Evaluando los requisitos de localización de datos con la libre circulación de datos no personales en el informe español para la Comisión Europea

Assessing Data Localisation Requirements under Free Flow of Non-Personal Data in the Spanish Report for the European Commission

por

CRISTINA ARGELICH COMELLES

Profesora de Derecho civil, acreditada a Profesor Titular

Universidad Autónoma de Madrid

RESUMEN: El presente trabajo tiene por objeto contextualizar y exponer el contenido del Informe español para la Comisión Europea, emitido en autoría individual, sobre la adecuación de los requisitos de localización de datos a las obligaciones legales derivadas de la libre circulación de datos no personales, bajo el estudio *"Supporting the evaluation of the Free Flow of Non-Personal Data Regulation, Open Data Directive and Data Governance Act"*. Por ello, se analizará primeramente el régimen jurídico de los requisitos de localización de datos, su adecuación al ordenamiento jurídico europeo, y las barreras regulatorias directas e indirectas ya detectadas por la Comisión Europea en 2017. Todo ello es necesario para observar el grado de adecuación de las Resoluciones de Transparencia de la Agencia Española de Protección de Datos, sobre la aplicación de los requisitos de localización de datos en el periodo 2020-2025, respecto de las obligaciones

https://doi.org/10.36151/rcdi.2025.812.03

legales derivadas de la libre circulación de datos no personales y la evitación de las barreras regulatorias.

ABSTRACT: This paper contextualises and describes the Spanish report for the European Commission, issued in individual authorship, on the adequacy of data localisation requirements to the duties arising from the free flow of non-personal data, under the study 'Supporting the evaluation of the Free Flow of Non-Personal Data Regulation, Open Data Directive and Data Governance Act'. Therefore, the paper discusses the Spanish regulation on data localisation requirements under European Law, as well as regulatory barriers advised by the European Commission in 2017. The purpose of this legal analysis is to properly assess the Transparency Resolutions of the Spanish Data Protection Agency, on data localisation requirements in the 2020-2025 period, with regard to the free flow of non-personal data duties and the avoidance of regulatory barriers.

PALABRAS CLAVE: protección de datos, libre circulación de datos no personales, datos abiertos, requisitos de localización de datos, barreras regulatorias.

KEYWORDS: data protection, free flow of non-personal data, open data, data localisation requirements, regulatory barriers.

I. CONSIDERACIONES INICIALES SOBRE LOS REQUISITOS DE LOCALIZACIÓN DE DATOS[1]

De conformidad con el Reglamento 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea[2], los Estados miembros deben permitir la utilización, recogida, almacenamiento, transferencia o gestión de datos no personales, así como utilizar centros de tratamiento de datos o servicios en la nube. Los datos no personales comprenden aquellos que no guardan relación con una persona física identificada o identificable, los que se han anonimizado, así como los conjuntos de datos personales y no personales mixtos e indisolubles. Por lo que respecta a los *Data Localisation Requirements* o requisitos de localización de datos, cuya regulación corresponde a los Estados miembros de la Unión Europea, supone que se pueda restringir la libre circulación de determinados datos no personales por motivos de seguridad pública. En el art. 7 del Reglamento 2018/1807, se impone la obligación legal de establecer un "punto de contacto único", mediante un sitio web oficial que contenga la información sobre los requisitos de localización de datos –cuyas resoluciones anonimizadas deben publicarse–, una dirección postal y un correo electrónico de contacto; en España, ello se encuentra en el Portal de la Agencia Española de Protección de Datos, en adelante, AEPD.

Sobre estas bases, el objeto del presente trabajo consiste en analizar las barreras regulatorias en la aplicación de la legislación española sobre los requisitos de localización de datos a las obligaciones legales derivadas de la normativa europea en materia de libre circulación de datos no personales, datos abiertos y gobernanza de datos. Para ello, se prestará atención al contenido del informe español para la Comisión Europea –emitido en autoría individual bajo el Estudio *"Supporting the evaluation of the Free Flow of Non-Personal Data Regulation, Open Data Directive and Data Governance Act"–,* en particular, en cuanto a la ausencia de modificaciones en los requisitos de localización de datos tras las barreras regulatorias advertidas por la Comisión Europea en 2017, así como su aplicación mediante las Resoluciones de Transparencia en el periodo 2020-2025[3] (AEPD, 2025). A estos efectos, los siguientes apartados se dedicarán al análisis del régimen jurídico de los requisitos de localización de datos en España y al exa-

men de las barreras regulatorias directas e indirectas detectadas en su aplicación, formulando diversas conclusiones para su mejora al final del trabajo.

II. LOS REQUISITOS DE LOCALIZACIÓN DE DATOS EN ESPAÑA A LA LUZ DEL ORDENAMIENTO JURÍDICO EUROPEO

La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno[4] dispone el derecho de acceso a la información pública en su art. 12, así como regula su ejercicio y los requisitos de localización de datos. En el art. 13, define la información pública como los contenidos o documentos, con independencia de su formato, que estén a disposición de los sujetos previstos en el art. 2, y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones. De conformidad con el art. 22 del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE[5] –en adelante RGPD–, el art. 15 de la Ley 19/2013, sobre protección de datos personales, advierte que si la información requerida los contiene, es necesario para autorizar el acceso el consentimiento expreso y por escrito del afectado, puesto que prevalece dicha protección frente al interés público en la divulgación. En este punto, conviene apuntar que, en las decisiones individuales automatizadas sobre datos personales y en la elaboración de perfiles –mediante algoritmos, incluyendo los que utilizan un sistema de inteligencia artificial no determinista–, será necesario o bien el consentimiento del interesado, o un acuerdo entre este y el responsable del tratamiento de datos, o que lo imponga una norma europea o de un Estado miembro *ex* art. 22 RGPD (LIPPI, 2022, 49-68; DE TORRES PEREA, 2025, 279-329; DE BARRÓN ARNICHES, 2024, 149-194). En este sentido, destacada doctrina ha propuesto algunas soluciones *de lege ferenda* (MARTINI, 2020, 114-119): la extensión de la divulgación de las obligaciones en materia de protección de datos mediante la supervisión pública, la auditoría de los algoritmos y el tratamiento de datos personales; la ampliación del deber de información sobre los procedimientos y aplicaciones de *software* que puedan afectar a los derechos de los usuarios *ex* art. 22 RGPD, en atención al derecho de no ser objeto de una decisión basada únicamente en el tratamiento automatizado y por la necesaria interpretación restrictiva de las excepciones a esta regla general; y, finalmente, la obligación de proporcionar información adecuada sobre las medidas para garantizar la protección de datos. Sin embargo, el principal obstáculo que presenta el RGPD es que no resulta aplicable a los datos de las personas fallecidas, quedando la ordenación *mortis causa* de sus datos personales sujeta a

la legislación de los Estados miembros (MORALEJO IMBERNÓN, 2020, 241-281; SANTOS MORÓN, 2018, 413-438; PATTI, 2019, 1-11; OTERO CRESPO, 2019, 89-133; ARGELICH COMELLES, 2023, 1135-1170) y siendo solo posible garantizar su control y acceso mediante un modo testamentario.

El ejercicio del derecho de acceso a la información pública se ve sujeto a unos límites o requisitos de localización de datos, dispuestos en el art. 14 de la Ley 19/2013. Estos límites deberán aplicarse de manera "justificada y proporcionada a su objeto y finalidad de protección", así como se atenderá a la concurrencia de un "interés público o privado" que justifique el acceso: ello se concreta, respectivamente, en el test del daño y en la justificación de un interés público o privado en las diversas Resoluciones de Transparencia de la AEPD[6]. En el caso de que la información requerida no contenga datos especialmente protegidos, según el art. 15.3, el acceso se debe conceder previa ponderación razonada y suficiente del interés público en la divulgación de la información, junto con los derechos de los afectados cuyos datos aparezcan en la información solicitada.

Las Resoluciones de Transparencia de la AEPD sobre la aplicación de los requisitos de localización de datos están disponibles en acceso abierto en su Portal (AEPD, 2025), en cumplimiento de la obligación de publicidad del art. 14.3, habiendo sido previamente notificadas y anonimizadas, sin perjuicio de lo dispuesto en el art. 20.3. Los límites al derecho de acceso a la información pública del art. 14 (REBOLLO DELGADO, 2017, 767-801), que no han sido modificados, sustituidos o derogados desde la aprobación de la norma tras las barreras regulatorias advertidas por la Comisión Europea en 2017 –un punto sobre el que se pedía expresamente informar–, se concretan en los siguientes, dispuestos ordenadamente: la seguridad nacional; la defensa; las relaciones exteriores; la seguridad pública; la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios; la igualdad de las partes en los procesos judiciales y la tutela judicial efectiva; las funciones administrativas de vigilancia, inspección y control; los intereses económicos y comerciales; la política económica y monetaria; el secreto profesional y la propiedad intelectual e industrial; la garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión; y, finalmente, la protección del medio ambiente. No obstante los límites al derecho de acceso a la información pública no se han modificado, se recuerda que los Estados Miembros debían derogar cualquier barrera regulatoria directa a la libre circulación de datos no personales en sus respectivas legislaciones antes del 30 de mayo de 2021, habiendo cumplido España con dicha obligación; a pesar de ello, se han detectado barreras regulatorias indirectas en las Resoluciones de Transparencia de la Agencia Española de Protección de Datos, en aplicación del art. 14.

