

FORO DE LA GOBERNANZA DE INTERNET EN ESPAÑA



09/07/2009

Identidad Digital

Reunión abierta al público del Foro de la Gobernanza de Internet. Ponentes: Fernando de Pablo, Salvador Soriano, Ruth Gamero, Pedro Sánchez Pernia, Enrique Dans

Foro de la gobernanza de Internet en España

IDENTIDAD DIGITAL

INTRODUCCIÓN

¿Qué es la Identidad Digital?

El uso de Internet en la vida diaria está contribuyendo a la configuración de las identidades digitales. Su gestión no es tarea fácil, y es que compartir información en la Red puede no ser compatible con tener el control y la propiedad sobre ella.

Por definición, identidad es aquel conjunto de rasgos propios de un individuo o colectividad que los caracterizan frente a los demás. La verificación de estos rasgos es lo que nos permite determinar que un individuo es quien dice ser. Algunos de estos rasgos son propios del individuo, otros son adquiridos con el tiempo. Por supuesto, no todos los rasgos son igualmente apreciables. Hay rasgos que son apreciables a simple vista, mientras que otros están ocultos y es necesario un conocimiento y, en ocasiones, herramientas para poder verificarlos.

Hasta hace poco, configurar la identidad personal era, en general, algo tan complicado como lo ha sido siempre pero, al menos, sólo había que gestionar, en la mayor parte de los casos, una única realidad: nuestro entorno cercano.

Sin embargo, con la popularización de Internet los individuos han revolucionado el concepto que hasta ahora se tenía de identidad personal y han forjado lo que se viene en llamar su **identidad digital**, cuya gestión es de vital importancia en un mundo en el que la información representa un aspecto importantísimo de nuestras vidas.

Al **conjunto de rasgos que caracterizan a un individuo o colectivo en un medio de transmisión digital** se le conoce como Identidad Digital.

La identidad digital hace referencia a la imagen que proyectamos de nosotros mismos a través de los soportes digitales y cómo nos ven los demás. Esta imagen es de gran importancia para todos, tanto si somos usuarios activos de Internet, participando en discusiones, foros, redes sociales o escribiendo en blogs, como si nos limitamos a leer páginas y nada más. Para bien o para mal, **la red se ha convertido en una enorme acumulación de información de todo tipo** que incluye a las personas y es más que probable que nuestro nombre aparezca en los buscadores aún cuando no hayamos hecho nada relevante en Internet. Esta información, que puede ser de lo más diversa y de fuentes totalmente insospechadas, **forma parte también de nuestra identidad digital** y nos definen y califican ante los demás.

Por qué abordar esta cuestión desde el Foro de la Gobernanza de Internet

Desde el Foro abordamos esta cuestión en un intento por promover sistemas de identidad digital adecuados a los nuevos retos de la Sociedad de la Información y hacer una llamada a la participación pública en su diseño y aplicación.

A medida que el mundo online se mueve hacia la Web 2.0, el concepto de identidad digital evoluciona y los sistemas de identificación existentes presentan inconvenientes. En esta cuestión la voz de la sociedad civil debe hacerse oír con su experiencia y sus necesidades.

La Identidad Digital constituye una cuestión emergente y como tal ha sido tratada en el *Internet Governance Forum* en talleres en 2006, 2007 y 2008. Se trata de un tema incluido en el mandato del IGF en su párrafo 72 (a, g, j, k), en el que se insta a debatir cuestiones de políticas públicas relacionadas con los elementos claves de Internet para fomentar el desarrollo de Internet, a identificar cuestiones emergentes y hacerlas llegar al público general y a ayudar a encontrar soluciones a las cuestiones relacionadas con el uso y el mal uso de Internet.

GESTIÓN DE LA IDENTIDAD DIGITAL

La gestión de la identidad es actualmente ya un elemento clave en el e-Comercio y la e-Administración y está adquiriendo una gran importancia en el tejido social y empresarial. Existen datos digitales sobre una persona que van desde ecografías pre-natales hasta certificados de defunción, pasando por todos los datos recolectados por distintas agencias y organizaciones a lo largo de la vida e incluyendo los blogs que se han publicado, los correos electrónicos enviados, los perfiles almacenados, etc., generando una significativa “huella digital” personal en el ciberespacio. Accesible o no, dejada de forma consciente o no, esta colección de datos, cuando analizados en conjunto, contribuye a la definición de la identidad propia.

