idd | Identidad y Derechos Digitales

ANÁLISIS DEL REGLAMENTO (UE) 2024/1183: LA CARTERA DIGITAL EUROPEA

JOSE MIGUEL MORENO LÓPEZ

Cuadernos de la Cátedra Fundación Integra sobre Identidad y Derechos Digitales de la Universidad de Murcia

1/2024

ANÁLISIS DEL REGLAMENTO (UE) 2024/1183: LA CARTERA DIGITAL EUROPEA

José Miguel Moreno López
LinkedIn: https://www.linkedin.com/in/jose-miguel-moreno-lopez

Resumen: El presente artículo pretende abordar el impacto de la nueva cartera digital europea en los sistemas de identificación electrónica ante la Administración española y el tratamiento de datos personales. Para ello, comienza definiendo los conceptos de identidad digital y sistema de identificación electrónica, analizando brevemente su evolución hasta el modelo Self-Sovereign Identity.
Posteriormente, contextualiza el estudio presentando los diversos sistemas de autenticación disponibles para los ciudadanos en su relación con la Administración Pública. Seguidamente, considerara los aspectos más relevantes del proceso de transformación digital que ha experimentado el sector público español en las últimas dos décadas, y las particularidades de los sistemas de identificación públicos en materia de protección de datos, poniendo de relieve las dificultades concretas de ambas realidades.
Finalmente, se ahonda en la repercusión del Reglamento eIDAS 2.0. en el régimen de autenticación electrónica vigente en España, explicando su funcionamiento y las implicaciones de la nueva regulatoria europea en el ámbito público español.

Palabras clave: Identidad digital, Identificación electrónica, Self-Sovereign Identity (SSI), Identidad autosoberana, Cartera Digital Europea, transformación digital, administración electrónica, Reglamento eIDAS, Reglamento eIDAS 2.0., DNIe, sistema Cl@ve, CERES, Tecnología de Registro Distribuido, Interoperabilidad, Ciberseguridad.

Tittle: Analysis of Electronic Identification Systems and the impact of the European Digital Wallet: The Case of the Spanish Public Sector.

Abstract: This article aims to address the impact of the new European Digital Wallet on electronic identification systems in interactions with the Spanish Administration and the processing of personal data. To this end, it begins by defining the concepts of digital identity and electronic identification systems, briefly analyzing their evolution up to the Self-Sovereign Identity model.
Subsequently, it contextualizes the study by presenting the various authentication systems available to citizens in their interactions with Public Administration. Then, it considers the most relevant aspects of the digital transformation process experienced by the Spanish public sector over the last two decades and the specificities of public identification systems concerning data protection, highlighting the specific challenges of both realities.
Finally, it delves into the foreseeable impact of eIDAS 2.0 EU Regulation on the current electronic authentication framework in Spain, explaining its operation and the implications of the new European regulation for the Spanish public sector.

Keywords: Digital Identity, Electronic Identification, Self-Sovereign Identity (SSI), Sovereign Identity, European Digital Wallet, Digital Transformation, E-Government, eIDAS Regulation, eIDAS 2.0 Regulation, eID (Electronic National ID), Cl@ve System, CERES, Distributed Ledger Technology, Interoperability, Cybersecurity.

Cómo citar este trabajo: MORENO LÓPEZ, José Miguel. Análisis del Reglamento (UE) 2024/1183: la cartera digital europea. *Cuadernos de la Cátedra Fundación Integra sobre Identidad y Derechos Digitales de la Universidad de Murcia* [en línea]. 2024, n. 1. Disponible en: <https://...>.

1. Introducción

La identificación electrónica se ha consolidado como un elemento indispensable en la relación entre los ciudadanos y las Administraciones Públicas. Aunque inicialmente concebida bajo modelos centralizados, estos sistemas de identificación han evolucionado hacia estructuras que buscan conferir mayor protagonismo al usuario, pese a enfrentar retos significativos como su baja adopción, vulnerabilidades en materia de ciberseguridad y conflictos con el derecho fundamental a la protección de datos personales, especialmente en lo relativo al principio de minimización de datos.

Soluciones como el DNIe o el sistema Cl@ve, diseñadas desde una perspectiva centrada en la administración, han priorizado la eficiencia operativa sobre las necesidades de los ciudadanos, lo que ha derivado en una percepción negativa respecto a su utilidad y seguridad. Ante esta situación, el concepto de "identidad digital autosoberana" ha emergido como respuesta, promoviendo un modelo en el que el usuario retoma el control sobre sus datos personales.

En este contexto, el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (en adelante, Reglamento eIDAS 2.0), introduce instrumentos como la cartera digital europea, que aspiran a establecer un sistema de identificación único, interoperable y respetuoso con la privacidad, capaz de restaurar la confianza ciudadana en el entorno digital y fortalecer la interacción con las administraciones públicas en el marco de la Unión Europea.

