SECCIÓN DEL TRIBUNAL CONSTITUCIONAL

TRIBUNAL CONSTITUCIONAL

8217 *Pleno. Sentencia 10/2023, de 23 de febrero de 2023. Recurso de inconstitucionalidad 718-2020. Interpuesto por el Gobierno de la Generalitat de Cataluña en relación con diversos preceptos del 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. Límites materiales de los decretos leyes: extinción parcial del proceso, constitucionalidad de los preceptos que modifican disposiciones legales relativas a la administración y firma electrónica e intervención, seguridad y disciplina de redes y servicios de comunicaciones.*

ECLI:ES:TC:2023:10

El Pleno del Tribunal Constitucional, compuesto por el magistrado don Cándido Conde-Pumpido Tourón, presidente, y las magistradas y magistrados doña Inmaculada Montalbán Huertas, don Ricardo Enríquez Sancho, doña María Luisa Balaguer Callejón, don Ramón Sáez Valcárcel, don Enrique Arnaldo Alcubilla, doña Concepción Espejel Jorquera, doña María Luisa Segoviano Astaburuaga, don César Tolosa Tribiño y doña Laura Díez Bueso, ha pronunciado

EN NOMBRE DEL REY

la siguiente

SENTENCIA

En el recurso de inconstitucionalidad núm. 718-2020, interpuesto por el Gobierno de la Generalitat de Cataluña contra los arts. 1, 2, 3, 4, 6 y 7; la disposición adicional única; las disposiciones transitorias primera y segunda y la disposición final primera del 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. Ha comparecido y formulado alegaciones el abogado del Estado. Ha sido ponente la magistrada doña María Luisa Balaguer Callejón.

I. Antecedentes

1. Mediante escrito presentado en el registro del Tribunal Constitucional el 4 de febrero de 2020, el Gobierno de la Generalitat de Cataluña interpone recurso de inconstitucionalidad contra los arts. 1, 2, 3, 4, 6 y 7; la disposición adicional única; las disposiciones transitorias primera y segunda y la disposición final primera del 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.

El recurso se fundamenta en los motivos que se exponen a continuación.

La demanda comienza haciendo referencia a que la norma impugnada tiene por objeto regular un marco normativo sobre la documentación nacional de identidad (arts. 1 y 2); en relación con la identificación electrónica ante las administraciones públicas y los datos que obran en su poder (arts. 3 y 4) y sobre la contratación pública (art. 5) y el sector de las telecomunicaciones (arts. 6 y 7). Tales medidas obedecen, según la exposición de motivos, de un lado, a la exigencia de establecer un marco jurídico que

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

garantice el interés general y, en particular, la seguridad pública, asegurando la adecuada prestación de los servicios públicos y que la administración pública se emplee para fines legítimos que no comprometan los derechos y libertades de los ciudadanos; de otro lado, a la necesidad de responder a los acontecimientos acaecidos en parte del territorio español.

Se alude a la diversidad de contenidos del Real Decreto-ley 14/2019 y al contexto normativo en el que se inserta la regulación que aprueba, señalando que se refiere a un ámbito complejo y sujeto a permanente revisión, como es el de las nuevas tecnologías, en el que las diversas instancias, tanto europeas como estatales y autonómicas, disponen ya de un marco normativo de referencia completo en el que se desarrollan cada una de las opciones dentro de sus respectivas competencias. Se mencionan específicamente el Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio, 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, y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que se 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, conocido como Reglamento general de protección de datos, (en adelante RGPD). Además, en el proceso de permanente reforma de la administración pública en relación con la organización y el procedimiento administrativo se han sucedido importantes cambios que incorporan las tecnologías de la información y las comunicaciones como herramienta. Se mencionan la Ley 11/2017, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos; la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público y otras normas relevantes con innovaciones que se ponen de manifiesto en el Plan estratégico de impulso y transformación de la administración pública 2018-2020, cuyo eje 1, sobre la transformación de la administración digital, plantea como objetivo estratégico la tramitación de procedimientos por medios electrónicos. Por otra parte, las medidas incorporadas por el Real Decreto-ley inciden en el ámbito de las comunicaciones electrónicas cuyo marco normativo europeo de referencia es la Directiva 2018/1972 sobre el Código europeo de comunicaciones electrónicas, pendiente de trasposición al ordenamiento jurídico interno. La Ley 9/2014, de 9 de mayo, general de telecomunicaciones (LGTel) constituye la norma estatal de desarrollo de las previsiones comunitarias junto con el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

De esa referencia al esquema normativo en el que se introducen las medidas que incorpora el Real Decreto-ley 14/2019, la demanda deduce: (1) que no está justificada su extraordinaria y urgente necesidad, puesto que ya existe a nivel comunitario y estatal un cuerpo normativo sobre la identificación digital y sus garantías; y (2) que estas medidas van más allá de garantizar un trato común en materia de identificación y firma electrónica e introducen limitaciones para el desarrollo por las comunidades autónomas de sistemas de identificación, prescindiendo de los mecanismos de colaboración y cooperación, e introduciendo cortapisas que inciden de forma directa en la autoorganización y desarrollo en ámbitos de sus propias competencias.

La interposición del recurso obedece a tres tipos de consideraciones: (a) se considera que se incumplen los requisitos previstos en el art. 86 CE sobre la extraordinaria y urgente necesidad, para la utilización del decreto-ley; (b) se formulan objeciones que responden a la falta de adecuación de los preceptos que se recurren con el orden constitucional y estatutario de distribución de competencias; y (c) se considera que algunas de las medidas contravienen las garantías de los derechos constitucionales, específicamente las relativas a telecomunicaciones.

A) Infracción del art. 86.1 CE.

El recurso sostiene que, del análisis de la exposición de motivos y del debate parlamentario de convalidación en el Congreso de los Diputados, no se infiere que

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

concurra una necesidad extraordinaria que justifique el uso de la potestad legislativa excepcional en los términos exigidos por la doctrina constitucional. Se hacen referencias genéricas a la necesidad de adaptación a la aceleración en el empleo de nuevas tecnologías por parte de la administración, que se complementan con consideraciones relativas a los desafíos de y carácter estratégico de las nuevas tecnologías para la seguridad nacional, haciendo mención específica a los «recientes y graves acontecimientos acaecidos en parte del territorio español». No obstante estos no se definen a pesar de considerar que precisan de una respuesta inmediata para evitar que se reproduzcan, estableciendo un marco preventivo con el objetivo de proteger los derechos y libertades constitucionalmente reconocidos y garantizar la seguridad pública de todos los ciudadanos. Para la demanda la aparente justificación no daría apoyo a la acreditación de los requisitos que constitucionalmente deben de permitir contrastar la concurrencia de la justificación que se precisa para la adopción del Real Decreto-ley 14/2019, más aún si se tiene en cuenta que ya se dispone de un marco jurídico completo.

Por otra parte, por lo que se refiere a las medidas incorporadas en el Real Decreto-ley 14/2019 que responden a razones de seguridad pública, debe tenerse en cuenta que esta dimensión de la seguridad está integrada en la estructura de los sistemas de información. No se exponen las razones que superan los riesgos que, en cualquier sistema de información, ya son tenidos en cuenta y se sujetan a la correspondiente verificación y control de riesgos. Se considera que la mera mención del riesgo por sí mismo y en los términos genéricos con que se expone no puede justificar la medida incorporada, cuando ello puede conllevar restricciones a los derechos fundamentales de libertad de comunicación e información, en los términos previstos en los arts. 18 y 20 CE.

Junto a la falta de excepcionalidad de la situación a atender, la demanda considera que no se acredita que se trate de responder a una necesidad urgente. Se alude a la circunstancia de que se habían disuelto las cámaras, razón también por la cual el Real Decreto-ley 14/2019 se convalida ante la Diputación Permanente del Congreso de los Diputados. También se añade la consideración sobre la limitación de que el Gobierno en funciones no puede presentar proyectos de ley para su tramitación. Según la abogada de la Generalitat de Cataluña la finalización y agotamiento de legislatura no debería comportar, por sí misma, un fundamento acreditativo del supuesto de la urgencia.

Por último, al no especificarse cuál es la situación extraordinaria que se quiere afrontar y que justifica la elaboración de un decreto-ley, es difícil vincular esta indeterminación con las medidas que el Real Decreto-ley 14/2019 adopta, por lo que no es posible analizar si las medidas adoptadas en el Real Decreto-ley 14/2019 responden de forma congruente con la situación que ha justificado su adopción.

