COMISIÓN
EUROPEA

Bruselas, 3.6.2021
COM(2021) 290 final

INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

sobre la evaluación del Reglamento (UE) n.º 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior («Reglamento eIDAS»).

{SEC(2021) 229 final} - {SWD(2021) 130 final}

1. INTRODUCCIÓN

El presente informe resume los resultados de la evaluación del Reglamento (UE) n.º 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior («Reglamento eIDAS»)[1]. El artículo 49 del Reglamento insta a la Comisión a revisar su aplicación y evaluar, en particular, si procede modificar su ámbito de aplicación o sus disposiciones específicas dada la experiencia adquirida en su aplicación y la evolución tecnológica, jurídica y del mercado[2], informe que, en su caso, debe ir acompañado de propuestas legislativas.

El documento de trabajo adjunto de los servicios de la Comisión contiene pruebas y análisis más pormenorizados que respaldan estas conclusiones.

1.1. El marco eIDAS

Con el Reglamento eIDAS, adoptado en 2014, la UE abría camino al introducir un primer marco transfronterizo para las identidades digitales de confianza y los servicios de confianza que hoy en día se reconoce y respeta en todo el mundo. El objetivo del Reglamento eIDAS era permitir a todos los ciudadanos de la UE acceder a servicios públicos en toda la Unión utilizando medios de identificación electrónica (eID) expedidos en su país de origen. Se trataba de reforzar la confianza en las transacciones electrónicas en el mercado interior proporcionando una base común para unas interacciones electrónicas seguras y sin interrupciones entre los ciudadanos, las empresas y las administraciones públicas e incrementando, en consecuencia, la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la UE. El Reglamento derogó la Directiva 1999/93/CE por la que se establece un marco comunitario para la firma electrónica, que en lo fundamental tan solo contemplaba la firma electrónica.

Tal como puede deducirse de la base jurídica del Reglamento —el artículo 114 del TFUE—, se buscaba eliminar los obstáculos existentes al funcionamiento del mercado interior impulsando la aproximación de las legislaciones de los Estados miembros, y en particular, el reconocimiento mutuo y la aceptación de la identificación electrónica, la autenticación, las firmas y sus correspondientes servicios de confianza a través de las fronteras cuando fuera necesario para el acceso y la finalización de procedimientos o transacciones electrónicos.

Antes de la entrada en vigor del Reglamento, no existía un marco global transfronterizo e intersectorial europeo para unas transacciones electrónicas seguras, fiables y de fácil utilización que comprendieran la identificación electrónica, la autenticación y los servicios de confianza. La propuesta de la Comisión [COM (2012) 238 final], de 4 de junio de 2012,

---

[1] Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (*DO L 257*), http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=ES.

[2] «La Comisión revisará la aplicación del presente Reglamento e informará al Parlamento Europeo y al Consejo a más tardar el 1 de julio de 2020. La Comisión evaluará en particular si es apropiado modificar el ámbito de aplicación del presente Reglamento o sus disposiciones específicas, incluidos el artículo 6, la letra f) del artículo 7 y los artículos 34, 43, 44 y 45, teniendo en cuenta la experiencia adquirida en la aplicación del presente Reglamento, así como la evolución tecnológica, del mercado y jurídica».

acompañada de la evaluación de impacto [SWD (2012) 135 final], establecía los cuatro objetivos generales siguientes:

- garantizar el desarrollo de un mercado único digital;
- promover el desarrollo de servicios públicos transfronterizos clave;
- estimular y reforzar la competencia en el mercado único;
- mejorar la facilidad de uso (ciudadanos y empresas).

Pese a cumplir muchos de sus objetivos y haberse convertido en un elemento fundamental a la hora de facilitar el mercado único en toda una serie de sectores (por ejemplo, en servicios financieros y para el acceso y reutilización de datos en procedimientos administrativos), el Reglamento adolece de una serie de limitaciones: no hay obligación de notificar los sistemas nacionales de identificación electrónica, son limitados los atributos (elementos de información personal) que pueden notificarse a terceros de forma fiable, la norma se centra en el sector público, y no hay incentivos claros para que las entidades privadas utilicen identificaciones electrónicas nacionales. Además, el ecosistema europeo de identidad electrónica se encuentra disperso entre entornos normativos nacionales, niveles de gobernanza digital y culturas diferentes, con grados variables de confianza en las instituciones públicas.

