El Real Decreto-Ley 14/2019: una nueva regulación del ciberespacio en clave nacional

Vicente Moret Millás | Letrado de las Cortes Generales y Of Counsel de Andersen Tax & Legal.

Tema

La aprobación del Real Decreto-ley 14/2019 por el que se adoptan medidas urgentes por razones de seguridad en materia de administración digital, contratación del sector público, y telecomunicaciones, ha supuesto una importante modificación del régimen jurídico aplicable a algunas de las tecnologías de la información más relevantes para gestionar la realidad digital.

Resumen

La regulación de la realidad digital por los Estados refleja el modelo político de cada uno. Mientras algunos tratan de preservar una Internet abierta y libre, otros como China o Rusia buscan fragmentarla del mismo modo que lo hacen con las fronteras físicas, en lo que se ha dado en llamar *"balcanización"* de la Red o incluso *splinternet*. La Unión Europea (UE) desarrolla una tercera vía de aproximación normativa que pretende proteger tanto la libertad de Internet como los derechos fundamentales y el uso de los datos personales de los ciudadanos.

Dentro de este proceso general para la regulación de la soberanía digital de los Estados y la gobernanza del ciberespacio, el Real Decreto-Ley (RDL) 14/2019 responde a la necesidad de regular la realidad digital para evitar su uso ilegítimo y poner en riesgo la seguridad nacional. Aprobado por el Consejo de Ministros y convalidado por el Congreso de los Diputados, espera ahora su trámite como Proyecto de Ley.

Análisis

El RDL 14/2019 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 que obran en poder de estas, la contratación pública o la regulación de las redes de comunicaciones.

Uno de los hechos novedosos que introduce esta norma en nuestro panorama jurídico es que por primera vez se justifica un RDL en el sustrato normativo de la Ley 36/2015 de Seguridad Nacional para que, según alega su exposición de motivos: "la administración digital se emplee para fines legítimos que no comprometan los derechos y libertades de los ciudadanos". El desarrollo tecnológico, se señala, implica una mayor exposición a nuevas amenazas, y la hiperconectividad actual agudiza algunas de las vulnerabilidades de la seguridad pública, por lo que es necesaria una mejor protección de redes y sistemas, así como de la privacidad y los derechos digitales del ciudadano.

Protección también necesaria frente a las actividades de desinformación, las interferencias en los procesos de participación política de la ciudadanía y el espionaje debido a las posibilidades que ofrece la sofisticación digital para acceder a ingentes volúmenes de información y datos sensibles.

Llama la atención la referencia abierta y sin equívocos a la razón fáctica por la cual se aprueba la norma que se incluye en la misma exposición de motivos: "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*".*

Según esto, estamos ante la adopción de una norma-medida que trae causa del proceso de destrucción de la Constitución en terminología de Smith que se está intentando llevar a cabo por parte de algunas fuerzas políticas catalanas desde 2014 y que alcanzó el máximo nivel de desafío a la legalidad en el referéndum del 1 de octubre y la fallida declaración de independencia de 10 de octubre de 2017. Ante esta situación, y ante la posibilidad de que ese proceso continúe utilizando las enormes posibilidades que el ciberespacio proporciona, el Estado decide actuar aprobando las siguientes normas que modifican seis leyes, una de ellas orgánica.

Modificación del régimen legal del Documento Nacional de Identidad

La novedad que se introduce materia es la de considerar al 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[1]. De esta forma se elimina cualquier posibilidad de que alguna Administración Pública pretenda introducir un nuevo documento de acreditación de la identidad con el propósito de sustituirle. Por esta misma razón, se modifica también el artículo 15.1 de la Ley 59/2003 de firma electrónica para reconocer ese mismo valor al DNI en su forma electrónica, con los efectos legales reconocidos en la Ley de Seguridad Ciudadana.

También se puede considerar como una manera de evitar intentos de introducción de documentos de identificación de la personalidad de forma ilegal como ya supuso en su día el denominado DNI vasco, emitido por la *Udalbiltza* a partir de 2001, y reiteradamente declarado ilegal por diversas sentencias judiciales. Según estas, es el Estado el que, sobre la base del artículo 149.1.2 de la Constitución tiene competencia exclusiva en materia de nacionalidad y en la ordenación de registros e instrumentos públicos según el artículo 149.1.8. En definitiva, se trata de evitar que la emisión de un documento de identificación por otras Administraciones distintas de la del Estado se

[1] Modifica el artículo 8.1 de la Ley Orgánica 4/2015 de protección de la seguridad ciudadana que no tiene el carácter de orgánico según establece la propia ley, en el sentido de afirmar su carácter único a la hora de ser por sí mismo suficiente para esa acreditación.

convierta en un intento de usurpación de funciones que pretendan dar una imagen de legitimación de Estado a un ente territorial que no lo es.

Medidas en materia de identificación electrónica ante las Administraciones Públicas y sobre la ubicación de determinadas bases de datos y datos cedidos a otras Administraciones Públicas

Se modifica la regulación de los medios de identificación electrónica de los interesados prevista en la Ley 29/2015 de Procedimiento Administrativo Común de las Administraciones Públicas para reducir los sistemas de identificación. 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 se fija una lista cerrada que antes sólo se citaba a modo de ilustración de las posibilidades existentes.

A partir de ahora, solamente se podrán emplear para acreditar la identidad digital los sistemas basados en certificados electrónicos cualificados de firma electrónica contenidos en la ''Lista de confianza de prestadores de servicios de certificación''. Con ello se da cumplimiento al artículo 22 del Reglamento (UE) 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. 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. 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.

Un cambio de mayor calado se refiere a los sistemas de clave concertada (usuario más contraseña) para identificar a los ciudadanos ante la Administración para cualquier actuación ante esta[2]. A partir de ahora seguirán siendo plenamente utilizables, pero requerirán la previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

La nueva redacción del artículo 9.2 de la Ley 39/2015 establece, no obstante, límites a esa necesidad de autorización previa por parte de la Administración del Estado. 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 y la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios (en este caso el silencio será negativo)[3]. El RDL ha tenido la prevención de dejar claro que esa autorización

[2] Se trata de una plataforma común para la identificación, autenticación y firma electrónica del ciudadano ante organismos de la Administración. En el caso de la Administración del Estado ese sistema se denomina Cl@ve y contempla la utilización de sistemas de identificación basados en claves concertadas y certificados electrónicos (incluyendo el DNIe).

[3] A pesar de que la Ley 39/2015 establece en su artículo 24 que el sentido del silencio administrativo será positivo, lo cierto es que a continuación señala la posibilidad de excepción en los supuestos en los que una norma con rango de ley establezca lo contrario, como es el caso que nos ocupa.

previa sólo podrá fundarse en aspectos relativos a la materia seguridad pública que es competencia del Estado, de forma tal que ese control que constituye la autorización por parte del Estado a otras Administraciones Públicas se basa en una competencia exclusiva del Estado y no es un control general, sino tan sólo limitado a esa materia.

En este sentido, la norma que ahora se analiza tiene bien presente la doctrina del Tribunal Constitucional expresadas en la Sentencia 55/2018 y citada en la propia exposición de motivos que reconoce la posibilidad de que cada Administración diseñe sus propios sistemas de identificación electrónica o admita los expedidos por otras entidades públicas o privadas según sus preferencias. Por ello 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. Si así fuera –y solo en este caso–, la Administración del Estado denegará dicha autorización.

Otra importante modificación introducida en el apartado 3 de este artículo 9 introduce 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 UE. Además, se establece una limitación adicional y es que esa localización deberá ser 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 que regula la Protección de Datos (RGPD). La modificación busca claramente reforzar la denominada soberanía digital, es decir, proteger activos electrónicos valiosos y decisivos a la hora de asegurar un correcto funcionamiento de los Estados, sus servicios y en general de las sociedades actuales, mediante el aseguramiento de la ubicación territorial en la UE y su jurisdicción, todo ello bajo el amparo regulatorio del marco de normas europeas, principalmente el Reglamento General de Protección de Datos (RGPD).

Así mismo, ciertos datos y sistemas se consideran tan sensibles que sólo podrán situarse físicamente en territorio español. En concreto esta imposición de la territorialización se ciñe a la categoría especial de datos incluidos en el artículo 9 del RGPD, es decir, datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud, y datos relativos a la vida sexual o las orientación sexuales de una persona física. El propio RGPD, consciente de la sensibilidad absoluta de estos datos, incluye una habilitación a los Estados para que puedan regular de forma adicional esta categoría de datos. Además, se fija con claridad la prohibición de transferencia a un tercer país u organización internacional, salvo que sean objeto de una decisión de adecuación de la Comisión Europea si su régimen jurídico y las garantías jurisdiccionales son adecuadas y equivalentes a las europeas (disponen de ellas Andorra, Argentina, Guernesey, Israel, Isla de Man, Japón, Jersey, Nueva Zelanda, Suiza, Uruguay, Estados Unidos y está próxima a concluirse el procedimiento con Corea del Sur) o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

Esta limitación responde a la situación generada desde 2017 por el Govern de la Generalitat de Cataluña que puso en marcha lo que se denominó la Republica Digital. Para ello empezó a establecer los fundamentos de una administración virtual en la que sus ciudadanos pudieran votar y hacer trámites o que incluso expidiera documentos de identidad. Se trata de un claro intento de construir una realidad estatal paralela con el objetivo de desplazar a la realidad estatal vigente en nuestro sistema constitucional, aprovechando el vacío regulatorio que en el ámbito internacional existe sobre muchas de estas áreas de actividad digital y que en el mundo físico son sencillamente delitos o infracciones administrativas. El objeto en este caso no es mejorar los servicios públicos o ejecutar competencias propias, es sencillamente sustituir una legalidad estatal por otra legalidad paralela y supuesta, cuya legitimidad no se basa en normas jurídicas sino en el vacío regulatorio y en 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". Se trataba de construir una república digital reconocida internacionalmente cuyos activos y servidores están alojados fuera del territorio de la UE, según información publicada, en territorios tan exóticos como la Isla de Nieves en las Antillas, precisamente para evitar la aplicación de ese marco jurídico europeo y español que pudiese perseguir la comisión de delitos o de infracciones administrativas desde esas ubicaciones territoriales extraeuropeas. Esta obligación de residencia podría parecer drástica pero el propio RGPD permite que la UE o los Estados miembros introduzcan disposiciones específicas con respecto a los datos especiales del artículo 9 para proteger los derechos fundamentales y los datos personales de las personas físicas.

Por todo lo anterior, se reconoce a los Estados miembros la capacidad para imponer restricciones a determinados principios y a los derechos de información, acceso, rectificación o supresión de datos personales, al derecho a la portabilidad de los datos, a las decisiones basadas en la elaboración de perfiles, entre otras, en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública. Así se recoge en el artículo 23 del propio RGPD, que establece la competencia de los Estados para limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos siempre que respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar entre otras la seguridad del Estado; la defensa; o la seguridad pública. Por otra parte, debe señalarse que estas obligaciones de almacenamiento territorializado se imponen sólo a las Administraciones Públicas y no a los particulares, ya que en este apartado en concreto la norma solo se está refiriendo a los datos que son necesarios para utilizar sistemas de clave concertada.

No obstante, cabría analizar si la restricción del flujo de los datos protegidos por el artículo 9 al territorio español puede producir una distorsión en el ámbito del Mercado Único Digital de la UE al limitar el tráfico de datos. Es muy probable que dicha excepción a la libre circulación y almacenamiento de datos en el marco de la UE pueda justificarse por motivos de seguridad nacional o de seguridad pública o jurídica, pero sería conveniente estudiar en el posterior trámite parlamentario que permita convertir este RDL en ley si tiene sentido mantener esa restricción en favor sólo del territorio nacional o si bastaría una limitación a la obligatoriedad de territorialización dentro de la propia UE.

Por último, el RDL prohíbe de forma tajante el uso de tecnologías de registro distribuido (*blockchain*). No serán admisibles en las relaciones de los interesados con las Administraciones 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.

Ubicación de los sistemas de información y transmisiones de datos entre Administraciones

El RDL modifica el artículo 46 de la Ley 40/2015 de Régimen Jurídico del Sector Público que regula la territorialización de unos sistemas de información especialmente relevantes desde el punto de vista del funcionamiento de cualquier Administración y de los Estados mismos. Por un lado, regula los sistemas para la recogida, almacenamiento, procesamiento y gestión del censo electoral[4] y los padrones municipales de habitantes y otros registros de población[5]. Por otro, los datos de los usuarios del sistema nacional de salud, equiparados con los anteriores por el Real Decreto-ley respecto a las obligaciones de localización, aunque plantea dudas respecto a la trascendencia político-administrativa que podría derivarse de su uso ilegítimo por las Administraciones, por lo que precisará debatir su equiparación en el futuro trámite parlamentario.

Además, el RDL introduce una serie de obligaciones relativas a las transmisiones de datos entre administraciones públicas. Cada una de ellas 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 para fines incompatibles con el fin para el cual se recogieron inicialmente los datos personales. En este caso lo que se está regulando es una manifestación del principio de lealtad institucional que debe presidir las relaciones entre las Administraciones Públicas regulado en el artículo 140 de la Ley 40/2015. 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.

Modificaciones en materia de contratación pública en materia de protección de datos

La Ley 9/2017 de Contratos del Sector Público se modifica para considerar obligatoria en ellos la referencia a la legislación aplicable en materia de protección de datos y, además, se considera causa de nulidad del contrato el incumplimiento de la obligación de hacer constar en los pliegos de contratación las obligaciones respecto a los datos

[4] La Ley Orgánica 5/1985 de Régimen Electoral General define en su artículo 31 que "El censo electoral contiene la inscripción de quienes reúnen los requisitos para ser elector y no se hallen privados, definitiva o temporalmente, del derecho de sufragio".

[5] La inscripción sólo considera obligatorios el nombre, sexo, domicilio habitual, nacionalidad, lugar y fecha de nacimiento, número de documento nacional de identidad o documento similar de extranjeros y los datos fiscales relacionados con tributos propios o cedidos.

tales como su sometimiento a la normativa, la ubicación de los servidores o la comunicación de los cambios y la subcontratación.

En materia de protección de datos es importante señalar que, con la nueva regulación del RDL, los subcontratistas quedarán obligados solo ante el contratista principal quien asumirá la total responsabilidad de la ejecución del contrato. Asimismo, se introduce una prohibición de contratar por incumplimiento de las especificaciones de protección de datos en otros contratos públicos anteriores debido a infracción grave, concurriendo dolo, culpa o negligencia. La finalidad última de estas reformas en la normativa de contratación es evitar que esos datos especialmente protegidos y que son relevantes desde el punto de vista administrativo puedan ser manipulados irregularmente mediante la externalización en favor de empresas adjudicatarias de contratos administrativos. De nada serviría establecer todo un régimen de limitaciones para las Administraciones Públicas si esas limitaciones pueden ser burladas utilizando empresas contratadas por esas mismas administraciones públicas.

Reforzamiento de las potestades del Estado en materia de Telecomunicaciones

El RDL modifica la Ley 9/2014 General de Telecomunicaciones (LGT) para habilitar al Gobierno, con carácter excepcional y transitorio, para que la Administración General del Estado asuma 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. Este reforzamiento de las potestades del Estado es relevante, aunque no tan novedoso y disruptivo como se ha venido defendiendo desde la aprobación del RDL. Esta facultad extraordinaria atribuida al Gobierno ya se aplicaba a los supuestos que afectasen a la "seguridad pública y la defensa nacional" y ahora se amplía a la seguridad nacional y el orden público como causas legitimadoras de esa intervención.

Por gestión directa hay que entender cualquier modo de prestación de servicios públicos que suponga que la Administración ejecuta directamente con sus propios medios o por medio de entes instrumentales, si se dan ciertas causas excepcionales. Se distingue así de otras formas de gestión indirecta de los servicios públicos tales como la concesión o el concierto. Ya que el artículo 2 de la LGT establece que éstas son servicios de interés general que se prestan en régimen de libre competencia, lo que se regula es el paso de una forma de gestión regulada por la ley por, en su caso privados, a una forma de gestión directa por el Estado si se dan ciertas causas excepcionales. El supuesto más excepcional es la intervención de las empresas privadas porque altera el principio de libertad de empresa en el marco de una economía de mercado consagrado en el artículo 38 de la Constitución, aunque se trata de un supuesto reconocido en el artículo 128 de la Constitución por razones de interés general por el que siguen permaneciendo bajo la titularidad de sus propietarios, pero su gestión y actividad se dirige por un órgano estatal que la toma de decisiones.

Así mismo, se establece la obligación de que las Administraciones Públicas comuniquen al Ministerio de Economía y Empresa todo proyecto de instalación o explotación de redes de comunicaciones electrónicas en régimen de autoprestación que haga uso del dominio público. Además, se considera infracción muy grave el incumplimiento de las

obligaciones en materia de acceso a redes o infraestructuras físicas susceptibles de alojar redes públicas de comunicaciones electrónicas, interconexión e interoperabilidad de los servicios. Este régimen restrictivo que aumenta el control del Estado sobre esas redes se refuerza mediante una serie de medidas cautelares que, si bien ya se recogían en el artículo 81 de la LGT, ahora se ha ampliado a otros supuestos. Previamente al inicio del procedimiento sancionador, mediante resolución sin audiencia previa, se podrá ordenar el cese de la presunta actividad infractora cuando existan razones de imperiosa urgencia basada la exista una amenaza inmediata y grave para el orden público, la seguridad pública, la seguridad nacional o la salud pública; cuando puedan producirse perjuicios graves al funcionamiento de los servicios de seguridad pública, protección civil y de emergencias, otros servicios o redes de comunicaciones electrónicas o a otros proveedores o usuarios de redes o servicios de comunicaciones electrónicas.

Esta modificación que parecería en exceso rigurosa no lo es tanto si se analiza en contexto, ya que en su redacción original este artículo de la LGT en 2014 ya recogió este procedimiento y ahora solamente se ha procedido a añadir otro supuesto de aplicación relativo a la amenaza inmediata y grave para el orden público, la seguridad pública o la seguridad nacional, en plena consonancia con el objetivo final de toda el RDL, que es precisamente evitar los ataques contra el orden constitucional desde el ciberespacio y las redes de comunicaciones. Por tanto, no se introduce una restricción general nueva, sino que se amplía a un supuesto adicional la aplicación de un procedimiento que ya existe.

No obstante, y como corresponde en general a la regulación de cualquier tipo de actuación excepcional de los poderes públicos, en la aplicación de esta medida provisional se determinará el ámbito objetivo y temporal de la medida, sin que pueda exceder del plazo de un mes, limitando así el posible efecto temporal de esta medida restrictiva. Por ello, la resolución que adopte este mecanismo deberá motivar muy bien las razones de esa decisión, así como los límites de esta en cuanto a su extensión material y temporal.

Medidas en materia de seguridad de las redes y sistemas de información

Por último, el RDL adopta medidas en materia de seguridad de las redes y sistemas de información consistentes en la modificación del RDL 12/2018 sobre la seguridad de las redes y sistemas de información. Esta modificación afecta de lleno al modelo de gobernanza de la ciberseguridad en España que se reguló con la trasposición de la Directiva NIS. Se refuerza el papel que el CCN/CNI ejercerá en cuanto a la coordinación de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (CSIRT) nacionales e internacionales.

Conclusiones

El RDL 14/2019, por su contenido y las circunstancias de su aprobación, es una norma de amplio calado que supone un antes y un después en cuanto a la utilización de la seguridad nacional como título competencial habilitante para la acción normativa del Estado. Representa una innovación legislativa para prevenir los intentos de quebrar el sistema constitucional utilizando las posibilidades que ofrece el ciberespacio para desestabilizar sistemas democráticos. Y aunque en todos los ordenamientos constitucionales de las democracias liberales existen mecanismos para la defensa de la Constitución, deben dotarse de instrumentos para hacer frente a las nuevas tecnologías que ponen en riesgo los sistemas constitucionales utilizando las libertades y derechos que precisamente ese régimen garantiza.

El texto de esta norma, convalidado por el Congreso de los Diputados, responde a la legitima finalidad para la que fue aprobada por el Consejo de Ministros y lo hace dentro del margen de atribución competencial que el Tribunal Constitucional ha ido reconociendo en el ámbito de las materias seguridad nacional y seguridad pública. Es un texto con un amplísimo margen de aplicabilidad, aunque es muy probable que algunos aspectos se modifiquen en su tramitación parlamentaria como proyecto de ley. Con las peculiaridades que afectan a la situación política española actual, esta nueva norma se inscribe en una nueva tendencia que se está manifestando masivamente en los últimos años, y que se corresponde con los intentos reiterados de muchos Estados y de la propia UE de regular el ciberespacio por la trascendencia económica, política, geopolítica y social que la realidad digital tiene para la gobernación de cualquier país.