2. Identidad legal e Identidad digital

Conforme al documento titulado "Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza", elaborado por el Grupo de Trabajo IV de la Comisión de las Naciones Unidas para el Derecho Mercantil internacional; la identidad legal se puede definir desde una triple perspectiva como: (1) conjunto de atributos relativos a una entidad; (2) información de un sujeto en forma de uno o diversos atributos que permiten diferenciarle en un contexto particular; (3) atributos de una persona que la describen inequívocamente en un contexto dado. Dichos caracteres son compilados y ratificados a través de sistemas de identificación, esto es, mecanismos que permiten a una persona obtener una determinada certificación de identidad que puede ser usada frente a terceros para probarla.

De conformidad con dicha definición, la identidad digital engloba un conjunto de atributos de los que una persona dispone en el entorno digital y que, de nuevo, permiten diferenciarla en dicho entorno. Por otro lado, la identificación electrónica es un proceso dirigido a determinar la exactitud de ciertos datos abarcados en la identidad digital de una persona, que la constriñen y la particularizan de entre cualquier otro operador digital (Batuecas, 2022, pp. 946-947).

La noción de identidad digital ha sufrido una transformación sustancial desde los primeros días de Internet, impulsada por la creciente complejidad de las actividades en el ámbito digital y la necesidad de garantizar la seguridad y confiabilidad en la identificación de los usuarios. Según Allen (2016), la evolución de los sistemas de identificación electrónica ha estado marcada por el control ejercido por distintos agentes a lo largo del tiempo.

En sus inicios, los sistemas de identidad se caracterizaban por su centralización. Este modelo se fundamentaba en la existencia de autoridades exclusivas que certificaban la identidad digital de los usuarios. Aunque eficaz en sus primeros años, esta estructura planteaba dos grandes limitaciones: la dependencia de las autoridades centrales, que restaba autonomía a los usuarios; y la falta de interoperabilidad más allá de las áreas específicas de operación de dichas entidades, lo que obligaba a los usuarios a desarrollar múltiples identidades digitales.

Posteriormente, el modelo evolucionó hacia sistemas federados, donde varias entidades colaboraban para ofrecer certificaciones electrónicas que permitían al usuario utilizar una única identidad en diferentes entornos digitales. Un ejemplo paradigmático de este enfoque fue el *Microsoft Passport* (1999), diseñado para facilitar el acceso rápido a múltiples sitios web mediante un único conjunto de credenciales. A pesar de representar un avance significativo, este modelo mantuvo una estructura subyacente de centralización que limitaba la plena autonomía del usuario.

Con el paso del tiempo, surgieron propuestas centradas en devolver el control de la identidad al individuo. El proyecto ASN (*Augmented Social Network*) buscó crear un entorno donde cada usuario pudiera gestionar su identidad digital y decidir con quién y cómo compartirla. Iniciativas como la *Internet Identity Workshop* (2005) impulsaron la creación de sistemas descentralizados, sentando las bases de tecnologías como OpenID, OAuth y FIDO. Sin embargo, estas soluciones, aunque innovadoras, no lograron abordar todas las necesidades de los usuarios en términos de privacidad y control.

La consolidación del modelo de identidad autogobernada, conocido como *Self-Sovereign Identity* (SSI), supuso un hito fundamental en este proceso evolutivo. Este enfoque pretende descentralizar por completo el almacenamiento y gestión de los datos de identidad, permitiendo a los usuarios determinar cómo y cuándo emplear su información personal sin depender de intermediarios.

El modelo de identidad autogobernada presenta una ruptura con los sistemas tradicionales al basarse en la autonomía del usuario y la descentralización de los datos. No obstante, en el contexto europeo, la regulación del eIDAS (*Electronic Identification, Authentication and Trust Services*) de 2016, se mantuvo alineada con un paradigma centralizado, enfocado en el desarrollo de sistemas gubernamentales para la gestión de identidades digitales. Este enfoque limitaba los atributos de la identidad digital a aspectos básicos como el nombre y la fecha de nacimiento, dejando fuera otros elementos relevantes como certificaciones, licencias o autorizaciones.

El Reglamento eIDAS 2.0 busca superar estas limitaciones adaptando la normativa al paradigma del SSI. Una de las innovaciones más destacadas es la introducción de una "cartera de identidad digital", diseñada para incluir no solo los datos esenciales de identidad, sino también atributos adicionales como diplomas académicos, certificados de vacunación, derechos de representación, o cualquiera otros. Este modelo reconoce tanto los métodos de identificación públicos como privados, avanzando hacia una descentralización progresiva en la gestión de la identidad digital.