1.2. Contexto

La prestación de identidades digitales atraviesa cambios fundamentales. Hay entidades tales como bancos, proveedores de servicios de comunicaciones electrónicas o empresas de servicios públicos, algunas obligadas por ley a recoger atributos de identidad, que utilizan sus trámites propios para actuar como proveedores de identidad verificada. Hay intermediarios de internet, incluidas las grandes plataformas de redes sociales y los programas navegadores[3], que actúan como guardianes *de facto* de las identidades digitales y ofrecen soluciones que permiten a los propios usuarios autenticarse en sitios web y servicios de terceros a través de sus perfiles de usuario (BYOI, *bring your own identity*). Es una comodidad que se ofrece a costa de perder el control sobre los datos personales comunicados; por otra parte, estos medios de identificación electrónica carecen de cualquier vínculo con identidad física verificada alguna, lo que dificulta aún más mitigar los riesgos de fraude y las amenazas a la ciberseguridad. Una amplia mayoría de ciudadanos de la UE querría tener acceso a una identidad digital segura que pudiera utilizar para acceder a los servicios en línea[4]. Por último, aunque hay muchos puntos de vista sobre el futuro de la identidad digital, hay que teneratenderse debidamente en cuenta el papel clave de las administraciones nacionales en el desarrollo de cualquier ecosistema digital de identificación de gran alcance.

Hoy en día, los usuarios cuentan con poder navegar *online* sin interrupciones y quieren disponer de aplicaciones móviles y soluciones de autenticación única que puedan utilizarse en servicios en línea públicos y privados para todos los casos de uso en que se exija una identificación, desde la conexión pseudónima a una plataforma en línea hasta la identificación segura en la Sanidad o la banca electrónicas. A medida que aumenta el número de servicios personalizados y sensibles a la identidad, cobran mayor importancia la identificación segura en línea y el intercambio de credenciales en forma de atributos. La capacidad de identificarse digitalmente se convertirá en factor importante de inclusión social, y el suministro de identidades digitales será un activo estratégico.

---

[3] Así, los usuarios de Facebook o Google pueden utilizar sus cuentas para iniciar sesión en Booking.com o en EU Login: https://developers.facebook.com/docs/facebook-login/overview https://developers.google.com/identity/

[4] Eurobarómetro 503, Actitudes hacia el impacto de la digitalización en la vida cotidiana, diciembre de 2019, véase: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2228

En su discurso sobre el estado de la Unión de 16 de septiembre de 2020, la presidenta de la Comisión Europea manifestaba la ambición de la Comisión de ofrecer una identidad digital segura y fiable a todos los ciudadanos de la UE: *«Queremos un conjunto de normas que sitúe a las personas en el centro. (...) Tiene que haber un control de nuestros datos personales, algo que todavía ocurre con demasiada poca frecuencia en la actualidad. Cada vez que una aplicación o un sitio web nos pide que creemos una nueva identidad digital o que nos conectemos fácilmente a través de una gran plataforma, en realidad no tenemos ni idea de lo que sucede con nuestros datos. Esta es la razón por la que la Comisión propondrá en breve una identidad electrónica europea segura. Una en la que confiemos y que cualquier ciudadano pueda utilizar en cualquier lugar de Europa para cualquier operación, desde el pago de sus impuestos hasta el alquiler de una bicicleta. Una tecnología con la que nosotros mismos podamos controlar qué datos compartimos y cómo se utilizan».*

El Consejo Europeo, respaldando la ambición de la Comisión, la instaba en sus Conclusiones de los días 1 y 2 de octubre de 2020 a presentar una propuesta de iniciativa marco europeo de identidad digital para mediados de 2021:

Las Conclusiones del Consejo Europeo llaman al «*desarrollo de una identificación electrónica pública segura para el conjunto de la UE, con la que los ciudadanos puedan tener el control de su identidad y sus datos en línea y se facilite el acceso a los servicios digitales públicos, privados y transfronterizos*. *El Consejo invita a la Comisión a que presente, antes de mediados de 2021, una propuesta de iniciativa relativa a la Identificación Digital Europea».*

La identificación electrónica permite a los ciudadanos y las empresas demostrar quiénes son al acceder a servicios en línea. Los servicios de confianza, tales como las firmas electrónicas, hacen las transacciones en línea más seguras, cómodas y eficientes. El Reglamento eIDAS es el único marco transfronterizo para una identificación electrónica de confianza tanto de personas físicas y jurídicas como de servicios de confianza. El eIDAS permite el reconocimiento transfronterizo de las identidades electrónicas de las administraciones para acceder a servicios públicos, a condición de que la identificación electrónica se haya notificado en el marco de eIDAS. Además, el eIDAS establece un mercado de la UE de servicios de confianza reconocidos a través de las fronteras y que tienen la misma categoría jurídica que los trámites tradicionales equivalentes en papel.

