Identidad digital y seguridad online

Javier Alonso Lecuit | Investigador senior asociado al Real Instituto Elcano y miembro del Grupo de Trabajo sobre Ciberpolítica

Tema

La identidad digital de las personas físicas y jurídicas y dispositivos conectados mediante Internet plantea desafíos de reputación, protección, identificación y autenticación que trascienden los riesgos de ciberseguridad clásicos.

Resumen

La identidad digital permite el reconocimiento y actuación de los individuos, las corporaciones o los poderes públicos en Internet. La ciberseguridad tradicional se ocupa de proteger la confidencialidad, integridad y disponibilidad de los sistemas, las redes y la información que discurren por Internet, pero la eclosión de la digitalización exige, además, salvaguardar los derechos y la reputación de quienes utilizan la identidad digital.

La protección de la identidad digital (*online*) 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, desarrollando mecanismos de identificación y autenticación que proporcionen un uso seguro de Internet y el aprovechamiento de las posibilidades y nuevos modelos de negocio que ofrece la economía digital.

Este ARI se aproxima a los conceptos de identidad digital (*online*) y anonimato, a los sistemas de identificación, autentificación, gestión y acceso y a las normas e instrumentos de protección en los ámbitos europeo y nacional.

Análisis

A diferencia de la identidad física (*offline*), la identidad digital (*online*) asociada a un individuo, organización o dispositivo electrónico se construye en el ciberespacio. Se pueden subir a Internet elementos identificativos del mundo físico (nombre, dirección, fechas, datos, documentos, productos…) y elementos digitales (imágenes, búsquedas, contactos, opiniones, comunidades, vídeos, redes sociales…) que conforman una identidad objetiva, a la que se añade otra derivada de la interpretación por terceros de la huella digital construida (rasgos de carácter sociológico, cultural, psicológico o económico), así como de sus omisiones (rasgos no compartidos).

Es importante distinguir entre **identidad *online*** –quiénes somos en Internet– y **reputación *online*** –qué dicen de nosotros en la Red–. Toda información u opinión publicada en páginas web, foros, blogs o redes sociales sobre una persona o empresa

e indexada por los buscadores afecta en mayor o menor medida a su reputación al estar visible ante terceros. Como resultado, los sujetos de identidad digital no sólo deben gestionar la seguridad y privacidad de las informaciones, sistemas y dispositivos que utilizan para participar en Internet, sino también de la reputación asociada a esa identidad.

Establecida la diferencia entre identidad física y digital, surge la necesidad de demostrar la correspondencia entre ambas mediante los mecanismos de identificación y autenticación *online*. Uno de los grandes retos del mundo *online* es contar con mecanismos seguros que permitan demostrar fehacientemente la identidad de una persona en el ámbito digital, es decir, que la persona natural o jurídica pueda probar que es quien afirma ser al realizar una transacción o acceder a un servicio *online*. A partir de este punto surgen los conceptos de identificación –decir quién se es– y autenticación –demostrar que se es quien se dice ser–, necesarios para utilizar la práctica totalidad de plataformas y servicios en la Red y en el ámbito de la empresa para acceder a los sistemas de información.

Construir un enlace fiable entre una identidad real y la identidad digital requiere un mecanismo de autenticación que acredite la correspondencia entre la identidad física y la digital. Los mecanismos de autenticación deben ser seguros frente a ciberataques, fiables –con una probabilidad de error tan pequeña como sea posible–, asequibles –con un coste proporcional al daño evitado– y de fácil uso para el cliente. Las plataformas de autenticación seguras emplean uno o más factores de verificación (*multifactor autentication* o MFA), que se obtienen a partir de algo que solo el usuario conoce –como una contraseña–, emplea –como su teléfono móvil– o le corresponde de forma inequívoca –como su información biométrica[1]–. Adicionalmente, puede tenerse en cuenta información de contexto; por ejemplo, la red de acceso utilizada, la firma digital del dispositivo o la ubicación.