A pesar de los avances significativos introducidos por la nueva regulación europea, la transición hacia sistemas basados en el SSI requiere el cumplimiento de diversos principios fundamentales, entre los que destacan: la interoperabilidad, la descentralización, la privacidad y la portabilidad de los datos. La implementación de estos principios no solo garantizará la seguridad y la confianza en los sistemas descentralizados, sino que también contribuirá a la equidad y accesibilidad para todos los ciudadanos europeos. Así, el Reglamento eIDAS 2.0 representa un paso decisivo hacia una concepción más moderna y adaptable de la identidad digital en el marco de la Unión Europea.

3. La transformación digital del sector público en los últimos años: el Gobierno Abierto

A principios de la década de los noventa se introdujo la “Nueva Gestión Pública” (NGP), un modelo de gerencia que vino a solventar las insuficiencias del anterior, traduciéndose en una primera gran transformación del sector público: flexibilizando los trámites ante la administración pública, extremadamente burocratizados; definiendo con mayor claridad los objetivos de las organizaciones y sus recursos humanos; primando la eficacia y la economía en los procesos; y abarcando una inclinación hacia la privatización de los servicios públicos (Ramírez-Alujas, 2010, p. 97). Pese a lo dicho, con la llegada de la crisis de 2008, algunos autores como Ramírez Alujas (2010, p. 97) pusieron de manifiesto cómo el escenario de incertidumbre y complejidad, en adición a la falta de recursos y preparación de las administraciones, derivaron en un fracaso del NGP. Así, muchos Estados introdujeron políticas encaminadas a “potenciar los niveles de transparencia, probidad y participación ciudadana en los asuntos públicos” (Ramírez-Alujas, 2010, p. 108).

En este contexto, nace el modelo de gobernanza adherido al concepto de gobierno abierto, que se erige como un canon ideal de seguimiento, cuya fundamentación se articula en tres premisas clave (Ramírez-Alujas, 2013, p. 115): (1) modernizar y mejorar la transparencia y el acceso a la información pública, (2) empoderar a la ciudadanía para facilitar su participación en la creación de políticas públicas y, (3) proliferar la colaboración entre administraciones públicas, ciudadanía y sector privado.

Para alcanzar estos objetivos ha sido necesaria —y continúa siéndolo— una enorme modernización de los procesos, pero también una adaptación de los

mecanismos legales a las nuevas tecnologías de la información y un cambio radical en la cultura organizacional de las administraciones (Salvador, Llanes, y Suárez, 2020, pp. 593-594). El gobierno abierto es un paradigma de gestión política que surge como respuesta a un problema de gran actualidad: la insatisfacción generalizada de la ciudadanía respecto del sistema gubernamental, la llamada "desafección política" (Botella, 2020, p. 202). Entre los ciudadanos europeos, el sentimiento de desafección no solo crece respecto de sus gobiernos nacionales, sino también del propio sistema político de la Unión. El euroescepticismo emana de una sociedad europea que "siente que el actuar de estos órganos es lento y hasta inexistente, por lo que se genera un descontento social que trae consigo el resentimiento y desentendimiento a la figura de la Unión Europea" (Veraldi, Ramírez, y Medicina, 2019, p. 63).

Ahora bien, pese a que el debate sobre el gobierno abierto se originó hace años, en la última década se han redoblado los esfuerzos por llevarlo a la práctica, favoreciendo la creación de un "ecosistema sobre el cual construir un nuevo modelo de gobernanza abierta y colaborativa, para, con y a través de los ciudadanos" (Ramírez-Alujas, 2013, p. 214). Así, desde el inicio del milenio han proliferado los proyectos dirigidos a hacer uso de las nuevas tecnologías para desarrollar sistemas de identificación electrónica. Estos sistemas —públicos, como el certificado de persona física de la GISS; y privados, como el certificado ciudadano de la ACCV— han surgido por la necesidad creciente de ofrecer a los administrados métodos seguros y eficientes para realizar trámites y comunicarse con las AA.PP.

Sin embargo, a pesar de que la implementación de diversos sistemas de identificación en el sector público español en los últimos años ha mejorado la relación con los administrados, estas estructuras aún enfrentan desafíos. De este modo, la arquitectura de esos sistemas se enfoca en las propias AA.PP. y no en el usuario final, tanto en términos de usabilidad como de control de datos. Por un lado, son sistemas que facilitan el proceso de autenticación para la administración, pero no resultan útiles para los ciudadanos debido a la cantidad tan reducida de datos que incorporan los certificados y la falta de conocimiento general sobre su funcionamiento, lo que limita su aplicabilidad. Por otro lado, todos los medios de autenticación de carácter público responden a un sistema de identidad digital centralizado, lo que degenera en la pérdida de control de los ciudadanos de sus datos personales, provocando un mayor nivel de preocupación por la privacidad y, finalmente, derivando en un uso menos extendido. Además, el propio fenómeno de desafección política, aunado a herramientas digitales poco intuitivas para el ciudadano, ha devenido en un escaso éxito de los medios de identificación vigentes. Finalmente, la falta de interoperabilidad de estos sistemas en algunos casos complica, por añadidura, la adopción generalizada de estas herramientas.