En suma, el Gobierno se limita a realizar una mera declaración formal de la necesidad de la aprobación rápida e inminente, sin aportar las razones que imposibilitan la consecución de la eficacia de las medidas pretendidas mediante su tramitación y aprobación parlamentarias. Una falta de justificación, no solo con respecto a la urgencia sino también sobre la congruencia entre la situación de extraordinaria y urgente necesidad y la regulación adoptada, que se convierte en especialmente reprobable al tratarse de una disposición legislativa provisional de alcance estructural. Se reforma con amplitud la administración digital por lo que se refiere a los sistemas de identificación y adopta medidas de intervención desproporcionada en las redes y servicios de comunicaciones electrónicas así como en cualquier infraestructura, recurso asociado o elemento o nivel de la red o del servicio que resulte necesario, limitando con ello, los derechos fundamentales sobre los que inciden dichos servicios. Por otra parte, el propio régimen transitorio, con la previsión de un calendario para hacer efectivas unas obligaciones que en algunos casos alcanza periodos de hasta seis meses, evidencia la falta de urgencia de dichas medidas.

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

B) Infracción del sistema de distribución de competencias.

a) La demanda sostiene que los arts. 1, 2 y 3 del Real Decreto-ley 14/2019 introducen restricciones a la determinación de los sistemas de identificación en los servicios de la Generalitat de Cataluña que son contrarias al orden competencial, limitando las competencias que sobre autoorganización y organización de sus propios servicios tiene reconocidas en los arts. 150 y 159 del Estatuto de Autonomía de Cataluña (en adelante EAC), respectivamente.

La demanda recuerda la doctrina constitucional sobre el título competencial relativo a la seguridad pública (cita las SSTC 86/2014 y 142/2018), así como respecto al art. 149.1.18 CE (cita la STC 55/2018), a partir de las cuales considera que las medidas introducidas por el Real Decreto-ley 14/2019 limitan y restringen la capacidad de la Generalitat de Cataluña para organizar su propia administración, en la vertiente relativa a los servicios de administración electrónica.

Por lo que se refiere a las medidas restrictivas en la determinación de los sistemas de identificación de los interesados ante la administración de la Generalitat de Cataluña, el Real Decreto-ley 14/2019 introduce modificaciones sobre la regulación del documento nacional de identidad (en adelante, DNI) y DNI electrónico (arts. 1 y 2); el sometimiento a autorización previa del Ministerio de Política Territorial y Función Pública de determinados sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido que permita garantizar la identidad del usuario (art. 3.1) y la prohibición de establecer sistemas de identificación por parte de las administraciones públicas basados en tecnologías de registro distribuido (art. 3.3).

La demanda cuestiona que las modificaciones introducidas vengan exigidas por el Derecho de la Unión Europea y menciona las disposiciones legales adoptadas por la Comunidad Autónoma respecto a esta cuestión (Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña, y Ley 29/2010, de 3 de agosto, del uso de los medios electrónicos en el sector público de Cataluña que fue objeto de desarrollo por la Orden GRI/233/2015, de 20 de julio, por la cual se aprueba el Protocolo de identificación y firma electrónica y se adoptó el Acuerdo GOV/147/2016, de 15 de noviembre, por el cual se aprueba el desarrollo del Sistema de identificación verificada de Cataluña). De todo ello se desprende que se dispone de un sistema de identificación electrónica que permite a los administrados relacionarse electrónicamente con la administración de la Generalitat y su sector público.

(i) Conforme a lo anterior, se considera que la configuración del DNI, con carácter exclusivo y excluyente, como 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 (arts. 1 y 2) restringe las competencias de la Generalitat para determinar sus propios sistemas de identificación de los interesados ante las administraciones públicas catalanas. Se limitan desproporcionadamente las competencias previstas en los arts. 150 y 159 EAC, puesto que en sus sistemas de identificación deberán ir precedidas de una identificación personal que únicamente se podrá acreditar mediante el DNI. El recurso no discute la configuración del DNI como documento único en el ámbito de la seguridad pública, pero sí que implique que en todos los procedimientos administrativos se requiera siempre de la identificación mediante DNI como elemento adicional de acreditación. La determinación del DNI como documento único con suficiente valor por sí solo, para la acreditación a todos los efectos de la identidad y datos personales de su titular solo impediría la creación de otro equivalente con la misma consideración y eficacia descrita en el art. 8.1 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, es decir circunscrita al ámbito de la seguridad. Pero no debería debilitar la validez de otros sistemas de identificación y firma electrónica mediante otros documentos identificativos ni implicar que en todos los procedimientos administrativos se requiera siempre de la identificación mediante DNI como elemento adicional de acreditación. Esta modificación incide de forma decisiva en actuaciones en las que las razones identificativas no obedezcan a motivos de seguridad pública o no se enmarquen

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

en ese contexto. En estos supuestos nada debería impedir que las administraciones públicas, para el ejercicio de determinados derechos o para el acceso a servicios o prestaciones públicas, pudiesen exigir, de acuerdo con las competencias estatutariamente asumidas, que los ciudadanos deban estar en posesión de otro documento acreditativo o que en el procedimiento administrativo se puedan identificar electrónicamente también a través de sistemas distintos al DNI. La previsión de que únicamente el DNI y el DNI electrónico, sean los únicos documentos con el suficiente valor para la acreditación de la identidad y los datos personales de su titular, es una restricción para las administraciones públicas concernidas, que por ello no pueden establecer, como prevé el artículo 9.1 de la Ley 39/2015, una verificación de identidad de los interesados mediante un documento identificativo equivalente.

(ii) Las consideraciones anteriormente expuestas también cabe referirlas a las medidas introducidas en el art. 3 del Real Decreto-ley 14/2019 que modifica los apartados c) de los arts. 9.2 y 10.2 de la Ley 39/2015 incorporando una autorización estatal, previo informe vinculante por razones de seguridad, para el establecimiento de determinados sistemas de identificación por parte de las administraciones públicas. Se introduce un control preventivo para las administraciones públicas que establezcan determinados sistemas de identificación, los comprendidos en la letra c) de los arts. 9.2 y 10.2 de la Ley 39/2015, quedando al margen de esta supervisión los restantes sistemas de firma electrónica avanzada previstos en el apartado a) y sistemas de sello del apartado b) de los mencionados preceptos de la Ley 39/2015. El art. 3 incorpora una tutela inconstitucional sobre la administración electrónica de la Generalitat de Cataluña, en cuanto regula una autorización estatal, previo informe vinculante por razones de seguridad, para el establecimiento de determinados sistemas de identificación por parte de las administraciones públicas. Se trata de un control indeterminado que desplaza de forma absoluta la competencia organizativa y de ejecución de la Generalitat de Cataluña, menoscabando las competencias sobre organización y régimen jurídico que tiene reconocidas en los arts. 150 y 159 EAC. La STC 142/2018 ya reconoció que correspondía a la comunidad autónoma la función de garantizar la ciberseguridad en la prestación de los servicios de identificación electrónica y de identidad y confianza digitales por parte de los prestadores establecidos en la comunidad autónoma o que ofrezcan servicios a la administración de la comunidad autónoma y a su sector público dependiente. Se trata de funciones inherentes a las medidas de protección que resultan de la legislación en materia de administración electrónica adoptadas en el ámbito de las competencias que se refieren a su propia organización.

(iii) El art. 3.3 es contrario a las competencias de la Generalitat por la restricción del uso de sistemas de identificación basados en tecnologías de registro distribuido. Se impide la autorización de sistemas de identificación basados en estas tecnologías y sistemas de firma basados en los anteriores, en tanto no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea. Se añade que, en todo caso, cualquiera que sea el sistema de identificación basado en tecnología de registro distribuido que prevea la legislación deberá contemplar que la administración general del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública. Ambas limitaciones se consideran inconstitucionales por desplazar totalmente la competencia de la Generalitat prevista en los arts. 150 y 159 EAC.

La demanda alude a que esta tecnología de registro distribuido para sistemas de identificación no encuentra enclave en el Reglamento eIDAS. Pero de ello no cabría deducir una prohibición en el uso de dicha tecnología, siempre que se cumpla con las debidas garantías que la normativa requiere para su utilización, especialmente la relativa a protección de datos contenida en el Reglamento general de protección de datos. La demanda denuncia el carácter preventivo del desapoderamiento del uso de este tipo de tecnología por parte de las administraciones públicas competentes para definir sus propios sistemas de identificación con los usuarios de sus servicios.

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

b) Respecto de los artículos 3.1 y 2 (nueva redacción de los arts. 9.3 y 10.3 Ley 39/2015), y del art. 4 del Real Decreto-ley 14/2019, la demanda denuncia la vulneración de las competencias autonómicas que deriva de la obligación de ubicación de los sistemas de información y comunicaciones, de regulación de las transferencias de datos a terceros países u organizaciones internacionales y de control de los datos cedidos. Considera la recurrente que la regulación incorporada en el Real Decreto-ley 14/2019 es una alteración del sistema de cesión de datos en el ámbito de las administraciones públicas que opera como una tutela que no se corresponde con el sistema de distribución competencial, constituyendo una injerencia en la competencia de la Generalitat de Cataluña en materia de organización prevista en los arts. 150 y 159 EAC para el desarrollo y ejecución de sus propias competencias.