Los apartados cuarto y quinto del art. 15 especifican que ello no aplica en los supuestos en los que el acceso se facilita previa disociación de los datos de carácter personal, en el caso de las resoluciones que están anonimizadas en su publicación, así como en el tratamiento posterior de los datos obtenidos en virtud del derecho de acceso a la información pública. Finalmente, el art. 16 reconoce el derecho de acceso parcial a la información pública en los supuestos en los que los límites del art. 14 no afecten a la totalidad de la información. En estos supuestos, se autoriza el acceso parcial a los datos previa omisión de la información afectada por el límite, salvo cuando la consecuencia sea la facilitación de una información distorsionada o que carezca de sentido, en cuyo caso se indicará al solicitante la parte de la información que ha sido omitida.

En los siguientes subapartados, se examinará brevemente el contenido del primer Estudio para la Comisión Europea en materia de requisitos de localización de datos –centrando la atención en las observaciones respecto de España–, así como la regulación europea sobre datos analizada en los informes nacionales y el régimen jurídico del ejercicio del derecho de acceso a la información pública en España.

II.1. El primer Estudio para la Comisión Europea sobre las restricciones a la localización de datos de 2017: *"Cross-border data flow in the digital single market: study on data location restrictions"*

El primer Estudio para la Comisión Europea sobre los requisitos de localización de datos se encuentra disponible en acceso abierto, bajo el título *"Cross-border data flow in the digital single market: study on data location restrictions"* (EUROPEAN COMMISSION, 2017). En cuanto a la evaluación sobre España en el Estudio, es necesario centrarse en las observaciones específicas que formula nuestro sector financiero, puesto que los únicos datos obrantes sobre nuestro Estado son los proporcionados por Eurostat. Por lo que respecta al sector financiero, se realizaron entrevistas a entidades financieras, así como a representantes de reguladores financieros a nivel europeo, mundial y nacional. En el informe, se subdividen los grupos de interés anonimizados entre: por una parte, las empresas que operan en el sector financiero y que encuentran obstáculos a la libre circulación de datos, como una entidad financiera española con presencia mundial y una federación bancaria europea; y, por otra parte, un regulador financiero nacional que toma decisiones sobre la libre circulación de datos a escala nacional.

Por lo que respecta al grupo de interés de las entidades financieras, en las entrevistas ponen de relieve los impedimentos que experimentan respecto del

uso de servicios en la nube, que habitualmente se externalizan. La institución financiera española entrevistada –que está anonimizada– expresó diversas observaciones de carácter negativo[7]. Por una parte, indicó que la regulación española limita la libre circulación de datos en la Unión Europea, y que ello se ve agravado por la falta de armonización de las normas entre los diversos Estados miembros. En este sentido, las entidades financieras españolas, a diferencia de otras entidades como las denominadas *Fintech* –que utilizan la innovación y el desarrollo tecnológico para el diseño, oferta y prestación de productos y servicios financieros–, deben notificar al Banco de España como autoridad nacional de supervisión financiera y bancaria la externalización de un servicio, incluyendo un servicio en la nube. La entidad financiera española advirtió que, en la práctica, el procedimiento para dicha autorización puede aumentar significativamente el tiempo de comercialización del servicio financiero y que, en consecuencia, agilizar dicho procedimiento y disponer de una armonización normativa en todos los Estados miembros es fundamental para que los bancos españoles sean competitivos en el mercado único digital. Por otra parte, esta entidad financiera manifestó que en España existen otros impedimentos, además de las barreras regulatorias, relativos a la falta de una cultura digital en la nube o la ausencia de una cultura basada en los datos, y que ello ocasiona incertidumbre en la utilización de nuevas tecnologías como los servicios de computación en la nube o *cloud computing*. Finalmente, la entidad financiera española declaró que utiliza la computación en la nube para actividades no esenciales del negocio bancario, como *Google Apps* y herramientas de colaboración para los empleados. No obstante, la entidad financiera española manifestó que le gustaría desarrollar el uso de la computación en la nube para el negocio principal en un futuro próximo, respecto de los datos financieros y los datos de los clientes.

El resto de las entidades financieras del primer grupo de interés entrevistadas indicaron que desarrollan el uso de la computación en la nube para almacenar y transferir datos –como los datos financieros y los datos de los clientes–, así como realizan estrategias para favorecer el proceso de externalización de determinados servicios de una manera más ágil y menos gravosa, con la finalidad de ser competitivos en el mercado único digital. Las entidades financieras entrevistadas recurren cada vez más al análisis de datos para desarrollar productos para sus clientes, pero se encuentran limitadas por los requisitos de localización de datos, según expresaron. Además, manifestaron que las diferencias entre estos requisitos nacionales de localización de datos y las normas sobre transferencia de datos y computación en la nube de Estados Unidos y la Unión Europea impactan directamente en la competitividad de las entidades financieras de la Unión, por la laxitud de la regulación estadounidense. A estos efectos, indicaron expresamente como ejemplo la transferencia de datos fuera

de la Unión Europea (GEIGER, 2003, 747-757). Complementariamente a lo indicado en el Estudio, es necesario apuntar que el marco normativo europeo para esta cuestión se encuentra dispuesto en diversos preceptos del RGPD, a saber: el art. 28 establece requisitos para los proveedores de servicios en la nube cuando actúan en nombre del responsable del tratamiento de datos; el art. 45 determina los caracteres de la transferencia de datos personales a terceros Estados; y el art. 49 impone requisitos para las transferencias de datos a terceros Estados, previa información de los riesgos, requiriendo el consentimiento expreso del titular. Finalmente, la STJUE de 4 de octubre de 2024 incide en que debe limitarse el uso de datos personales para la publicidad en línea[8], así como debe restringirse el uso de datos personales disponibles públicamente a los fines previstos para su publicación.

El segundo grupo de interés, relativo a los reguladores financieros, declaró que su actividad de supervisión puede tener un impacto en el desarrollo de servicios en la nube. En este sentido, indicaron que, si se realiza una supervisión prudencial, la atención se focaliza en la posición de solvencia, la liquidez y los riesgos operativos, por lo que aumenta el margen de autonomía de las entidades financieras nacionales, en contraposición con la supervisión basada en normas. En el mismo sentido, un regulador nacional que se rija por el principio de supervisión prudencial se preocupa de que las entidades financieras realicen un análisis de riesgos adecuado, así como que garanticen el derecho de auditoría en la subcontratación o en los contratos de externalización de servicios. El regulador nacional al que se entrevistó manifestó que se recibían muchas consultas acerca del requisito de presentar un análisis de riesgo en la externalización de servicios en la nube, porque se trata de un requisito de difícil cumplimiento, para cuya solución se creó un modelo de análisis de riesgos. El mismo regulador señaló que la mayoría de los proveedores de servicios en la nube no indican en sus contratos los requisitos legales y reglamentarios aplicables, en concreto, las condiciones generales de la contratación que los proveedores de servicios pueden incluir para restringir la actividad de supervisión pública.

II.2. La regulación europea sobre datos de los informes nacionales para la Comisión Europea: el Reglamento 2018/1807, sobre la libre circulación de datos no personales, la Directiva 2019/1024, sobre los datos abiertos, y el Reglamento 2022/868, sobre la gobernanza de datos

En este apartado, se examinarán brevemente las normas sobre las que se evalúan los requisitos de localización de datos en los informes nacionales para la Comisión Europea: el Reglamento 2018/1807 del Parlamento Europeo y del

Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea; la Directiva 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público[9]; y el Reglamento 2022/868 del Parlamento y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento 2018/1724[10], conocido como *Data Governance Act*, en adelante, DGA.

Por lo que se refiere al Reglamento sobre la libre circulación de datos no personales –previamente apuntado por la vinculación con los requisitos de localización de datos en las legislaciones nacionales[11]–, tiene como finalidad eliminar los obstáculos a su transmisión entre los Estados miembros de la Unión Europea y los sistemas informáticos en su seno. Por ello, las disposiciones del Reglamento garantizan el almacenamiento y el procesamiento transfronterizo de datos, la disponibilidad de datos para su control por la Administración, incluyendo su almacenamiento y procesamiento en la nube, así como la facilitación del cambio de proveedores de servicios en la nube para usuarios profesionales y la garantía de la seguridad respecto de su almacenamiento y procesamiento.

Por lo que respecta a la Directiva sobre los datos abiertos, pretende fomentar la reutilización de la información del sector público mediante un mercado europeo de datos regulado, con especial atención a la transparencia y competencia. La armonización normativa en virtud de esta Directiva estimula la publicación de datos dinámicos y la creación de interfaces gráficas adecuadas, limita las excepciones que permiten a los organismos públicos cobrar más que los costes marginales de difusión en materia de reutilización de sus datos, a la vez que amplía el ámbito de aplicación de la Directiva. En este sentido, los datos de las empresas públicas tienen que poder reutilizarse, y los datos de investigación resultantes de la financiación pública deben facilitarse en acceso abierto. Finalmente, los datos de alto valor o aquellos que poseen beneficios para la sociedad o la economía disponen de un régimen jurídico diferenciado, que garantiza su disponibilidad gratuita, se proporcionan mediante interfaces adecuadas y se permite su descarga masiva.