Identidad digital y anonimato

Dado que la construcción de la identidad y la huella digital se materializa a través de un conjunto de identificadores de acceso a la Red (dirección IP, dirección Mac, configuraciones de los dispositivos, etc.), esto ha propiciado la monitorización permanente de los titulares de esos identificadores con distintos fines (comerciales, sociológicos o de seguridad, entre otros). La pérdida del anonimato y de la privacidad en un mundo hiperconectado permite predecir conductas o realizar evaluaciones financieras, sociales, políticas y legales de los titulares de una identidad digital. Sea con fines de control social por Estados autoritarios, por intereses económicos o por simple curiosidad, los titulares de una identidad digital se ven sujetos a una monitorización generalizada y sistemática, por lo que recurren a pseudónimos o alias que sustituyen una identidad *online* conocida y asociada a un identificador por otra sin datos asociados, lo cual plantea un antagonismo problemático entre identidad y anonimato (los sistemas digitales necesitan identidades que puedan validarse). Asimismo, existen varias

[1] La autenticación biométrica resulta particularmente segura al ser medible y única para cada persona. Puede basarse en los rasgos físicos (iris, retina, huellas dactilares, rasgos geométricos de las manos, rostro, etc.) o los conductuales (escritura, firma, voz, pulso, etc.).

tecnologías que facilitan el anonimato en la Red, como, por ejemplo, navegadores que bloquean *cookies*, rastreadores o la huella digital del dispositivo; redes privadas virtuales (VPN); enrutamientos a través de servicios proxy-IP; redes superpuestas a Internet cifradas y anonimizadas (p. ej. TOR), o el uso de cifrado de extremo a extremo de clave efímera, entre otros.

La identidad autosoberana

La identidad autosoberana (*self-sovereign identity* o SSI) es un mecanismo *online* que permite a su titular, de forma segura y legal, utilizar una identidad digital universal única para controlar la trasferencia y uso de sus datos; por ejemplo, mediante una aplicación instalada en su teléfono móvil. Estos mecanismos cuentan con tres elementos: un titular de la identidad, es decir el individuo, organización u objeto conectado; un identificador descentralizado o alias (*decentralized identifier* o DID), que es único y no requiere autoridad central de registro, dado que forma parte de un directorio distribuido y descentralizado, y un documento con los datos legales o biométricos vinculados al DID anterior (*DID document*). El empleo de estos mecanismos reduce la huella digital de sus titulares por las bases de datos sin necesidad de contar con un validador externo. Otorgan mayor protección –soberanía– sobre la identidad digital a sus titulares, pero no garantizan un anonimato absoluto, porque el uso de un mismo DID en múltiples ocasiones, o en un número limitado de ellas, hace posible la deducción de perfiles a partir de datos ciertos y precisos atribuibles a una misma identidad digital –para asegurar el anonimato es esencial utilizar un pseudónimo irrepetible–. La identidad autosoberana también plantea cuestiones relacionadas con la soberanía y la nacionalidad que competen a los Estados, responsables de la generación de la identidad de sus ciudadanos y de la custodia de sus datos personales, otra cuestión ya analizada en *CIBER elcano*.

Los sistemas de identidad y gestión de acceso corporativas (sistemas IAM)

La identidad y la reputación *online* constituyen activos intangibles de gran valor. Los mecanismos de monitorización y conformación de la identidad digital permiten, a través de redes sociales o medios de comunicación *online*, gestionar la identidad, la reputación corporativa y la marca. Dado el ámbito global y abierto de las redes corporativas e Internet, el modelo de seguridad perimetral ha dejado de ser válido y ha evolucionado hacia un modelo de "confianza cero" que exige una verificación estricta de identidades para cada persona o dispositivo que intente acceder a los recursos de la red, asumiendo que todo acceso es, *a priori*, una intrusión.

Los sistemas de gestión de la identidad y el acceso (*identity and access management* o IAM) a las redes corporativas por las distintas identidades individuales con las que interactúan (empleados, colaboradores, socios comerciales, clientes finales, suministradores…) adquieren máxima importancia en un entorno altamente digitalizado y expuesto a ciberamenazas. Los sistemas IAM en empresas y organismos públicos se han convertido en una piedra angular para el desarrollo de modelos de negocio en entornos altamente digitalizados, para la mejora de la experiencia del usuario en su interacción con los servicios *online* y para la prevención de ciberataques.

