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
[*BOE* n.º 266, de 5-XI-2019]

UN PASO MÁS HACIA LA CONFIGURACIÓN DE UNA REGULACIÓN EFECTIVA DEL CIBERESPACIO

Los procesos de digitalización y datificación de la sociedad a los que estamos asistiendo en nuestros días implican una sobreexposición a nuevas amenazas, especialmente las asociadas al ciberespacio, tales como el robo de datos personales 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.

Ante esta compleja tesitura, el Real Decreto-Ley 14/2019, de 31 de octubre, modifica el régimen jurídico de materias importantes tales como el documento nacional de identidad, la identificación electrónica ante las Administraciones Públicas, el almacenamiento de los datos personales que obran en poder de estas, la contratación pública o la regulación de las redes de telecomunicaciones. En el presente estudio se pretende realizar un análisis de los distintos artículos que configuran el Real Decreto-Ley, poniendo el acento en aquellas cuestiones que desde nuestro particular punto de vista suponen modificaciones legislativas de profundo calado para el ordenamiento jurídico español, huyendo con ello, intencionadamente, del manido debate acerca del cumplimiento o incumplimiento del presupuesto habilitante de extraordinaria y urgente necesidad, reflejado en la Constitución Española (artículo 86.1), cuestión que, por otra parte, ha sido analizada extensamente.

El Real Decreto-Ley objeto de estudio 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. De esta forma se elimina la posibilidad de que cualquier Administración Pública pretenda introducir un nuevo documento de acreditación de la identidad con el propósito de sustituir el DNIe, respuesta que no solo contribuye a fortalecer la seguridad jurídica, sino también a garantizar la interoperabilidad administrativa, y con ello la eficacia y la

Ars Iuris Salmanticensis,
vol. 8, Junio 2020, 217-223
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND

eficiencia de los procesos de implementación de la Administración electrónica. Con esta finalidad, el artículo 1 del citado Real Decreto-Ley modifica el artículo 8.1 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana y el artículo 15.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Mayor importancia revisten las medidas introducidas en el capítulo II de la norma objeto de estudio, las cuales establecen importantes modificaciones en materia de identificación electrónica ante las Administraciones Públicas —elemento clave para el ejercicio de derechos y el acceso a la prestación de servicios esenciales ante los poderes públicos—, la ubicación de determinadas bases de datos y en lo referente a la transmisión de datos personales entre las Administraciones Públicas. La finalidad de estas medidas no es otra que la de reforzar la seguridad pública, tanto en las relaciones entre las distintas Administraciones Públicas cuando traten datos personales, como entre ellas y los ciudadanos y Administraciones Públicas cuando proceden a la recopilación, tratamiento y almacenamiento de datos personales en el ejercicio de una función pública.

En este sentido, el artículo 3 del Real Decreto-Ley 14/2019 modifica los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), a la vez que introduce una nueva disposición adicional sexta a la misma.

Mientras que en la anterior redacción del artículo 9.2 de la ley citada se permitía esa identificación «a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad», ahora solamente se podrán emplear para acreditar la identidad digital los 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» y los 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». Con ello se pretende dar cumplimiento al artículo 22 del 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 elDAS, que establece un marco legal común para las identificaciones y firmas electrónicas en la Unión Europea. Según él, cada Estado miembro debe establecer, mantener y publicar listas de confianza con información relativa a los prestadores cualificados de servicios electrónicos de confianza, es decir, certificaciones electrónicas, firma y sellos electrónicos. De esta forma, el Ministerio de Energía, Turismo y Agenda Digital será el único competente para elaborar la Lista de Confianza que gozará de todas las presunciones legales de veracidad y legitimidad a nivel europeo.