2. PRINCIPALES CONCLUSIONES DE LA EVALUACIÓN

Basándose en los criterios de evaluación, seguidamente se resumen las principales conclusiones.

2.1. Eficacia

Las disposiciones en materia de identidad electrónica han llevado a la creación de la red eIDAS, cuyo objetivo es permitir a los titulares de los sistemas de identificación electrónica notificados acceder a servicios públicos en línea a través de las fronteras. A escala de la UE, solo se ha conseguido garantizar la interoperabilidad de un número limitado de sistemas de identificación electrónica[5].

[5] Desde la entrada en vigor de la parte del Reglamento relativa a la identificación electrónica, en septiembre de 2017, 14 Estados miembros han notificado al menos un sistema de identificación electrónica y cuatro han notificado varios sistemas. En total, se han notificado hasta la fecha 19 sistemas de identificación electrónica: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview

El Reglamento eIDAS consigue garantizar la seguridad jurídica en materia de responsabilidad, carga de la prueba, efectos jurídicos y aspectos internacionales de los servicios de confianza, si bien quedan pendientes algunas cuestiones. Desde la introducción del Reglamento eIDAS, aunque han aumentado la disponibilidad y la aceptación de los servicios de confianza en la UE, persisten las diferencias entre los Estados miembros y los distintos servicios de confianza.

Pese a sus logros, el Reglamento no ha alcanzado todo su potencial en términos de eficacia. Apenas se ha notificado un número limitado de identificaciones electrónicas, lo que limita la proporción de ciudadanos de la UE que disponen de un sistema de identificación electrónica notificado (el 59 % de la población). Hay una limitada aceptación de las identificaciones electrónicas notificadas: no todos los nodos eIDAS están en funcionamiento, son escasos los servicios públicos que ofrecen la notificación eIDAS o están conectados a la infraestructura, y hay errores técnicos que impiden a los usuarios autenticarse sin dificultad.

Por lo que se refiere a los servicios de confianza, el objetivo del Reglamento de mantener la neutralidad tecnológica ha dado lugar a interpretaciones dispares de los requisitos por parte de los Estados miembros, lo que también obedece al hecho de que no se adoptaran disposiciones de ejecución adicionales. No cabe concluir que se hayan alcanzado plenamente unas condiciones de competencia equitativas en toda la UE. No obstante, el Reglamento eIDAS ha establecido un marco sólido, que puede complementarse con las normas y requisitos necesarios para reducir la actual fragmentación del mercado y las divergencias de interpretación entre los organismos de supervisión y evaluación de la conformidad, y para aumentar la cooperación entre los organismos de supervisión.

2.2. Eficiencia

La evaluación inicial indica que los costes cuantificables han sido hasta ahora superiores a los beneficios. En el área de la identificación electrónica, esto se debe a su baja aceptación, que no permite materializar los beneficios.

Los principales grupos de partes interesadas para quienes el componente de identificación electrónica del Reglamento eIDAS ha generado costes y beneficios son las administraciones nacionales, los operadores de nodos de eIDAS, los proveedores de identificación electrónica y los proveedores de servicios. En el caso de los servicios de confianza, para los principales grupos de partes interesadas, los principales costes y beneficios corresponden a la acreditación, la evaluación de la conformidad y los organismos de supervisión, y los proveedores de servicios de confianza cualificados y no cualificados.

Para las partes interesadas, una parte considerable son beneficios esperados (descontados como beneficios futuros) y, por tanto, difícilmente cuantificables. Los costes recurrentes de la gobernanza en el ámbito de los servicios de confianza son limitados y están principalmente relacionados con garantizar el cumplimiento. Para las partes interesadas, una proporción considerable de los beneficios es por ahora hipotética (descontada como beneficios futuros) y difícilmente cuantificables. Los proveedores de servicios de confianza obtienen beneficios en forma de ingresos al prestar servicios de confianza en otros países de la UE y al ampliarse la base de mercado.

2.3. Pertinencia

Desde la introducción del Reglamento eIDAS, el ecosistema de la identificación electrónica ha cambiado profundamente y es cada vez mayor la presencia de proveedores de identidad privados. Dado el auge de las transacciones digitales, todos los ciudadanos de la UE deben tener acceso a una identidad digital segura e interoperable, lo que no ocurre en la actualidad. Los objetivos del marco jurídico eIDAS siguen siendo pertinentes para abordar los problemas observados inicialmente, y en particular la necesidad de reducir la fragmentación del mercado al garantizar la interoperabilidad transfronteriza e intersectorial de los servicios de confianza adoptando normas comunes. Se antojan demasiado limitados el ámbito de aplicación y el objeto del Reglamento eIDAS, centrado como está actualmente en los sistemas de identificación electrónica notificados por los Estados miembros de la UE y en permitir el acceso a servicios públicos en línea.

Una serie de obstáculos clave a la aceptación por los usuarios y los proveedores de servicios del sector privado vienen impidiendo que el marco regulador alcance todo su potencial. Pese a la introducción de referencias a las soluciones eIDAS en una serie de disposiciones legislativas sectoriales de la UE, el Reglamento eIDAS no atiende aún a las necesidades de sectores específicos (por ejemplo, educación, banca, viajes o aviación). Uno de los factores de esa limitación de que adolece el marco actual en relación con estas necesidades sectoriales es la falta de atributos específicos por dominios.

El punto de tensión más importante es la capacidad del eIDAS de mantener el ritmo de los últimos avances tecnológicos en materia de servicios de confianza. La ampliación de la lista de servicios de confianza —en particular, con un servicio de confianza de archivado electrónico, otro que permita el uso de credenciales de identidad portátiles y otro para registros electrónicos— permitiría atender a una serie de casos de uso y ofrecería a los ciudadanos y las empresas la posibilidad de demostrar digitalmente su identidad, sus atributos o sus características sin necesidad de documentos físicos.

2.4. Coherencia

La evaluación indica que la parte del Reglamento relativa a la identificación electrónica está respaldada por un sistema generalmente coherente de reconocimiento mutuo de las identificaciones electrónicas basado en la notificación y la revisión *inter pares*. El marco de los servicios de confianza ofrece un sistema coherente de supervisión de este tipo de servicios. Sin embargo, se observan algunos problemas de coherencia interna del Reglamento.

En el caso de las identificaciones electrónicas, el sistema de notificación y revisión *inter pares* que contempla el marco eIDAS intentaba definir una visión común del nivel de garantía ofrecido a través de un sistema de identificación electrónica, pero la evaluación de su aplicación práctica indica que no siempre es así. Si bien favorece la flexibilidad y la neutralidad tecnológica, sigue faltando una visión común de lo que constituye un nivel de garantía sustancial y elevado. La atención centrada en los servicios públicos contrasta con la posibilidad de que el usuario limite los datos transmitidos al mínimo necesario para la autenticación en un servicio específico, ya que siempre se transmite el conjunto mínimo de datos que permite identificar a una persona. La implantación del sistema eIDAS actual no facilita al usuario la aplicación de los principios del RGPD de minimización de datos y privacidad por defecto mediante el control de los datos que comparte y con quién.

Las normas para evaluar a los proveedores de servicios de confianza en relación con los requisitos funcionales del Reglamento para obtener la cualificación presentan ciertas deficiencias, pues no hay suficientes detalles sobre las obligaciones, responsabilidades y nivel de competencia de los organismos de evaluación de la conformidad. Algunas disposiciones dejan a discreción de los Estados miembros el reconocimiento en el ámbito nacional de determinados métodos de identificación (como la verificación biométrica), lo que perjudica a la igualdad de condiciones ante la normativa y genera inseguridad.

2.5. Valor añadido de la UE

El Reglamento eIDAS creó incentivos para que los Estados miembros desplegaran soluciones nacionales de identificación electrónica, pero el valor añadido del marco de identificación electrónica presenta grandes limitaciones debido a su escasa cobertura, aceptación y uso. En el caso de los servicios de confianza, el Reglamento establece un marco jurídico común para su uso que reduce la fragmentación del mercado y contribuye a su aceptación. Con ayuda de los servicios de confianza, las administraciones públicas pueden modernizar y digitalizar los servicios y expedir certificados digitales, reduciendo así la carga administrativa.

