

## I. DISPOSICIONES GENERALES

### JEFATURA DEL ESTADO

**15790** *Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.*

I

La sociedad actual requiere de adaptaciones en la esfera digital que exigen de una traducción en el plano normativo. El desarrollo y empleo de las nuevas tecnologías y redes de comunicaciones por parte de las Administraciones Públicas se está acelerando. Ello exige establecer sin demora un marco jurídico que garantice el interés general y, en particular, la seguridad pública, asegurando la adecuada prestación de los servicios públicos y, al mismo tiempo, que la administración digital se emplee para fines legítimos que no comprometan los derechos y libertades de los ciudadanos.

El carácter estratégico para la seguridad pública de las materias reguladas en este real decreto-ley se ve avalado por la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que describe los riesgos asociados a las nuevas tecnologías como uno de los principales desafíos de la sociedad actual.

La Estrategia de Seguridad Nacional 2017, aprobada mediante Real Decreto 1008/2017, de 1 de diciembre, identifica las ciberamenazas y el espionaje como amenazas que comprometen o socavan la seguridad nacional y, en coherencia con ello, singulariza la ciberseguridad como uno de sus ámbitos prioritarios de actuación. El desarrollo tecnológico implica una mayor exposición a nuevas amenazas, especialmente las asociadas al ciberespacio, tales como el robo de datos e información, el *hackeo* de dispositivos móviles y sistemas industriales, o los ciberataques contra infraestructuras críticas. La hiperconectividad actual agudiza algunas de las vulnerabilidades de la seguridad pública y exige una mejor protección de redes y sistemas, así como de la privacidad y los derechos digitales del ciudadano.

Entre los principales desafíos que las nuevas tecnologías plantean desde el punto de vista de la seguridad pública se encuentran las actividades de desinformación, las interferencias en los procesos de participación política de la ciudadanía y el espionaje. Estas actividades se benefician de las posibilidades que ofrece la sofisticación informática para acceder a ingentes volúmenes de información y datos sensibles.

En este punto juega un papel decisivo el proceso de transformación digital de la Administración, ya muy avanzado. La administración electrónica agudiza la dependencia de las tecnologías de la información y extiende la posible superficie de ataque, incrementando el riesgo de utilización del ciberespacio para la realización de actividades ilícitas que impactan en la seguridad pública y en la propia privacidad de los ciudadanos.

Los recientes y graves acontecimientos acaecidos en parte del territorio español han puesto de relieve la necesidad de modificar el marco legislativo vigente para hacer frente a la situación. Tales hechos demandan una respuesta inmediata para evitar que se reproduzcan sucesos de esta índole estableciendo un marco preventivo a tal fin, cuyo objetivo último sea proteger los derechos y libertades constitucionalmente reconocidos y garantizar la seguridad pública de todos los ciudadanos.

El presente real decreto-ley tiene por objeto regular este marco normativo, que comprende medidas urgentes relativas a la documentación nacional de identidad; a la identificación electrónica ante las Administraciones Públicas; a los datos que obran en poder de las Administraciones Públicas; a la contratación pública y al sector de las telecomunicaciones.

## II

El presente real decreto-ley consta de una parte expositiva y una parte dispositiva estructurada del modo siguiente: capítulo I (artículos 1 y 2), un capítulo II (artículos 3 y 4), un capítulo III (artículo 5), un capítulo IV (artículo 6), un capítulo V (artículo 7), una disposición adicional, tres disposiciones transitorias y tres disposiciones finales.

El capítulo I contempla dos medidas en materia de documentación nacional de identidad, dirigidas a configurar el Documento Nacional de Identidad, con carácter exclusivo y excluyente, como el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular. Con esta finalidad, el artículo 1 del presente real decreto-ley modifica el artículo 8.1 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. En coherencia con ello, el artículo 2 del real decreto-ley modifica la regulación del Documento Nacional de Identidad electrónico recogida en el artículo 15.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

El capítulo II del presente real decreto-ley, que contiene los artículos 3 y 4, establece varias medidas en materia de identificación electrónica ante las Administraciones Públicas, ubicación de determinadas bases de datos y datos cedidos a otras Administraciones Públicas. La finalidad de estas medidas es garantizar la seguridad pública, tanto en las relaciones entre las distintas Administraciones Públicas cuando traten datos personales, como entre ciudadanos y Administraciones Públicas cuando las últimas proceden a la recopilación, tratamiento y almacenamiento de datos personales en ejercicio de una función pública.