El Reglamento sobre la gobernanza de datos regula el intercambio de datos B2B, B2C y B2G y es también objeto de los informes nacionales para la Comisión Europea. Este Reglamento, junto con el Reglamento 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento 2017/2394 y la Directiva 2020/1828[12], conocido como *Data Act* y que no es objeto del informe, suponen el *legal transplant* del instrumento de *soft law "ALI-ELI Principles for a Data Economy – data transactions and data rights"* —en adelante, *ALI-ELI Principles*— elaborado por el *American Law Institute* y

el *European Law Institute* sobre la transmisión, uso y derechos sobre los datos (ARGELICH COMELLES, 2024, 1-23). La *Data Governance Act* permite crear los procesos y estructuras necesarias para el intercambio de datos (CASTRO CARRANZA, 2022, 1-15; MARTÍNEZ MARTÍNEZ, 2021, 1-18; FERNÁNDEZ HERNÁNDEZ, 2022, 1-10; CASTRO CARRANZA, 2022, 1-15), siendo el intercambio B2G la novedad de este Reglamento con respecto al RGPD. La parte II de los *ALI-ELI Principles,* relativa a los *data contracts,* dispone el contenido de las cláusulas contractuales sobre el suministro e intercambio de datos, cuya correspondencia se encuentra en los arts. 10-22 DGA (CAROVANO, 2023, 1-18). Estas cláusulas se aplican también a otros intercambios de datos como los *data pooling arrangement* o la puesta en común de datos, el intercambio o uso compartido (PALOMAR OLMEDA, 2017, 435-488), lo que se corresponde con el *data monitoring,* así como los servicios de intermediación de datos regulados en el art. 12 DGA (SPIECKER, 2022, 132-145; CÁMARA LAPUENTE, 2020, 141-175; CAROVANO, 2023, 1-18).

Una vez presentada brevemente la *Data Governance Act,* conviene centrarse en aquellas disposiciones que inciden en los requisitos de localización de datos en España y su adecuación al ordenamiento jurídico europeo. El art. 5 DGA establece diversas condiciones para la reutilización de los datos por parte de organismos del sector público (RUOHONEN, 2023, 1-9), lo que tiene incidencia en las resoluciones a las que se debe dar publicidad, como las Resoluciones de Transparencia de la AEPD: la anonimización de los datos; la modificación y el agregado de su tratamiento cuando tengan carácter confidencial; la reutilización a distancia, facilitada y controlada por el organismo público; así como que el acceso y reutilización de los datos se sujete a unas normas de seguridad estrictas. Complementariamente, los organismos del sector público impondrán las condiciones para la integridad del funcionamiento de los sistemas técnicos del entorno de tratamiento seguro, pudiendo adoptar como decisión la prohibición de la reutilización de manera comprensible y transparente en los siguientes casos: por ausencia de observancia de la confidencialidad; por falta de la obtención del consentimiento de los interesados; por infracción de los derechos de propiedad intelectual; o por ausencia de información al organismo público de la transmisión de estos datos a un tercer Estado. Asimismo, la Comisión Europea adoptará actos delegados para los datos que afecten, entre otros, la seguridad y salud públicas (ECHEZARRETA FERRER, 2021, 263-314; GERST, 2023, 204-210), así como los que puedan entrañar el riesgo de la identificación de datos anonimizados. Ello ha sido identificado, junto con su operatividad, los desajustes en materia financiera, de recursos humanos, de riesgos y seguridad, así como en relación con la innovación tecnológica, como los principales riesgos de la gobernanza de datos (MAHANTI, 2021, 53-64).

II.3. Régimen jurídico del ejercicio del derecho de acceso a la información pública en España: la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno

Finalmente, procede examinar brevemente las disposiciones sobre el ejercicio del derecho de acceso a la información pública *ex* arts. 17-24 de la Ley 19/2013. Respecto de la solicitud de acceso a la información, el art. 17 indica que debe dirigirse al titular del órgano administrativo que posea la información, y regula su presentación. En el art. 18, se disponen las causas de inadmisión y, en el art. 19, la tramitación de dicha solicitud y su eventual subsanación. Respecto del análisis de las Resoluciones de Transparencia de la AEPD[13], procede detenerse en el art. 20, relativo a la resolución por la que se conceda o deniegue el derecho de acceso a la información pública. Dicha resolución debe notificarse al solicitante y a los terceros afectados en el plazo máximo de un mes desde la recepción de la solicitud, ampliable por un mes más en atención al volumen o la complejidad de la información. Las resoluciones que denieguen el acceso a la información pública, las que concedan el acceso parcial o mediante una modalidad distinta a la solicitada, así como las que permitan el acceso con oposición de un tercero deben estar motivadas. En el caso de que la mera indicación de la existencia o inexistencia de la información suponga la vulneración de los límites del derecho de acceso, deberá advertirse en la resolución.

Una vez transcurrido el plazo máximo para resolver el expediente administrativo, el silencio administrativo se considerará negativo. Las resoluciones en esta materia son susceptibles de recurso ante la jurisdicción contencioso-administrativa, *ex* art. 23, sin perjuicio de la reclamación potestativa en vía administrativa contemplada en el art. 24. Se considerará una infracción grave el incumplimiento reiterado de la obligación de resolver en plazo. El art. 22 establece que el acceso a la información se realizará preferentemente por vía electrónica, salvo cuando no sea posible o el solicitante indique expresamente otro medio. Como se analizará, la necesidad de almacenamiento local es una de las barreras regulatorias detectadas por la Comisión Europea, por la falta de acceso electrónico y las dificultades para los proveedores extranjeros, que a su vez se encuentra en algunas de las Resoluciones de Transparencia de la AEPD[14]. En el caso de que no pueda proporcionarse el acceso en el momento de notificar la resolución, se tendrá que efectuar en un plazo no superior a diez días.

III. LAS BARRERAS REGULATORIAS A LA LIBRE CIRCULACIÓN DE DATOS NO PERSONALES Y LA APLICACIÓN DE LOS REQUISITOS DE LOCALIZACIÓN DE DATOS EN ESPAÑA

A los efectos de realizar una adecuada evaluación de la conformidad de los requisitos españoles de localización de datos, regulados en la Ley 19/2013, con

el Reglamento 2018/1807, la Directiva 2019/1024 y el Reglamento 2022/868, es necesario examinar primeramente las barreras regulatorias directas e indirectas a la libre circulación de datos no personales detectadas por la Comisión Europea, para posteriormente identificarlas en las Resoluciones de Transparencia de la AEPD[15].

III.1. Las barreras regulatorias directas e indirectas a la libre circulación de datos no personales detectadas en el primer Estudio para la Comisión Europea de 2017

Por lo que respecta a las barreras regulatorias directas e indirectas a la libre circulación de datos no personales, se encuentran diversas claves en el primer estudio para la Comisión Europea *"Cross-border data flow in the digital single market: study on data location restrictions"* (EUROPEAN COMMISSION, 2017). La primera y la más relevante es que en las barreras regulatorias directas e indirectas, contenidas en las tablas comparativas donde constan los Estados donde se han detectado, España no figura porque no ha sido analizada. La única aportación específica sobre España en el Estudio es la entrevista a la entidad financiera referida anteriormente[16], junto con los datos estadísticos de Eurostat sobre cada Estado miembro. Con base en las barreras regulatorias advertidas por la Comisión Europea, se realizará su identificación en las Resoluciones de Transparencia de la AEPD del periodo 2020-2025[17]. En este sentido, una barrera será directa cuando una norma nacional establezca explícitamente el lugar de almacenamiento o transferencia de los datos, así como cuando imponga que solamente es posible cumplir con dicha obligación cuando los datos estén en una ubicación específica. Se apunta aquí que los Estados Miembros debían derogar las barreras regulatorias directas en sus respectivas legislaciones antes del 30 de mayo de 2021, y se adelanta que no han sido detectadas en la legislación española. Las barreras serán indirectas cuando la legislación contenga requisitos que, una vez aplicados, restrinjan la ubicación o la circulación de los datos, como por ejemplo que deban estar permanentemente accesibles para un supervisor nacional, que tengan que ser eliminados sin posibilidad de recuperarlos, o que el acceso sea exclusivo para su titular.