Los sistemas IAM verifican la identidad y autorizan o deniegan el acceso a los sistemas de información de la organización asegurando su usabilidad y el cumplimiento de la regulación sectorial –p. ej. la Directiva de Servicios de Pago de la UE (PSD 2) en el sector financiero–. Esto implica verificar si el usuario puede tener acceso a un determinado recurso en un momento dado y con un propósito legítimo. Suman dificultad a esta tarea las interacciones de las empresas con sus cadenas de suministro, en ocasiones muy complejas, y el uso generalizado de dispositivos móviles personales por los clientes y los empleados. Además, es particularmente importante asegurar el acceso a las cuentas privilegiadas de los sistemas de la empresa, la custodia de estas identidades y la gestión de credenciales de empleados y desarrolladores autorizados.
Un sistema IAM ha de contar con capacidad para gestionar las distintas identidades de una persona dependiendo de la relación que en cada momento establece con la corporación (*identity relationship management* o IRM), dando permisos en función del rol que la persona desempeñe en cada momento en la organización –el rol pasa a ser un atributo más de una identidad, sumándose a otros como el dispositivo móvil o la ubicación desde la que se accede–. Asimismo, la gestión de las identidades mediante una plataforma global IAM ha de evolucionar al ritmo de la digitalización del negocio, por lo que es necesario definir una política IAM eficaz y segura, adaptada a las características de la organización, monitorizar su cumplimiento y adoptar medidas técnicas de seguridad embebidas en los procesos y productos.

Los procesos de control de identidades generan un volumen ingente de datos asociados al ciclo de vida de la identidad del usuario, sus permisos y actividad. Para facilitar su gestión, se utilizan técnicas de robotización de procesos (*robotic process automation* o RPA) y analítica avanzada de la información aplicada al IAM con dos finalidades: detectar y prevenir ciberincidentes a partir de la interpretación de patrones y riesgos vinculados a la actividad del usuario y generar indicadores según el rol que desempeñe el usuario y su aportación de valor al negocio.

En consecuencia, toda corporación ha de implantar su propia estrategia de IAM, promovida por el responsable del negocio con el apoyo del CISO, dotada de presupuesto, que involucre a la alta dirección y cuente con la participación de las distintas áreas de negocio en el proyecto (ciberseguridad, sistemas, auditoría interna, DPO, negocio…) junto con la colaboración de un integrador encargado de coordinar las distintas tecnologías y áreas implicadas en la implantación de una plataforma IAM que priorice la gestión de las cuentas privilegiadas y que desarrolle con flexibilidad nuevas capacidades al ritmo del negocio.

La identidad de los dispositivos conectados (IDoT) y su gestión

Los dispositivos conectados en el ámbito del hogar (IoT) y en la industria (IIoT) plantean un debate conceptual sobre si éstos tienen una identidad *online* propia vinculada a su huella digital en la medida en que tengan autonomía funcional, de decisión y de acción –gracias al uso de inteligencia artificial– en sus interacciones con otros dispositivos conectados y con el entorno, que arrastran la huella digital de sus actuaciones *online* junto con información sensible vinculada a terceras personas y empresas. Directamente relacionado con la gestión de la identidad de los objetos conectados, se derivan

asimismo graves riesgos de ciberseguridad si éstos no se identifican, autentican y controlan debidamente a lo largo de la vida útil del dispositivo.

Un punto de partida indispensable es cumplir unas medidas mínimas de ciberseguridad por diseño enfocadas a asegurar la instalación de actualizaciones del *firmware* o evitar manipulaciones –remotas o *in situ*– del dispositivo que puedan facilitar el acceso a la red y a los datos almacenados como paso previo a perpetrar un ciberataque o un ciberdelito. La complejidad de la gestión de identidades y del control de acceso a sistemas corporativos de los IIoT aumentará en la medida en que proliferen objetos (auto)conectados a través de redes 5G en entornos industriales 4.0.

Para gestionar mejor la identidad de los dispositivos conectados (IDoT), se plantea establecer un registro de la identidad del dispositivo que contenga información sobre la vinculación dispositivo-identidad y su autenticación; ampliar el sistema de gestión de activos para inventariar y documentar los dispositivos IIoT; gestionar las identidades IDoT teniendo en cuenta cómo interactúan las diferentes elementos entre sí y con el resto de las infraestructuras (IRM); revocar permisos finalizada la vida útil del dispositivo; incorporar la IDoT en el sistema de gestión global de identidades IAM; llevar a cabo una gestión de riesgos y el control de su cumplimiento; establecer un plan ante fallos y brechas de seguridad de los activos IIoT, e implementar un sistema de gestión de usuarios privilegiados para asegurar el acceso de los administradores a la plataforma de monitorización y control de estos dispositivos.