Se entiende que la obligación de ubicar los sistemas de información en territorio de la Unión Europea y especialmente en territorio español, restringe las competencias de la Generalitat y es una medida contraria a las previsiones del Reglamento general de protección de datos. Lo mismo sucede con las limitaciones de las transferencias de datos a terceros países solo para los supuestos de decisión de adecuación de la Comisión o cuando lo exija el cumplimiento de obligaciones internacionales. Por su parte, la obligación de comunicar previamente a la administración cedente, cuando se pretenda realizar un tratamiento ulterior de datos para que se pueda comprobar que no sea para fines incompatibles para el cual se recogieron, se considera una medida de control inconstitucional sobre la administración de la Generalitat de Cataluña.

(i) Por lo que se refiere a la obligación de ubicar los sistemas de información y comunicaciones, el art. 3 del Real Decreto-ley 14/2019 añade un nuevo apartado tercero para los supuestos de identificación de la letra c) de los arts. 9 y 10 de la Ley 39/2015, incorporando la obligación de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de los sistemas citados en dichos preceptos deben encontrarse situados en el territorio de la Unión Europea. Esta obligación se restringe al territorio español para el supuesto de tratamiento de categorías especiales de datos a los que se refiere el art. 9 RGPD. Asimismo el art. 4 del Real Decreto-ley 14/2019 introduce un nuevo art. 46 *bis* en la Ley 40/2015, estableciendo la obligación de ubicar y prestar dentro del territorio de la Unión Europea, los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión de determinadas bases de datos como son el 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.

Estas medidas contrastan con el objetivo del propio Reglamento general de protección de datos en el sentido de garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar obstáculos a la circulación de datos personales dentro del territorio de la Unión, precisamente para que dicha regulación fuese equivalente en todos los estados miembros. Por tanto, aquellas medidas que suponen un fraccionamiento geográfico en la aplicación de este régimen jurídico, como son las medidas incorporadas en el Real Decreto-ley 14/2019, son contrarias al derecho comunitario, máxime cuando además no se conoce cuál es la justificación de dicha norma. Estas medidas resultan extrañas por no constituir en sí mismas ninguna garantía suplementaria del propio régimen al cual están sujetas, siendo en cambio restrictivas para las administraciones públicas en su capacidad de organización de los servicios. El Reglamento general de protección de datos al definir en la Unión Europea el ámbito de aplicación territorial de la prestación de servicios en materia de protección de datos, ha delimitado implícitamente también el ámbito en el que las administraciones públicas pueden ejercer sus competencias para la organización de sus propios servicios. Una restricción territorial del ámbito en el que pueden ubicarse los datos comporta, al mismo tiempo, una vulneración del derecho europeo y una vulneración del ámbito competencial autonómico para la organización de sus servicios y la ubicación de los datos personales que gestionan.

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

(ii) Las limitaciones de las transferencias de datos a terceros países solo para los supuestos de decisión de adecuación de la Comisión o cuando lo exija el cumplimiento de obligaciones internacionales restringe las competencias de la Generalitat y la libre circulación de datos personales con las debidas garantías prevista en el Reglamento general de protección de datos. Este reglamento establece que los datos personales pueden transferirse a un país tercero si este garantiza un nivel de protección adecuado a tales datos. Se reconocen en el Reglamento diversos mecanismos jurídicos para garantizar que la transferencia de los datos se realiza con las garantías adecuadas, constituyendo la decisión de adecuación de la Comisión de la Unión Europea uno de los instrumentos previstos. Pero el Reglamento también prevé que, a falta de una decisión de la Comisión, el responsable del tratamiento puede llevar a cabo transferencias basadas en otro tipo de instrumentos jurídicos que incorporen las garantías apropiadas para la protección de los datos transferidos. Las medidas introducidas por el Real Decreto-ley 14/2019 constituyen una restricción desproporcionada que vulnera con carácter general la libre circulación de datos personales prevista en el Reglamento y limitan injustificadamente las competencias de la Generalitat en la organización de sus servicios en lo que a la definición de sus sistemas de información se refiere.

(iii) La obligación de comunicar previamente a la administración cedente tratamientos ulteriores de datos para fines distintos, contemplada en el art. 4, es una medida de control inconstitucional sobre la administración de la Generalitat de Cataluña. El Real Decreto-ley 14/2019 prevé con carácter general el acceso de las restantes administraciones públicas a los datos relativos a los interesados que obren en su poder, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad. Se afirma también que en ningún caso podrá procederse a un tratamiento ulterior de los datos para fines incompatibles con el fin para el cual se recogieron los datos personales y solo considera compatible con los fines iniciales el tratamiento ulterior para fines de archivo, investigación y estadística. Fuera de estos supuestos, el Real Decreto-ley 14/2019 establece que el tratamiento ulterior para una finalidad distinta que la administración cesionaria considere compatible, deberá ser comunicarlo previamente a la administración cedente a los efectos de que esta administración pública lo pueda comprobar. Además, cuando la administración pública cedente sea la administración general del Estado, excepcionalmente se establece que se pueda suspender la transmisión de datos por razones de seguridad nacional de forma cautelar por el tiempo estrictamente indispensable para su preservación.

c) En tercer lugar, se denuncia a continuación que los arts. 6 y 7 vulneran el orden constitucional de distribución de competencias respecto a los servicios de telecomunicaciones autonómicos.

(i) El art. 6.1 permite 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. Con respecto a la regulación anterior, se amplían las causas que justificarían dicha medida introduciendo la genérica alusión al concepto indeterminado de orden público y, por otra parte, se añade, en cuanto al objeto intervenido, los recursos e infraestructuras asociadas o elementos o nivel de red o del servicio que resulte necesario. La versión anterior de este régimen de intervención ya fue examinada por el Tribunal Constitucional en las SSTC 72/2014 y 20/2016. En aquellos supuestos no se mencionaba la referencia a las razones por las que el orden público puede justificar la asunción de la gestión directa o la intervención de redes y servicios de comunicaciones electrónicas, que solo se refería a razones de seguridad pública y defensa nacional. La referencia a la seguridad nacional puede explicarse por los ajustes debidos a la regulación de la Ley 36/2015, de 28 de septiembre, de seguridad nacional, en términos que sustituyen la anterior referencia a la defensa nacional. Sin embargo, la inclusión del orden público como causa de justificación no dispone de equivalente

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

normativo de referencia. Por tanto, queda indeterminado el ámbito o circunstancia a los que se referirá la inclusión de esta causa de justificación, suponiendo con esta imprecisión una injerencia inconstitucional en las competencias de la Generalitat de Cataluña y una restricción de los derechos fundamentales mencionados sobre secreto de las comunicaciones y libertad de información contenidos en los arts. 18 y 20 CE. Esta previsión además, se incorpora sin ninguna referencia a los límites, garantías o controles destinados a asegurar el carácter excepcional de la medida, ni su transitoriedad.

(ii) La obligación prevista en el art. 6.2 de comunicar al Ministerio de Economía y Empresa las redes de comunicaciones en régimen de autoprestación de la Generalitat de Cataluña que hagan uso del dominio público es una medida redundante que incorpora un mecanismo de control inconstitucional en cuanto comporta una invasión de las competencias autonómicas.

La demanda reconoce que esta regulación se incardina en el ámbito del régimen general de comunicaciones puesto que se trata del régimen de explotación de las redes y de prestación de los servicios de comunicaciones electrónicas, pero destaca que se trata de una obligación que se agrega a las ya existentes previamente en la Ley general de telecomunicaciones (arts. 7.3 y 10), a lo que cabe añadir las potestades de inspección y sanción. La demanda denuncia un exceso en la previsión de mecanismos informativos sobre ámbitos en los que la administración del Estado ya dispone de la correspondiente información. Por otra parte, considera que no podría ser usado en su posible proyección sobre la capacidad de intervención y asunción por la Administración General del Estado de la gestión directa o sobre 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. Se concluye por todo ello que esta obligación de comunicación constituye una vulneración de las competencias de la Generalitat de Cataluña en materia de comunicaciones electrónicas prevista en el art. 140.7 EAC y en el ámbito de la organización de sus propios recursos, de acuerdo con lo previsto en los arts. 150 y 159 EAC.

(iii) La medida cautelar consistente en el cese de la actividad presuntamente infractora, antes de iniciar un procedimiento sancionador, cuando concurran amenazas sobre el orden público, la seguridad pública y la seguridad nacional, introducida por el art. 6.5 en el régimen de infracciones y sanciones de la Ley general de telecomunicaciones se considera contraria a las competencias autonómicas. Se trata de un conjunto de medidas de intervención de las redes y servicios de las comunicaciones electrónicas en las que se desplaza de forma absoluta de su gestión a los titulares de dichas prestaciones, en este caso la Generalitat de Cataluña, amparándose en razones de seguridad nacional, seguridad pública y orden público, sin indicar las condiciones, circunstancias, duración u otros indicadores que definan las características de dicha intervención. La regulación alcanza al conjunto de las redes públicas de comunicación y recursos asociados que soportan todas las prestaciones digitales de la administración autonómica y en régimen de autoprestación cuya titularidad corresponde a la Generalitat, afectando así a las competencias autonómicas.