Las barreras regulatorias a la libre circulación de datos no personales se concretan en las siguientes manifestaciones abstraídas por la Comisión Europea conforme a la casuística de las legislaciones nacionales. Por ello, su tratamiento en este apartado se dividirá entre las que han sido detectadas en las Resoluciones de Transparencia de la AEPD, y las que, en sentido contrario, no se han identificado. De conformidad con estas barreras regulatorias directas e indirectas, se analizarán las Resoluciones de Transparencia del periodo 2020-2025 en el siguiente subapartado. Por lo que respecta a las barreras regulatorias identificadas en las Resoluciones de Transparencia, se encuentran la prohibición del acceso o la divulgación a terceros de los datos no personales en aras de la confidencialidad cuando no existe una investigación en curso,

así como el almacenamiento pasivo externo al titular de los datos cuando no existe una investigación en curso; en ambos supuestos la información a la que se ha accedido no requiere ningún tratamiento posterior por parte del proveedor de servicios de almacenamiento. Cabe indicar que una barrera regulatoria que se ha solucionado en las diversas Resoluciones de Transparencia es aquella relativa a que los mecanismos de control y las auditorías de los supervisores nacionales no pueden obstaculizarse, porque ello dificulta la tarea de las autoridades, siendo el fundamento de la denegación de acceso a la información en diversos supuestos.

En cuanto a las barreras regulatorias que no se han detectado en las Resoluciones de Transparencia, se encuentran las siguientes, cuya correlación se refiere separadamente.

- Los requisitos técnicos nacionales de almacenamiento o intercambio de datos, por los obstáculos que pueden suponer para los proveedores extranjeros.
- La autorización nacional de los proveedores de servicios de almacenamiento de datos, por las dificultades de acceso para otros proveedores.
- La obligación de disponer de registros de datos con almacenamiento local, que no se encuentren en la nube, por suponer una restricción en el acceso.
- El requisito de mantener una copia local de la documentación con restricciones de acceso específicas, que pueda suponer la necesidad de un almacenamiento pasivo externo.
- El requisito de comunicar datos electrónicos a una autoridad pública, porque puede perjudicar la interoperabilidad transfronteriza.
- La aplicación de esquemas específicos de gestión de riesgos a los subcontratistas que, por su determinación por los Estados miembros, sean difíciles de conocer para los proveedores extranjeros.
- El hecho de que los subcontratistas deban estar oficialmente autorizados como proveedores de servicios, por las dificultades de su autorización cuando presten sus servicios en diversos Estados.
- La existencia de una supervisión comparable en el Estado del establecimiento del proveedor del servicio, lo que supone que el proveedor solo puede operar desde Estados donde exista dicha supervisión.
- La negociación caso por caso con el regulador previa a la circulación transfronteriza de datos hacia proveedores desconocidos, lo que dificulta la prestación del servicio por proveedores extranjeros.
- La imposición de una ley aplicable favorable al Estado del regulador público, que conlleva que los proveedores deban cumplir con los requisitos de diversas jurisdicciones para poder operar.
- La designación de una entidad específica que gestione una base de datos oficial, porque el almacenamiento o la transferencia de datos solo puede prestarse en exclusiva.

- El hecho de que el acceso o la utilización de los datos deba estar autorizada por una norma o autoridad competente, lo que supone un requisito de difícil cumplimiento para los proveedores de servicios en el extranjero.
- La obligación de que los datos se destruyan en determinadas circunstancias, una previsión que es ineficaz sin almacenamiento local.
- La gestión o actualización conjunta de los datos, porque dificulta su gestión por un tercero.
- La imposición de obligaciones de confidencialidad a quien tenga acceso a los datos, por suponer una prohibición de almacenamiento pasivo externo, en atención a la ausencia de tratamiento de los datos posterior.
- El establecimiento de una protección contra confiscaciones de información, porque dificulta su cumplimiento por un proveedor de servicios externo.
- La obligación de que los destinatarios de los datos conserven ciertos certificados, por la prohibición implícita de almacenamiento pasivo que supone.
- La prohibición de transferencias de datos sin intervención humana, por las dificultades que plantea su cumplimiento por proveedores extranjeros, ya sea por su disponibilidad o por los requisitos lingüísticos.
- Los controles que limitan el *hardware* o el *software* de procesamiento de datos, por las dificultades que conlleva para los proveedores extranjeros.
- Los requisitos en el uso del cifrado de datos, que dificulten la prestación del servicio por proveedores extranjeros.
- Los requisitos de segregación de datos, por los problemas que plantea para los proveedores extranjeros.
- La recuperabilidad de la información por las autoridades supervisoras durante un tiempo determinado, por los impedimentos que supone para un almacenamiento descentralizado.
- La instalación del almacenamiento de datos dentro de las fronteras nacionales, o fuera de las mismas con autorización de la autoridad supervisora, por los límites geográficos que supone.
- El hecho de que el formato y método de la entrega de datos deba especificarse por la autoridad nacional durante las verificaciones, por las dificultades que implica para los proveedores extranjeros.

III.2. Análisis de las barreras regulatorias indirectas en las Resoluciones de Transparencia de la Agencia Española de Protección de Datos sobre los requisitos de localización de datos en el periodo 2020-2025

Las Resoluciones de Transparencia de la AEPD del periodo 2020-2025, analizadas en el informe español para la Comisión Europea bajo el estudio

"Supporting the evaluation of the Free Flow of Non-Personal Data Regulation, Open Data Directive and Data Governance Act", se encuentran disponibles en acceso abierto en su Portal (AEPD, 2025). Con carácter previo a su examen, conviene apuntar algunas cuestiones. En primer lugar, los límites del derecho de acceso a la información pública o los requisitos de localización de datos –previstos en el art. 14 de la Ley 19/2013– que no se han aplicado corresponden a: la seguridad nacional, la defensa, la seguridad pública, la política económica y monetaria, y la protección del medio ambiente. En segundo lugar, con respecto a la protección de datos personales *ex* art. 15.3 de la Ley 19/2013, las causas de ponderación que obran en las Resoluciones de Transparencia son expresamente las siguientes: la justificación por los solicitantes del acceso de fines históricos, científicos o estadísticos; el menor perjuicio de los derechos de los afectados cuando los documentos contuviesen únicamente datos de carácter meramente identificativo; y la mayor garantía de los derechos de los afectados en los supuestos de afectación a la intimidad, la seguridad o cuando se refieran a personas menores de edad. Diversas de las Resoluciones de Transparencia conceden el acceso parcial a la información por los motivos contemplados en el art. 16 de la Ley 19/2013. Como comentario general a todas las Resoluciones de Transparencia, que serán analizadas cronológicamente, en muchas ocasiones se observa una reiteración e identidad literal en los fundamentos jurídicos por los que se aplican los requisitos de localización de datos. Por otra parte, las Resoluciones de Transparencia que figuran duplicadas en el Portal de la AEPD, de 21 de agosto de 2024 y de 10 de noviembre de 2022, provienen respectivamente de sendos asuntos. Finalmente, el acceso o la utilización de los datos no personales autorizado por una norma o autoridad competente, con base en los requisitos de localización de datos, pretende garantizar la seguridad y la confidencialidad, apoyar la rendición de cuentas y la supervisión, mantener el control nacional sobre los recursos esenciales, así como prevenir pérdidas económicas a largo plazo. No obstante, es oportuno ponderar dichos límites del derecho de acceso a la información pública con las barreras regulatorias a la libre circulación de datos no personales, con la finalidad de equilibrar ambos intereses. A continuación, se identificarán las barreras regulatorias indirectas expuestas anteriormente en las Resoluciones de Transparencia[18], así como se sistematizarán en función de si se han detectado.

III.2.A. Resoluciones con barreras regulatorias indirectas a la libre circulación de datos no personales

En la Resolución sobre solicitud de acceso a la información pública de 25 de noviembre de 2020[19], se otorga el acceso parcial a la información solicitada con

base en las causas establecidas en el art. 14.1 e), g) y h) de la Ley 19/2013. Los fundamentos jurídicos son los siguientes: respecto del art. 14.1 h), los posibles perjuicios a los intereses económicos y comerciales del autor de la notificación; en cuanto al art. 14.1 e), los posibles perjuicios a la investigación de ilícitos administrativos o penales; y, finalmente, en cuanto al art. 14.1 g), por los posibles perjuicios a las funciones de vigilancia, inspección y control. La Resolución autoriza parcialmente el acceso mediante la remisión electrónica en un documento en formato *Portable Document Format* –en adelante, pdf–, que contenga los ficheros registrados debidamente, habiendo disociado los datos personales. En cuanto al acceso en formato pdf, se ha advertido anteriormente como una barrera regulatoria a la libre circulación de datos no personales, por la necesidad de almacenamiento local externo del documento y por los impedimentos para los proveedores extranjeros. Para evitar la necesidad de almacenamiento local, debe proponerse su acceso o en formato electrónico, como un enlace web, o bien en un documento almacenado en la nube sin restricciones de acceso.

En la Resolución sobre solicitud de acceso a la información pública de 28 de junio de 2022[20], se deniega el acceso a la información para fines de investigación científica en virtud del art. 14.1 h), j) y k) de la Ley 19/2013; se argumenta que la divulgación de la información a terceros puede afectar los intereses económicos y comerciales, la propiedad intelectual e industrial del afectado, así como ocasionaría un perjuicio a la garantía de confidencialidad con la que esa información fue comunicada a la AEPD. En este caso, se observa como barrera regulatoria que la prohibición de acceso a un tercero, en aras de la confidencialidad, prohíbe a su vez el almacenamiento pasivo externo al titular de los datos, pues la finalidad del acceso a dichos datos es científica y no se observa una obstaculización a las funciones administrativas de control y auditoría que justifique la denegación.