Igualmente, el Real Decreto-Ley objeto de estudio introduce una serie de novedades relevantes en lo que se refiere a los sistemas de clave concertada contemplados en la letra c) del apartado 2 de los artículos 9 y 10 LPACAP, con la finalidad de garantizar

Ars Iuris Salmanticensis,
vol. 8, Junio 2020, 217-223
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND

la seguridad pública en relación con su empleo y validez. Esta medida está íntimamente relacionada con lo expuesto en el Capítulo I del Real Decreto-Ley objeto de estudio, ya que si bien es cierto que 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», de conformidad con lo establecido por el Tribunal Constitucional en su Sentencia 55/2018, de 24 de mayo, se 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 previamente mencionados. 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.

Adicionalmente, el Real Decreto-Ley incorpora un nuevo apartado 3, que se añade tanto al artículo 9 como al artículo 10 LPACAP, estableciendo la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de los sistemas de clave concertada se encuentren situados en territorio de la Unión Europea, y en territorio español en caso de que se trate de categorías especiales de datos personales 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. Con todo ello se pretende reforzar la denominada soberanía digital o, lo que es lo mismo, proteger los activos electrónicos valiosos y decisivos a la hora de asegurar un correcto funcionamiento de los Estados, los servicios esenciales y, en general, las sociedades actuales, mediante el establecimiento de dichos recursos técnicos en el ámbito territorial de la Unión Europea, bajo el paraguas regulatorio del Derecho comunitario, en el que destaca especialmente el *poderoso* Reglamento General de Protección de Datos (RGPD).

Con estas limitaciones, el Estado español pretende dar respuesta —y evitar— los intentos de construcción de una administración virtual paralela, problemática ya manifestada en Cataluña en 2017 con la denominada «Republica Digital», iniciativa cuya finalidad, lejos de mejorar los servicios públicos o ejecutar competencias propias del Estado autonómico, pretendía sustituir la legalidad estatal por otra legalidad ficticia, paralela y supuesta, cuya legitimidad no procedía del respeto al ordenamiento normativo y a la seguridad jurídica, sino más bien del vacío regulatorio y de la dificultad de aplicar el derecho en el ciberespacio al amparo de marcos normativos nacionales diversos o sencillamente inexistentes, como ocurre en los llamados paraísos digitales (MORET MILLÁS, 2020).

Por último, el artículo 3 de la norma objeto de estudio incorpora una disposición adicional sexta a la Ley 39/2015, de 1 de octubre, que prevé que en las relaciones de

Ars Iuris Salmanticensis,
vol. 8, Junio 2020, 217-223
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND

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 —blockchain— y los sistemas de firma basados en los mismos, en tanto en cuanto no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea.

Por su parte, el artículo 4 del Real Decreto-Ley 14/2019 procede, por una parte, a la modificación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP) introduciendo un nuevo artículo 46 bis, referente a la ubicación de los sistemas de información y comunicaciones para el registro de datos, al tiempo que aporta una nueva redacción al artículo 155 LRJSP.

Así, 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 en las actuaciones de transmisión de datos personales, introduciendo una serie de obligaciones que las Administraciones públicas deben respetar en todo caso al efecto de garantizar la adecuada utilización y protección de los datos de carácter personal. De esta forma, cada Administración pública deberá facilitar el acceso de las restantes a los datos de interesados especificando las condiciones, protocolos y criterios funcionales o técnicos con las máximas garantías de seguridad, integridad y disponibilidad. En este sentido, y en cumplimiento de un principio de lealtad institucional, se prohíbe el tratamiento ulterior de los datos personales para fines incompatibles con el fin para el cual se recogieron inicialmente los datos personales, salvo que dicho tratamiento ulterior se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, supuestos compatibles de conformidad con lo establecido en el artículo 5.1.b) RGPD. Fuera de estos supuestos cuando la Administración cesionaria de los datos pretenda el tratamiento ulterior de los mismos para una finalidad que estime compatible con el fin inicial, deberá comunicarlo previamente a la Administración cedente, la cual podrá oponerse.

El capítulo III del Real Decreto-Ley 14/2019 regula varias medidas en materia de contratación pública, todas ellas dirigidas a reforzar el cumplimiento de la normativa sobre protección de datos personales y la protección de la seguridad pública en este ámbito, consciente del ingente volumen de datos personales que los procedimientos de contratación pública generan.

