

Dictamen del Comité Económico y Social Europeo sobre la «Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea»

[COM(2021) 281 final — 2021/0136 (COD)]

(2022/C 105/12)

Ponente: **Tymoteusz Adam ZYCH**

Consulta	Parlamento Europeo, 8.7.2021 Consejo, 15.7.2021
Fundamento jurídico	Artículo 114 del Tratado de Funcionamiento de la Unión Europea.
Sección competente	Mercado Único, Producción y Consumo
Aprobado en sección	30.9.2021
Aprobado en el pleno	20.10.2021
Pleno n.º	564
Resultado de la votación (a favor/en contra/abstenciones)	229/2/5

1. Conclusiones y recomendaciones

1.1. El Comité Económico y Social Europeo (CESE) acoge con satisfacción la propuesta de la Comisión Europea de un instrumento que modifica el Reglamento eIDAS en lo que respecta al establecimiento de un marco para una identidad digital europea, propuesta que adaptaría dicho acto jurídico a las necesidades actuales del mercado. La evaluación del Reglamento vigente ha puesto de manifiesto la necesidad de ofrecer soluciones mejoradas para los servicios digitales que amplíen el acceso tanto al sector privado como al público y que estén disponibles para la gran mayoría de ciudadanos y residentes europeos.

1.2. Sin embargo, el CESE observa que la digitalización de los servicios propuesta puede conducir a la exclusión de partes de la sociedad europea, en particular de personas de edad avanzada, personas con escasa alfabetización digital y personas con discapacidad. Por consiguiente, el CESE pide a la Comisión Europea y a los Estados miembros que establezcan el marco necesario para la campaña de educación e información digitales, que debería servir al mismo tiempo para aumentar la sensibilización en el ámbito de la protección de los datos personales.

1.3. El CESE acoge con satisfacción que el uso de la cartera de identidad digital europea vaya a ser discrecional y gratuito. No obstante, la introducción de nuevas soluciones digitales implica necesariamente un tiempo y un gasto considerables. Por ello, el CESE pide a la Comisión Europea que profundice en la evaluación del tiempo necesario para la aplicación real del nuevo Reglamento a fin de no afectar negativamente al mercado y que proporcione un análisis más detallado y una mayor claridad en el Reglamento respecto a los costes previstos de su aplicación.

1.4. El CESE observa que la sección 9 del Reglamento propuesto prevé el reconocimiento transfronterizo obligatorio de las declaraciones electrónicas de atributos cualificadas emitidas en un Estado miembro. Sin embargo, teniendo en cuenta que las disposiciones del Derecho interno varían a menudo considerablemente entre los Estados miembros, el CESE reconoce la necesidad de aclarar que el reconocimiento de una declaración electrónica de atributos cualificada en un Estado miembro se limita a la confirmación de los hechos, de manera análoga a lo establecido en el apartado 4 del artículo 2 del Reglamento (UE) 2016/1191 del Parlamento Europeo y del Consejo por el que se facilita la libre circulación de los ciudadanos simplificando los requisitos de presentación de determinados documentos públicos en la Unión Europea⁽¹⁾: «El presente Reglamento no se aplica al reconocimiento en un Estado miembro de los efectos jurídicos relativos al contenido de los documentos públicos expedidos por las autoridades de otro Estado miembro».

⁽¹⁾ Reglamento (UE) 2016/1191 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, por el que se facilita la libre circulación de los ciudadanos simplificando los requisitos de presentación de determinados documentos públicos en la Unión Europea y por el que se modifica el Reglamento (UE) n.º 1024/2012 (DO L 200 de 26.7.2016, p. 1).

1.5. Desde el punto de vista del CESE, la protección efectiva de los datos debe examinarse especialmente en el contexto de la protección de los derechos fundamentales, en particular el derecho a la intimidad y el derecho a la protección de los datos personales. El CESE respalda por ello plenamente el requisito de que el marco para una identidad digital europea proporcione a los usuarios los medios para controlar quién tiene acceso a su gemelo digital y a qué datos puede acceder exactamente. El CESE invita a la Comisión y a los Estados miembros a que incluyan en las consultas sobre los aspectos técnicos del marco para una identidad digital europea la creación de un registro que permita a los usuarios rastrear cualquier acceso a sus datos.