En la Resolución sobre solicitud de acceso a la información pública de 10 de abril de 2024[21], se concede parcialmente el acceso a la información con base en el art. 14.1 e), g) y k) de la Ley 19/2013, constando la tramitación de diversos expedientes conjuntamente por parte de la AEPD respecto del mismo solicitante. Respecto del primer expediente, se deniega el acceso por obrar en poder del solicitante la información requerida. Respecto del segundo expediente, se autoriza el acceso a la información, pero habida cuenta del volumen del citado expediente –que impide su envío en papel–, el acceso se habilita en formato pdf, debidamente anonimizado, almacenado en una memoria *Universal Serial Bus* –en adelante, USB–, y remitido por correo postal junto con la Resolución. Respecto de este acceso a la información, cabe señalar como barrera regulatoria la necesidad de almacenamiento local en un USB del documento en formato pdf, así como las dificultades que entrañaría para los proveedores extranjeros, por lo que debería proponerse su acceso o bien en formato electrónico o en un do-

cumento almacenado en la nube sin restricciones de acceso. En cuanto al tercer expediente, se habilita el acceso a una copia de la información en papel, con los datos personales anonimizados, lo que también supone una barrera regulatoria relativa a la necesidad de almacenamiento externo. Por lo que respecta al cuarto expediente, nuevamente se habilita el acceso a una copia del expediente en papel, debidamente anonimizada, lo que implica la misma barrera regulatoria de almacenamiento externo indicada. En cuanto al quinto expediente, su difusión supondría un perjuicio para la actividad de investigación y sanción penal, por lo que se concede el acceso parcial a la información con base en las causas contenidas en el art. 14.1 e), g) y k) de la Ley 19/2013. En este último expediente de autorización parcial, no se observan barreras regulatorias, en atención a que las funciones administrativas de control y auditoría no se pueden obstaculizar.

En la Resolución sobre solicitud de acceso a la información pública de 30 de octubre de 2024[22], se concede parcialmente el acceso a la información en virtud del art. 14.1 k) y j) de la Ley 19/2013, respecto de la obtención de la copia completa de un expediente de la Subdirección General de Inspección de Datos de la AEPD. En la Resolución, se concede el acceso parcial a la información relativa al expediente, previa disociación de los datos personales y en formato pdf, pero se deniega el acceso al informe de auditoría de ciberseguridad porque su divulgación podría conllevar un riesgo. Por lo que respecta al acceso parcial a la información, se detecta la barrera regulatoria relativa a la necesidad de almacenamiento pasivo externo, por lo que se tendría que haber proporcionado o bien en formato electrónico o en la nube sin restricciones de acceso. Por lo que respecta a la denegación de acceso al informe de auditoría, resulta correcta en aras de la observancia de la barrera regulatoria relativa a la ausencia de obstaculización a la Administración en sus funciones de control y auditoría.

III.2.B. Resoluciones en las que se no han detectado barreras regulatorias indirectas a la libre circulación de datos no personales

En la Resolución sobre solicitud de acceso a la información pública de 2 de febrero de 2021[23], se concede parcialmente dicho acceso en virtud del art. 14.1 h) de la Ley 19/2013, por tratarse de ofertas técnicas que contienen una información empresarial sensible sobre las estrategias y relaciones comerciales. Por ello, en la Resolución se incluye un Anexo I, accesible desde el Portal de la AEPD, que contiene una tabla que enlaza a la información publicada en la Plataforma de Contratación del Sector Público. Dicha Resolución también concede parcialmente el acceso, previa disociación de los datos personales, a la información no publicada en la referida Plataforma sobre los contratos de difusión y los contratos

de formación, en sus Anexos II y III, accesibles desde el Portal de la AEPD. No se observan barreras regulatorias en esta Resolución, en atención a la facilitación en acceso abierto de toda la documentación.

En la Resolución sobre solicitud de acceso a la información pública de 19 de mayo de 2021[24], se deniega el acceso con base en las funciones administrativas de vigilancia, inspección y control, previstas en el art. 14.1 g) de la Ley 19/2013, porque las actuaciones inspectoras de la AEPD estaban en curso y cualquier divulgación de información las podía perjudicar. Tampoco se observan barreras regulatorias en este supuesto, en aras de la preservación de las funciones de control y auditoría de la Administración.

En la Resolución sobre solicitud de acceso a la información pública de 1 de junio de 2021[25], se concede parcialmente el acceso a la información en virtud del art. 14.1 e) de la Ley 19/2013, en atención al eventual perjuicio para la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios. En este caso, el tercero afectado informa que con respecto al titular de la empresa solicitante existe un procedimiento en curso en el orden jurisdiccional penal. En esta Resolución, no se observan barreras regulatorias, en aras de las funciones de control y auditoría de la Administración.

En la Resolución sobre solicitud de acceso a la información pública de 12 de enero de 2022[26], se concede parcialmente el acceso a la información con base en el art. 14.1 e) de la Ley 19/2013. En este supuesto, referido a una infracción administrativa, se autoriza la información en cuanto al número de reclamaciones recibidas, su estado de tramitación y las sanciones impuestas. En esta Resolución, no se observan barreras regulatorias, por la preservación de las funciones administrativas de control y auditoría.

En la Resolución sobre solicitud de acceso a la información pública de 21 de enero de 2022[27], se deniega el acceso a la información en virtud del art. 14.1 e) y k) de la Ley 19/2013, por afectar a investigaciones en curso de la Subdirección General de Inspección de Datos de la AEPD. Tampoco se observan barreras regulatorias en este supuesto, por la garantía de las funciones administrativas de control y auditoría.

En la Resolución sobre solicitud de acceso a la información pública de 26 de enero de 2022[28], se deniega el acceso a la información solicitada con base en el art. 14.1 e) y k) de la Ley 19/2013, por estar pendientes investigaciones judiciales en curso sobre la información requerida, y por el perjuicio que podría suponer la revelación de su contenido a terceros. No se detectan barreras regulatorias en este supuesto por las funciones administrativas de control y auditoría, que deben ser preservadas.

En la Resolución sobre solicitud de acceso a la información pública de 10 de mayo de 2022[29], se concede el acceso a la información sobre los expedientes con-

cluidos que constan en la AEPD, así como las resoluciones relacionadas. Consta en la Resolución el acceso desde el Portal de la AEPD a toda la documentación mediante enlaces web, de manera que no se observan barreras regulatorias. Por otra parte, se deniega el acceso a otra información en virtud del art. 14.1 e) y k) de la Ley 19/2013, por tratarse de expedientes de investigación abiertos, cuya revelación menoscabaría la adecuada toma de decisiones sin injerencias externas. Por la preservación de las funciones administrativas de control y auditoría, no se detectan barreras regulatorias.

En la Resolución sobre solicitud de acceso a la información pública de 8 de junio de 2022[30], se autoriza el acceso a la información sobre la unidad, dirección o departamento concreto de los organismos a los que la AEPD dirigió un cuestionario, por tratarse todos ellos de instituciones públicas. No obstante, se deniega el acceso a la información sobre el contenido concreto del cuestionario, con base en el art. 14.1 c) de la Ley 19/2013, por corresponder a la AEPD el ejercicio de las funciones relacionadas con la acción exterior del Estado sobre protección de datos. En aras de la preservación de las funciones de control y auditoría, no se observan barreras regulatorias en esta Resolución.

En la Resolución sobre solicitud de acceso a la información pública de 18 de julio de 2022[31], se deniega el derecho de acceso a la información con base en el art. 14.1 f) de la Ley 19/2013, en atención a los perjuicios que pudieran derivarse de la revelación de información a terceros sobre un procedimiento administrativo sancionador de la AEPD del que está pendiente la resolución de un recurso en el orden jurisdiccional contencioso-administrativo. La AEPD entiende que debe prevalecer el respeto a la igualdad de las partes en el proceso y la tutela judicial efectiva. No se observa ninguna barrera regulatoria, puesto que se garantizan las funciones administrativas de control y auditoría.

En la Resolución sobre solicitud de acceso a la información pública de 8 de agosto de 2022[32], se deniega el derecho de acceso a la información en virtud del art. 14.1 k) y h) de la Ley 19/2013. En este caso, la revelación de información sobre los procedimientos, documentos y detalles relativos a la seguridad de la organización afectada, así como de sus auditorías de seguridad interna a un tercero pueden perjudicar seriamente a la entidad afectada por un procedimiento sancionador de la AEPD. En este supuesto, no se observa ninguna barrera regulatoria, en aras de la garantía de las funciones de control y auditoría de la Administración.