Esta medida cautelar es también inconstitucional por no incorporar las debidas garantías en la adopción de medidas de esta naturaleza en la medida en que omite la necesidad de motivación y la previa audiencia del afectado, con lo que se infringen los arts. 9.3 y 25 CE. Se aparta con ello de la regulación de este tipo de medidas que se contiene en el art. 56.2 de la Ley 39/2015, tratándose de una regulación que, conforme a la propia disposición adicional primera de la Ley 39/2015, prevalece sobre la general, dado su carácter de ley específica y de aplicación preferente a la regulación más completa y con las debidas garantías sobre medidas cautelares contenidas en el art. 56 de la Ley 39/2015.

(iv) Las medidas de refuerzo de la coordinación en materia de seguridad de las redes y sistemas de información del art. 7 vulneran los arts. 150 y 159 EAC, al omitir cualquier mención a las competencias autonómicas en la materia. No han tenido en cuenta las competencias que en materia de seguridad pública, seguridad ciudadana y

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

protección de datos y comunicaciones electrónicas corresponden a la Generalitat de Cataluña, especialmente cuando estas se refieren a servicios que se corresponden con el ámbito propio de competencias proyectándose la vulneración también en el ámbito de los arts. 150 y 159 EAC. No se contiene ninguna mención a los sistemas y condiciones de coordinación que afectarán a ámbitos en los que corresponde gestionar los incidentes a la Generalitat, especialmente aquellos que afecten a Cataluña y a sus instituciones, lo que contraviene también la doctrina de la STC 142/2018.

C) Vulneración de los arts. 18 y 20 CE.

Por último, la demanda sostiene que el art. 6 incurre en una vulneración mediata de los derechos fundamentales reconocidos en los arts. 18 y 20 CE (derechos personalísimos y libertades informativas), en cuanto configura un marco de intervención administrativa susceptible de afectarlos.

El acceso a internet determina en buena medida la viabilidad del ejercicio de los derechos fundamentales como es el caso del derecho a la libertad de expresión y de información (art. 20 CE) y, en cuanto que opera como infraestructura, se configura como una condición instrumental de las comunicaciones y la transmisión de datos afectando con ello formalmente a los derechos al secreto de las comunicaciones y a la intimidad (arts. 18.1 y 18.3 CE). La demanda alude a la doctrina del Tribunal Europeo de Derechos Humanos y del propio Tribunal Constitucional, reiterando la necesidad de que toda injerencia estatal en el ámbito de los derechos fundamentales y libertades públicas requiere de habilitación legal y ha destacado la importancia de que esta reúna las condiciones mínimas sobre seguridad jurídica (art. 9.3 CE) y que concrete las modalidades y extensión del ejercicio del poder otorgado con suficiente claridad para dar al individuo una protección adecuada contra la arbitrariedad. En este caso la finalidad de la incorporación de las limitaciones en la Ley general de telecomunicaciones obedece a razones de orden público, seguridad pública y seguridad nacional. Según la doctrina del Tribunal Constitucional, el concepto de seguridad publica era una noción más precisa que el de orden público, que merece un examen caso por caso siguiendo el criterio del Tribunal Europeo de Derechos Humanos, que no puede ser utilizado por la legislación de manera excesivamente expansiva hasta convertirse en un instrumento de restricción o de obstaculización de las libertades y los derechos fundamentales, especialmente en los ámbitos de los derechos de la libertad de expresión y los derechos de participación política en sentido amplio. La intervención regulada en el art. 6.1 del Real Decreto-ley 14/2019, incorporando una facultad gubernativa de intervención amplia y de alcance general sobre el conjunto de redes y servicios de las comunicaciones electrónicas introduce una potestad de enorme discrecionalidad para el Gobierno que puede activar la intervención sobre las comunicaciones electrónicas, y su carácter omnicomprensivo del conjunto de la red y los servicios que en ella operan. Junto a ello, la ausencia de previsión alguna de delimitación funcional, ni procedimiento o garantía en cuanto a los contenidos o los sujetos susceptibles de ser afectados por la intervención, convierten el precepto en una cláusula genérica de intervención gubernamental, especialmente grave, pues tampoco alude en ningún caso a la intervención judicial.

A pesar de que se considere que el nuevo art. 4.6 LGTel únicamente concierne a las infraestructuras y no se refiere a los contenidos, ni a la información, o que únicamente se intervendría el sistema con la finalidad de restablecimiento del servicio universal en supuestos de caída del sistema, la demanda entiende que esta interpretación no impide que se desprenda una afectación en el ejercicio de determinados derechos, como la libertad de expresión, por el bloqueo, la interrupción o la obstaculización del acceso universal a la red por la que circula la información y la comunicación. Tampoco se observa la necesaria proporcionalidad que ha de observar toda medida restrictiva de derechos fundamentales, pues la indeterminación, generalidad, imprecisión y ambigüedad con que está prevista pone de manifiesto que la intervención no dispone de criterios de referencia que modulen su ejercicio.

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

Mediante otrosí, la abogada de la Generalitat de Cataluña plantea incidente de recusación del magistrado don Andrés Ollero Tassara, por las causas previstas en los apartados 9 y 10 del art. 219 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (LOPJ), en términos coincidentes con el ya planteado en otros procesos constitucionales.

2. Por providencia de 25 de febrero de 2020 el Pleno, a propuesta de la Sección Primera, acordó admitir a trámite el recurso de inconstitucionalidad promovido por el Gobierno de la Generalitat de Cataluña en relación con los arts. 1, 2, 3, 4, 6 y 7; disposición adicional única; y por conexión, contra las disposiciones transitorias primera y segunda y disposición final primera del 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; dar traslado de la demanda y documentos presentados, conforme establece el art. 34 de la Ley Orgánica del Tribunal Constitucional, al Congreso de los Diputados y al Senado, por conducto de sus presidentes, y al Gobierno, a través del ministro de Justicia, al objeto de que, en el plazo de quince días, puedan personarse en el proceso y formular las alegaciones que estimaren convenientes; oír a las partes sobre la posible acumulación a este recurso del registrado con el núm. 762-2020, promovido por el Parlamento de Cataluña y publicar la incoación del recurso en el «Boletín Oficial del Estado».

3. Por diligencia de ordenación de 25 de febrero de 2020 de la secretaria de justicia del Pleno se dio cuenta de la propuesta de recusación del magistrado de este tribunal don Andrés Ollero Tassara planteada por la representación letrada del Gobierno de la Generalitat de Cataluña. Por ATC 34/2020, de 25 de febrero, se inadmitió la recusación formulada.

4. Mediante escrito registrado el día 10 de marzo de 2020, la presidenta del Congreso de los Diputados comunicó el acuerdo de la mesa de la cámara, por la que se persona en el proceso y ofrece su colaboración a los efectos del art. 88.1 de la Ley Orgánica del Tribunal Constitucional. Lo mismo hizo la presidenta del Senado por escrito que tuvo entrada en este tribunal ese día 10 de marzo de 2020.

5. La abogada de la Generalitat de Cataluña, mediante escrito registrado el día 12 de marzo de 2020, manifiesta que no tiene nada que objetar a la acumulación al presente recurso del tramitado con el número 762-2020, interpuesto por el Parlamento de Cataluña.

6. El abogado del Estado, en la representación que ostenta, se personó en el proceso por escrito registrado el día 12 de marzo de 2020, solicitando una prórroga del plazo inicialmente conferido para formular alegaciones. Prórroga que le fue concedida por diligencia de ordenación de la secretaría de justicia del Pleno de 5 de junio de 2020 en la que se prorrogó en ocho días más el plazo inicialmente concedido, a contar desde el siguiente al de expiración del ordinario.

7. Las alegaciones del abogado del Estado interesando la íntegra desestimación del recurso se registraron en este tribunal el día 17 de junio de 2020.

El escrito de alegaciones a la demanda alude, en primer lugar al objeto del recurso de inconstitucionalidad, así como a los antecedentes de la norma y manifiesta su parecer favorable a la acumulación al presente recurso del tramitado con el número 762-2020 interpuesto por el Parlamento de Cataluña.

A) Infracción del art. 86.1 CE.