Por esta razón, los sistemas SSI encarnados en la *wallet* digital europea se articulan como un mecanismo de identificación que viene a solucionar toda esta clase de problemáticas, proporcionando una solución innovadora y segura para la gestión de identidades digitales en un entorno descentralizado y orientado al usuario, una realidad necesaria para hacer efectivos los planteamientos del Gobierno Abierto.

4. El tratamiento de datos personales en el sector público español.

En el caso concreto de la relación entre Administraciones Públicas y administrados, los aspectos más relevantes en materia de protección de datos se articulan en tres vertientes fundamentales.

La primera cuestión se refiere a los sujetos del tratamiento. Primeramente, por lo que respecta a la figura del responsable, la base del tratamiento más habitual en el sector público implica que el interesado no puede negarse a este pues se funda en el cumplimiento de una obligación legal (Valero, 2023, p. 379). La especial responsabilidad de las AA.PP. conlleva que "la acción de la administración debe dirigirse, de inicio, a la protección de datos personales" y "debe hacerse desde una vertiente activa" (Romeo, 2020, p. 142). Así, es necesario que las administraciones, a la hora de conformar sistemas de identificación electrónica, diseñen desde un primer instante políticas de protección de datos que concreten las medidas técnicas y organizativas que van a adoptar en cada etapa del tratamiento, ajustándose al RGPD y al ENS (Romeo, 2020, p. 142).

En lo tocante al encargado del tratamiento, tradicionalmente, un mismo órgano desempeñaba simultáneamente las funciones de certificación y validación, por lo que existía un riesgo práctico de que pudiera conocer cuál era el uso especifico que se le daba el certificado. Sin embargo, precisamente con los medios de autenticación introducidos en el sector público español desde principios del siglo XXI, se desarrollaron de forma separada Autoridades de Certificación y de Validación para evitar este riesgo, diversificando las actividades de tratamiento. Ahora bien, todavía existen entidades como la FNMT-RCM que actúan paralelamente como AC —mediante la expedición del Certificado Ciudadano, con más de 15 millones de certificados activos— y como AV —del DNIe, nada menos—. En cualquier caso, el empleo de los datos personales con una finalidad distinta a la autenticación provocaría una inobservancia del artículo 5 RGPD —principio de limitación de la finalidad—, vulnerando el derecho fundamental a la protección de datos y deviniendo el acto en nulo de pleno derecho conforme al artículo 47.1 a) LPAC

Finalmente, en lo concerniente a la figura del interesado, existe una singular significancia en la confrontación imperante entre el derecho de acceso a la información pública y el derecho a la protección de datos. En este sentido, las Administraciones quedan obligadas a los mismos deberes de salvaguardia que son exigibles a cualquier otro operador que trate datos personales; al tiempo que debe velar por el cumplimiento de una serie de compromisos de transparencia, especialmente relevantes en la coyuntura del Gobierno Abierto (Lara-Ortiz, 2019, p. 5).

Una segunda cuestión significativa es la base jurídica en la que se fundamenta el tratamiento de datos. Aunque en el caso de las AA.PP., normalmente, la base jurídica del tratamiento se funda en el cumplimiento de una norma legal o en la ejecución de un contrato, resulta preciso insistir en la necesidad de lograr un consentimiento válido de los administrados (Romeo, 2020, p. 144). Además, "no por ello deja de ser exigible que se proporcione la información necesaria a los sujetos afectados en los términos a que se refieren los artículos 13 y 14 RGPD (…)" (Valero, 2023, p. 374). Por lo general, esto implica que el interesado debe firmar un

documento que indique que ha sido debidamente informado, a fin de contar con un medio de prueba de dicha comunicación. Sin embargo, esta es una actividad predominantemente carente de sentido, pues los usuarios no entienden la naturaleza de estas notificaciones (siendo habitualmente confundidas con la prestación de consentimiento para el tratamiento de datos) y, por supuesto, no suelen prestar atención al contenido de las políticas de privacidad de los tratamientos a los que se someten.

En este sentido, el Eurobarómetro especial de junio de 2019 con motivo de la publicación del RGPD recogió el sentimiento de la ciudadanía europea acerca del grado de control percibido de sus datos personales, reconociendo un clamoroso 30% sentir que no tenían ningún tipo de control sobre sus datos; si bien es cierto que más de la mitad creía tener, al menos, un control parcial. Además, de entre estos, hasta un 62% estaban preocupados por no tener un control total de sus datos personales. Asimismo, resulta conveniente señalar que solo un 22% considera que siempre se le informa de las condiciones de la recolección y uso de sus datos personales. Finalmente, solo un 13% lee de forma completa las políticas de privacidad.