Ars Iuris Salmanticensis,
vol. 8, Junio 2020, 217-223
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND

En este sentido, el Real Decreto-Ley modifica la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, con la finalidad de introducir medidas que garanticen en todas las fases de la contratación (expediente de contratación, licitación y ejecución del contrato) el respeto por parte de contratistas y subcontratistas de la legislación de la Unión Europea en materia de protección de datos.

Así, en primer lugar, la norma objeto de estudio modifica el artículo 35 de la Ley 9/2017, de 8 de noviembre, para incluir, como contenido mínimo de los contratos, la referencia expresa al sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos de carácter personal.

En segundo lugar, y por lo que respecta al régimen de invalidez de los contratos, se añade un subapartado al artículo 39.2 LCSP para incluir, como causa de nulidad de pleno derecho, la celebración de contratos por parte de poderes adjudicadores que omitan mencionar en los pliegos las obligaciones del futuro contratista en materia de protección de datos personales, la ubicación de los servidores en los que se alojarán los datos que ceda la Administración con motivo de la ejecución de un contrato público o desde dónde se van a prestar los servicios asociados a los mismos.

En tercer lugar, y en el contexto de la regulación de los requisitos para contratar con el sector público, se modifica el artículo 116.1 LCSP, para incluir, como circunstancia que impedirá a los empresarios contratar con las entidades del Sector público, el haber dado lugar a la resolución firme de cualquier contrato celebrado con una de tales entidades por incumplimiento de las especificaciones de protección de datos en otros contratos públicos anteriores debido a infracción grave, concurriendo dolo, culpa o negligencia.

En cuarto lugar, se da una nueva redacción al artículo 116.1 LCSP, introduciendo un segundo párrafo relativo al expediente de contratación cuya ejecución requiera de la cesión de datos por parte de entidades del sector público al contratista. En virtud de esta modificación, se incluye la obligación del órgano de contratación de especificar en el expediente cuál será la finalidad de los datos que vayan a ser cedidos.

En quinto lugar, se otorga una nueva redacción al artículo 122.2 LCSP, relativo a los pliegos de cláusulas administrativas particulares. En concreto, se añade un párrafo tercero a este apartado para incluir la obligación de los pliegos de mencionar expresamente la obligación del futuro contratista de respetar la normativa vigente en materia de protección de datos. Asimismo, se añade un párrafo cuarto relativo a los contratos que exijan el tratamiento por el contratista de datos personales por parte del responsable del tratamiento, indicando que en estos casos será obligatorio hacer constar en el pliego tanto la finalidad de la cesión de datos como la obligación de la empresa adjudicataria de mantener al contratante al corriente de la ubicación de los correspondientes servidores. También se añade un párrafo quinto para establecer que los extremos mencionados en el párrafo cuarto deben hacerse constar en los pliegos como obligaciones esenciales a los efectos del régimen de resolución del contrato.

Ars Iuris Salmanticensis,
vol. 8, Junio 2020, 217-223
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND

En sexto lugar, el Real Decreto-Ley da una nueva redacción al artículo 202.1 LCSP, regulador de las condiciones especiales de ejecución del contrato de carácter social, ético, medioambiental —manifestación primordial de la contratación estratégica—. En concreto, se introduce un párrafo tercero relativo a los pliegos correspondientes a contratos cuya ejecución implique la cesión de datos por las entidades del sector público al contratista. Mediante esta adición se impone la exigencia de que los pliegos incluyan, como condición especial de ejecución, la obligación del contratista de someterse a la normativa nacional y de la Unión Europea en materia de protección de datos. Asimismo, en los pliegos debe advertirse al contratista de que esta obligación tiene el carácter de obligación contractual esencial a los efectos del régimen de resolución del contrato.

Finalmente, el artículo 5 de la norma objeto de estudio proporciona una nueva redacción al artículo 215.4 LCSP, relativo a la subcontratación, para incluir, entre las obligaciones del contratista principal, la de asumir la total responsabilidad de la ejecución del contrato frente a la Administración también por lo que respecta a la obligación de sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos de carácter personal.

