LA RAZÓN

Publicación	La Razón Cataluña, 56	Fecha	01/12/2023
Soporte	Prensa Escrita	País	España
Circulación	8421	V. Comunicación	154 028 EUR (168,042 USD)
Difusión	7321	Tamaño	450,37 cm² (72,2%)
Audiencia	37 510	V.Publicitario	26 672 EUR (29 099 USD)

La identidad digital se está gestando en Europa desde 2014

La nueva identidad digital europea, en entredicho por falta de seguridad

La UE ultima una app móvil desde la que se podrá acceder a todos los datos privados, desde el padrón a la formación. La idea es facilitar gestiones, garantizando la privacidad. Sin embargo, un polémico artículo deja a los estados la posibilidad de controlar nuestro tráfico online

Eva M. Rull. MADRID

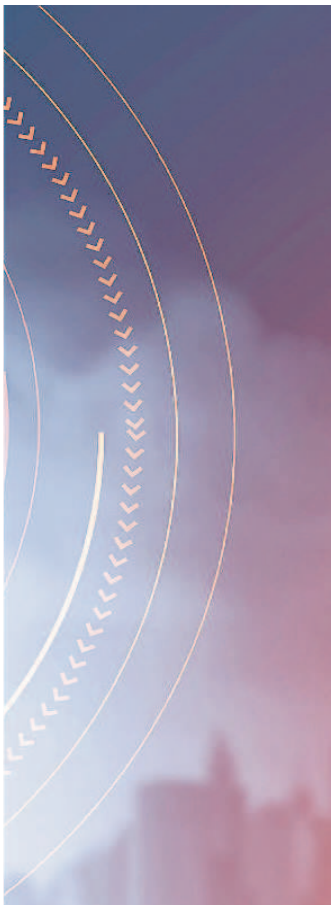
Todos llevamos en nuestra cartera un DNI con chip. Gracias a él, se supone, podríamos realizar cualquier trámite público con facilidad. Sin embargo, pocos meses bastaron para descubrir que aquel intento de digitalización era un completo fracaso; solo un 0,02% de personas lo utilizaban según el informe eEspaña 2014. A pesar del fiasco, el DNI ha seguido ahí infrautilizado y sumando, además, problemas de seguridad. En 2017 la policía desactivó la firma digital de los DNI expedidos a partir de 2015 por un fallo.

Quizá la sociedad no estaba tan digitalizada en 2013 como lo está ahora pero, en cualquier caso, no era fácil manejarse con el chip. Además de un PC, tenías que instalar un software y nadie (menos ese 0.02) parece que fue capaz de configurarlo y hacerlo funcionar. Ahora estamos más digitalizados, es cierto, pero ¿estamos preparados para tener toda nuestra vida en una App móvil? Porque precisamente es lo que prepara la UE. Estos días se acaba de aprobar el reglamento eIDAS 2, la nueva identidad digital Europea. «El eIDAS de 2014 preveía una gestión de identidad digital de los ciudadanos por cada país, que en España se centraba en el DNI electrónico, pero que tuvo poco éxito en lo relativo a la interoperabilidad transfronteriza. Se suponía que un ciudadano podría hacer gestiones en un estado diferente del propio con el sistema de identidad proporcionado por su país de origen. Y tras varios años de funcionamiento, se vio que habría que cambiar de enfoque. El resultado es que el Reglamento eIDAS 2 contempla la emisión de una «Cartera IDUE» (Identidad Digital de la Unión Europea) por cada Estado (una app) que permitirá a sus ciudadanos demostrar la identidad, hacer gestiones frente a las Administraciones Públicas, o frente a entidades privadas (incluso la posibilidad de utilizarlo en el comercio electrónico), y gestionar sus credenciales (carné de conducir, titulaciones, formaciones no oficiales, colegiaciones profesionales…)», explica Julián Inza, director del laboratorio de confianza digital del Observatorio LegalTeh & New Law de Comillas ICADE y presidente de EAD Trust.