Una última cuestión clave a determinar son las deficiencias que presentan los sistemas de identificación existentes en el sector público español respecto de los principios del tratamiento que establece el RGPD.

Uno de los aspectos determinantes en esta materia es la falta de conformidad de los sistemas de autenticación electrónica con el principio de minimización de datos. Este principio implica, según dispone el propio Reglamento, que los datos recogidos deben reunir tres características: deben ser adecuados, pertinentes y limitados para los fines propios del tratamiento. En este extremo, los sistemas de identificación electrónicos disponibles para el ciudadano no garantizan el cumplimiento del principio de minimización. En muchas ocasiones, el proceso administrativo requiere la verificación de un atributo concreto de la identidad, pero la autenticación ante el sector público implica, necesariamente, la transferencia de todos los datos que consten en el certificado electrónico habilitado. Esta deficiencia se debe a la propia tecnología que subyace a dichos sistemas, en los cuales el portador del certificado no puede elegir ni el destinatario ni los datos concretos que transmite.

Por ejemplo, para la obtención de datos protegidos de los inmuebles inscritos en el catastro se puede emplear el certificado del DNIe mediante el sistema Cl@ve, no obstante, en este proceso se transmiten datos adicionales que no son relevantes para la consulta telemática.

Por otro lado, también existen ciertas limitaciones en relación con el principio de exactitud. Cuando los datos que constan en un certificado electrónico varían —verbigracia, porque se ha producido un cambio de domicilio— se procede a la revocación del certificado y a la expedición de uno nuevo, sistema que es incompatible con la acreditación de datos de carácter dinámico que fluctúan en el medio plazo.

Finalmente, son reprochables las vulnerabilidades en materia de ciberseguridad

acaecidas como la vulnerabilidad ROCA de 2017. A estas dificultades presentes en los propios certificados electrónicos, deben aunarse la alta cantidad de ciberataques que afectan al sector público cada año y que muestran la debilidad del sistema de seguridad. Por ejemplo, un ciberataque acaecido en marzo de 2024 expuso los datos personales y sanitarios de "decenas de miles de agentes y miembros de las Fuerzas Armadas" (Cabrera, 2024).

5. Análisis del Reglamento eIDAS 2.0.: impacto en los sistemas de identificación

La exposición de motivos del Reglamento 2024/1183 por el que se modifica el Reglamento eIDAS, incorpora los objetivos fundamentales de la nueva norma, que se pueden resumir en los que siguen:
1) La configuración de sistemas de identificación electrónica e identidad digital más seguros y fiables sobre los que se sustenten servicios públicos y privados, garantizando, a su vez, el acceso de personas físicas y jurídicas a dichas prestaciones mediante las soluciones digitales que contiene el Reglamento.
2) La seguridad de que dichos sistemas permitan incorporar una cantidad variable de atributos de la identidad que puedan ser objeto de intercambios selectivos de datos, salvaguardando el principio de minimización de datos del RGPD.
3) Garantizar la interoperabilidad de los servicios de confianza en el ámbito de la Unión Europea en un régimen de prestación que asegure la igualdad de condiciones.

La propia exposición de motivos del Reglamento eIDAS 2.0 hace referencia a una evaluación negativa del Reglamento eIDAS, identificado como un marco legal incapaz de asumir las exigencias del mercado por las limitaciones que presenta en lo tocante al Sector Público, así como la insuficiencia y falta de flexibilidad de los sistemas operantes de identidad electrónica. La norma reconoce que esta actualización requiere de un nuevo sistema con un nivel de seguridad suficientemente alto como para soportar la expedición de una cartera de identidad digital europea, esto es, una infraestructura armonizadora de los sistemas vigentes de autenticación y de los mecanismos de seguridad, que proporcione confianza en los ciudadanos de la Unión y garantice una solución de identificación electrónica para el acceso a servicios públicos que abarque, cuando menos, a un 80% de la población europea.

Por lo que respecta al contenido de la cartera, únicamente los atributos reconocidos se almacenarán en esta como parte de su software; mientras que los datos de identidad central, como los que componen el DNIe, previsiblemente se conservarán en el "hardware seguro o e-sim" (Schwalm y Alamillo, 2021, p. 100).