Respecto de la primera cuestión planteada en la demanda, la Abogacía del Estado alega que el Real Decreto-ley 14/2019 cumple el presupuesto habilitante exigido por la doctrina constitucional. Señala que la exposición de motivos de la norma recoge cómo 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

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

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. En el debate parlamentario de convalidación se aludió especialmente a este extremo, en relación con las medidas acerca del documento nacional de identidad, de identificación ante las administraciones públicas y de ubicación de datos, con el que guardan la necesaria conexión de sentido.

En segundo término, tanto en la exposición de motivos como en el debate parlamentario se explicitan suficientemente los riesgos para los ciudadanos y para la propia administración derivados de la aceleración de la transformación digital de las administraciones públicas y, por ende, se justifica la conexión de la situación con las medidas de prevención que se concretan en el articulado en los arts. 3, 4 y 6 impugnados, es decir, las medidas de prevención como urgente respuesta a los riesgos que se describen y que legitiman la intervención del legislador de urgencia. Lo mismo sucede con el art. 7 respecto al esquema de seguridad allí previsto.

B) Infracción del sistema de distribución de competencias.

Plantea a continuación la cuestión del encuadramiento competencial de la norma impugnada, aludiendo a su disposición final primera y a la propia parte expositiva del Real Decreto-ley 14/2019, e indicando que debe hacerse referencia particular a la ciberseguridad como materia incardinada en la competencia estatal sobre seguridad pública *ex* artículo 149.1.29 CE, y que, a juicio del abogado del Estado, este es el título competencial prevalente en los arts. 1, 2, 3, 4 y 7. A tales efectos transcribe, sin citarla, partes de la fundamentación jurídica de la STC 142/2018 y señala que se trata de medidas para hacer frente a cuestiones que exceden del ámbito territorial de Cataluña y que no pueden afrontarse desde las medidas de autoprotección que para el ejercicio de su potestad de autoorganización pueda desarrollar la comunidad autónoma. El abogado del Estado destaca que el recurso del gobierno de la Generalitat de Cataluña considera en su argumentación que el título competencial prevalente es el art. 149.1.18 CE, para luego entender vulnerados los arts. 150 y 159 EAC. Sin embargo, las medidas de prevención adoptadas en el ejercicio de la competencia estatal en materia de seguridad pública están vinculadas por el Real Decreto-ley 14/2019 al interés general y tienen por finalidad proporcionar al Estado la capacidad de reacción ante situaciones que afecten a la seguridad nacional y al orden público. Se alude a la doctrina de la STC 142/2018 en la que, según el abogado del Estado, se reconoce que la creación, diseño y mantenimiento de una infraestructura de administración electrónica se integra en la potestad autonómica de autoorganización, pero al mismo tiempo, por otro lado, se postula su posible afectación a la seguridad pública y a la seguridad nacional. Enmarcados en estos términos la referencia al art. 149.1 29 CE y la competencia estatal sobre seguridad pública y ciberseguridad en su relación con la competencia autonómica de autoorganización, procede el examen concreto de los preceptos impugnados.

a) Respecto a las medidas en relación con el DNI, el abogado del Estado, tras referirse a los argumentos del recurso, cita la STC 55/2018, según la cual es perfectamente constitucional que el Estado establezca un sistema de identificación común para los interesados ante todas las administraciones públicas. Lo que hace el Real Decreto-ley 14/2019 es extender la validez del DNI electrónico para acreditar la identidad personal ante las administraciones públicas, también al ámbito de la administración digital, estableciendo un sistema de identificación común. Teniendo en cuenta que el DNI es un derecho y una obligación para todas las personas con nacionalidad española, todos los ciudadanos cuentan con este documento que les ofrece total garantía para poder acreditar su identidad ante cualquier administración pública y ejercer sus derechos y acceder a los servicios públicos. Por tanto, la regulación del DNI en los arts. 1 y 2 en nada afecta a las competencias de autoorganización de Cataluña, puesto que se permite a las comunidades autónomas regular sus propios sistemas de identificación, dentro de los límites necesarios en materia de seguridad pública, para

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

preservar el interés general. El recurso interpreta que hay una obligación de los interesados de identificarse —previa y obligatoriamente— mediante su DNI electrónico y que esto invade la competencia de la comunidad autónoma para el establecimiento de sus propios sistemas de identificación. Para el abogado del Estado esa interpretación es errónea, máxime si tenemos en cuenta que, a continuación, los arts. 3 y 4 del mismo texto legal permiten otros sistemas de identificación.

La regulación impugnada no impone este sistema como el único posible para la identificación electrónica de los interesados ante las administraciones públicas, sino que elimina la posibilidad de introducir un nuevo documento de acreditación de la identidad con el propósito de sustituirle. Esta regulación se corresponde, en el ámbito del procedimiento administrativo común, con la competencia reconocida al Estado en el art. 149.1.18 CE para establecer un sistema de identificación común ante las administraciones públicas (con cita de la STC 55/2018). En cuanto a su regulación como el único documento con suficiente valor por sí solo para la acreditación también en el ámbito de la administración digital de la identidad del titular, el abogado del Estado señala que no impide la posibilidad de otros sistemas de identificación, pero sí que se dote a esos otros sistemas de la misma consideración y eficacia descrita en el artículo 8.1 de la Ley Orgánica 4/2015, de 30 de marzo, para el DNI.

Respecto al art. 3 del Real Decreto-ley 14/2019, se analiza en primer lugar la exigencia de previa autorización estatal para la utilización de determinados sistemas de identificación y firma por motivos de seguridad pública vinculados a la ciberseguridad. El abogado del Estado alude a los diferentes sistemas previstos en el Reglamento eIDAS, señalando que determinadas exigencias de seguridad no se aplican a los sistemas de identificación que se despliegan conforme a lo previsto en el artículo 9.2 c) y 10.2 c) de la Ley 39/2015, por lo que tales sistemas pasan a estar sujetos a una autorización previa de verificación de su seguridad. La verificación trae causa de la necesidad de salvaguardar la seguridad pública en el proceso de transformación digital de la administración, que extiende el riesgo de ataques que impactan en la seguridad pública y en la propia intimidad de los ciudadanos. La competencia autonómica para autoorganizar la ciberseguridad de sus sistemas de administración electrónica se entiende sin perjuicio de la competencia exclusiva del Estado en materia de seguridad pública, proyectada en este caso sobre la ciberseguridad aplicada a las bases del régimen jurídico de la administración electrónica en el conjunto de las administraciones públicas. Se trata de una medida perfectamente coherente con la doctrina constitucional establecida en la STC 55/2018, de forma que cumpliendo una función típica de las normas de procedimiento administrativo común, se garantiza un «tratamiento común de los administrados ante todas las administraciones públicas», salvaguardando su ciberseguridad con un criterio transversal de seguridad pública aplicado a determinados casos y sin afectar en modo alguno los amplios márgenes de autoorganización de las administraciones públicas. Las diferentes administraciones públicas pueden seguir aceptando los sistemas de identificación electrónica que estimen convenientes, una vez garantizada su seguridad. Lo anteriormente expuesto es de aplicación a los sistemas de firma electrónica admitidos en las relaciones con las administraciones públicas (art. 10.4 y 5 de la Ley 39/2015).

Por otra parte, el abogado del Estado considera que la nueva disposición adicional sexta de la Ley 39/2015, se limita a restringir provisionalmente el uso de los sistemas de identificación basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores pero únicamente mientras no haya 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. Con la medida prevista en el Real Decreto-ley 14/2019 se pretende, de forma cautelar y temporal, suspender la posibilidad de implantar esta tecnología en el ámbito de la identificación y firma electrónicas ante las administraciones públicas, hasta que en el marco de la Unión Europea se produzcan desarrollos legislativos al efecto, que permitirán proceder a su eventual implantación,

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

cuando las condiciones de seguridad, interoperabilidad y protección de derechos se encuentren oportunamente definidas y acordadas.

b) Acerca de la regulación sobre la ubicación de determinadas bases de datos y en torno a la cesión de datos a otras administraciones públicas prevista en los arts. 3 y 4 el abogado del Estado indica que la obligación de localización de los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de los sistemas de identificación del art. 9.2 c) y de firma del 10.2 c) de la Ley 39/2015 tiene por objeto proteger los datos sensibles que los ciudadanos entregan a las administraciones públicas, que de este modo quedan sujetos a la normativa europea, evitando la posibilidad de su manipulación y tratamiento en ubicaciones que no están sujetas a la legislación comunitaria. Hace notar que, a estos efectos, se incluyen también como lugares en los que es posible albergar estos sistemas y datos, aquellos que no siendo territorio de la Unión Europea han sido objeto de una decisión de adecuación de la Comisión Europea. En definitiva aquellos que también cumplen con los requisitos de protección a los ciudadanos con las mismas garantías que se establecen en la Unión Europea. Descarta a continuación las denuncias de vulneración del Reglamento general de protección de datos, pues no es tarea propia de la jurisdicción constitucional el examen de este tipo de cuestiones, sin que tampoco sea posible apreciar una contradicción material con el Derecho de la Unión Europea. Desde el punto de vista competencial se trata de una medida perfectamente consistente con lo establecido en la STC 55/2018, de forma que cumpliendo una función típica de las normas de procedimiento administrativo común, se garantiza un tratamiento común de los administrados ante todas las administraciones públicas, salvaguardando su ciberseguridad con un criterio transversal de seguridad pública aplicado a determinados casos y sin afectar en modo alguno los amplios márgenes de autoorganización de las administraciones públicas.