La interacción en la red puede estar basadas (en ocasiones debe ser así) en una información muy reducida sobre cada una de las partes. Sin embargo, a medida que la actividad online toma un rumbo paralelo a la experiencia del mundo físico, se han ido desarrollando infraestructuras y sistemas de tecnologías de la información y las comunicaciones más adecuadas. Resulta útil, por ejemplo, que las preferencias personales y los perfiles de los usuarios estén disponibles cuando se hacen compras en la web, sin necesidad de exigir a los usuarios que introduzcan esta información repetidas veces. En este escenario, la gestión de la identidad digital resulta fundamental en la creación de una “experiencia de usuario” y la protección de la privacidad.

Las Redes Sociales en la forja de la Identidad Digital¹

Las redes sociales tienen un papel fundamental a la hora de potenciar nuestra propia identidad difundirla a conocidos y/o extraños y facilitando nuevas formas de relación social. No sólo las redes sociales: también los blogs, los foros de discusión, las salas de chats y todas las herramientas que han permitido que **Internet haya evolucionado** en apenas un lustro **no sólo para usar la Red sino para estar -y por tanto, ser- en ella.**

"Las TIC están creando una identidad expandida en la mayoría de sus usuarios. Potencian sus habilidades y los capacitan para estar en contacto con otros con diferentes niveles de relación, intimidad, compromiso, etc. Por eso vemos la creación de nuevos grupos, comunidades y relaciones de contacto o amistad virtual que están creando un nuevo tejido social". Lo explica para el Boletín de Red.es [Juan Varela](#), consultor de comunicación, periodista y reconocido blogger. Según él, "una gran parte de los internautas ya están desarrollando esas capacidades y utilizando las ventajas de la

¹ La forja de una Identidad digital (RED.ES) <http://www.red.es/reportajes/articulos/id/3545/forja-una-identidad-digital-.html>

identidad digital en diferentes oportunidades con diferentes grados de compromiso, adscripción o revelación de su privacidad".

Existen dos grandes contenedores donde ejercer nuestra vida digital: las redes de amigos y las redes de interés. En el primer caso estaríamos hablando de algo así como "comunidades íntimas a tiempo completo", como son los casos de Tuenti, Facebook o TecnoTribu. En el segundo, las relaciones de nuestro 'Yo' digital tienen un alcance más global y se establecen en base a intereses similares, siendo canales para ganar visibilidad y reputación entre pares, normalmente a nivel profesional. Aquí podemos hablar perfectamente de redes tipo LinkedIn, Viadeo o Networking Activo. Especialmente en esta segunda clasificación los datos vienen a decir que, en las redes profesionales, se tiende a buscar el contacto personal y que ellas no suponen más que una herramienta destinada a tal fin por lo que, también en eso, la gestión de la identidad digital mejora nuestras relaciones sociales y la gestión de la identidad real". Las redes virtuales profesionales permiten dar a conocer nuestros perfiles en el mundo empresarial. De lo que se trata es que cuando un responsable de recursos humanos escriba el nombre de una persona en un buscador, dicha persona aparezca en un sitio web riguroso y demuestre que se mantienen contactos asiduos y profesionalmente ricos con otras personas destacadas del sector.

PERSONALIDAD E IDENTIDAD DIGITAL EN LA SOCIEDAD DE LA INFORMACIÓN

A medida que la sociedad empieza a adentrarse en el entorno ubicuo de la información, una cuestión clave es si los principios de protección de datos necesitan ser reforzados. En términos de gestión de la identidad, es fundamental diseñar un entorno legal y tecnológico que respeten ciertas "propiedades de la identidad"; si no se genera un entorno adecuado para la protección de los datos, no hay "rendición de cuentas" y, sin esta responsabilidad, no hay confianza. El gráfico más abajo muestra cómo estos elementos se construyen uno sobre otro:



ILUSTRACIÓN 1

FUENTE: OECD (2007) AT A CROSSROADS: "PERSONHOOD" AND DIGITAL IDENTITY IN THE INFORMATION SOCIETY STI WORKING PAPER 2007/7

La Identidad es tanto un concepto del "mundo real" como un artificio digital. En este documento hacemos referencia a "identidad digital" como a lo que los tecnólogos en el campo de la gestión de la identidad conciben como una "representación digital de un conjunto de alegaciones hechas sobre una parte sobre sí mismo o sobre otro sujeto"².

² Definición desarrollada en una lista de correo de Identity Gang, un grupo que comprende a más de 2000 profesionales en esta área. La definición de "identidad digital" tal como es utilizada por este grupo aparece en el diccionario de Identity Gang en http://identitygang.org/moin.cgi/Digital_Identity.

