Medidas digitales urgentes por razones de seguridad pública.

Breve comentario al Real Decreto-Ley 14/2019, de 31 de octubre.

MIGUEL ÁNGEL BERNAL BLAY
Profesor titular de Derecho Administrativo. Universidad de Zaragoza.

Invocando razones de «seguridad pública», el Gobierno aprobó el pasado 31 de octubre el Real Decreto-Ley 14/2019, por el que se adoptan determinadas medidas en el ámbito digital. La Exposición de Motivos de la norma esgrime como motivos para justificar la intervención del Gobierno por esta vía extraordinaria[1], de una parte, la necesidad de garantizar la seguridad pública ante el desarrollo y empleo de las nuevas tecnologías y redes de comunicaciones por parte de las Administraciones Públicas, y especialmente, para asegurar que la administración digital se emplee para fines legítimos que no comprometan los derechos y libertades de los ciudadanos. Descendiendo un escalón en el nivel de justificación de la necesidad de promulgación de la norma se alude expresamente a «los recientes y graves acontecimientos acaecidos en parte del territorio español» que, contextualizados, parecen referirse a los episodios de violencia acaecidos en la Comunidad Autónoma de Cataluña tras conocerse el fallo de la Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 459/2019, de 14 de octubre de 2019. En este sentido se afirma que «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», respuesta que se materializa en la adopción de una serie de medidas en las áreas de Administración electrónica, contratación pública y telecomunicaciones.

En materia de administración electrónica, destaca la modificación de los artículos 9 y 10 de la Ley 39/2015, de procedimiento administrativo común, relativos a los

[1] Según se indica en la Exposición de Motivos del Real Decreto-Ley, «la alternativa de introducir estas medidas mediante un proyecto de ley no es factible en el presente caso, habida cuenta de que las Cámaras se encuentran disueltas y no es posible dilatar su adopción hasta la constitución de las Cortes Generales, y, aun utilizándose entonces el trámite de urgencia, no se lograría reaccionar a tiempo».

"En los contratos que exijan el tratamiento por el contratista de datos personales será obligatorio hacer constar en el pliego tanto la finalidad de la cesión de datos como la obligación de la empresa adjudicataria de mantener a la entidad contratante al corriente de la ubicación de los correspondientes servidores (art. 122.4 LCSP). Esta obligación deberá recogerse en los pliegos con el carácter de esencial a los efectos del régimen de resolución del contrato."

sistemas de identificación y firma ante las Administraciones públicas. La nueva redacción de dichos preceptos somete a autorización previa de la Secretaría General de Administración Digital (SGAD) del Ministerio de Política Territorial y Función Pública la adopción por las Administraciones públicas de sistemas de identificación y firma diferentes a los basados en certificado electrónicos expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación». Se trata de una opción que contrasta con la doctrina sentada por el Tribunal Constitucional, en Sentencia 55/2018, sobre el sistema anterior que reconocía a las Administraciones libertad para decidir el sistema de identificación a utilizar, y del que se decía «dinamiza la autoorganización administrativa» (FJ 9). En cambio, ahora, la necesidad de autorización previa de la SGAD puede alterar esas consideraciones del Alto Tribunal.

Además, se dispone la prohibición ("no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados") de utilización de sistemas de identificación y firma basados en tecnologías de registro distribuido. La Ministra de Economía, en el trámite de defensa del Real Decreto-Ley para su convalidación ante la Diputación Permanente del Congreso de los Diputados, justificó esta medida en aplicación del principio de precaución en el ámbito concreto de la identificación y firma electrónica ante las Administraciones públicas. Sin embargo, resulta llamativo que ese principio de precaución únicamente se aplique en el ámbito de las relaciones con la Administración, y no se extienda, por las mismas razones de «seguridad pública» a otros ámbitos, como el financiero. Para éste, en cambio, es conocida la intención de crear un «sandbox»[2]. El establecimiento de un «sandbox» para analizar el desarrollo de servicios públicos de identidad electrónica utilizando tecnología de registro distribuido hubiera sido una alternativa menos restrictiva y respetuosa con el principio de autoorganización de las Administraciones públicas que la prohibición establecida[3].

[2] El propio Ministerio de Economía y Empresa ha tramitado un proyecto de Ley de transformación digital del sistema financiero que incluye un «regulatory sandbox», un conjunto de disposiciones que amparan la realización controlada y delimitada de pruebas dentro de un proyecto que puede aportar una innovación financiera de base tecnológica, definida como aquella que pueda dar lugar a nuevos modelos de negocio, aplicaciones, procesos o productos con incidencia sobre los mercados financieros, la prestación de servicios financieros y complementarios o el desempeño de las funciones públicas en el ámbito financiero.».