1.6. El CESE desea destacar las preocupaciones en materia de seguridad relacionadas con el proceso de digitalización, en particular las referidas al desarrollo de los enormes sistemas que almacenan y procesan datos vulnerables al fraude y la pérdida. El CESE también es consciente de que actualmente no existe ningún sistema de seguridad capaz de ofrecer una protección completa de los datos. Así pues, el CESE considera que debe garantizarse a los usuarios de carteras de identidad digital europea una indemnización por cualquier situación indeseable relacionada con sus datos (por ejemplo, el robo o la divulgación de estos). Esta garantía debe ser independiente de que exista o no culpa del proveedor.

2. Introducción

2.1. El objeto del presente Dictamen es la propuesta de Reglamento de la CE por el que se modifica el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo ⁽²⁾ («Reglamento eIDAS») en lo que respecta al establecimiento de un marco para una identidad digital europea.

2.2. Como se señala en la exposición de motivos, el Reglamento eIDAS proporcionaría las siguientes protecciones y beneficios: 1) acceso a soluciones de identidad electrónica altamente seguras y fiables; 2) la garantía de que los servicios públicos y privados puedan apoyarse en soluciones de identidad digital fiables y seguras; 3) la garantía de que las personas físicas y jurídicas puedan utilizar soluciones de identidad digital; 4) la seguridad de que dichas soluciones presenten un conjunto de atributos y permitan el intercambio selectivo de datos de identidad, y de que dichos datos se limiten a las necesidades del servicio específico solicitado; y 5) la garantía de la aceptación de los servicios de confianza en la Unión Europea y de la igualdad de condiciones para su prestación. Las modificaciones propuestas responden al aumento de la demanda de soluciones digitales transfronterizas fiables que satisfagan la necesidad de identificar y autenticar a los usuarios con un elevado nivel de garantía.

3. Observaciones generales

3.1. El CESE es consciente de las nuevas demandas del mercado interior en cuanto al desarrollo de servicios electrónicos de identificación y confianza para las transacciones electrónicas transfronterizas. Las soluciones existentes previstas en el Reglamento eIDAS, que empezaron a surtir efectos jurídicos en varias fases a partir de julio de 2016, no satisfacen dichas demandas, lo que se confirma por el hecho de que, en este momento, solo el 59 % de los residentes en la UE tengan acceso a soluciones seguras y fiables de identidad electrónica. Además, el acceso transfronterizo a estos servicios resulta limitado por la falta de interoperabilidad entre los sistemas que ofrecen los distintos Estados miembros.

3.2. Por ello, el CESE acoge con satisfacción la nueva propuesta de la Comisión Europea de un instrumento que modifica el Reglamento eIDAS en lo que respecta al establecimiento de un marco para una identidad digital europea, propuesta que adaptaría dicho acto jurídico a las necesidades actuales del mercado. Se calcula que las soluciones propuestas en el documento de la Comisión podrían contribuir a aumentar el número de usuarios de la identidad digital hasta el 80 % o incluso el 100 % de todos los ciudadanos y residentes de la UE.

3.3. El CESE acoge con especial satisfacción las soluciones destinadas a aumentar la seguridad de los datos personales de los usuarios garantizando la discrecionalidad de compartir o no dichos datos y la posibilidad de controlar la naturaleza y la cantidad de datos facilitados a las partes usuarias. Según la propuesta, los Estados miembros mantendrán el control sobre los proveedores de servicios digitales, por lo que garantizarían que los conjuntos de datos sensibles (por ejemplo, relacionados con la salud, la religión y las creencias, las opiniones políticas o el origen racial o étnico) solo sean facilitados por los proveedores de servicios, cuando se les solicite, tras una decisión informada adoptada por el titular de la identidad de conformidad con la legislación nacional aplicable.

3.4. El CESE señala que el calendario para la aplicación de determinadas disposiciones del nuevo Reglamento es bastante optimista e invita a la Comisión Europea a que, al establecer los plazos de aplicación definitivos, también tenga en cuenta el tiempo necesario para que los proveedores de servicios mejoren sus sistemas informáticos para cumplir las nuevas obligaciones. Por consiguiente, el CESE pide a la Comisión que analice en más profundidad el tiempo necesario para la

⁽²⁾ 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 de 28.8.2014, p. 73).

aplicación real del nuevo Reglamento y, en consecuencia, amplíe el plazo de aplicación a fin de no afectar al mercado pertinente. Por ejemplo, la entrada en vigor del Reglamento obligará a que los actuales proveedores cualificados de servicios de confianza que ofrezcan la posibilidad de firma a distancia basada en dispositivos cualificados de creación de firmas electrónicas se conviertan en proveedores cualificados para ese servicio específico; estos proveedores necesitarán tiempo tanto para poner en práctica los aspectos técnicos como para completar el procedimiento de autorización.