Es decir un documento digital o wallet que controle todo y permita el acceso a cualquier trámite o gestión tanto pública como privada. Una de las ventajas que se le ven es que en teoría al funcionar con credenciales o información agrupada en bloques, podremos compartir solo la información que se nos pide en internet sin tener que proporcionar innecesariamente datos personales. «Si voy a comprar en una web y necesito demostrar que soy mayor de 18 años, ahora mismo la única forma que tengo de hacerlo es mandando una fotocopia de mi DNI en la que además de la edad figuran otros datos privados como dónde vivo o mi género; un montón de información privada innecesaria. La UE quiere apostar por una identidad, llamémosla soberana, que al tener credenciales separadas me permite mandar solo aquello que necesito enviar. Como cada uno somos soberanos de nuestros datos, en teoría estaríamos menos expuestos a la venta de datos por parte de

LA RAZÓN

Publicación	La Razón Cataluña, 57	Fecha	01/12/2023
Soporte	Prensa Escrita	País	España
Circulación	8421	V. Comunicación	154 028 EUR (168,042 USD)
Difusión	7321	Tamaño	439,40 cm² (70,5%)
Audiencia	37 510	V.Publicitario	26 213 EUR (28 598 USD)



terceros o a robos, etc.», explica Óscar Lage, responsable de Ciberseguridad de Tecnalia.

Otra ventaja tiene que ver con las garantías en la contratación de servicios. Para Unión Profesional, asociación que agrupa a los Consejos Generales y Colegios Nacionales de las profesiones tituladas y colegiadas españolas, el hecho de que el wallet incluya hasta las titulaciones es una oportunidad para que los usuarios verifiquen la formación o colegiación de la persona a quien contratan. «Se pretende que sea reconocido por todas las empresas y administraciones públicas de la UE y de esta forma pretende ofrecer garantías de seguridad, disponibilidad y mayor control sobre la información. Ahora bien, preocupan las cuestiones en torno a la privacidad y en particular la huella digital o el rastro que va a dejarse tras el uso o empleo de esta identidad digital europea. Preocupa los posibles usos

NUEVA IDENTIDAD DIGITAL

Solicitud de un préstamo bancario

AHORA

1. Fijar una cita con el banco
2. Reunión con el banco
3. Proporcionar todos los documentos en papel

Falta un documento

4. El banco envía la propuesta
5. Fijar otra cita con el banco
6. Nueva reunión en el banco para firmar el contrato del préstamo

DESPUÉS

1. El usuario tiene todos sus documentos en su cartera digital personal, desde el DNI hasta la declaración de ingresos
2. Solo selecciona los documentos que le pide el banco para solicitar el préstamo. Se los envía fácilmente y con total seguridad
3. El banco recibe los documentos por vía electrónica. Si falta alguno basta un clic para mandarlo. Ya puede tramitarse la solicitud

La identidad digital europea armoniza y agiliza el trámite

Ventajas de la Identidad Digital de la UE

- El derecho de toda persona que pueda optar a un documento nacional de identidad a tener una identidad digital reconocida en cualquier lugar de la UE
- Una manera sencilla y segura de controlar cuánta información queremos compartir con servicios que requieren compartir información
- Funciona a través de carteras digitales disponibles en aplicaciones para teléfonos móviles y otros dispositivos, para:
  - Identificarse en línea y fuera de línea
  - Almacenar e intercambiar información
  - Utilizar la información como confirmación del derecho a residir, trabajar o estudiar en un determinado Estado miembro

La identidad digital de la UE puede ser utilizada en muchos casos, por ejemplo:

- El acceso a servicios públicos, como solicitar un certificado de nacimiento o médico o comunicar un cambio de domicilio
- La apertura de una cuenta bancaria
- La presentación de una declaración de impuestos
- La solicitud de plaza en una universidad, en el país de residencia o en otro Estado miembro
- El almacenamiento de una receta médica para poder utilizarla en cualquier lugar de Europa
- La demostración de la edad
- El alquiler de un coche utilizando un permiso de conducir digital
- El registro en un hotel

Fuente: Comisión Europea

A. Cruz / LA RAZÓN

Europa, ¿más cerca del control de China?