Por lo que respecta a las transmisiones de datos entre administraciones públicas del art. 4.2, que da nueva redacción al art. 155 de la Ley 40/2015, se argumenta que no tiene por objeto regular el derecho fundamental a la protección de datos personales, sino que introduce medidas de régimen jurídico de las administraciones públicas en las que las limitaciones que se imponen son conformes a la normativa de protección de datos y con el propio Reglamento general de protección de datos. La limitación de las transferencias internacionales de datos se ampara en los arts. 45 y 49.5 RGPD, que prevén que para que pueda realizarse una transferencia de datos personales a un tercer país u organización internacional es preciso que la Comisión haya decidido que el país u organización de que se trate garantizan un nivel de protección adecuado. Y que, en ausencia de esta decisión, el derecho de los Estados miembros podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional. Por lo que se refiere a la prohibición de tratamiento incompatible (art. 155.2 Ley 40/2015), debe recordarse que uno de los principios básicos aplicable al tratamiento de datos personales es el de limitación de la finalidad, actualmente recogido en el art. 5.1 b) RGPD, de modo que los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. En cuanto a las medidas en caso de afección a la seguridad nacional el abogado del Estado recuerda que el mencionado Reglamento no se aplica a las actividades relativas a la seguridad nacional.

c) Sobre el art. 6, relativo a los cambios introducidos en la Ley general de telecomunicaciones, el abogado del Estado indica en primer lugar que los preceptos impugnados se encuadran en el art. 149.1.21 CE, recordando la doctrina constitucional al respecto (cita las SSTC 8/2012 y 235/2012, entre otras).

En cuanto a las modificaciones en el art. 4.6 LGTel resalta que añade el orden público a las razones que justifican la asunción de la gestión directa o la intervención de redes y servicios de comunicaciones electrónicas por el Gobierno; amplía el objeto intervenido que se extiende a cualquier infraestructura, recurso asociado o elemento o

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

nivel de la red o del servicio que sea necesario, y elimina la referencia a la ley de contratos aplicable a las administraciones públicas.

A continuación, el abogado del Estado recalca que las medidas contenidas en el art. 4.6 tienen como finalidad garantizar el pleno ejercicio de los derechos fundamentales y no son nuevas, pues tradicionalmente han formado parte del régimen de las telecomunicaciones. El objetivo de la habilitación concedida al Gobierno no puede ser otro que el de restablecer el suministro de la red o servicio de que se trate, devolviéndolo a la situación anterior a ese «anormal funcionamiento» al que se refiere el último párrafo del artículo 4.6. La gestión o «intervención» a las que alude el precepto, en ningún caso se refiere a una intervención de comunicaciones privadas sino meramente a una gestión material o a una toma de decisiones dirigidas a restablecer el normal funcionamiento de la red o servicio. La Ley general de telecomunicaciones no afecta al control de los contenidos que circulan por las redes, por lo que toda intervención conforme al art. 4.6 no puede tener otro objetivo que el restablecimiento de redes o servicios, no existiendo otro epígrafe que se refiera a este supuesto, ya que el último párrafo del artículo 4.6 deja claro que se refiere a los casos de gestión directa o intervención «a los que se refieren los párrafos anteriores».

Por tanto, dicho restablecimiento sí afecta a derechos fundamentales en cuanto restituir sus posibilidades materiales de ejercicio, precisamente porque tiene por objetivo eliminar el bloqueo, interrupción u obstaculización del acceso a las redes o servicios y con ello preservar el ejercicio de los derechos constitucionalmente garantizados. Los intereses perseguidos por el artículo 4.6 LGTel son intereses «públicos» plasmados en la finalidad de mantener bienes jurídicos de gran trascendencia en un Estado democrático de derecho, como el orden público, la seguridad pública o la seguridad nacional. Por tanto, este precepto no habilita al Gobierno para adoptar la gestión directa o para intervenir una red «privada» o en autoprestación, en la medida en que el marco jurídico de las telecomunicaciones se refiere a operadores que actuando bajo los principios de libre mercado y competencia plena, instalan y despliegan sus redes y prestan servicios de comunicaciones electrónicas a los ciudadanos y empresas. El art. 4.6 LGTel no se refiere a las redes privadas o en autoprestación, sino solamente a aquellos casos en los que la red es pública, en el sentido de que con ella el titular presta servicios disponibles al público en general, esto es, a los ciudadanos, a las empresas, a las administraciones y a otros operadores, y por tanto, solo cuando las redes o servicios de telecomunicaciones son servicios de interés general que se prestan en libre competencia.

El abogado del Estado recuerda la doctrina de la STC 72/2014, que consideró conforme con el orden competencial la redacción anterior de este precepto; conclusión que es predicable también ahora por cuanto se trata de una medida extraordinaria y temporal, que solo puede adoptarse, de acuerdo a los principios de justificación objetiva, racionalidad, motivación y proporcionalidad, por el tiempo estrictamente necesario y cuando no existan otras medidas menos restrictivas para la garantía o restablecimiento de la red o servicio. Es cierto que el precepto no delimita en detalle los límites de esta potestad, más allá de predicar su excepcionalidad y transitoriedad, pero, en primer lugar, no existe en este caso peligro alguno de vulneración de derechos fundamentales sino únicamente la pretensión de garantía de los mismos, y en segundo lugar, resulta evidente que ante situaciones excepcionales resultará necesario adoptar medidas igualmente extraordinarias que resulta imposible prever de antemano. Eso no supone que estas medidas no estén sometidas a la necesaria justificación y control, debiendo ser en el momento de su adopción y control judicial posterior cuando habrá de analizarse el necesario cumplimiento de los principios de necesidad, justificación objetiva, motivación, proporcionalidad, eficacia y no discriminación que, entre otros, deben guiarlas. En definitiva, las modificaciones introducidas en nada afectan al contenido esencial del precepto, ni por tanto a su incidencia en competencias autonómicas o derechos fundamentales, ya que se trata de modificaciones mínimas y puntuales, exclusivamente dirigidas a facilitar la comprensión y aplicación del precepto y a alinear su redacción con la de otras normativas ya en vigor.

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

Para el abogado del Estado la introducción de una referencia al orden público en nada modifica el sentido del precepto, en la medida en que este concepto ya forma parte o se encuadra dentro del concepto más general de seguridad pública, el cual a su vez se encuadra dentro del término más omnicomprensivo de la seguridad nacional (cita las SSTC 86/2014 y 84/2016). Esta referencia al orden público se conecta también con las competencias estatales en materia de ciberseguridad y concuerda con las referencias que a esta cuestión se incluyen en la Ley de seguridad nacional y en el propio Código europeo de las comunicaciones electrónicas. Se limita a introducir conceptos que figuran en las últimas normas relativas a telecomunicaciones y situaciones de seguridad nacional, clarificando que las telecomunicaciones, en cuanto servicio de interés general, han de ser protegidas de cualquier atentado a la convivencia que impida su normal funcionamiento. Similar razonamiento cabe hacer respecto a la inclusión de una referencia expresa a que el objeto de intervención o gestión directa no solo puede ser una red de comunicaciones electrónicas sino también cualquier infraestructura, recurso asociado o elemento o nivel de la red o del servicio que sea necesario. Esa modificación responde a la evolución del régimen de las telecomunicaciones que ha pasado a incluir en su regulación los elementos físicos que resultan necesarios poder instalar y desplegar una red. Se refuerzan así las potestades del Gobierno para actuar sobre las redes y servicios de comunicaciones electrónicas en supuestos que atenten al orden público, la seguridad pública o la seguridad nacional, siempre con la finalidad de restablecer o mantener el funcionamiento de esas redes o servicios cuyo normal funcionamiento se ha visto alterado, tal como ha interpretado el Tribunal Constitucional en la STC 72/2014. El abogado del Estado reitera que este precepto no afecta a las redes privadas ni a los servicios de comunicaciones electrónicas en autoprestación, ya sean titularidad de un ciudadano, de una empresa privada o de una administración pública, y, por tanto, no afecta a las redes y servicios en autoprestación de la Generalitat, no menoscabando o vulnerando en consecuencia las competencias de la Comunidad Autónoma de Cataluña.