De conformidad con el artículo 45 ter del Reglamento eIDAS 2.0., quedará en manos de cada Estado Miembro determinar la validez de la declaración electrónica de atributos de la cartera digital como mecanismo suficiente para la autenticación de la identidad y el acceso a los servicios públicos. En adición, la norma obliga a los EE.MM. a proporcionar mecanismos de validación de las carteras, en concreto, para garantizar la validez y autenticidad de estas, de las declaraciones de atributos que contenga y de los datos de identificación del propietario de la cartera. En el

ámbito del sector público español, la autoridad de validación de carácter universal del DNIe es la FNMT-RCM, mientras que el Ministerio de Hacienda presta servicios de validación al conjunto de las AA.PP.; ergo, es plausible que estos sean los organismos que tengan encomendada esta función de validación respecto al EUDW en España.

En este sentido, cabe recalcar que, a pesar de que el Reglamento eIDAS 2.0. ha sido considerado como paradigma de los SSI, la necesaria existencia de prestadores de servicios de confianza cualificados y no cualificados como terceros actores de los servicios digitales definidos en la norma, implica una limitación de la naturaleza descentralizada del sistema (Schwalm y Alamillo, 2021, p. 103). A este respecto, los nuevos servicios de libros mayores electrónicos actuarán como una pieza clave que asegure la integridad de los datos personales, lo cual es fundamental para aunar datos provenientes de fuentes centralizadas y para preservar las soluciones de identidad autosoberana.

Aparte, contamos con cierta información de la posible realidad práctica de la EUDW. En mayo de 2023 se pusieron en práctica cuatro proyectos piloto para probar la eficacia de la EUDI en diversos escenarios del sector público y privado (European Commission, 2024). Entre los fines de estos prototipos, destaca la exploración de la funcionalidad de la cartera digital como solución para el acceso de los ciudadanos a servicios públicos. La propia CE pone como ejemplos de servicios públicos a los que se podría acceder mediante el uso de la EUDW como sistema de identificación electrónica: la solicitud para la expedición del pasaporte o la licencia de conducir, presentar impuestos o acceder a información de la SS, etc.; servicios de los que tradicionalmente se dispone en España mediante sistemas como el DNIe o la herramienta Cl@ve.

Para el desarrollo de estas propuestas se adoptó en enero de 2023 *The European Digital Identity Wallet Architecture and Reference Framework* (ARF) por el Grupo Experto del eIDAS, un marco de referencia que recogía las especificaciones, estándares y prácticas comunes para coordinar los diversos proyectos. Si bien es cierto que este documento no tiene ninguna trascendencia legal, se puede interpretar como una base razonable de los criterios de diseño de la arquitectura necesaria para la futura implementación de las carteras digitales.

Tal y como especifica el ARF, con base en el texto del Reglamento eIDAS 2.0., el proveedor de la cartera EUDW puede ser tanto los propios EE.MM., como organizaciones autorizadas o reconocidas por estos. Estos organismos son los que ofrecerán las soluciones digitales a los usuarios finales, asegurando el control total de estos sobre su información personal; en este extremo, el ARF especifica: “esto también puede implicar garantizar al usuario el control exclusivo sobre material criptográfico sensible (por ejemplo, claves privadas) relacionado con el uso de sus datos en algunos escenarios, incluida la identificación electrónica, firma o sello”. Otro sujeto fundamental en el flujo de datos será el proveedor de datos de identificación personal (*Person Identification Data Providers*). Su objeto será el de prestar servicios de confianza relativos a la verificación de la identidad de los usuarios de la EUDW. El documento ARF especifica que podrán ejercer como PID las

mismas organizaciones que actualmente emiten los documentos de identidad oficiales. Los mecanismos a través de los cuales se originen los organismos PID dependen, en exclusiva, de los EE.MM., los cuales únicamente deben atenerse a la normativa en materia de protección de datos vigente. También se ha comentado la exclusiva competencia de los EE.MM. para determinar los sistemas de identificación operantes, por lo que en ningún caso la EUDW viene a sustituir el régimen vigente en las administraciones españolas. Por ende, lo esperable es que la cartera digital europea actúe como un instrumento añadido a los ya existentes. Si bien, en la medida en que garantice mayor autonomía a los usuarios en la disponibilidad de sus datos, y la aplicación concreta en la que se materialice tenga un diseño cómodo y accesible, la generalidad de su uso puede ir desbancando la utilización de los sistemas de identificación operantes ante la Administración Pública.

