador y, en principio, imprevisible para el atacante. Estas medidas hubiesen dificultado el ataque a los sistemas de *On Boarding* Digital si no fuese porque la Inteligencia Artificial ha querido desarrollar en su seno lo que se podría llamar **Generación Sintética de Artesanía** (Synthetic Media), entendida la artesanía como actividad realizada por seres humanos.

Dentro de esa panoplia que son los Synthetic Media está (1) la síntesis de imágenes y de videos, y (2) la síntesis de audio, más en particular de discursos de voz, con la que se pueden, en principio, falsificar las pruebas de vida que se proponen en los sistemas de *On Boarding* Digital.

Desarrollos como los de NVIDIA para la **traducción video-to-video**[12] o el Proyecto **Face2Face**[13] abren el melón de las **Máscaras Digitales** en las cuales, como en aquella canción de Radio Futura[14], una Historia de Play Back[15], "*alguien dicta en la sombra y tú sólo mueves los labios*". Gracias a estas tecnologías "sintéticas", cualquier posible "prueba de vida" de los sistemas de *On Boarding* Digital sería falsificable.

Lo que da un poco de margen a los defensores de las pruebas de vida digitales es que la Inteligencia Artificial sigue procedimientos tediosos y computacionalmente caros, por lo que las **síntesis de medios en tiempo real y suficiente calidad** todavía es algo que habrá de llegar y tendrá, al principio, asociados costes computacionales importantes. No hay que perder de vista la posibilidad de que no sea la IA la que consiga realmente hacerse con la generación de máscaras digitales. Siempre se puede intentar la síntesis *ab inito* de caras, expresiones y discursos. Sólo hay 43 músculos en la cara de un humano, por lo que se podría llegar a reducir el problema a 43 funciones actuando simultánea y concurrentemente para dar la impresión de que lo que tenemos a través del móvil es realmente un ser humano. Esa tecnología tendría muchísimo futuro (y financiación) en Hollywood y en el desarrollo de juegos de ordenador. No olvidemos aquella máxima de que "***los ataques criptográficos, como los criptoanalíticos, con el tiempo sólo pueden mejorar***".

La capacidad que tenemos los humanos para determinar la autenticidad de cualquier registro u objeto digital es absolutamente nula. Nuestro deambular digital siempre se hace a través de representantes, de instrumentos digitales que realmente no controlamos. Por ello, los seres analógicos y usuarios de Internet, estamos condenados a que nos engañe cualquiera manipulando las imágenes, discursos, declaraciones y datos que recibamos a través de las pantallas.

Nuestra situación es análoga a la del psicólogo Kris Kelvin cuando le encargan ir a investigar qué está ocurriendo en una estación espacial orbitando la estrella de neutrinos conocida como **Solaris**[16].

Después de dormir en la estación, se le aparece en su dormitorio una réplica física y viva de Hari, su difunta esposa. Kelvin intenta deshacerse de ella por considerarla no-auténtica y la lanza al espacio exterior, pero pocas horas después vuelve a inexplicablemente aparecer. Esta vez Kelvin la acepta, vive con ella y no la deja ni un solo momento sola.

Solaris creaba a Hari utilizando los recuerdos que tenía Kris de ella, y la Hari presente, aunque no sea humana, piensa y siente como si lo fuese. Es comprensible que la tentación de quedarse a vivir con esta segunda oportunidad sea superior al prurito autenticador del protagonista. La virilidad masculina nunca tuvo mucho que hacer frente a los oníricos encantos de los súcubos[17], y algo parecido nos pasa a tod@s cuando nos zambullimos en lo digital. ■

[5] Ver https://en.wikipedia.org/wiki/Facebook - Cambridge_Analytica_data_scandal
[6] Ver https://en.wikipedia.org/wiki/Cambridge_Analytica
[7] Ver https://en.wikipedia.org/wiki/Internet_troll
[8] Ver https://en.wikipedia.org/wiki/Sock_puppet_account
[9] Ver https://es.wikipedia.org/wiki/Testaferro
[10] Ver https://www.electronicid.eu/en/blog/post/digital-onboarding-process-financial-sector/en
[11] Ver https://en.wikipedia.org/wiki/Synthetic_media
[12] Ver https://github.com/NVIDIA/vid2vid
[13] Ver https://github.com/datitran/face2face-demo
[14] Ver https://es.wikipedia.org/wiki/Radio_Futura
[15] Ver y oír https://youtu.be/8ClZoQiSvvA
[16] Ver https://en.wikipedia.org/wiki/Solaris_(1972_film)
[17] Ver https://es.wikipedia.org/wiki/Súcubo

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es