El artículo 3 del presente real decreto-ley modifica los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, a la vez que introduce una nueva disposición adicional sexta a la misma.

La modificación de la letra a) del apartado 2 de los artículos 9 y 10 responde a la necesidad de adaptar sus contenidos al 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 el que se deroga la Directiva 1999/93/CE, conocido como Reglamento eIDAS, que establece un marco legal común para las identificaciones y firmas electrónicas en la Unión Europea.

La modificación de la letra c) del apartado 2 de los artículos 9 y 10 tiene como finalidad garantizar la seguridad pública en relación con el empleo de sistemas de identificación y firma electrónicas de los interesados cuando se realizan con clave concertada o mediante cualquier otro sistema que cuente con un registro previo como usuario que permita garantizar su identidad y que las Administraciones Públicas consideren válido. Así, en palabras del propio Tribunal Constitucional expresadas en la Sentencia 55/2018, de 24 de mayo, se mantiene la posibilidad de que «cada administración diseñe sus propios sistemas de identificación electrónica o admita los expedidos por otras entidades públicas o privadas y, con ello, que estos sean más o menos complejos según sus preferencias y la relevancia o características del trámite o servicio correspondiente». Ahora bien, para garantizar la seguridad pública, competencia exclusiva del Estado conforme dispone el artículo 1.1 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, la modificación efectuada somete a un régimen de autorización previa por parte de la Administración General del Estado a los sistemas que sean distintos a aquellos del certificado y sello electrónico. Dicha autorización tendrá por objeto, exclusivamente, verificar si el sistema validado tecnológicamente por parte de la Administración u Organismo Público de que se trate puede o no producir afecciones o riesgos a la seguridad pública, de modo que, si así fuera y solo en este caso, la Administración del Estado denegará dicha autorización con base en dichas consideraciones de seguridad pública.

En la misma línea, el nuevo apartado 3, que se añade tanto al artículo 9 como al artículo 10 de la Ley 39/2015, de 1 de octubre, establece la obligatoriedad de que, en relación con los sistemas previstos en la letra c) del apartado 2 de los artículos 9 y 10, los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de

dichos sistemas se encuentren situados en territorio de la Unión Europea, y en territorio español en caso de que se trate de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 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. Salvo las excepciones que se introducen en la ley, estos datos no podrán ser objeto de transferencia a un tercer país u organización internacional y, en cualquier caso, se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Por último, el artículo 3 del presente real decreto-ley incorpora una disposición adicional sexta a la Ley 39/2015, de 1 de octubre, que prevé que en las relaciones de los interesados con las Administraciones Públicas no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificaciones basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea. Además, la nueva disposición adicional sexta establece que cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal deberá contemplar que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública.

Las restricciones impuestas a los sistemas de identificaciones y firmas basados en tecnologías de registro distribuido en ningún caso suponen una prohibición general. Simplemente, se restringe puntualmente y de forma meramente provisional su uso como sistema de identificación y firma de los interesados cuando estos últimos se interrelacionan con la Administración y mientras no haya más datos o un marco regulatorio *ad hoc* de carácter estatal o europeo que haga frente a las debilidades que implica su uso para los datos y la seguridad pública. La falta de un marco regulatorio *ad hoc* sobre estas nuevas tecnologías justifica que, con carácter urgente y en ejercicio de su competencia para dictar legislación básica, el Estado intervenga sobre la materia con carácter provisional hasta que se avance en el seno de la Unión Europea en el tratamiento de este tipo de tecnologías.

El artículo 4 del presente real decreto-ley procede, por una parte, a la modificación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público introduciendo un nuevo artículo 46 bis, y dando una nueva redacción al artículo 155.