Tal y como los términos “individuo” y “perfil” sugieren, la información sobre la identidad pueden ser utilizadas por diferentes personas para describir a una persona. Tal y como se entiende por la Unión Europea, cuando la información en una identidad digital está relacionada con una persona natural identificada o identificable, constituye “datos de carácter personal”.

La gestión de la identidad digital debe incluir tecnologías que permitan a una persona permanecer anónima al mismo tiempo que se intercambian datos sobre sí misma, en cuyo caso estaríamos hablando de “información personal”, como término más genérico para los datos referidos a una persona, ya sea identificada/identificable o no.

Identidad Digital vs Identidad Electrónica

No debe confundirse “Identidad Digital” con “Identidad Electrónica”. Esta última tiene como característica utilizar una sola tarjeta o identificación para acceder a ciertos servicios que existen en el mundo físico. De tal manera que técnicamente entendemos identidad electrónica como el conjunto de elementos necesarios para garantizar (dentro de lo razonable), la identidad a través de medios electrónicos, así como todos los elementos que permiten gestionar y proporcionar funcionalidad en este medio.

Actualmente la identidad electrónica incluye principalmente los siguientes elementos:

- Certificados digitales (incluido su soporte físico)
- Firma electrónica
- Gestión y propagación de derechos.
- Simplificación de identificación en múltiples entornos (SSO)

La cuestión de la Identidad Electrónica

El uso de certificados electrónicos acreditativos de nuestra identidad supone para la mayoría de las personas **una novedad que nos genera bastantes interrogantes**.

El ejemplo más evidente de Identidad Electrónica lo supone el DNI electrónico que actualmente para el caso español **cumple los estándares europeos** y que, por tanto, puede ser leído por cualquier lector de certificados digitales. Sin embargo, en el certificado del DNI-e **sólo están los datos de identificación** de la persona, es decir, los mismos que figuran visibles en el plástico soporte del certificado. Otra cuestión es que servicios puedan utilizarse en los distintos países de la UE identificándose con el DNI-e español, aunque la urgencia más acuciante es que puedan utilizarse con el DNI-e los servicios del propio país.

Una cuestión que preocupa, y mucho, es la de las **identidades múltiples**: como ciudadano de un país, como empleado de una empresa, como cliente de un determinado servicio. Lo cual plantea las siguientes preguntas: ¿Qué entendemos por identidad si las identidades son distintas en cada contexto? ¿Quién entidad u organismo define la identidad, el Gobierno para unos casos pero no para otros? ¿Quién gestiona la identidad teniendo en cuenta que el documento físico de identidad es único y, en teoría no se puede copiar pero sí los datos que están contenidos en él? ¿Quién asegura que alguien es realmente la persona que afirma ser?

Aparentemente el DNI-e resuelve dichas cuestiones en el sentido que el documento aporta los datos necesarios para cada caso en servicios de consulta de administración pública.

En cualquier caso, la tendencia futura, según los expertos, es hacia sistemas de identificación biométrica. Los sistemas de identificación “**cero conocimiento**” aportarían seguridad al tratarse de sistemas de acceso a servicios que no requieran desvelar la identidad del usuario.

Identidad Electrónica en la UE³

El pasado 30 de mayo de 2008 la Comisión Europea anunció un proyecto piloto cuyo objetivo era garantizar el **reconocimiento transfronterizo de los sistemas nacionales de identidad electrónica (eID)** y facilitar el acceso a los servicios públicos en 13 Estados miembros. El proyecto de la Comisión permitiría que los ciudadanos de la UE demuestren su identidad y utilicen los sistemas nacionales de identidad electrónica (contraseñas, tarjetas de identidad, códigos PIN y otros) no solamente en su país, sino también en la UE. El plan consiste en armonizar y conectar estos sistemas, sin sustituir lo que ya existe. El proyecto durará tres años y será financiado con 10 millones de euros por la Comisión Europea y con una cifra idéntica por los socios participantes.

La comisaria europea Viviane Reding afirmó entonces “Este proyecto, que se apoya en el desarrollo de los sistemas nacionales de eID y fomenta el reconocimiento mutuo de las identidades electrónicas entre los Estados miembros, nos acerca un paso más a ese desplazamiento transparente de un país de la UE a otro que esperan los europeos de un mercado único europeo sin fronteras”

El principal objetivo del proyecto es unificar los sistemas de identificación entre los países comunitarios o al menos, hacerlos compatibles entre sí.