3.5. El CESE señala que, independientemente de sus beneficios, la digitalización de los servicios propuesta puede conducir a la exclusión de partes de la sociedad europea, en particular de personas de edad avanzada, personas con escasa alfabetización digital y personas con discapacidad. El CESE reconoce el papel esencial de la educación de la ciudadanía europea para combatir dicha exclusión; al mismo tiempo, dicha educación debe servir para aumentar la sensibilización en el ámbito de la protección de los datos personales.

4. Disponibilidad de un marco para una identidad digital europea y discrecionalidad de su uso

4.1. El CESE acoge favorablemente la idea de ofrecer soluciones mejoradas para los servicios digitales que amplíen el acceso no solo a los servicios públicos, sino también al sector privado. Por otra parte, el CESE está de acuerdo con los intentos de la Comisión Europea de poner un marco para una identidad digital europea a disposición de la inmensa mayoría de los ciudadanos europeos. Debido a los obstáculos que existen para el acceso transfronterizo a los servicios de identidad electrónica (por ejemplo, la falta de interoperabilidad entre los sistemas de identidad electrónica desarrollados por los Estados miembros), muchos residentes de la UE no los utilizan en absoluto. Las nuevas soluciones basadas en las carteras de identidad digital europea pueden contribuir a que al menos el 80 % de los europeos dispongan de servicios en línea fiables.

4.2. Por tanto, el CESE respalda la propuesta de requerir que los Estados miembros emitan una cartera de identidad europea, un instrumento que permitiría a los usuarios: 1) solicitar y obtener, almacenar, seleccionar, combinar y compartir de forma segura, transparente y rastreable por el usuario, los datos de identificación de persona jurídica y la declaración electrónica de atributos que sean necesarios para autenticarse en línea y fuera de línea con el fin de acceder a servicios públicos y privados en línea; y 2) firmar por medio de firmas electrónicas cualificadas.

4.3. Además, el CESE acoge favorablemente la propuesta de garantizar que la cartera de identidad digital europea sea igualmente accesible para las personas con discapacidad de conformidad con las disposiciones del anexo I de la Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo⁽³⁾, en consonancia con el principio de no discriminación de la UE establecido en el artículo 21 de la Carta de los Derechos Fundamentales de la Unión Europea. Con el fin de evitar la exclusión digital en ese ámbito, el CESE propone que todas las soluciones se desarrollen en cooperación con las instituciones competentes y las ONG para personas con discapacidad, aplicando un enfoque basado en la participación de múltiples partes interesadas.

4.4. Desde el punto de vista del CESE, el hecho de que el uso de una cartera de identidad digital europea sea discrecional para los ciudadanos y residentes también es un aspecto positivo. El CESE considera que los usuarios no deberían estar obligados a utilizar dicha cartera para acceder a servicios privados o públicos, sino simplemente tener la posibilidad de hacerlo.

4.5. Desde el punto de vista de la asequibilidad, el CESE acoge con satisfacción que el uso de la cartera de identidad digital europea vaya a ser gratuito para los usuarios. No obstante, el CESE pide a la Comisión Europea que analice y aclare más detalladamente en el Reglamento los siguientes aspectos: i) el coste de emisión para las personas físicas, ii) los costes (de emisión y uso) para las entidades jurídicas y iii) los costes de añadir atributos de identidad digital a dicha cartera, ya que el CESE considera que cada una de estas adiciones representaría un servicio de confianza, por lo que conllevaría costes para el propietario de la cartera.

5. Aspectos relativos a la facilidad de uso de un marco para una identidad digital europea

5.1. El CESE acoge con satisfacción la iniciativa de la Comisión Europea de mejorar la facilidad de uso de los medios de identificación electrónica mediante la creación de un marco común para una identidad digital europea basado en la confianza transfronteriza en las carteras de identidad digital europea.