Por una parte, el artículo 46 bis obliga a que, por motivos de seguridad pública, los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión del censo electoral, los padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de los usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, se ubiquen y presten dentro del territorio de la Unión Europea. Asimismo, establece que solo puedan ser cedidos a terceros países cuando estos cumplan con las garantías suficientes que les permitan haber sido objeto de una decisión de adecuación de la Comisión Europea, o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

Por otra parte, la finalidad de la modificación del artículo 155 es permitir un mayor control de los datos cedidos entre Administraciones Públicas, al efecto de garantizar la adecuada utilización de los mismos. Se permite excepcionalmente que la Administración General del Estado pueda adoptar la medida de suspender la transmisión de datos por razones de seguridad nacional de forma cautelar por el tiempo estrictamente indispensable para su preservación.

La licitud del tratamiento de los datos personales para finalidades distintas de las finalidades iniciales viene determinada por la circunstancia de que se trate de finalidades compatibles. Tratándose de finalidades incompatibles, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, prohíbe su tratamiento. No obstante, el propio Reglamento declara ya unas finalidades que estima compatibles: tratamiento ulterior de los datos personales con fines de archivo en interés público, fines

El Documento Nacional de Identidad es un documento público y oficial y tendrá la protección que a estos otorgan las leyes. Es el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular.»

Artículo 2. *Modificación de la Ley 59/2003, de 19 de diciembre, de firma electrónica.*

Se modifica el apartado 1 del artículo 15 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, en los siguientes términos:

«1. El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular, en los términos establecidos en el artículo 8 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, y permite la firma electrónica de documentos.»

## CAPÍTULO II

### **Medidas en materia de identificación electrónica ante las Administraciones Públicas, ubicación de determinadas bases de datos y datos cedidos a otras Administraciones Públicas**

Artículo 3. *Modificación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.*

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas queda modificada en los siguientes términos:

Uno. Se modifica el apartado 2 del artículo 9, que queda con el siguiente contenido y se añade un nuevo apartado 3, renumerando el apartado 3 que pasa a ser el apartado 4:

«2. Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas siguientes:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la “Lista de confianza de prestadores de servicios de certificación”.

b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la “Lista de confianza de prestadores de servicios de certificación”.

c) Sistemas de clave concertada y cualquier otro sistema, que las Administraciones consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todo procedimiento, aun cuando se admita para ese mismo procedimiento alguno de los previstos en la letra c).

3. En relación con los sistemas de identificación previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del

Reglamento (UE) 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, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

4. En todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo.»

Dos. Se modifica el apartado 2 del artículo 10, que queda con el siguiente contenido, y se añade un nuevo apartado 3, renumerando los apartados 3 y 4 que pasan a ser 4 y 5:

«2. En el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la “Lista de confianza de prestadores de servicios de certificación”.

b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico expedidos por prestador incluido en la “Lista de confianza de prestadores de servicios de certificación”.

c) Cualquier otro sistema que las Administraciones Públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todos los procedimientos en todos sus trámites, aun cuando adicionalmente se permita alguno de los previstos al amparo de lo dispuesto en la letra c).

3. En relación con los sistemas de firma previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

4. Cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

5. Cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma.»

Tres. Se añade una nueva disposición adicional sexta, con la siguiente redacción:

«Disposición adicional sexta. *Sistemas de identificación y firma previstos en los artículos 9.2 c) y 10.2 c).*

1. No obstante lo dispuesto en los artículos 9.2 c) y 10.2 c) de la presente Ley, en las relaciones de los interesados con los sujetos sometidos al ámbito de aplicación de esta Ley, no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificación basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea.

2. En todo caso, cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal a que hace referencia el apartado anterior deberá contemplar asimismo que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública.»

Artículo 4. *Modificación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.*

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público queda modificada en los siguientes términos:

Uno. Se introduce un nuevo artículo 46 bis, que queda redactado como sigue:

«Artículo 46 bis. *Ubicación de los sistemas de información y comunicaciones para el registro de datos.*

Los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión del censo electoral, los padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de los usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, deberán ubicarse y prestarse dentro del territorio de la Unión Europea.