Un acceso fácil a los servicios públicos en toda la UE es algo esencial para los ciudadanos comunitarios que se desplazan por Europa por motivos profesionales, de estudio o de ocio, y contribuye a potenciar la movilidad de los trabajadores en Europa.

DNI-e⁴

El Documento Nacional de Identidad (DNI), emitido por la Dirección General de la Policía (Ministerio del Interior), es el documento que acredita, desde hace más de 50 años, la identidad, los datos personales que en él aparecen y la nacionalidad española de su titular

A lo largo de su vida, el Documento Nacional de Identidad ha ido evolucionado e incorporando las innovaciones tecnológicas disponibles en cada momento, con el fin de aumentar tanto la seguridad del documento como su ámbito de aplicación.

Con la llegada de la Sociedad de la Información y la generalización del uso de Internet se hace necesario adecuar los mecanismos de acreditación de la personalidad a la nueva realidad y disponer de un instrumento eficaz que traslade al mundo digital las mismas certezas con las que operamos cada día en el mundo físico y que, esencialmente, son:

- Acreditar electrónicamente y de forma indubitada la identidad de la persona

³ Más información en:

Identidad electrónica: http://ec.europa.eu/information_society/activities/egovernment/policy/key_enablers/eid/index_en.htm

Administración electrónica: <http://ec.europa.eu/egovernment>

PAP TIC: http://ec.europa.eu/ict_psp

PIC: http://ec.europa.eu/cip/index_en.htm

Iniciativa europea i2010: http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm

⁴ DNI-e Informe INTECO http://www.inteco.es/extfrontinteco/img/File/intecocert/dnie/pdf/presentacion_dnie.pdf

- Firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita

Para responder a estas nuevas necesidades nace el Documento Nacional de Identidad electrónico (DNle), similar al tradicional y cuya principal novedad es que incorpora un pequeño circuito integrado (chip), capaz de guardar de forma segura información y de procesarla internamente.

Para poder incorporar este chip, el Documento Nacional de Identidad cambia su soporte tradicional (cartulina plastificada) por una tarjeta de material plástico, dotada de nuevas y mayores medidas de seguridad. A esta nueva versión del Documento Nacional de Identidad nos referimos como DNI electrónico nos permitirá, además de su uso tradicional, acceder a los nuevos servicios de la Sociedad de la Información, que ampliarán nuestras capacidades de actuar a distancia con las Administraciones Públicas, con las empresas y con otros ciudadanos.

En la medida que el DNI electrónico vaya sustituyendo al DNI tradicional y se implanten las nuevas aplicaciones, podremos utilizarlo para:

- Realizar compras firmadas a través de Internet
- Hacer trámites completos con las Administraciones Públicas a cualquier hora y sin tener que desplazarse ni hacer colas
- Realizar transacciones seguras con entidades bancarias
- Acceder al edificio donde trabajamos
- Utilizar de forma segura nuestro ordenador personal
- Participar en una conversación por Internet con la certeza de que nuestro interlocutor es quien dice ser.

Demanda por mayor control de usuario

A medida que las empresas aumentan su dependencia de Internet, se enfrentan a retos tales como el aumento de amenazas de fraude y robo de la identidad; mayores requisitos regulatorios; crecimiento de la demanda del consumidor en protección de la privacidad; y la necesidad competitiva de asociarse con otras empresas para interconectar sus servicios online. Estas nuevas fuerzas de mercado influirán en la construcción de un mercado de la identidad digital.

Prácticamente todas las actividades online, incluyendo el envío de correo electrónico, presentación de la declaración de la renta, gestión de las cuentas bancarias, compra de bienes, juegos online, conectarse a la intranet de una empresa y encontrarse con otras personas en un mundo virtual, exigen el intercambio de información de la identidad entre dos o más partes. La abundancia de diferentes situaciones y tipos de información de identidad sugiere la necesidad de contar con una infraestructura flexible y centra en el usuario para la gestión de la identidad. Esta infraestructura debe ser lo suficientemente flexible para sostener los múltiples mecanismos y protocolos de identidad que existen y están surgiendo, y los diferentes tipos de plataformas, aplicaciones y patrones de arquitectura orientadas a servicios en uso.