En la Resolución sobre solicitud de acceso a la información pública de 10 de noviembre de 2022[33], se concede parcialmente el acceso a la información *ex* art. 14.1 e) y k) de la Ley 19/2013. La primera petición de acceso a la información se centra en las reclamaciones presentadas a una empresa. La entidad, sujeta a las investigaciones de la AEPD, fue informada de la solicitud y no se opuso a

dicho acceso previa disociación de los datos personales. Por ello, en este caso se facilita el acceso a los datos anonimizados, sin que se observe ninguna barrera regulatoria por disponerse en un Anexo en el Portal de la AEPD. En cuanto al siguiente expediente vinculado al mismo caso y que se encuentra en tramitación, se deniega el acceso con base en el art. 14.1 e) y k) de la Ley 19/2013, puesto que la revelación a terceros de documentos en esta fase del procedimiento puede perjudicar la investigación en curso, la confidencialidad, así como se añaden impedimentos técnicos por el gran tamaño de los documentos. No se observan barreras regulatorias en este supuesto, en atención a que las actividades de control y auditoría de la Administración no pueden ser obstaculizadas. Se informa de que, con respecto a los expedientes concluidos, las resoluciones se encuentran publicadas en el Portal de la AEPD y como Anexo a la Resolución. Por lo que respecta al tercer expediente vinculado al mismo caso, se deniega el acceso a la información en virtud del art. 14.1 e) y k) de la Ley 19/2013, porque se solicitan unos datos a la AEPD sin que el solicitante haya ejercido su derecho ante el responsable del tratamiento.

En la Resolución sobre solicitud de acceso a la información pública de 28 de noviembre de 2022[34], se deniega el derecho de acceso a la información con base en el art. 14.1 h) y j) de la Ley 19/2013, en atención a que el acceso a los informes sobre la conformidad con la normativa de protección de datos de un nuevo proyecto de negocio elaborado por la AEPD supone un considerable perjuicio económico y comercial, así como una pérdida de ventaja competitiva. Asimismo, se argumenta que la solicitud no está motivada, por lo que no se ha justificado un interés legítimo privado superior que pueda desvirtuar la confidencialidad. En cuanto a las barreras regulatorias, no se detectan porque este supuesto entra dentro de las funciones de auditoría de la Administración, que deben preservarse.

En la Resolución sobre solicitud de acceso a la información pública de 16 de enero de 2023[35], se deniega el derecho de acceso a la información en virtud del art. 14.1 f) de la Ley 19/2013. En cuanto al test del daño, la entidad afectada ha sido sancionada por la AEPD, y ha recurrido la misma ante la jurisdicción contencioso-administrativa, por lo que la revelación de cualquier información a terceros puede perjudicar su derecho de defensa. En cuanto a la ponderación de intereses, el solicitante no ha alegado ningún interés público o privado prevalente que justifique el acceso, por lo que debe prevalecer el respeto a la igualdad de las partes en el proceso y la tutela judicial efectiva. No se identifican barreras regulatorias en atención a las funciones de control y auditoría de la Administración.

En la Resolución sobre solicitud de acceso a la información pública de 10 de marzo de 2023[36], se deniega el acceso a la información con base en el art. 14.1 f) de la Ley 19/2013. Por una parte, la entidad afectada ha sido sancionada administrativamente por la AEPD, cuya solicitud tiene como finalidad la interposición de

un recurso, por lo que la revelación de información a un tercero puede perjudicar el derecho a la defensa. En cuanto a la ponderación de intereses, la AEPD indica que la solicitante no ha alegado ningún interés público o privado para el acceso a los datos. En este supuesto, tampoco de detectan barreras regulatorias, en aras de la salvaguardia de las funciones de control y auditoría de la Administración.

En la Resolución sobre solicitud de acceso a la información pública de 28 de noviembre de 2023[37], se deniega el acceso en virtud del art. 14.1 e) y g) de la Ley 19/2013. La solicitud versa sobre un problema de seguridad en materia de datos personales, comunicado a la AEPD, por lo que la difusión de los datos perjudicaría las funciones administrativas de control u otras investigaciones. En este caso, no se observan barreras regulatorias, por la garantía de las funciones administrativas de control y auditoría.

En la Resolución sobre solicitud de acceso a la información pública de 20 de diciembre de 2023[38], se deniega el acceso con base en el art. 14.1 k) de la Ley 19/2013. En este sentido, el acceso público al análisis de riesgos y a la evaluación de impacto del Sistema Interno de Información y Defensa del Informante de la AEPD expone estos sistemas a un riesgo, por la actividad de tratamiento y las medidas de seguridad previstas. En este caso, tampoco se detectan barreras regulatorias, para la garantía de las funciones administrativas de control y auditoría.

En la Resolución sobre solicitud de acceso a la información pública de 16 de febrero de 2024[39], se ha autorizado parcialmente el acceso en virtud del art. 14.1 k) de la Ley 19/2013. La solicitud versa sobre los datos, procedimientos y referencias obrantes en la AEPD sobre la aplicación de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción[40]. Para dicha protección, los denunciantes y las personas afectadas tienen derecho a la confidencialidad. Por otra parte, el acceso público a la información sobre invocaciones, citas, procedimientos y resoluciones en aplicación de la Ley 2/2023 expone a un riesgo al Canal de Protección del Informante y a los denunciantes. Por ello, en primer lugar, se concede el acceso a la información solicitada referente a la implantación del Canal de Protección del Informante, mediante unos enlaces web en la propia Resolución, por lo que no se observan barreras regulatorias relativas al almacenamiento pasivo externo. En segundo lugar, se limita el acceso a la información relativa a las invocaciones, citas, procedimientos y resoluciones en aplicación de la Ley 2/2023, en virtud del art. 14.1 k) de la Ley 19/2013, por lo que no se detectan barreras regulatorias por la garantía de las funciones administrativas de control y auditoría.

En la Resolución sobre solicitud de acceso a la información pública de 10 de junio de 2024[41], se deniega el derecho de acceso en virtud del art. 14.1 h) de la Ley 19/2013, por el que se solicitaba la copia completa de un expediente de

la Subdirección General de Inspección de Datos de la AEPD. En atención a los perjuicios que se podrían causar, y por entender que no existe un interés público o privado superior, se deniega el derecho de acceso. No se detectan barreras regulatorias al respecto, en atención a la actividad de control y auditoría de la Administración.

En la Resolución sobre solicitud de acceso a la información pública de 12 de julio de 2024[42], por la que se solicitaba el acceso a una documentación presentada a la AEPD en virtud de un expediente en trámite, se deniega dicho acceso con base en el art. 14.1 h) de la Ley 19/2013. El expediente contiene información cuya divulgación puede resultar perjudicial y no existe un interés público o privado que justifique su revelación. Tampoco se detectan barreras regulatorias, habida cuenta de la evitación de obstáculos a las actividades de control y auditoría de la Administración.

En la Resolución sobre solicitud de acceso a la información pública de 21 de agosto de 2024[43], se concede parcialmente el acceso a la copia completa de un expediente de la AEPD sobre el tratamiento de datos personales entre dos empresas por el art. 14.1 h) de la Ley 19/2013. En atención a los posibles perjuicios derivados del test del daño, por la información que se contiene, se autoriza el acceso a dicho expediente, previa disociación de los datos personales, una vez que haya transcurrido el plazo previsto para interponer un recurso contencioso-administrativo. No obstante, se deniega el acceso a la información del contrato celebrado en estas dos empresas responsables del tratamiento de datos. No se observan barreras regulatorias en este supuesto, en aras de la garantía de la actividad de control y auditoría de la Administración.

En la Resolución sobre solicitud de acceso a la información pública de 7 de octubre de 2024[44], se deniega el acceso a la copia íntegra un expediente sancionador de la AEPD con base en el art. 14.1 e) de la Ley 19/2013. Este asunto se encuentra en fase de instrucción de un procedimiento penal en el momento de solicitar el acceso a la información. No se identifican barreras regulatorias, en atención a la preservación de la actividad de control y auditoría de la Administración.

En la Resolución sobre solicitud de acceso a la información pública de 23 de octubre de 2024[45], se deniega el derecho de acceso a la información en virtud del art. 14.1 f) de la Ley 19/2013, en atención a que la resolución del procedimiento administrativo sancionador de la Subdirección General de Inspección de Datos de la AEPD se ha recurrido ante la jurisdicción contencioso-administrativa. Se deniega el acceso en atención al test del daño y a que no existe un interés público o privado superior. En este asunto, no se observa ninguna barrera regulatoria, en atención a la preservación de las funciones de control y auditoría de la Administración.

En la Resolución sobre solicitud de acceso a la información pública de 23 de octubre de 2024[46], se concede parcialmente el acceso con base en el art. 14.1 k)

de la Ley 19/2013, en atención a que el solicitante requiere una copia completa de un expediente tramitado por la Subdirección General de Inspección de Datos de la AEPD. La información solicitada tiene carácter confidencial y su divulgación puede suponer un problema de seguridad, por lo que se concede su acceso parcial con la anonimización de los datos de carácter personal. En este supuesto, no se observan barreras regulatorias por las funciones administrativas de control y auditoría.

En la Resolución sobre solicitud de acceso a la información pública de 7 de noviembre de 2024[47], por la que se solicita la copia de un expediente tramitado y resuelto por la Subdirección General de Inspección de Datos de la AEPD, se deniega el acceso con base en el art. 14.1 f) de la Ley 19/2013. Respecto del test del daño, se aprecia un eventual perjuicio porque la resolución se ha recurrido ante el orden jurisdiccional contencioso-administrativo, a la vez que no se identifica ningún interés público o privado que legitime la divulgación. En este caso, no se observa ninguna barrera regulatoria, habida cuenta de la salvaguardia de las funciones de control y auditoría de la Administración.