Los datos a que se refiere el apartado anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.»

Dos. Se da nueva redacción al artículo 155, que queda redactado como sigue:

«Artículo 155. *Transmisiones de datos entre Administraciones Públicas.*

1. De conformidad con lo dispuesto en el Reglamento (UE) 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 y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y

Disposición transitoria primera. *Régimen transitorio de las modificaciones introducidas en el artículo 3.*

1. Las entidades del Sector Público que quieran habilitar sistemas de identificación o firma conforme a las letras c) de los artículos 9.2 y 10.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, a partir de la entrada en vigor de este real decreto-ley, deberán solicitar la autorización prevista en dichos preceptos. Los sistemas que, antes de la citada entrada en vigor, ya estén validados y plenamente operativos en los procedimientos administrativos de que se trate, no requerirán someterse a dicha autorización.

2. Las entidades pertenecientes al Sector Público deberán adoptar las medidas necesarias para cumplir la obligación prevista en los artículos 9.3 y 10.3 de la Ley 39/2015, de 1 de octubre, en el plazo máximo de seis meses a partir de la entrada en vigor de este real decreto-ley cuando gestionen directamente o a través de medios propios los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de los sistemas de identificación y firma.

3. En el caso de que la gestión de los recursos citados en el apartado anterior se lleve a cabo mediante la licitación de contratos del Sector Público, directamente por los sujetos a los que es de aplicación la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público o por sus medios propios, la obligación de adaptarse a lo preceptuado en estos artículos no se aplicará a los expedientes de contratación iniciados antes de la entrada en vigor de este real decreto-ley, que se regirán por la normativa anterior. Los contratos adjudicados en virtud de dichos expedientes, aun cuando mantendrán su plena validez y eficacia, no podrán ser objeto de modificación que vulnere lo establecido en los citados preceptos. Tampoco podrán ser objeto de prórroga salvo que previamente sean objeto de modificación para adaptarse a las disposiciones que en ellos se contienen, siempre y cuando ello sea posible conforme a la Ley 9/2017, de 8 de noviembre.

4. A los efectos de lo dispuesto en esta disposición transitoria se entenderá que los expedientes de contratación han sido iniciados si se hubiera publicado la correspondiente convocatoria del procedimiento de adjudicación del contrato. En el caso de procedimientos negociados sin publicidad, para determinar el momento de iniciación se tomará en cuenta la fecha de aprobación de los pliegos.

5. En el plazo de tres meses desde la entrada en vigor de este real decreto-ley, las distintas Administraciones Públicas remitirán a la Comisión Sectorial de Administración Electrónica la información sobre todos los contratos vigentes que tengan por objeto los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de los sistemas de identificación y firma, así como de aquellos cuyos expedientes ya estén iniciados conforme al apartado anterior.

Disposición transitoria segunda. *Régimen transitorio de las modificaciones introducidas en el artículo 4.*

1. Las entidades pertenecientes al Sector Público deberán adoptar las medidas necesarias para cumplir la obligación prevista en el artículo 46 bis de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el plazo máximo de seis meses a partir de la entrada en vigor de este real decreto-ley cuando gestionen directamente o a través de medios propios los sistemas de información y comunicaciones a que dicho precepto se refiere.

2. En el caso de que la gestión de los sistemas citados en el apartado anterior se lleve a cabo mediante la licitación de contratos del Sector Público, directamente por los sujetos a los que es de aplicación la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público o por sus medios propios, la obligación de adaptarse a lo preceptuado en el artículo 46 bis de la Ley 40/2015, de 1 de octubre, no se aplicará a los expedientes de contratación iniciados antes de la entrada en vigor de este real decreto-ley, que se regirán por la normativa anterior.

Disposición final segunda. *Desarrollo reglamentario y ejecución.*

Se habilita al Gobierno y a las personas titulares de los departamentos ministeriales, en el ámbito de sus competencias, a dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo dispuesto en este real decreto-ley.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto-ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Dado en Madrid, el 31 de octubre de 2019.

FELIPE R.

El Presidente del Gobierno,  
PEDRO SÁNCHEZ PÉREZ-CASTEJÓN