Amenazas y medidas de seguridad para la identidad digital

Además de las medidas de ciberseguridad recomendadas para proteger los terminales de usuarios privados y corporativos y evitar la sobreexposición a las redes sociales, deben adoptarse otras medidas de seguridad específicas para proteger la identidad digital. Una de las principales vías para cometer fraudes y ciberataques es la suplantación de identidades (*phishing*) mediante el robo de credenciales y el envío masivo de correos electrónicos (*spam-phishing*) que suplantan a una determinada entidad (plataforma *online*, entidad bancaria, tienda…) con el fin de obtener las credenciales de acceso del usuario.

El correo electrónico es actualmente el principal medio de intrusión en las redes corporativas y de robo de credenciales[2], a pesar de las precauciones que adoptan los responsables de ciberseguridad de las corporaciones o de las buenas prácticas que recomiendan los centros de alerta oficiales. Una modalidad cada vez más frecuente son los ataques respaldados por prácticas de ingeniería social dirigidos a personas, organizaciones o empresas específicas (*spear-phishing*) para cometer estafas o instalar *malware* que facilite la intrusión a la red corporativa.

En el ámbito personal, tanto de usuarios privados como de empleados, es necesario adoptar una gestión segura de las claves de acceso activando –siempre que el sistema

[2] La asociación internacional APWG estima en 65.000 el número medio mensual de recursos en la web (URL) dedicados al robo de identidades (phishing) en los servicios de correo (30%), instituciones financieras (19,4%) o medios de pago (19,8%). “Phishing Activity Trends Report”, 4.º trimestre de 2019.

lo permita– al menos dos factores de autenticación y utilizando un gestor de claves o un inicio de sesión único (*single sign on* o SSO), que facilitan el acceso a varias aplicaciones o sistemas mediante las credenciales de una sola cuenta o plataforma. Para reducir la probabilidad de ser objetivo de ataques dirigidos de suplantación, es aconsejable limitar la exposición de información personal en redes sociales.

Por último, cabe señalar que la presencia en Internet de las empresas a través de páginas web, redes sociales, blogs, etc. requiere la adopción de medidas orientadas a proteger el perfil corporativo y evitar accesos de terceros que mediante la suplantación de la identidad corporativa causen daños comerciales y reputacionales.

Derechos asociados a la identidad y reputación *online*

Los derechos asociados a la identidad física de personas naturales y jurídicas se extienden a la identidad digital y, por lo tanto, le son aplicables a pesar de que no tenga reconocimiento legal como tal. De este modo, el Estado es garante de su cumplimiento a través de sus entidades judiciales, teniendo en cuenta dificultades tales como que la protección de un derecho vulnerado en Internet puede suponer la concurrencia de diferentes legislaciones, jurisdicciones y geografías. Este marco jurídico protege a las personas y su identidad ante delitos cometidos en la Red tales como injurias o calumnias vertidas a través de blogs, plataformas o redes sociales, suplantación de la identidad o el ejercicio del derecho al olvido o borrado de datos personales.

Dentro de la legislación aplicable, destacan el artículo 79 y siguientes de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, donde se establece que “los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación”. Entre otros, cabe mencionar la protección de datos de los menores en Internet (art. 92); el reconocimiento del derecho al olvido en búsquedas de Internet (art. 93), servicios de redes sociales y equivalentes (art. 94), o el derecho al testamento digital (art. 96).

Varias y notables son las modificaciones constituidas en la nueva regulación del ciberespacio en España establecida por el Real Decreto Ley 14/2019 en el ámbito de la identidad y administración electrónica. La nueva regulación, ya analizada en *CIBER elcano*, pone en evidencia la importancia de la identidad digital de los ciudadanos en el ámbito de la soberanía de los Estados. Entre otras medidas, considera el documento nacional de identidad, con carácter exclusivo y excluyente, como el único documento con suficiente valor por sí solo para la acreditación de la identidad y los datos personales de su titular. El real decreto ley establece medidas en materia de identificación electrónica ante las Administraciones Públicas y sobre la ubicación de determinadas bases de datos y datos cedidos a otras Administraciones Públicas; en relación con los sistemas de clave concertada para identificar a los ciudadanos ante la Administración, o sobre la prohibición del uso de tecnologías de registro distribuido (*blockchain*) en las relaciones con las Administraciones.