En la Resolución sobre solicitud de acceso a la información pública de 29 de noviembre de 2024[48], se deniega el derecho de acceso en virtud del art. 14.1 f), h) y k) de la Ley 19/2013, por el que se solicita la copia de un expediente sancionador de la Subdirección General de Inspección de Datos de la AEPD. No se supera el test del daño porque la resolución se ha recurrido ante la jurisdicción contencioso-administrativa, en la que el tercero que solicita los datos está investigado. Asimismo, la AEPD indica que la divulgación de la información contenida en el expediente perjudicaría el derecho a la confidencialidad y los intereses económicos y comerciales. En este supuesto, no se observan barreras regulatorias, en atención a la garantía de la actividad de control y auditoría de la Administración.

En la Resolución sobre solicitud de acceso a la información pública de 20 de diciembre de 2024[49], se autoriza parcialmente el derecho de acceso a la información con base en el art. 14.1 e) y g) de la Ley 19/2013. Sobre este asunto, se deniega el derecho de acceso a la información obrante en la AEPD porque su difusión afectaría a las funciones administrativas de control. No obstante, se facilita el enlace web a las resoluciones sancionadoras en el Portal de la AEPD. En este caso, no se observan barreras regulatorias, en atención a la preservación de las funciones de control y auditoría de la Administración, así como el acceso a las resoluciones sancionadoras se contiene en formato electrónico accesible.

Por último, en la Resolución sobre solicitud de acceso a la información pública de 14 de marzo de 2025[50], se deniega el derecho de acceso en virtud del art. 14.1 e), g) y h) de la Ley 19/2013. Los fundamentos son que la difusión de la información puede perjudicar las funciones administrativas de control encomendadas a la AEPD, a la vez que dicho acceso podría perjudicar los intereses económicos

y comerciales. No se observan barreras regulatorias en este caso, en atención a la salvaguardia de las funciones de control y auditoría de la Administración.

IV. CONCLUSIONES

I. Tras las observaciones contenidas sobre las barreras regulatorias en el primer Estudio para la Comisión Europea *"Cross-border data flow in the digital single market: study on data location restrictions"* (EUROPEAN COMMISSION, 2017), no se ha producido ninguna adaptación normativa en los límites del derecho de acceso a la información pública, o requisitos de localización de datos, contenidos en el art. 14 de la Ley 19/2013. Asimismo, los límites contenidos en los cuatro primeros apartados del art. 14.1 de la Ley 19/2013 no se han aplicado nunca en las Resoluciones de Transparencia obrantes en la AEPD, a saber: la seguridad nacional, la defensa, la seguridad pública, la política económica y monetaria, y la protección del medio ambiente. Las Resoluciones de Transparencia de la AEPD están motivadas, y la denegación o concesión parcial del derecho de acceso guarda una relación directa con los límites al derecho de acceso a la información pública dispuestas en la Ley 19/2013. Como crítica común a todas las Resoluciones de Transparencia, se observa identidad literal en los fundamentos jurídicos de las Resoluciones que convendría adaptar al caso concreto.

II. Una vez examinadas las barreras regulatorias detectadas en las Resoluciones de Transparencia, cabe constatar la identificación –y, en ocasiones, reiteración– de las siguientes barreras regulatorias indirectas, pues las barreras regulatorias directas debían ser derogadas por los Estados Miembros antes del 30 de mayo de 2021: el acceso a la información en papel, en formato pdf, o su almacenamiento en un USB, por requerir un almacenamiento local o almacenamiento pasivo externo y por las dificultades de acceso para los proveedores extranjeros; y la prohibición de acceso a la información pública a un tercero con base en la confidencialidad, cuando su finalidad difiera de la garantía de las funciones de control y auditoría de la Administración, en atención a los perjuicios que supone para los proveedores extranjeros, así como que prohíbe el almacenamiento pasivo externo. Cabe destacar que, en uno de los supuestos de denegación del derecho de acceso a la información pública, su finalidad era científica y no se perjudicaba ninguna función administrativa de control o auditoría que legitimase la denegación. En este sentido, se ha subvenido correctamente en diversas Resoluciones la barrera regulatoria consistente en que las funciones de control y auditoría de la Administración no se pueden obstaculizar. Finalmente, se observa una progresiva mejora en la facilitación de la documentación no afectada por los límites del derecho de acceso a la información pública en formato electrónico accesible en el Portal de la AEPD.

V. ÍNDICE DE LAS RESOLUCIONES CITADAS

Resoluciones de Transparencia de la Agencia Española de Protección de Datos[51].

- Resolución sobre solicitud de acceso a la información pública de 25 de noviembre de 2020, Ref. 001-048144.
- Resolución sobre solicitud de acceso a la información pública de 2 de febrero de 2021, Ref. 001-049977.
- Resolución sobre solicitud de acceso a la información pública de 19 de mayo de 2021, Ref. 001-056314.
- Resolución sobre solicitud de acceso a la información pública de 1 de junio de 2021, Ref. 001-056662.
- Resolución sobre solicitud de acceso a la información pública de 12 de enero de 2022, Ref. 001-062916.
- Resolución sobre solicitud de acceso a la información pública de 21 de enero de 2022, Ref. 001-064051.
- Resolución sobre solicitud de acceso a la información pública de 26 de enero de 2022, Ref. 001-064296.
- Resolución sobre solicitud de acceso a la información pública de 10 de mayo de 2022, Ref. 001-067958.
- Resolución sobre solicitud de acceso a la información pública de 8 de junio de 2022, Ref. 001-068925.
- Resolución sobre solicitud de acceso a la información pública de 28 de junio de 2022, Ref. 001-068426.
- Resolución sobre solicitud de acceso a la información pública de 18 de julio de 2022, Ref. 001-069130.
- Resolución sobre solicitud de acceso a la información pública de 8 de agosto de 2022, Ref. 001-069515.
- Resolución sobre solicitud de acceso a la información pública de 10 de noviembre de 2022, Ref. 001-071793.
- Resolución sobre solicitud de acceso a la información pública de 28 de noviembre de 2022, Ref. 001-072647 y 001-072727.
- Resolución sobre solicitud de acceso a la información pública de 16 de enero de 2023, Ref. 001-073247.
- Resolución sobre solicitud de acceso a la información pública de 10 de marzo de 2023, Ref. 00001-00076802 y 00001-00076685.
- Resolución sobre solicitud de acceso a la información pública de 28 de noviembre de 2023, Ref. 00001-00083538.
- Resolución sobre solicitud de acceso a la información pública de 20 de diciembre de 2023, Ref. 00001-00084193.

- Resolución sobre solicitud de acceso a la información pública de 16 de febrero de 2024, Ref. 00001-00086732.
- Resolución sobre solicitud de acceso a la información pública de 10 de abril de 2024, Ref. 00001-00085828.
- Resolución sobre solicitud de acceso a la información pública de 10 de junio de 2024, Ref. 00001-00087344.
- Resolución sobre solicitud de acceso a la información pública de 12 de julio de 2024, Ref. 001-091026.
- Resolución sobre solicitud de acceso a la información pública de 21 de agosto de 2024, Ref. 001-093139.
- Resolución sobre solicitud de acceso a la información pública de 7 de octubre de 2024, Ref. 00001-00094728.
- Resolución sobre solicitud de acceso a la información pública de 23 de octubre de 2024, Ref. 00001-00096610.
- Resolución sobre solicitud de acceso a la información pública de 23 de octubre de 2024, Ref. 00001-00095175.
- Resolución sobre solicitud de acceso a la información pública de 30 de octubre de 2024, Ref. 00001-00094816.
- Resolución sobre solicitud de acceso a la información pública de 7 de noviembre de 2024, Ref. 00001-00095559.
- Resolución sobre solicitud de acceso a la información pública de 29 de noviembre de 2024, Ref. 00001-00096494.
- Resolución sobre solicitud de acceso a la información pública de 20 de diciembre de 2024, Ref. 00001-00099010.
- Resolución sobre solicitud de acceso a la información pública de 14 de marzo de 2025, Ref. 00001-00101343.

Jurisprudencia.

- STJUE de 4 de octubre de 2024, ECLI:EU:C:2024:834.

VI. BIBLIOGRAFÍA

AEPD. (2025). *Resoluciones de Transparencia de la Agencia Española de Protección de Datos,* [En línea], disponible en https://www.aepd.es/la-agencia/transparencia/resoluciones-de-transparencia.

ARGELICH COMELLES, C. (2023). "Sucesión testamentaria en *blockchain* y herencia de activos digitales en el Metaverso: del Derecho español e italiano al *soft law* del ELI y UNIDROIT", *Diritto Delle Successioni E Della Famiglia,* 3, pp. 1135-1170.

ARGELICH COMELLES, C. (2024). "De los *ALI-ELI Principles for a data economy* a la *Data Governance Act* y la *Data Act:* datos, derechos y activos", *Actualidad Civil,* 11, pp. 1-23.