En medios como Wired se ha apuntado a que con la introducción de este artículo, las autoridades europeas buscaban «acercar los navegadores estadounidenses a la esfera de influencia de los gobiernos europeos y mantenerlos bajo control. Pero tal como está formulada, la reforma corre el riesgo de otorgar a los usuarios una navegación menos segura y a los gobiernos un mayor poder de vigilancia, en lugar de aumentar la protección de los ciudadanos». En otros medios, se ha llegado a decir que esta acción equivale a colocar a Europa al nivel de China en cuanto a las capacidades del gobierno de espiar las comunicaciones. Hay que recordar que el país asiático implantó hace unos años un carnet por puntos para controlar el buen comportamiento de sus ciudadanos. El crédito social supone el acceso a determinados servicios para quien acumula puntos por consumir, por ejemplo.

secundarios por parte de gobiernos y el posible control que ello puede comportar. Por ello es fundamental garantizar el anonimato en muchas fases del tratamiento», opina Eduard Blasi, profesor de derecho en la UOC y divulgador en el canal de Instagram TechAndLaw.

Artículo 45

Y es que si hay un detalle que ha levantado ampollas de la identidad digital se trata, sin duda, del artículo 45. «La propuesta actual amplía radicalmente la capacidad de los gobiernos para vigilar tanto a sus ciudadanos como a los residentes en la UE, proporcionándoles los medios técnicos para interceptar el tráfico web cifrado, además de socavar los mecanismos de supervisión existentes». Así de contundentes se expresan los 400 firmantes, entre expertos en ciberseguridad y organizaciones como la Fundación Mozilla o la Fundación Linux, en una carta abierta que veía la luz hace unos días. En ella, advierten de que el texto obliga a los navegadores a limitar los requisitos de seguridad y aceptar como confiables todos las «Certification Authority» propuestas por los estados. «Cada vez que te conectas a una web, detrás hay una CA autorizada por el navegador que te garantiza que la web donde estés es segura y realmente la que afirma ser. Si alguna empresa certificadora la lía, le dan de baja. En el artículo 45 se dice que cualquier estado puede designar una CA, pero ¿qué sucede cuando se trata de un país que ha tenido problemas como Hungría con sistemas como Pegasus? ¿Y si emiten certificados, por ejemplo, para Gmail, pero en realidad nos lleva a una copia de Gmail que roba nuestros datos?», dice Lage, quien además es uno de los firmantes de la carta. Hay que recordar que hace ahora dos años, se detectó en Hungría un uso abusivo del software espía Pegasus. Fueron identificados los teléfonos de más de 300 ciudadanos a los que se estaba espiando. «El gobierno húngaro debe dar inmediatamente una respuesta significativa a esta reciente revelación del Proyecto Pegasus y aclarar si conocía o aprobó la vigilancia encubierta de periodistas, miembros del empresariado y otras personas. Si las autoridades húngaras conocían estas violaciones, deben explicar con qué fundamento las permitieron», decía entonces Dávid Vig, director de Amnistía Internacional Hungría.

Una relación de confianza

Hasta ahora, los navegadores son quienes deciden en qué empresas confían. «Hace menos de un año Google, Mozilla y Microsoft rechazaron Truscor porque estaba vinculado a una empresa de software espía y Camerafirma, porque no era lo suficientemente seguro. En este ámbito, al menos por una vez, los intereses de las grandes tecnológicas y los de los usuarios están alineados, porque los navegadores tienen interés en ofrecer una conexión segura si no quieren perder credibilidad», explica en un reportaje la revista Wired.

El artículo 45 no es nuevo, en gran parte lleva en gestación desde 2014, pero «esa frase que se cuela supone un riesgo para la privacidad de los datos personales y la confidencialidad de las empresas. Se podría descifrar todo el tráfico de internet. Con esta frase se obliga a los navegadores a tener que dar por bueno a esos CA y no darles de baja. Si estos CA no son seguros, están corrompidos o han recibido un ataque, alguien puede meterse en medio de la navegación en internet», concluye Lage.