La protección de la identidad digital progresa a medida que la jurisprudencia la asocia a los derechos fundamentales inherentes al ser humano. Entre ellos se encuentran el derecho a la dignidad de la persona, al honor, a la intimidad personal y a la propia imagen. Todos ellos se recogen en la Declaración Universal de los Derechos Humanos (artículo 12) y el Convenio Europeo de Derechos Humanos (artículo 8). En España estos derechos están reconocidos en la Constitución Española (artículos 10, 18, 20.4 y 96), la Ley Orgánica 1/82, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el Reglamento General de Protección de Datos de la Unión Europea (RGPD) y el Real Decreto Ley 14/2019 sobre medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

Algunas sentencias judiciales, como la sentencia del Tribunal Supremo de 10 febrero de 2011, protegen la reputación *online* de las personas físicas apoyándose en la normativa que protege el honor de la persona física. Otras, como la sentencia del Tribunal de Justicia de la UE de 13 de mayo de 2014 del caso Google sobre derecho al olvido, permiten solicitar la eliminación de los datos personales que afecten a la reputación *online* —en septiembre de 2019 el TJUE limitó el ejercicio del derecho al olvido al territorio de la UE—. Finalmente, la sentencia del Tribunal Constitucional 139/1995, de 26 de septiembre, reconoce el derecho al honor de las personas jurídicas y su aplicabilidad a su identidad digital y reputación *online*. Por consiguiente, las empresas quedan protegidas ante los delitos cometidos en la Red de injurias o calumnias vertidas sobre la actividad mercantil, los productos o servicios ofrecidos por la empresa, la afectación a la imagen o marca de la empresa, el uso no autorizado de la marca o la suplantación de la identidad corporativa.

Por último, pero no menos importante, hay que mencionar varios instrumentos relacionados con el uso de la identidad digital de los ciudadanos y empresas españoles:

- la Ley 59/2003 de Firma Electrónica equipara la firma electrónica reconocida a la firma manuscrita, exige una serie de garantías que deben cumplir los dispositivos de creación de firma, reconoce como prueba documental el soporte en el que figuran los datos firmados electrónicamente, impone requisitos especiales a los responsables de la custodia de tales datos y regula la actuación de las personas jurídicas firmantes;

- el DNIe como medio de autenticación de la identidad, de firma electrónica y de certificación de la integridad de documentos o del documento de viaje;

- el sistema Cl@ve, orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos;

- el sistema europeo y Reglamento eIDAS para el reconocimiento de identidades electrónicas en el terreno de las transacciones económicas entre empresas en la UE;

- la Directiva PSD 2, regulación sectorial que establece, entre otras, medidas de refuerzo para la protección de la identidad, las operaciones *online* y los datos de los clientes en sus relaciones con las entidades financieras.

Conclusiones

La relevancia de gestionar y asegurar la identidad *online* de las personas naturales, empresas y dispositivos ha crecido debido al vertiginoso proceso de digitalización de la sociedad, la industria y las Administraciones Públicas. Los sistemas de gestión de la identidad y acceso *online* a empresas y organismos públicos son una piedra angular para el desarrollo de modelos de negocio y una Administración Pública eficiente y eficaz en la atención a sus ciudadanos, así como para la prevención de intrusiones en los sistemas de información como primer paso de ciberataques.

La Unión Europea y la Administración española han implantado instrumentos legales para el reconocimiento de la firma electrónica, la identificación personal (DNI electrónico) o el reconocimiento de identidades electrónicas en el terreno de las transacciones económicas entre empresas en la UE (sistema eIDAS).

Parejo a esta realidad, nuevas leyes y regulaciones extienden la salvaguarda de los derechos constitucionales de ciudadanos, corporaciones y estados en la Red. Reconocen y garantizan de este modo la protección de un conjunto de derechos digitales ante ciberdelitos y ciberataques cometidos en un gran número a partir de la suplantación y robo de las credenciales de los usuarios, el principal riesgo en la actualidad.