El concepto de “centrado en el usuario” es nuevo en el marco de la gestión de la identidad digital. En primer lugar, los mecanismos de gestión deben estar “centrados en el usuario” ya que los usuarios finales

están en el núcleo mismo: la infraestructura debe otorgar poderes a los usuarios para llevar a cabo controles efectivos sobre su información de identidad. Algunos aspectos de esta tendencia se han materializado y madurado a lo largo de los últimos años (amplio desarrollo de plataformas y mecanismos para la identificación a través de *smart cards* o servicios de inscripción); al mismo tiempo, los modelos de administración evolucionan a medida que todas los elementos en una red, incluyendo los físicos como dispositivos y los virtuales como las políticas, necesitan ser identificados y representados correctamente.

La industria está dando lugar a una oferta competitiva en cuanto a marcos que capturen la creciente abstracción de la identidad. Al mismo tiempo, aumenta la necesidad de gobiernos y empresas de aumentar sus capacidades de identificación y localización rápida y efectiva de individuos y objetos, ya sea en asuntos relacionados con el terrorismo o la trazabilidad de objetos, con una mayor disponibilidad de tecnologías como RFID o GPS, y un problema latente relacionado con el robo de identidad especialmente acuciante en el caso de las entidades financieras.

La protección de la información personal sensible es crítica y las regulaciones de privacidad están en aumento. Aunque desde un punto de vista tecnológico, las prioridades pueden ser autorización y control, éstos no son siempre los elementos clave en cuanto a posibilitar al usuario final con los controles necesarios para proteger la información de su identidad: los usuarios deben ser informados sobre qué datos se le solicitan y cómo se tratan sus datos personales (por ejemplo, propósito con el que se recaban los datos y quién puede acceder a ellos). A través de este proceso, los usuarios pueden decidir si proporcionar sus datos y dar su consentimiento.

Hay un interés tremendo en las nuevas tecnologías de la web 2.0 que no sólo prometen una experiencia más rica para el usuario, sino que también se centran específicamente en el valor de conectar a la gente y amplificar el potencial de trabajar en equipo. Los retos específicos para la infraestructura de identidad en esta área están precisamente en orientarlo a las personas y acomodar la naturaleza dinámica y auto-organizativa de estos entornos.

Tecnologías orientadas a la privacidad

A lo largo de los últimos treinta años se ha realizado amplia investigación en tecnologías y criptografía para el desarrollo de tecnologías orientadas a la privacidad (PET, *Privacy Enhancing Technologies*). Se trata de un conjunto diverso de tecnologías generalmente orientadas a proteger el anonimato de los individuos, la desvinculación de las transacciones y la no-observación de las comunicaciones. Entre los ejemplos encontramos: criptografía orientada a firmas ciegas y revelación selectiva de atributos; redes de comunicación anónimas; gestión de bases de datos y resistencia a ataques; gestión de datos cifrados y búsqueda cifrada...

En muchos contextos se pueden sustituir los sistemas de identificación por sistemas de autenticación; la autenticación no tiene por qué requerir la identificación de un individuo. La autenticación es el proceso por el que se verifica un requisito que se exige a una entidad, un atributo perteneciente a una identidad, o un conjunto de atributos.

CUESTIONES CLAVES

- En la sociedad de la información, ¿tendría sentido garantizar el derecho de los individuos a acceder y hacer uso de las tecnologías orientadas a la privacidad? ¿Cómo podrían formularse y delimitarse estos derechos? ¿Debería tratarse de derechos fundamentales o sólo tiene sentido esbozarlos en el contexto de gobiernos opresores?
- ¿Debería establecerse la obligación de que ciertos tipos de sistemas de información implementen tecnologías orientadas a la privacidad?

- En el panorama actual de redes sociales y web 2.0, ¿están en funcionamiento las plataformas adecuadas para garantizar la desvinculación de los distintos roles que adquiere una persona en función de la actividad que realiza en Internet? ¿Constituye una demanda del usuario?
- Las diferentes legislaciones sobre protección de datos y las grandes diferencias entre los enfoques que se aplican desde distintas regiones (por ejemplo, Estados Unidos y Europa), ¿son suficientes para garantizar la privacidad del usuario en un entorno inherentemente global?
- ¿Está el usuario adecuadamente formado e informado para el uso de tecnologías para la protección de su privacidad?
- Desde un punto tecnológico, ¿puede construirse la gestión de la identidad de forma que proporcione seguridad y privacidad al mismo tiempo? ¿Se trata de un compromiso?
- ¿Cuáles son las implicaciones desde el punto de vista de las políticas públicas? ¿Es necesaria una mayor coordinación a nivel internacional?