Sin embargo, es necesario recalcar las dos ventajas comparativas fundamentales que presenta la EUDW frente a los sistemas de identificación tradicionales. Por un lado, la descentralización en el manejo de datos gracias a la presencia de múltiples operadores, la cual permite que los usuarios puedan ejercer su derecho a la identidad digital de manera autónoma. Con la generalización de registros electrónicos descentralizados basados en tecnología DLT, los usuarios podrán tener un mayor control sobre sus datos personales. Precisamente, los sistemas de identidad digital SSI se basan en documentos identificativos descentralizados, eliminando la necesidad de un registro central, creando así una tecnología que supera a los sistemas PKI tradicionales y facilita la implementación de infraestructuras descentralizadas de clave pública (DKPI) (Alamillo, 2020, pp. 14-15). Además, la EUDW incorpora una red distribuida de datos para verificar la validez del documento certificado y confirmar su emisión por una entidad autorizada. Esta multiplicidad de actores promueve un proceso más robusto y confiable. Por añadidura, al descentralizar la verificación, la red elimina posibles puntos de fallo únicos, fortaleciendo aún más la seguridad de los datos y aumentando la integridad del sistema en su conjunto; debido a que en los sistemas DLT cada bloque o grupos de transacción "se encuentra replicado en diversos nodos", creando una cadena de referencias descentralizada (Delgado, 2023).

Por otro lado, es imprescindible subrayar la especial relevancia que el certificado de atributos puede tener en las relaciones con la administración como instrumento jurídico que garantice la minimización datos en los procedimientos con el sector público. Esto se debe, como se adelantó, a que el acceso a una gran parte de servicios o prestaciones públicas requieren de la validación de uno o varios atributos concretos de la identidad digital, siendo posible con la EUDW transmitir esta información particular sin tener que revelar todos los datos personales que contenga el certificado de atributos.

En adición, el Reglamento eIDAS 2.0. modifica el régimen impuesto por la Orden ETD/465/2021, exigiendo a partir de su entrada en vigor que los métodos de identificación deban garantizar la identidad de una persona con un nivel alto de confianza. De esta forma, los Evaluadores de Conformidad ya no acatarán los estándares de seguridad marcados por el artículo 6 de la citada Orden, sino los requisitos adscritos a la norma ETSI TS 119 461, reduciendo así las posibilidades de

suplantación de la identidad (Inza, s.f.).

En cuanto a la debilidad expuesta respecto a los sistemas de identificación vigentes por el que ciertas autoridades de certificación podrían, teóricamente, mediante una actividad de monitoreo de datos, conocer para qué se emplea el certificado que ha expedido; el Reglamento eIDAS 2.0. introduce un requisito de "no trazabilidad" cuya aplicabilidad se ha extendido a todas las AC, tanto para las entidades emisoras de certificados de atributos cualificados y no cualificados, como a los propios proveedores de la cartera digital (C. Timón López, comunicación personal, 5 de mayo de 2024). De esta forma, estas autoridades solo recibirán información estrictamente necesaria para la provisión de la cartera. Dicho requisito implica, por lo demás, que los protocolos de autenticación imperante basados en la validación del certificado no podrían ser utilizados, considerándose otros mecanismos que permitan comprobar la validez sin la necesidad de interactuar con la AC o la AV, aunque este aspecto técnico depende de ciertos aspectos concretos todavía indeterminados.

Finalmente, cabe señalar el impacto del Reglamento eIDAS 2.0. en el derecho a no aportar documentos que obren en poder de la Administración. Este modelo de gestión de la información de la LPAC "implica considerar que los ciudadanos prefieren delegar en la Administración pública la gestión de la información que les incumbe" (Delgado, 2023, p. 354). Precisamente, los sistemas SSI, mediante el empleo de certificados de atributos, buscan orientar las soluciones de identidad digital hacia el ciudadano, de forma que este pueda disponer de toda su información y transmitirla a quien desee.

6. Conclusiones

La cartera digital europea se presenta como una solución innovadora y prometedora para abordar los problemas inherentes a los sistemas de identificación electrónica tradicionales en el sector público, conformando un avance significativo en la gestión de la identidad digital en la Unión Europea. A través de sus características clave y disposiciones específicas, la cartera digital europea ofrece respuestas concretas a los desafíos de seguridad, privacidad y eficiencia identificados y analizados a lo largo del artículo.

En primer lugar, respecto a los desafíos de seguridad, el Reglamento eIDAS 2.0. supone un cambio de paradigma al ofrecer un ecosistema más amplio de operadores y aprovechar tecnologías como la DLT y el blockchain para minimizar el impacto de posibles brechas de seguridad; así como mejorar la integridad y autenticidad de los datos proporcionando registros descentralizados de transacciones. Además, la aprobación del Esquema de Certificación de Ciberseguridad Europeo garantiza un alto nivel de seguridad en las carteras digitales mediante estándares de evaluación y certificación más robustos. Estas medidas contribuyen a aumentar la confianza de los ciudadanos en los sistemas de identificación electrónica al garantizar la protección de sus datos personales y

elaborar un plan firme de actuación protocolaria a nivel europeo.