5.2. Según la propuesta, la facilidad de uso puede mejorarse con los medios previstos en el nuevo artículo 12 *ter* del Reglamento eIDAS. Dicho artículo contiene una serie de requisitos relativos al reconocimiento de las carteras de identidad digital europea, dirigidos no solo a los Estados miembros sino también a las partes usuarias privadas prestadoras de servicios y a las «plataformas en línea de muy gran tamaño», definidas en el artículo 25, apartado 1, de la Ley de Servicios Digitales propuesta⁽⁴⁾. Sobre la base de estas nuevas disposiciones, algunos sectores privados (transporte, energía, servicios

⁽³⁾ Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los requisitos de accesibilidad de los productos y servicios (DO L 151 de 7.6.2019, p. 70).

⁽⁴⁾ COM (2020) 825 final.

bancarios y financieros, seguridad social, salud, agua potable, servicios postales, infraestructuras digitales, educación y telecomunicaciones) deberán aceptar el uso de carteras de identidad digital europea para la prestación de servicios en los casos en que la legislación nacional o de la UE o las obligaciones contractuales exijan una autenticación reforzada del usuario para la identificación en línea. Según la propuesta de la Comisión, este mismo requisito se aplicaría a las plataformas en línea de muy gran tamaño (por ejemplo, las redes sociales), las cuales deberían aceptar el uso de carteras de identidad digital europea en relación con los atributos mínimos necesarios para un servicio en línea determinado para el que se solicite autenticación, como la acreditación de la edad.

5.3. El CESE señala que, para garantizar la disponibilidad generalizada y facilidad de uso de los medios de identificación electrónica, incluidas las carteras de identidad digital europea, los proveedores privados de servicios en línea (que no sean considerados «plataformas de muy gran tamaño») deberían participar en el desarrollo de «códigos de conducta» de autorregulación que faciliten una amplia aceptación de los medios de identificación electrónica. La Comisión Europea debe ser la encargada de evaluar la eficacia y facilidad de uso de dichas disposiciones para los usuarios de carteras de identidad digital europea.

6. Cuestiones relativas a los efectos jurídicos de las carteras de identidad digital europea

6.1. El CESE respalda la propuesta en lo que se refiere a la mejora del acceso a los servicios públicos digitales, en particular en situaciones transfronterizas.

6.2. La nueva sección 9 propuesta del Reglamento eIDAS establece que una declaración electrónica de atributos cualificada emitida en un Estado miembro debe reconocerse como declaración electrónica de atributos cualificada en cualquier otro Estado miembro.

6.3. Sin embargo, por lo que se refiere al Derecho interno de los Estados miembros, que en algunos casos puede diferir significativamente de un Estado a otro, el CESE señala que los atributos cotejados con fuentes auténticas en un Estado miembro deben limitarse únicamente a la confirmación de circunstancias de hecho y no deben producir efectos jurídicos en otros Estados miembros, a menos que los atributos en cuestión se ajusten a su legislación nacional. En esencia, las soluciones jurídicas propuestas no deben afectar al reconocimiento en un Estado miembro de efectos jurídicos relacionados con el contenido de atributos cotejados con fuentes auténticas en otro Estado miembro, por analogía con lo dispuesto en el Reglamento (UE) 2016/1191. Un ejemplo de ello pueden ser determinados datos personales (relativos a la religión o las creencias de una persona). En algunos países de la UE, este tipo de información surte efectos jurídicos (por ejemplo, en Alemania, los datos del registro civil incluyen información sobre la religión, que determina la obligación de pagar un impuesto eclesiástico para casarse por ceremonia religiosa), mientras que en otros países (como Polonia) carece de tales efectos.

6.4. Por consiguiente, el CESE invita a la Comisión Europea a que considere la posibilidad de aclarar el texto de la sección 9 a fin de dejar claro que el reconocimiento en cualquier otro Estado miembro de una declaración electrónica de atributos cualificada se limita a la confirmación de las circunstancias de hecho relacionadas con el atributo en cuestión y no produce efectos jurídicos en otros Estados miembros a menos que los atributos declarados se ajusten a su legislación nacional.

7. Aspectos de seguridad

A. Protección de datos en el contexto de los derechos fundamentales

7.1. El CESE observa que, debido a la falta de un marco común para una identidad digital europea, en la mayoría de los casos los ciudadanos y otros residentes se enfrentan a obstáculos para el intercambio digital transfronterizo de información relacionada con su identidad, así como para intercambiar dicha información de forma segura y con un nivel elevado de protección de datos.