DE BARRÓN ARNICHES, P. (2024). "Vulneraciones automatizadas del derecho a la protección de datos personales y mecanismos de tutela", *Revista de Derecho Civil,* 1, [En línea], disponible en https://nreg.es/ojs/index.php/RDC/article/view/918, pp. 149-194.

CÁMARA LAPUENTE, S. (2020). "Resolución contractual y destino de los datos y contenidos generados por los usuarios de servicios digitales". En: E. Arroyo Amayuelas, S. Cámara Lapuente (dirs.), *El derecho privado en el nuevo paradigma digital,* Madrid, Marcial Pons, pp. 141-175.

CAROVANO, G., FINCK, M. (2023). "Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy", *Computer Law and Security Review,* 50, pp. 1-18.

CASTRO CARRANZA, J. (2022). "El Reglamento *Data Governance Act:* un paso adelante en la Estrategia Europea de Datos", *Derecho digital e innovación,* 12, pp. 1-15.

ECHEZARRETA FERRER, M. T. (2021). "Datos personales en materia de salud: interés, inmunización/tratamiento y defensa". En: E. Rodríguez Pineau, E. Torralba Mendiola (dirs.), *La protección de las transmisiones de datos transfronterizas,* Cizur Menor, Thomson Reuters Aranzadi, pp. 263-314.

EUROPEAN COMMISSION. (2017). *Cross-border data flow in the digital single market: study on data location restrictions,* [En línea], disponible en https://data.europa.eu/doi/10.2759/92602.

FERNÁNDEZ HERNÁNDEZ, C. (2022). "Estructura y contenido del Reglamento (UE) 2022/868, de 30 de mayo, relativo a la gobernanza europea de datos o Reglamento de Gobernanza de Datos", *Derecho digital e innovación,* 12, pp. 1-10.

GERST, C., GEYKEN, S., AHMED, R. (2023). „Die Bereitstellung von Daten aus klinischen Prüfungen", *Medizinrecht,* 41, pp. 204-210.

LIPPI, M. E. (2022). "Data rights and control over personal data on digital platforms". En: E. Bargelli, V. Calderai, (eds.), *A Contract Law for the Age of Digital Platforms?,* Pisa, Pacini, pp. 49-68.

MAHANTI, R. (2021). *Data Governance and Compliance. Evolving to Our Current High Stakes Environment,* Singapore, Springer, pp. 53-64.

MARTÍNEZ MARTÍNEZ, R. (2021). "Data Governance Act. La construcción de un espacio europeo del dato", *La Ley privacidad,* 9, pp. 1-18.

MARTINI, M. (2020). "Regulating Algorithms. How to Demystify the Alchemy of Code". En: S. Navas, M. Ebers (eds.), *Algorithms and Law,* Cambridge, Cambridge University Press, pp. 114-119.

MORALEJO IMBERNÓN, N. (2020). "El testamento digital en la nueva Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *Anuario de Derecho Civil,* Tomo LXXIII, fasc. I, pp. 241-281.

OTERO CRESPO, M. (2019). "La sucesión en los «bienes digitales». La respuesta plurilegislativa española", *Revista de Derecho Civil,* vol. VI, 4, pp. 89-133.

PALOMAR OLMEDA, A. (2017). "El marco jurídico de los datos personales en el ámbito de la Administración de Justicia: cesiones, usos compartidos, intercambio de datos". En: S. Oubiña Barbolla, M. A. Catalina Benavente (coords.), I. Colomer Hernández (dir.), *Cesión de datos personales y evidencias entre procesos penales y*

procedimientos administrativos sancionadores o tributarios, Cizur Menor, Thomson Reuters Aranzadi, pp. 435-488.

PATTI, F. P., BARTOLINI, F. (2019). "Digital Inheritance and *Post Mortem* Data Protection: The Italian Reform", *Bocconi Legal Studies Research Paper Series,* 3397974, [En línea], disponible en https://ssrn.com/abstract=3397974, pp. 1-11.

REBOLLO DELGADO, L. (2017). "Estudio de los límites en la Ley de Transparencia, acceso a la información pública y buen gobierno". En: A. Troncoso Reigada (dir.), *Comentario a la ley de transparencia, acceso a la información pública y buen gobierno,* Madrid, Civitas, pp. 767-801.

RUOHONEN, J., MICKELSSON, S. (2023). "Reflections on the Data Governance Act", *Digital Society,* vol. 2, 10, pp. 1-9.

SANTOS MORÓN, M. J. (2018). "La denominada "herencia digital": ¿necesidad de regulación? Estudio de Derecho español y comparado", *Cuadernos de Derecho Transnacional,* vol. 10, 1, pp. 413-438.

SPIECKER, I., DÖHMANN, G. (2022). "AI and Data Protection". En: L. Dimatteo, M. Cannarsa, C. Poncibò (eds.), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics,* Cambridge, Cambridge University Press, pp. 132-145.

DE TORRES PEREA, J. M. (2025). "La patrimonialización de datos ante la contaminación digital. Una perspectiva civil ante un reto a nuestro sistema", *Revista de Derecho Civil,* vol. XII, 1, [En línea], disponible en https://www.nreg.es/ojs/index.php/RDC/article/view/1035, pp. 279-329.

NOTAS

[1] Autora individual del informe español para la Comisión Europea sobre los requisitos de localización de datos, bajo el Estudio *"Supporting the evaluation of the Free Flow of Non-Personal Data Regulation, Open Data Directive and Data Governance Act"*. Este trabajo es resultado de una estancia de investigación realizada en el *Max Planck Institute for Comparative and International Private Law* de 1 de marzo a 31 de mayo de 2025 y un *Erasmus+ Teaching Mobility* en la *Universität Hamburg*. Sitio web profesional: https://sites.google.com/view/cristinaargelich/.

[2] DOUE de 28 de noviembre de 2018.

[3] Véase *infra* apartado III.2.

[4] BOE de 10 de diciembre de 2013.

[5] DOUE de 4 de mayo de 2016.

[6] Véase *infra* apartado III.2.

[7] EUROPEAN COMMISSION. (2017). *Cross-border data flow in the digital single market: study on data location restrictions,* [En línea], disponible en https://data.europa.eu/doi/10.2759/92602, pp. 74-75: "for example, our interviewee at a Spanish financial institution mentioned that national financial regulations limit the free flow of data across the EU, which is amplified by the fact that these rules differ from one EU Member State to another. In Spain, banks (so no other financial organisations such as Fintechs) have to notify the national Financial Supervisory Authority each time they want to outsource a service (including a cloud service). In practice, this authorisation process can significantly increase time to market. Thus "bringing agility to this procedure and having harmonisation across EU member States is fundamental for banks to be competitive in the Digital Single Market." In Spain, other non-legal barriers identified are related to a lack of a digital cloud culture or a lack of a data-driven culture, which can be translated in uncertainty in using new technologies such as cloud computing services. Our interviewee in Spain declared "at the moment we use cloud computing for non-core business activities such as google apps and collaborative tools for employees; however, the bank would like to develop the use of cloud computing also to the core business (e.g. financial data, client data) in the near future".

[8] ECLI:EU:C:2024:834.

[9] DOUE de 26 de junio de 2019.

[10] DOUE de 3 de junio de 2022.

[11] Véase *supra* apartado I.

[12] DOUE de 22 de diciembre de 2023.

[13] Véase *infra* apartado III.2.

[14] Véase *infra* apartado III.2.

[15] Véase *infra* apartado III.2.

[16] Véase *supra* apartado II.1.

[17] Véase *infra* apartado III.2.

[18] Véase *supra* apartado III.1.

[19] Ref. 001-048144.

[20] Ref. 001-068426.

[21] Ref. 00001-00085828.

[22] Ref. 00001-00094816.

[23] Ref. 001-049977.

[24] Ref. 001-056314.

[25] Ref. 001-056662.
[26] Ref. 001-062916.
[27] Ref. 001-064051.
[28] Ref. 001-064296.
[29] Ref. 001-067958.
[30] Ref. 001-068925.
[31] Ref. 001-069130.
[32] Ref. 001-069515.
[33] Ref. 001-071793.
[34] Ref. 001-072647 y 001-072727.
[35] Ref. 001-073247.
[36] Ref. 00001-00076802 y 00001-00076685.
[37] Ref. 00001-00083538.
[38] Ref. 00001-00084193.
[39] Ref. 00001-00086732.
[40] BOE de 21 de enero de 2023.
[41] Ref. 00001-00087344.
[42] Ref. 001-091026.
[43] Ref. 001-093139.
[44] Ref. 00001-00094728.
[45] Ref. 00001-00096610.
[46] Ref. 00001-00095175.
[47] Ref. 00001-00095559.
[48] Ref. 00001-00096494.
[49] Ref. 00001-00099010.
[50] Ref. 00001-00101343.
[51] AEPD. (2025). *Resoluciones de Transparencia de la Agencia Española de Protección de Datos,* [En línea], disponible en https://www.aepd.es/la-agencia/transparencia/resoluciones-de-transparencia.