En cuanto a la privacidad y el control de los datos personales, la cartera digital europea ofrece a los usuarios la posibilidad de determinar qué información incluir en su certificado de atributos, cómo operar con ella y cuáles son los destinatarios de su información. Esta capacidad de autogestión brinda a los ciudadanos un mayor control sobre su información personal, empoderándoles y alineándose con los principios de minimización de datos, exactitud, confidencialidad y limitación de la finalidad del RGPD. Del mismo modo, la pluralidad de prestadores de servicios de certificación, tanto públicos como privados, reduce el riesgo de concentración de datos y garantiza un mayor nivel de privacidad para los usuarios. Así pues, en adición a la garantía introducida por el artículo 45 septies del Reglamento, se logra una mayor seguridad, a la vez que vela por que los datos certificados se usen únicamente para los fines previstos atendiendo a la base jurídica del tratamiento.

En términos de eficiencia, la adopción institucional de los SSI y la interoperabilidad de los sistemas de identificación electrónica simplifican los procedimientos administrativos y facilitan el acceso a los servicios públicos en toda la Unión Europea. Esto se traduce en una mejora significativa en la experiencia del usuario y en la eficacia de las AA.PP., lo que contribuye a restaurar la confianza de la ciudadanía en las instituciones europeas.

Aun con todo, el reglamento Reglamento eIDAS 2.0. deja grandes incógnitas acerca del funcionamiento real de la cartera digital. Uno de los aspectos más destacados se refiere al régimen de conservación de datos personales, al no haberse definido con claridad cómo se gestionarán y almacenarán los datos dentro de las carteras digitales, especialmente en lo que respecta a la responsabilidad de los PSC en este proceso. Otra área que plantea interrogantes es el funcionamiento del certificado de atributos y su compatibilidad con elementos de la identidad digital que pueden cambiar o evolucionar con el tiempo. Aunque el reglamento establece principios claros en cuanto al control y la gestión de los datos por parte de los usuarios, aún falta por determinar cómo se manejarán los atributos dinámicos y cómo se garantizará su integridad y actualización en el contexto de la cartera digital.

7. Bibliografía más relevante.

Alamillo Domingo, I. (2020). *How eIDAS can legally support digital identity and trustworthy DLY-based transactions in the Digital Single Market*. European Comission. https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

Alamillo Domingo, I. (2018). *Identificación electrónica y confianza en las transacciones electrónicas: la regulación jurídico-administrativa de las instituciones de acreditación de la actuación electrónica*. [Tesis doctoral, Universidad de Murcia] Facultad de Derecho, Murcia. https://digitum.um.es/digitum/bitstream/10201/61019/6/Ignacio%20Alamillo%20Domingo%20Tesis%20Doctoral.pdf

Alamillo Domingo, I. (2017). Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autenticación de los ciudadanos. En E. Gamero Casado, *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público* (Vol. 1, pp. 675-768). Tirant lo blanch.

Allen, C. (26 de abril de 2016). The Path to Self-Sovereign Identity. *Life with Alacrity*. https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/

European Commision. (enero de 2023). *The European Digital Identity Wallet Architecture and Reference Framekor*. ec.europa.eu.

https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

European Commission. (4 de abril de 2024). *EU Digital Identity Wallet Pilot Implementation*. commission.europa.eu. https://digital-strategy.ec.europa.eu/policies/eudi-wallet-implementation

Inza, J. (s.f.). Decae la Orden ETD/465/2021. *Inza Blog*. https://inza.blog/2024/05/01/decae-la-orden-etd-465-2021/

Ramiréz-Alujas, Á. (2013). Gobierno abierto. *Economía. Revista en Cultura de la Legalidad* (5), 201-216.

https://e-revistas.uc3m.es/index.php/EUNOM/article/view/2180/1116

Ramírez-Alujas, Á. V. (2010). Innovación en la gestión pública y open government (gobierno abierto). Una vieja nueva idea. *Revista Buen Gobierno* (9), 94-133. https://www.redalyc.org/pdf/5696/569660529006.pdf

Schwalm, S., y Alamillo Domingo, I. (2021). Self-Sovereign-Identity & eIDAS: a contradiction? Challenges and Chances of eIDAS 2.0. *European Review Of Digital Administration & Law*, 89-108. doi:9791259947529 10

Valero Torrijos, J., y Cerdá, J. I. (2020). Transparencia, acceso y reutilización de la información ante la transformación digital del sector público: enseñanzas y desafíos en tiempos del COVID-19. *Eunomía. Revista en Cultura de la Legalidad*(19), 103-126. doi: https://doi.org/10.20318/eunomia.2020.5705

Valero Torrijos, J. (2023). Las singularidades del tratamiento de datos de carácter personal en entornos de inteligencia artificial en el sector público en E. Gamero Casado (Ed.), *Inteligencia Artificial y sector público. Retos, límites y medios* (353-396). Tirant lo blanch.

UNIVERSIDAD DE MURCIA

Región de Murcia

fundación Integra _digital