El capítulo IV del Real Decreto-Ley 14/2019 se destina a regular diferentes medidas para reforzar la seguridad en materia de telecomunicaciones. Así, el artículo 6 de esta norma acomete cinco modificaciones de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, con el objetivo de potenciar las facultades atribuidas al Gobierno, a través del Ministerio de Economía y Empresa, para afrontar la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicas en determinados supuestos excepcionales que puedan afectar al orden público, la seguridad pública o la seguridad nacional

Así, en concreto, se modifican los artículos 4.6 y 6.3 de la Ley 9/2014, de 9 de mayo, para reforzar las potestades del Ministerio de Economía y Empresa para llevar a cabo un mayor control y para mejorar sus posibilidades de actuación cuando la comisión de una presunta actuación infractora a través del uso de las redes y servicios de comunicaciones electrónicas pueda suponer una amenaza grave e inmediata para el orden público, la seguridad pública o la seguridad nacional o cuando en determinados supuestos excepcionales que también puedan comprometer el orden público, la seguridad pública y la seguridad nacional sea necesaria la asunción de la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicas.

Estas mayores posibilidades de actuación que se reconocen no se limitan en su aplicación a un concepto estricto de una red o un servicio de comunicaciones electrónicas, sino que extienden su eficacia a los elementos que necesariamente acompañan a la instalación o despliegue de una red o la prestación de un servicio de comunicaciones electrónicas, como son las infraestructuras susceptibles de alojar redes públicas de comunicaciones electrónicas, sus recursos asociados o cualquier elemento o nivel de la red o del servicio que resulte necesario para preservar o restablecer el orden público, la seguridad pública y la seguridad nacional.

Ars Iuris Salmanticensis,
vol. 8, Junio 2020, 217-223
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND

En necesaria correlación con este reforzamiento de funciones públicas en estas situaciones excepcionales, se potencia igualmente la potestad sancionadora del Ministerio de Economía y Empresa con el objetivo de hacer efectivas y reales las actuaciones que pueda adoptar en uso de estas nuevas facultades de actuación dirigidas a preservar o restablecer el orden público, la seguridad pública y la seguridad nacional. Con esta finalidad, el presente real decreto-ley da una nueva redacción a los artículos 76.15, 77.28 y 81.1 de la Ley 9/2014, de 9 de mayo. En particular, se amplían los supuestos en los que el Ministerio de Economía y Empresa puede adoptar medidas cautelares en casos de razones de imperiosa urgencia sin audiencia previa del presunto infractor, que puede incluir el cese de la actividad o la prestación de servicios, incorporando al efecto algunos de los supuestos que contemplados con dicha finalidad figuran en el artículo 30.6 del Código Europeo de las Comunicaciones Electrónicas, aprobado por la Directiva 2018/1972, de 11 de diciembre de 2018, del Parlamento Europeo y del Consejo, en especial, los relativos a la existencia de una amenaza inmediata y grave para el orden público, la seguridad pública o la seguridad nacional.

Por último, el capítulo V incorpora medidas para reforzar la coordinación en materia de seguridad de las redes y sistemas de información, modificaciones que afectan de lleno al modelo de gobernanza de la ciberseguridad en España que se reguló con la trasposición de la Directiva NIS. Para ello, efectúa una modificación del Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en virtud del cual el Centro Criptológico Nacional (CCN) ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del sector público. Adicionalmente, se prevé que el CCN ejercerá la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las Administraciones Públicas con los CSIRT internacionales en la respuesta a los incidentes y gestión de riesgos de seguridad.

José Luis DOMÍNGUEZ ÁLVAREZ
Personal Investigador en Formación (FPU)
Área de Derecho Administrativo
Universidad de Salamanca
jldoal@usal.es

Ars Iuris Salmanticensis,
vol. 8, Junio 2020, 217-223
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND