G A _ P

Gómez-Acebo & Pombo

El Gobierno puede intervenir las redes de telecomunicaciones (pero no bloquear los contenidos) por razones de seguridad pública

Ana I. Mendoza Losana

Profesora titular de Derecho Civil de la Universidad de Castilla-La Mancha

Consejera académica de Gómez-Acebo & Pombo

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.

Da la impresión de que, cuando la fundamentación de un real decreto ley es casi más extensa que la parte dispositiva de la propia norma, es cuestionable que concurran las circunstancias de extraordinaria y urgente necesidad que justificarían la utilización de este instrumento normativo y, lo que es peor, puede resultar cuestionable su eficacia, de modo que la norma llamada a atender esa situación de urgencia no sirva para alcanzar el objetivo perseguido. Si, además, este real decreto ley se aprueba justo un día antes de la inauguración de la campaña electoral y a pocos días de la publicación de la polémica sentencia del Tribunal Constitucional sobre el conflicto catalán, esa impresión se convierte en certeza. Es lo que ocurre con el 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 (la exposición de motivos ocupa nueve de las veinte páginas de la norma).

Es dudoso que se requiriera tanta urgencia en la implantación del documento nacional de identidad (DNI) como único documento acreditativo de la identidad y de los datos personales de su

N. de la C.: En las citas literales se ha rectificado en lo posible —sin afectar al sentido— la grafía de ciertos elementos (acentos, mayúsculas, símbolos, abreviaturas, cursivas...) para adecuarlos a las normas tipográficas utilizadas en el resto del texto.

titular (modificación del artículo 8.1 de la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana, y del artículo 15.1 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica) o en la imposición de deberes de protección de datos de carácter personal derivados de la normativa vigente a las propias Administraciones Públicas y a quienes contratan con ellas, pudiendo ser causa de nulidad del contrato la omisión de la mención de tales deberes (modificación de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, 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 del 2014).

Sí podría haber cierta urgencia en la adopción de medidas para reforzar la seguridad en materia de telecomunicaciones (modificación de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones — LGTel—), en la modificación de los instrumentos de identificación electrónica ante las Administraciones Públicas o en las restricciones de uso de sistemas de identificación y firma basados en tecnologías de registro distribuido *(blockchain)* (arts. 9.2, 9.3 y 9.4 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas). A continuación, se exponen brevemente tales medidas:

1. Intervención gubernamental de redes y servicios de comunicaciones electrónicas

La nueva norma reconoce al Gobierno la potestad de asumir la gestión directa o de intervenir las redes y servicios de comunicaciones electrónicas, con carácter excepcional y transitorio y por razones de orden público, seguridad pública y seguridad nacional (nuevo art. 4.6 LGTel).

Obsérvese que, aunque se hace hincapié en el carácter «excepcional» y «transitorio» de la medida, ésta tiene un alcance tan amplio que queda bastante indeterminada. Las razones que justifican la intervención de las redes y servicios de telecomunicaciones obedecen a conceptos jurídicos indeterminados (orden público, seguridad pública y seguridad nacional); no se acotan los plazos máximos en los que las redes y servicios podrán estar intervenidos; la intervención podrá afectar a cualquier infraestructura, recurso asociado o 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, y la máxima expresión de la indefinición es que no se da contenido a esta «intervención» ni a los rasgos que la diferencian de la «gestión directa» a la que se refiere la norma o de la «expropiación», que no se menciona en la norma, pero que podría equipararse a dicha intervención.

No se prevé la obligación de comunicar la intervención (ni inmediatamente, ni a corto o medio plazo) a la autoridad judicial. Hay que puntualizar que esta potestad de intervención gubernamental sin orden ni control judicial se refiere a la infraestructura de red y no a los contenidos (páginas web, canales de YouTube, canales de televisión…). Éstos son servicios de contenidos excluidos del ámbito de aplicación de la Ley General de Telecomunicaciones (art. 1.2 LGTel). La clausura o intervención de estos medios requerirá seguir el procedimiento de intervención de la autoridad audiovisual (que se presupone

independiente del Gobierno) previsto en la Ley 7/2010, General de Comunicación Audiovisual (arts. 38 y 39), o, en su caso, incoar el correspondiente expediente sancionador que puede obligar al cese de actividad (art. 60 Ley 7/2010). Asimismo, el bloqueo de páginas web exige la tramitación del procedimiento previsto en el artículo 8 de la Ley 34/2002, de Servicios de la Sociedad de la Información, y, en su caso, de la autorización judicial, si la restricción pudiera afectar a derechos y libertades constitucionales (art. 8.1). Esto añade aún más dudas acerca del alcance de esta intervención, ¿en qué consistirá la intervención si el Gobierno no puede bloquear las webs o impedir el acceso a los contenidos que se transmiten a través de la red o infraestructura intervenida?

2. Deber de las Administraciones Públicas de comunicar al Ministerio de Economía y Empresa sus proyectos de instalación o explotación de redes de comunicaciones electrónicas

El real decreto ley glosado obliga a las Administraciones Públicas a comunicar 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, tanto si dicha instalación o explotación la va a efectuar de manera directa una entidad o sociedad dependiente de ella como si la va a realizar una entidad o sociedad a la que se le haya otorgado una concesión o habilitación (nuevo art. 6.3 LGTel). Igualmente, la comunicación se debe producir cuando la capacidad excedentaria de la red sea utilizada para la prestación de servicios por terceros. Todo ello, sin perjuicio del deber preexistente de comunicar al Registro de Operadores los proyectos de instalación o explotación de redes de comunicaciones electrónicas en régimen de autoprestación que hagan uso del dominio público (art. 7.3 LGTel).

Del tenor literal del nuevo artículo, se deduce que la preceptiva nueva comunicación pretende facilitar la comprobación del cumplimiento de lo previsto en el artículo 9 de la Ley General de Telecomunicaciones (instalación y explotación de redes públicas y prestación de servicios de comunicaciones electrónicas en régimen de prestación a terceros por las Administraciones Públicas). En esta línea, se tipifica como infracción administrativa muy grave o grave (nuevos arts. 76.15 y 77. 28, respectivamente) 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. Obsérvese que estas infracciones ya existían, si bien la propia norma definía a los posibles sujetos de dicha infracción (los operadores). Conforme a la nueva redacción, podrá ser sancionado cualquiera que incumpla estas obligaciones (también las Administraciones Públicas).

Esta obligación de comunicación se extiende a los procesos ya iniciados, de modo que las Administraciones Públicas deberán comunicar al Ministerio de Economía y Empresa en el plazo de un mes desde la entrada en vigor del real decreto ley (6 de noviembre del 2019) las redes de comunicaciones electrónicas en régimen de autoprestación que usen el dominio público y que hayan sido instaladas o estén en proceso de instalación o explotación (disp. adic. primera RDL 14/2019).

Hay quien apunta que esta medida pretende controlar el despliegue de una red de fibra óptica por la Generalitat de Cataluña. Ante esto, la cuestión es inmediata: ¿para conseguir ese fin es necesario obligar a todas las Administraciones Públicas (independentistas o no) a comunicar al ministerio las redes ya existentes o los proyectos que puedan acometer en el futuro? ¿Es proporcionada la medida?

3. Ampliación de los supuestos en los que el ministerio podrá ordenar el cese inmediato de actividad de una red o servicio de telecomunicaciones sin audiencia previa

El real decreto ley comentado amplía los supuestos en los que el Ministerio de Economía y Empresa podrá ordenar, como medida cautelar, antes del inicio del procedimiento sancionador y sin audiencia previa, el cese inmediato de una actividad por razones de «imperiosa urgencia». Esta previsión ya estaba en la normativa anterior para los casos en los que la supuesta actividad infractora pudiera producir perjuicios graves al funcionamiento de los servicios de seguridad pública, protección civil y de emergencias; pudiera poner en peligro la vida humana o pudiera interferir gravemente en otros servicios o redes de comunicaciones electrónicas.

En la nueva redacción del artículo 81.1 de la Ley 9/2014, no sólo se amplían los supuestos, sino que también se relaja el nivel de exigencia en cuanto a los supuestos que justificarían el cese. Ya no se exige que se perciba un riesgo para la vida humana y basta que se creen problemas económicos u operativos a otros operadores. Los nuevos supuestos se definen así: *a*) cuando exista una amenaza inmediata y grave para el orden público, la seguridad pública o la seguridad nacional; *b*) cuando exista una amenaza inmediata y grave para la salud pública; *c*) cuando puedan producirse perjuicios graves al funcionamiento de los servicios de seguridad pública, protección civil y de emergencias; *d*) cuando se interfiera gravemente en otros servicios o redes de comunicaciones electrónicas; *e*) cuando se creen graves problemas económicos u operativos a otros proveedores o usuarios de redes o servicios de comunicaciones electrónicas o demás usuarios del espectro radioeléctrico.

El Gobierno explica que esta ampliación de motivos comprende algunos de los supuestos recogidos en el artículo 30.6 del Código Europeo de las Comunicaciones Electrónicas, aprobado por la Directiva 2018/1972, de 11 de diciembre, 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. Sin embargo, hay diferencias sustanciales entre el artículo 30.6 del citado código europeo y el nuevo artículo 81.1 de la ley de telecomunicaciones española. El artículo 30.6 prevé expresamente dar audiencia a la empresa afectada y limita la duración de la medida a un máximo de tres meses prorrogables por idéntico periodo («la autoridad competente acordará a [*sic*] la empresa interesada una *oportunidad razonable de exponer su punto de vista y proponer posibles soluciones*»); en cambio, el artículo 81.1 no se refiere a medidas cautelares adoptadas una vez iniciado el procedimiento sancionador, sino a medidas previas adoptadas «antes del inicio del procedimiento sancionador» (*cfr*. arts. 81 y 82 LGTel) «mediante resolución sin audiencia previa» y sin límite de plazo.

4. Obligación impuesta a las entidades públicas de alojar sus servidores de datos sensibles en la Unión Europea o en España

El real decreto ley comentado también contiene medidas de protección de datos. Destaca especialmente la obligación de que las entidades públicas ubiquen en la Unión Europea los servidores de datos que alberguen bases como el censo electoral, padrones municipales, registros de población, datos fiscales y datos nacionales de salud. En caso de tratarse de datos sensibles o de «categoría especial» en los términos del artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril (como los relacionados con el origen étnico o racial, datos genéticos, biométricos o relativos a la orientación sexual), dichos servidores deberán estar en territorio español (nuevo art. 9.3 de la Ley 39/2015).

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 los ciudadanos y dichos organismos cuando éstos traten datos personales en ejercicio de una función pública.

La norma exige que, en cualquier caso, los datos se encuentren disponibles para las autoridades judiciales y administrativas competentes y que no puedan ser transferidos a un tercer país u organización internacional, salvo 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 España.

5. Control sobre los instrumentos de identificación electrónica

En la línea de adopción de medidas de control por razones de seguridad pública, el real decreto ley comentado también obliga a someter a la aprobación del Ministerio de Economía y Empresa la implantación por parte de las Administraciones Públicas de sistemas de identificación y firma electrónicas distintos a los previstos en la normativa estatal (nuevos arts. 9.2 y 10 de la Ley 39/2015). 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 éstos sean más o menos complejos según sus preferencias y la relevancia o características del trámite o servicio correspondiente» (STC 55/2018, de 24 de mayo). Sin embargo, invocando la seguridad pública como competencia exclusiva del Estado, la modificación efectuada somete a un régimen de autorización previa por parte de la Administración General del Estado a los sistemas que sean distintos de los del certificado y sello electrónico.

La 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 fuere y sólo en este caso, la Administración del Estado denegará tal autorización basándose en dichas consideraciones de seguridad pública.

Además, se prohíbe el uso de sistemas de identificación y firma basados en tecnologías de registro distribuido *(blockchain)* hasta que no sean objeto de regulación específica (nueva disp. adic. sexta de la Ley 39/2015).

6. Fortalecimiento de las funciones del Centro Criptológico Nacional

El Centro Criptológico Nacional (CCN) coordinará a nivel nacional la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés) en las redes y sistemas de información del sector público. Además, el centro ejercerá la función de enlace para garantizar la cooperación transfronteriza entre los mencionados equipos de respuesta de las Administraciones Públicas y los internacionales en los incidentes y la gestión de riesgos de seguridad (modificación del Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información).

7. Impacto

El nuevo real decreto ley se ha presentado como un instrumento de lucha contra la denominada *República Digital Catalana*, como una forma de preservar el control y, en su caso, la capacidad de intervención sobre la red de fibra óptica desplegada por la Generalitat, así como un instrumento para evitar la organización de votaciones digitales independentistas. El texto normativo no menciona a Cataluña, pero la exposición de motivos sí se refiere a «los recientes y graves acontecimientos acaecidos en parte del territorio español [que] han puesto de relieve la necesidad de modificar el marco legislativo vigente para hacer frente a la situación» y declara que «las medidas contenidas en el presente real decreto ley tienen como finalidad incrementar el estándar de protección de la seguridad pública frente a las crecientes amenazas que plantea el uso de las nuevas tecnologías y a la luz siempre de los últimos sucesos en territorio español».

Con todo, la indefinición de algunas de las medidas adoptadas, la escasez de garantías que rodean su adopción y la desproporcionalidad de la intervención a nivel general para solucionar un problema particular ponen la norma en tan grave riesgo de inconstitucionalidad como de ineficacia.