[3] En este sentido, recordemos que, en palabras del Parlamento Europeo, «la tecnología de registros distribuidos (TRD) y las cadenas de bloques pueden constituir un instrumento que capacite a los ciudadanos dándoles la oportunidad de controlar sus propios datos y de decidir qué datos compartir en el registro, así como la capacidad de elegir quién más puede ver dichos datos» Cfr. Resolución del Parlamento Europeo, de 3 de octubre de 2018, sobre las tecnologías de registros distribuidos y las cadenas de bloques: fomentar la confianza con la desintermediación (2017/2772(RSP)).

La prohibición establecida difícilmente puede conectarse con ningún «episodio violento» de los referidos por el Real Decreto Ley en su exposición. Antes al contrario, parece ser la reacción a la presentación, el pasado mes de septiembre, del proyecto IDentiCAT por parte de la Generalitat de Cataluña. Un proyecto que pretende implantar un sistema de identificación electrónica auto-soberana (Self-Sovereign Identity), esto es, gestionada directamente por el ciudadano utilizando tecnologías de registro distribuido, y que quizás se vislumbró como una «amenaza» al medio de identificación oficial, el Documento Nacional de Identidad. Eso explica la modificación de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana para aclarar que «el Documento Nacional de Identidad ... 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» (nueva redacción del artículo 8.1).

Quizás la medida más mediática es la que dispone que los "servidores" donde se almacenen determinados datos personales en poder de las Administraciones públicas "deberán ubicarse dentro del territorio de la Unión Europea". Se hace una referencia expresa al «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» (nuevo artículo 46 bis de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público). Junto a ello, y en relación con los sistemas de identificación y firma antes mencionados, 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 territorio español, en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, 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 (RGPD)[4].

En materia de contratación del sector público, se modifican hasta siete preceptos de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, con el objetivo de asegurar el uso correcto de los datos personales por parte de los contratistas del sector público que tengan acceso a los mismos en ejecución de los contratos públicos. Lo cierto es que, tras la aprobación de la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, muchas entidades del sector público habían incluido en los pliegos de sus contratos, cuando las prestaciones implicaban la cesión de datos, cláusulas específicas que definían el régimen de obligaciones en materia de protección de datos al que quedaba sujeto el contratista e incluso los eventuales subcontratistas.

Las modificaciones introducidas en la Ley de Contratos del Sector Público proyectan sin embargo una preocupación formal porque se consigne en los contratos (art. 35 LCSP) y en los pliegos (art. 122.2 LCSP) la obligación del contratista de respetar la normativa sobre protección de datos, hasta el punto de deducir de la ausencia de dichas referencias la nulidad de pleno derecho del contrato (art. 39.2 LCSP). En mi opinión, la verdadera protección de los datos proviene, en su caso, de la aplicación del régimen sancionador previsto en la Ley Orgánica de Protección de Datos Personales, y no tanto de disponer la nulidad de pleno derecho del pliego para el caso de que omita mencionar las obligaciones del futuro contratista en esa materia, y ello porque dichas obligaciones provienen de una Ley de aplicación general, y no dependen de que se incorporen o no a la relación contractual. Al margen de esta consideración personal, el primer efecto derivado de esta medida es la necesidad de adaptar los pliegos de cláusulas administrativas, bajo sanción, en caso contrario, de nulidad de pleno derecho por los órganos de recurso.

Asimismo, en los contratos que exijan el tratamiento por el contratista de datos personales será obligatorio hacer constar en el pliego tanto la finalidad de la cesión de datos como la obligación de la empresa adjudicataria de mantener a la entidad contratante al corriente de la ubicación de los correspondientes servidores (art. 122.4 LCSP). Esta obligación deberá recogerse en los pliegos con el carácter de esencial a los efectos del régimen de resolución del contrato.

Estas medidas se completan con un régimen transitorio del que destaca la previsión expresa de aplicación de las modificaciones introducidas en la LCSP a las modificaciones de los contratos que se inicien con posterioridad

[4] El precepto señalado se refiere a datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

a la entrada en vigor del Real Decreto-Ley, rompiendo la tradición de no aplicar modificaciones de preceptos legales a contratos que se estuviesen ejecutando pero que hubiesen sido adjudicados con anterioridad a la entrada en vigor de esas modificaciones legales.

Cierran el grupo de medidas acordadas varias modificaciones de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, con el objetivo de potenciar las facultades de que dispone el Gobierno, a través del Ministerio de Economía y Empresa, para afrontar situaciones que pueden afectar al mantenimiento del orden público, la seguridad pública o la seguridad nacional. En partícular, se faculta al Gobierno para, sin necesidad de recabar autorización judicial ni de arbitrar un trámite contradictorio con eventuales interesados, acordar, con carácter excepcional y transitorio, «la asunción por la Administración General del Estado de 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 y la seguridad nacional». ✱