En cuanto a identificación electrónica, las necesidades inicialmente observadas para la adopción del Reglamento siguen siendo pertinentes, y derogarlo daría lugar a fragmentación y consecuencias negativas para otros ámbitos legislativos supeditados a este. Introducir algunas adaptaciones en el marco regulador podría aumentar su valor añadido europeo (por ejemplo, al facilitar el uso por parte del sector privado de identificaciones electrónicas de confianza expedidas por la administración y definir un marco para el intercambio de atributos y credenciales específicos emitidos por los sectores público y privado). En el caso de los servicios de confianza, persisten algunos obstáculos derivados de interpretaciones o divergencias entre legislaciones nacionales, que limitan la utilización de los servicios de confianza.

3. REVISIÓN DEL MARCO EIDAS

El Reglamento eIDAS es un elemento fundamental a la hora de facilitar el mercado único en una serie de sectores: por ejemplo, en el bancario, a fin de suministrar parte de los datos de identidad necesarios para facilitar el cumplimiento de las normas contra el blanqueo de capitales[6], la Directiva sobre servicios de pago (PSD2)[7] se basa en servicios de confianza eIDAS tales como precintos electrónicos y certificados de autenticación de sitios web cualificados (QWAC), que permiten identificar la autenticidad de los sitios web por parte de los proveedores de pagos terceros, y los certificados de identificación electrónica basados en el eIDAS son un requisito esencial para el intercambio transfronterizo de datos, además de ser fundamentales para la aplicación y funcionamiento satisfactorios del principio de «solo una vez» a partir de 2023[8]. El marco de los servicios de confianza, reconocido internacionalmente,

[6] Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión.

[7] Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE.

[8] A partir de 2023, el principio de «solo una vez» permitirá a las administraciones públicas reutilizar y compartir de manera transparente y segura los datos y documentos previamente facilitados por los ciudadanos. (Artículo 14 del Reglamento (UE) 2018/1724 del Parlamento Europeo y del Consejo de 2 de octubre de 2018 relativo a la creación de

es la base de un proyecto de disposición[9], que se espera que en 2021 se convierta en una ley modelo de las Naciones Unidas sobre servicios de confianza en el comercio electrónico, y también para las actuales negociaciones comerciales en el marco de la OMC[10].

Sin embargo, mucho ha cambiado desde la adopción del Reglamento eIDAS en 2014. El marco se basa en sistemas nacionales de identificación electrónica que aplican normas diferentes y se centra en un segmento relativamente pequeño de las necesidades de identificación electrónica de los ciudadanos y las empresas: garantizar el acceso transfronterizo a los servicios públicos. Los servicios destinatarios afectan principalmente al 3 % de la población de la UE[11] que reside en un Estado miembro distinto de aquel en el que nació.

Desde entonces ha aumentado drásticamente la digitalización de todas las actividades de la sociedad. Sin olvidar la pandemia de COVID-19, que ha tenido un efecto muy fuerte en la rapidez de la digitalización. El resultado es que la prestación de servicios, tanto públicos como privados, se da cada vez más por vía digital. Ciudadanos y empresas tienen expectativas de un alto nivel de seguridad y comodidad para cualquier actividad en línea: presentar declaraciones fiscales, matricularse en una universidad extranjera, abrir una cuenta bancaria a distancia o solicitar un préstamo, alquilar un vehículo, crear una empresa en otro Estado miembro, autenticar pagos por internet, presentar ofertas en una licitación en línea, etc.

De ahí que haya aumentado radicalmente la demanda de medios de identificación y autenticación en línea, y también para el intercambio digital de identidades, atributos o cualificaciones relacionados con la información de forma segura y con un alto nivel de protección de datos[12]. Esto ha llevado a un cambio de paradigma: se evoluciona hacia soluciones avanzadas y cómodas, capaces de integrar diferentes datos y certificados verificables del usuario. En la actualidad, dadas sus limitaciones actuales, el marco eIDAS no permite satisfacer esta demanda con los medios de identificación electrónica y los servicios de confianza que en él se regulan. Los medios de identificación o autenticación desarrollados por el sector privado al margen del eIDAS solo responden parcialmente a este reto. Aunque ofrecen servicios de autenticación por terceros de fácil manejo (por ejemplo, una cuenta de Facebook o Google para conectarse a diferentes servicios), suelen emplearse para acceder a servicios *online* privados, no regulados y que no requieren un alto nivel de seguridad. No puede así garantizarse el mismo nivel de seguridad jurídica, protección de datos y privacidad, principalmente porque estos sistemas se remiten a sí mismos y no pueden ofrecer un vínculo con una identificación electrónica de una administración que sea fiable y segura.

En febrero de 2020, en su Estrategia para configurar el futuro digital de Europa[13], la Comisión se comprometió a revisar el Reglamento eIDAS para mejorar su eficacia, ampliar su aplicación al sector privado e impulsar identidades digitales de confianza para todos los ciudadanos y empresas de la UE. La urgencia de esta revisión quedó patente con el brote de la pandemia de COVID-19. Las perturbaciones de los servicios públicos y privados presenciales y la repentina necesidad de acceder y utilizar todos los tipos de servicios públicos y privados

---

una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas, DO L 295 de 21.11.2018).

9 https://undocs.org/en/A/CN.9/WG.IV/WP.167

10 Véanse, por ejemplo, los documentos de sesión para el Grupo de Trabajo IV de la CNUDMI/Comercio Electrónico, sesión 6-9 de abril de 2021: https://uncitral.un.org/en/working_groups/4/electronic_commerce

11. https://ec.europa.eu/eurostat/statistics-explained/index.php/EU_citizens_living_in_another_Member_State_-_statistical_overview

12 Por ejemplo, a finales de 2019, el número de usuarios de SPID (introducido en 2016) en Italia era de aproximadamente 5 millones. Hoy tiene más de 18 millones de usuarios activos (https://avanzamentodigitale.italia.it/it/progetto/spid), con un crecimiento continuo de alrededor de un millón de usuarios al mes. El uso de SPID pasó de unos 55 millones en todo 2019 a unos 32,4 solo en el mes de febrero de 2021.

13 Comisión Europea (2020). Estrategia para configurar el futuro digital de Europa.

online puso de manifiesto las limitaciones del eIDAS a la hora de ofrecer los beneficios esperados a los ciudadanos, las empresas y las administraciones seis años después de su adopción. Un Reglamento eIDAS revisado y reforzado permitiría responder a las nuevas demandas del mercado y de la sociedad atendiendo a las necesidades de soluciones basadas en la fiabilidad de las identidades electrónicas de las administraciones públicas, pero también de atributos y credenciales facilitados por el sector público y privado, todo ello plenamente gestionado por el usuario y reconocido en toda la UE a la hora de acceder a servicios públicos y privados. Esto serviría de apoyo para gran número de marcos normativos existentes o propuestos que reforzarían el mercado único de la UE.

4. CONCLUSIONES

En general, el Reglamento eIDAS ha contribuido a un mayor desarrollo del mercado único. Ha sentado las bases para el desarrollo de un mercado de servicios de identidad y confianza en la UE al atender a la necesidad cada vez mayor de transacciones digitales seguras. Sin embargo, con una perspectiva de futuro —que ha evolucionado en lo cuanto a los objetivos y expectativas de los usuarios—, el Reglamento eIDAS debe mejorarse en términos de eficacia, eficiencia, coherencia y pertinencia para alcanzar los nuevos objetivos políticos y satisfacer las expectativas de los usuarios y la demanda del mercado, teniendo también en cuenta la evolución reciente en materia de digitalización.

Lo que está apareciendo en el mercado es un nuevo entorno en el que, de hacer hincapié en la prestación y el uso de identidades digitales rígidas, se pasa a hacerlo en el suministro de atributos específicos relacionados con dichas identidades y la confianza en los mismos. Hay una mayor demanda de soluciones de identidad electrónica que puedan ofrecer estas capacidades y aporten mejoras de eficiencia y un alto nivel de confianza en los servicios en toda la UE, tanto en el sector público como en el privado, dada la necesidad de identificar y autenticar a los usuarios con altos niveles de garantía.

El actual Reglamento eIDAS no puede atender a estas nuevas exigencias del mercado debido a su limitación inherente al sector público, a la complejidad que para los proveedores *online* privados reviste conectarse al sistema, a su insuficiente disponibilidad en todos los Estados miembros y a su falta de flexibilidad para atender a diversas situaciones.