7.2. El CESE acoge por ello positivamente los intentos de crear un sistema interoperable y seguro basado en carteras de identidad electrónica europea, que podría mejorar el intercambio de información entre los Estados miembros en relación con las situaciones laborales o los derechos sociales, entre otras cuestiones. En este contexto, el CESE espera que el nuevo marco para una identidad digital europea genere, por ejemplo, posibilidades de aumentar rápidamente las oportunidades de empleo transfronterizo y de ampliar la concesión automática de derechos sociales sin procedimientos de solicitud u otros esfuerzos administrativos adicionales.

7.3. Sin embargo, desde el punto de vista del CESE, la protección efectiva de los datos es la principal preocupación que debe abordarse en el contexto de la protección de los derechos fundamentales, especialmente el derecho a la intimidad y el derecho a la protección de los datos personales.

7.4. Por lo tanto, el CESE apoya plenamente el requisito de que el marco para una identidad digital europea proporcione a todas las personas los medios para controlar quién tiene acceso a su gemelo digital y a qué datos puede acceder exactamente (también en relación con el acceso desde el sector público). Como se indica en la propuesta, esto requerirá asimismo un nivel alto de seguridad en todos los aspectos de la provisión de la identidad digital, incluida la expedición de una cartera de identidad digital europea, y la infraestructura necesaria para la recopilación, el almacenamiento y la divulgación de datos de identidad digital.

7.5. En este contexto, el CESE acoge favorablemente la propuesta de que los usuarios tengan derecho a revelar de forma selectiva sus atributos, limitándolos a los que sean necesarios en una situación determinada. En virtud de la propuesta, al utilizar la cartera de identidad digital europea el usuario podrá controlar la cantidad de datos que proporciona a terceros, y deberá ser informado de los atributos requeridos para la prestación de un determinado servicio.

7.6. El CESE apoya la propuesta de separar física y lógicamente los datos personales relacionados con la provisión de carteras de identidad digital europea de cualquier otro dato almacenado por los emisores de dichas carteras, y respalda el requisito de que los proveedores de servicios cualificados de declaración electrónica de atributos deban constituir una entidad jurídica separada.

7.7. Además de la necesidad de garantizar una protección eficaz de los datos, resulta esencial que los usuarios tengan control sobre sus datos. En ese sentido, el CESE también respaldaría la creación de un marco para una identidad digital europea basado en identidades legales expedidas por los Estados miembros y en la provisión de atributos de identidad digital cualificados y no cualificados.

7.8. El CESE subraya que, para garantizar un elevado nivel de protección jurídica de sus datos, los usuarios deberían tener un mayor control sobre las carteras de identidad de datos europea, en particular mediante la rastreabilidad del acceso a los datos de cada usuario. A tal fin, los aspectos técnicos —que se determinarán durante los debates posteriores a la aprobación de la propuesta— deben incluir la creación de un registro que permita al usuario verificar, previa solicitud, cualquier acceso a sus datos que se produzca.

B. Otros aspectos relacionados con la seguridad y la responsabilidad

7.9. De acuerdo con la propuesta, el nuevo marco para una identidad digital europea proporcionará mecanismos para prevenir el fraude y garantizar la autenticación de los datos de identificación personal. La propuesta incluye una disposición que introduce medios que permiten el cotejo de los atributos con fuentes auténticas: esto podría mejorar, por ejemplo, la seguridad en línea de los niños y niñas impidiéndoles acceder a contenidos inadecuados para su edad. El CESE señala que, a nivel nacional, tal protección no existe actualmente o es muy ineficaz.

7.10. El CESE acoge con satisfacción la idea de que los navegadores web deban garantizar la compatibilidad e interoperabilidad con los certificados cualificados para la autenticación de sitios web previstos en el Reglamento eIDAS. A tal efecto, deben reconocer y mostrar certificados cualificados para la autenticación de sitios web con objeto de ofrecer un nivel alto de seguridad, lo que permitiría a los propietarios de los sitios web demostrar su identidad como propietarios de un sitio web y a los usuarios identificar a los propietarios de los sitios web con un alto grado de certeza. Al mismo tiempo, el CESE considera necesario proporcionar mecanismos de recurso sencillos, rápidos y eficaces para garantizar el desbloqueo de los sitios web que hayan sido marcados indebidamente como peligrosos. También deben establecerse normas en materia de responsabilidad en relación con todos los casos en que un sitio web sea calificado incorrectamente como peligroso.

7.11. El CESE desea destacar que toda digitalización de datos plantea problemas de seguridad, especialmente por lo que se refiere a los enormes sistemas de almacenamiento y procesamiento de datos, que constituyen una fuente de información vulnerable al fraude y la pérdida. El CESE también es consciente de que hoy por hoy no existe un sistema de seguridad plenamente eficaz (es decir, sin lagunas ni errores) capaz de eliminar por completo esta amenaza.

7.12. Señala por ello que, para minimizar todas estas situaciones indeseables relacionadas con los datos de los usuarios, la arquitectura técnica del marco para una identidad digital europea desarrollado por los Estados miembros en coordinación con la Comisión debería centrarse en medidas que aumenten la seguridad de los datos y proporcionen mecanismos de control de los datos. Estos mecanismos son importantes, por ejemplo, en contextos en los que los datos recabados de los usuarios se utilicen para fines distintos de los previstos inicialmente. Al mismo tiempo, el CESE considera que la arquitectura técnica debe desarrollarse respetando los derechos fundamentales y el principio de soberanía de los Estados miembros.

7.13. El CESE constata que el artículo 13, apartado 1, del Reglamento eIDAS establece que los proveedores de servicios de confianza serán responsables por los daños causados de forma intencionada o por negligencia a cualquier persona física o jurídica como consecuencia del incumplimiento de las obligaciones derivadas de dicho Reglamento (y de las obligaciones de gestión de los riesgos para la ciberseguridad contempladas en el artículo 18 de la Directiva SRI2 propuesta, según se establece en la propuesta de la Comisión). Esta disposición debe aplicarse de conformidad con las normas nacionales en materia de responsabilidad (artículo 13, apartado 3).

7.14. En el contexto de las preocupaciones relativas a la responsabilidad, el CESE desea señalar que las cuestiones relacionadas con la definición de los daños, su cuantía y la indemnización correspondiente están reguladas por el Derecho interno de los Estados miembros. La responsabilidad de los proveedores de servicios de confianza puede verse limitada en virtud de las disposiciones pertinentes del Derecho interno y de las «políticas de prestación de servicios», que son definidas por los proveedores.

7.15. El CESE considera que debe garantizarse a los usuarios de carteras de identidad digital europea una indemnización por cualquier situación indeseable relacionada con sus datos, entre otras el robo, pérdida o divulgación de datos o el uso de estos para fines distintos de los previstos originalmente. Esta obligación debe incluir todas las situaciones mencionadas, independientemente de que exista o no culpa del proveedor (por dolo o negligencia).

7.16. Cualquier robo, divulgación no autorizada o pérdida de datos (especialmente datos personales) puede causar un daño a largo plazo a su propietario. Una vez difundida la información digital, muchas entidades pueden hacerse con ella a lo largo del tiempo en contra de la voluntad de su propietario. El CESE anima a la Comisión y a los Estados miembros a que busquen y desarrollen mecanismos eficaces que amparen a los propietarios de los datos en tales casos.

7.17. Las soluciones propuestas del nuevo sistema obligarán a los proveedores de servicios a mejorar significativamente sus sistemas de seguridad electrónica a un nivel mucho más elevado, prestando especial atención a la ciberseguridad. El CESE prevé que esto conlleve costes significativos y una modernización de la infraestructura informática actual y pueda suponer una carga excesiva para algunos proveedores de servicios, que podría incluso dar lugar a la desaparición, en algunos mercados, de los proveedores de servicios que no puedan permitirse tales inversiones en un breve período de tiempo. Por lo tanto, el CESE considera que la Comisión y los Estados miembros deberían buscar soluciones que protejan a los proveedores frente a la discriminación en este ámbito y permitan un «aterrizaje suave» en ese sentido, en particular ofreciendo la posibilidad de garantizar el cumplimiento de los nuevos requisitos en varias fases, dentro de un plazo razonable.

Bruselas, 20 de octubre de 2021

La Presidenta
del Comité Económico y Social Europeo
Christa SCHWENG