Por último, la eliminación de la referencia a la Ley de contratos del sector público responde a una mejora técnica del precepto, eliminando una referencia errónea, ya que, al no tratarse de servicios públicos sino de redes y servicios que son calificados de interés general, pero que se prestan en régimen de libre competencia, no existía ningún precepto de la Ley de contratos que pudiera resultar aplicable. En cuanto a la obligación de informe preceptivo de la Comisión Nacional de los Mercados y la Competencia (CNMC), la contestación a la demanda señala que su previsión en relación al supuesto de gestión directa por incumplimiento de obligaciones de servicio público no tiene por objetivo establecer limitaciones a dicha gestión, sino constatar que se ha producido dicho incumplimiento y que existe el motivo habilitador para la actuación del Gobierno.

Sobre las modificaciones introducidas en el art. 6.3 LGTel, en relación con la disposición adicional única del Real Decreto-ley 14/2019, el abogado del Estado considera que la mera comunicación que allí se prevé no es susceptible de afectar a las competencias autonómicas, en cuanto que se incardina dentro de los principios de coordinación, cooperación y eficacia. Responde a la finalidad de garantizar, de conformidad con la normativa comunitaria, que no existan distorsiones a la competencia que puedan conllevar la apertura de procedimientos de infracción al Reino de España por incumplimiento de la normativa sobre ayudas de Estado a la que se refieren los artículos 107 y 108 del Tratado de Funcionamiento de la Unión Europea, debidas a actuaciones de operadores públicos en zonas en las que existe plena competencia entre operadores privados. Si bien es cierto que se aumenta mínimamente la carga administrativa, no parece que en las relaciones entre administraciones públicas pueda señalarse este como argumento para defender su inconstitucionalidad, no existiendo, en todo caso, afectación alguna de las reglas establecidas en el art. 9 LGTel, ni vulneración de competencias autonómicas estatutariamente reconocidas.

La constitucionalidad de la regulación de las medidas cautelares de la nueva redacción del art. 81.1 LGTel es defendida por el abogado del Estado, señalando que estas medidas vienen contempladas en el art. 30.6 del Código europeo de las

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

comunicaciones electrónicas, medidas a las que les son aplicables las garantías que, especialmente en el ámbito del procedimiento sancionador, protegen a los administrados, como los requisitos de motivación, necesidad de su adopción o proporcionalidad, a los que se refiere el art. 56.2 de la Ley 39/2015. Por lo demás, el precepto establece las condiciones en las que puede declararse el cese de la actividad sin audiencia previa del presunto infractor y se aplica a todo aquel que haya cometido la actividad infractora, con independencia de que se trate de una persona física o jurídica, pública o privada.

El abogado del Estado también niega que exista vulneración de derechos fundamentales en la nueva regulación del art. 4.6 LGTel, en la medida en que este precepto no habilita al Gobierno a intervenir servicios digitales ni servicios audiovisuales o medios de comunicación, por cuanto no se han alterado el ámbito objetivo y las definiciones que vienen establecidas en la Ley general de telecomunicaciones. Insiste el abogado del Estado en que la finalidad del precepto no es el control de la red o la interrupción de acceso a internet o a parte de ella, sino su mantenimiento o restablecimiento ante situaciones provisionales y extraordinarias de anormal funcionamiento por motivos tasados, que son los recogidos en el propio art. 4.6 LGTel.

Finalmente, se descarta que el art. 7 del Real Decreto-ley 14/2019 infrinja las competencias autonómicas, en cuanto se limita a incorporar medidas para reforzar la coordinación ante incidentes de seguridad en las redes y sistemas de información que encuentran amparo en las competencias estatales en materia de telecomunicaciones y de seguridad pública (art. 149.1.21 y 29 CE).

8. Con fecha 10 de febrero de 2023, el magistrado don Juan Carlos Campo Moreno formuló su abstención en relación con el presente proceso constitucional, abstención que fue considerada justificada por el Pleno en el auto de 21 de febrero de este año dictado en el recurso de inconstitucionalidad núm. 4129-2018, lo que dio lugar a apartarle definitivamente del presente recurso y de todas sus incidencias.

9. Por providencia de 21 de febrero de 2023, se señaló para deliberación y votación de la presente sentencia el día 23 del mismo mes y año.

II. Fundamentos jurídicos

1. Objeto del recurso y posiciones de las partes.

El objeto de la presente resolución es resolver el recurso de inconstitucionalidad interpuesto por el Gobierno de la Generalitat de Cataluña contra los arts. 1, 2, 3, 4, 6 y 7; la disposición adicional única; las disposiciones transitorias primera y segunda y la disposición final primera del 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.

Los preceptos impugnados se refieren a la modificación de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (en adelante, LOPSC) y de la Ley 59/2003, de 19 de diciembre, de firma electrónica, en cuanto al DNI y DNI electrónico, respectivamente (arts. 1 y 2); a la modificación de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, en cuestiones relativas a la administración electrónica (art. 3 y disposición transitoria primera); a la reforma de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, en aspectos relacionados con la ubicación de los sistemas de información y comunicaciones para el registro de datos y las transmisiones de datos entre administraciones públicas (art. 4 y disposición transitoria segunda); a la modificación de la Ley 9/2014, de 9 de mayo, general de telecomunicaciones, respecto a la potestad gubernamental de intervención de redes y servicios de comunicaciones, a la adopción de medidas previas al procedimiento sancionador, así como en relación a los deberes de suministro de información que se imponen (art. 6 y disposición adicional única) y a la

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

reforma del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en lo relativo a la organización para la respuesta a incidentes de seguridad informática (art. 7). La disposición final primera relaciona los títulos competenciales estatales a cuyo amparo se dicta la norma.

La interposición del recurso se fundamenta en argumentos que pueden agruparse en torno a tres tipos de infracciones constitucionales:

a) Se considera que se incumplen los requisitos previstos en el art. 86 CE respecto a la utilización del decreto-ley. La demanda argumenta que no se acredita la concurrencia de una situación excepcional que justifique el recurso a la norma de urgencia. Tampoco habrían quedado acreditadas la emergencia o urgencia, en el sentido de que las medidas aprobadas no hubieran podido ser adoptadas mediante el procedimiento legislativo ordinario o, en su caso, de urgencia. La falta de identificación de la situación extraordinaria que se quiere afrontar determina también que no pueda analizarse si las medidas adoptadas responden de forma congruente con la situación que ha justificado su adopción.

b) Se alega que determinadas previsiones del Real Decreto-ley 14/2019 no se adecuan al orden constitucional y estatutario de distribución de competencias. Los arts. 1 a 4 serían, de uno u otro modo, contrarios a las competencias autonómicas para la organización de su propia administración reconocidas en los arts. 150 y 159 EAC, en relación específicamente a la creación y mantenimiento de servicios de administración electrónica. Los arts. 3 y 4 serían también contrarios a las competencias autonómicas en lo relativo a la obligación de ubicar los sistemas de información en territorio de la Unión Europea y especialmente en territorio español. Lo mismo sucede con las limitaciones de las transferencias de datos a terceros países. Por su parte, la obligación de comunicar previamente a la administración cedente, cuando se pretenda realizar un tratamiento ulterior de datos para fines distintos, a fin de que se pueda comprobar que el tratamiento posterior no sea para fines incompatibles con aquel para el que se recogieron, se considera una medida de control inconstitucional sobre la administración de la Generalitat de Cataluña. Asimismo se alega que los arts. 6 y 7 del Real Decreto-ley 14/2019 exceden de las competencias estatales en materia de telecomunicaciones y seguridad de las redes y sistemas de información (art. 149.1.21 CE), vulnerando las competencias de la comunidad autónoma respecto a los servicios de telecomunicaciones autonómicos (arts. 150 y 159 EAC).

c) La intervención regulada en el art. 6.1 del Real Decreto-ley 14/2019, al dar nueva redacción al art. 4.6 LGTel, incorporando una facultad gubernativa de intervención amplia y de alcance general sobre el conjunto de redes y servicios de las comunicaciones electrónicas, amparada en el orden público, contraviene las garantías de los derechos constitucionales de los arts. 18 y 20 CE, específicamente en relación con las telecomunicaciones. Asimismo, al art. 6.5 se le reprocha que reduce las garantías exigibles para la adopción de medidas provisionales en el procedimiento sancionador.

Como se ha expuesto pormenorizadamente en el relato de antecedentes, el abogado del Estado ha negado las vulneraciones constitucionales denunciadas, interesando, en consecuencia, la íntegra desestimación del recurso.

2. Observaciones sobre la pervivencia del objeto del recurso de inconstitucionalidad.

Después de la interposición del recurso de inconstitucionalidad núm. 718-2020, el 4 de febrero de 2020, el contenido del 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, ha sido modificado en varias ocasiones, a través de la revisión de las leyes que este Real Decreto-ley 14/2019 venía a modificar en sus siete preceptos. Concretamente han sido derogadas la Ley 59/2003, de 19 de diciembre, de firma electrónica (y por tanto modificado en el sentido en que se verá el contenido del art. 2 del Real Decreto-

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

ley 14/2019) y la Ley 9/2014, de 9 de mayo, general de telecomunicaciones (a la que introdujo modificaciones el artículo 6 del Real Decreto-ley 14/2019). Por su parte, ha sido modificada —en parte de los preceptos cuya regulación se impugna en el presente recurso— la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (a la que se refiere el artículo 3 del Real Decreto-ley 14/2019).

Antes de analizar el contenido de las modificaciones normativas que afectan al objeto del recurso conviene recordar, citando el fundamento jurídico 1 del ATC 147/2009, de 12 de mayo, que este tribunal viene manteniendo que, en el caso de recursos de inconstitucionalidad como el que ahora nos ocupa, «puede decirse que por regla general la modificación, derogación o pérdida de vigencia de los preceptos legales controvertidos conlleva la extinción del objeto del proceso constitucional (al respecto, STC 196/1997, de 13 de noviembre, FJ 2)». Ello se aplica en particular cuando nos encontramos ante impugnaciones basadas en motivos sustantivos, como puede ser la vulneración de derechos fundamentales, en cuyo caso, la sola constatación de que la redacción impugnada ha dejado de estar en vigor determina, como regla general, la pérdida sobrevenida de objeto del recurso de inconstitucionalidad [por todas, STC 140/2016, FJ 2 b)].

A esta regla general válida para los recursos de inconstitucionalidad, sin embargo, le acompañan dos excepciones que se identifican claramente en nuestra jurisprudencia previa.

La primera se refiere a la impugnación, mediante recurso abstracto, de la constitucionalidad de los decretos-leyes por falta de concurrencia del presupuesto habilitante (*ex* art. 86.1 CE). En estos casos una reiterada jurisprudencia sostiene que la modificación legislativa posterior del decreto-ley impugnado, no impide a la jurisdicción constitucional controlar si la potestad reconocida al Gobierno por el art. 86.1 CE se ejerció siguiendo los requisitos establecidos en dicho precepto constitucional. La razón de ser del mantenimiento del interés del recurso y, por tanto, de la conservación del objeto del mismo, es asegurar que el Tribunal vele «por el recto ejercicio de la potestad de dictar decretos-leyes, dentro del marco constitucional, decidiendo la validez o invalidez de las normas impugnadas, sin atender a su vigencia o derogación en el momento en que se pronuncia el fallo [SSTC 31/2011, de 17 de marzo, FJ 2, y 182/2013, de 23 de octubre, FJ 2 B)]» (STC 34/2017, de 1 de marzo, FJ 2).

La segunda excepción se identifica en materia de impugnaciones de base competencial, que se articulan a través del recurso de inconstitucionalidad dirigido contra una norma con rango de ley posteriormente derogada o modificada. Aquí, la posición de la jurisprudencia constitucional se basa en el mismo principio sobre la pervivencia del objeto del recurso que inspira la excepción relativa al recurso contra decretos-leyes.

En estos supuestos, el mantenimiento del objeto del recurso dependerá de si la nueva normativa, sustitutoria de la impugnada, viene a plantear o no los mismos problemas competenciales señalados en el recurso de inconstitucionalidad [por todas, STC 134/2011, de 20 de julio, FJ 2 b)]. Si los problemas competenciales subsisten, ello justifica la pervivencia del objeto del recurso de la competencia para resolverlo del Tribunal porque «la función de preservar los ámbitos respectivos de competencias no puede quedar enervada por la sola derogación o modificación de las disposiciones cuya adopción dio lugar al litigio» (STC 18/2016, de 4 de febrero, FJ 2, y jurisprudencia allí citada). Por ello, si «la normativa en relación con la cual se trabó el conflicto no es simplemente derogada, sino parcialmente sustituida por otra que viene a plantear en esencia los mismos problemas competenciales, la doctrina de este tribunal avala la conclusión de la no desaparición del objeto del conflicto» [STC 134/2011, FJ 2 b)].

El anterior planteamiento exige analizar, artículo por artículo de los que se han visto derogados o modificados, si las nuevas disposiciones que han venido a sustituirlos plantean los mismos problemas competenciales que se suscitan en el recurso de inconstitucionalidad, de modo tal que si los problemas siguen presentes, se considerará persistente el objeto del recurso.

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

(i) El impugnado art. 2 del Real Decreto-ley 14/2019 modifica el art. 15.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que viene a ser derogada por la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. El art. 15.1 de la Ley 59/2003, en la redacción dada por el precepto impugnado, se refería al documento nacional de identidad electrónico, cuestión a la que hace asimismo referencia la disposición adicional tercera de la ley 6/2020, que establece en su apartado primero que el «el Documento Nacional de Identidad electrónico es el Documento Nacional de Identidad que permite acreditar 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, así como la firma electrónica de documentos». Por tanto, la redacción cuestionada en el presente recurso de inconstitucionalidad se lleva íntegramente a la disposición adicional tercera de la Ley 6/2020. Debe entenderse, por tanto, que el problema competencial suscitado respecto del art. 2 del Real Decreto-ley 14/2019 no ha desaparecido del ordenamiento jurídico y, por tanto, se mantiene este concreto objeto del recurso, sobre el que deberemos pronunciarnos.

(ii) El art. 3 del Real Decreto-ley, modifica los arts. 3, 10 y la disposición adicional sexta de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas. Algunos apartados de los arts. 9 y 10 serán sucesivamente modificados por la Ley 11/2022, de 28 de junio, general de telecomunicaciones.

Concretamente, el art. 9.2 c) de la Ley 39/2015, será modificado por la disposición final 1.1 LGTel, resultando que la nueva redacción de este apartado es la siguiente: «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 y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud. 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)».

Por su parte, el art. 10.2 c) de la Ley 39/2015, queda modificado por la disposición final 1.2 LGTel, siendo su redacción actual la que sigue: «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 y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud. 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)».

De la nueva redacción, que no hace referencia al sistema de clave concertada en particular, se deduce que el sistema previsto en el Real Decreto-ley 14/2019, que contemplaba que los sistemas de clave concertada u otros sistemas previstos por las

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

administraciones debían ser previamente autorizados por la Secretaría General de Administración Digital, en las condiciones previstas en el precepto, ha sido sustituido por un modelo de comunicación previa acompañada de declaración responsable, que solo excepcionalmente, y mediante intervención jurisdiccional, puede encontrar oposición de la Secretaría General de Administración Digital. Por tanto, la modificación normativa ha hecho desaparecer el motivo de impugnación, porque ha sustituido el modelo de autorización, que era el considerado inconstitucional por los recurrentes por oposición a los arts. 150 y 159 EAC, por el modelo de comunicación previa acompañado de declaración responsable. El recurso de inconstitucionalidad en este punto se ha visto afectado por una pérdida sobrevenida del objeto, por lo que el Tribunal no dará respuesta a la queja relativa a los apartados 9.2 c) y 10.2 c) de la Ley 39/2015 en la redacción dada por el art. 3.1 y 2 del Real Decreto-ley 14/2019.

(iii) El art. 6 Real Decreto-ley 14/2019 modifica varios preceptos de la Ley 9/2014, de 9 de mayo, general de telecomunicaciones. Esta fue derogada, a excepción de su disposición adicional decimosexta y las disposiciones transitorias séptima, novena y duodécima, por la disposición derogatoria única a) de la Ley 11/2022, de 28 de junio, general de telecomunicaciones. No obstante, los contenidos de la antigua Ley general de telecomunicaciones se mantienen en buena medida en la nueva Ley general de telecomunicaciones y, en particular, lo hacen respecto de lo regulado en el art. 6 del Real Decreto-ley 14/2019.

El antiguo art. 4 de la Ley 9/2014 (rubricado «Servicios de telecomunicaciones para la defensa nacional, la seguridad pública, la seguridad vial y la protección civil»), pasa a ser en el art. 4 de la Ley 11/2022 (servicios de telecomunicaciones para la seguridad nacional, la defensa nacional, la seguridad pública, la seguridad vial y la protección civil). El apartado 6 de la primera, que es el que interesa al objeto del presente recurso, pasa a tener, en la segunda, la siguiente dicción literal:

«6. El Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la administración general del Estado de la gestión directa de determinados servicios de comunicaciones electrónicas disponibles al público, distintos de los servicios de comunicaciones interpersonales, independientes de la numeración o de la explotación de ciertas redes públicas de comunicaciones electrónicas, para garantizar la seguridad pública y la seguridad nacional, en los términos en que dichas redes y servicios están definidos en el anexo II, excluyéndose en consecuencia las redes y servicios que se exploten o presten íntegramente en autoprestación. Esta facultad excepcional y transitoria de gestión directa podrá afectar a cualquier infraestructura, recurso asociado o elemento o nivel de la red o del servicio que resulte necesario para preservar o restablecer la seguridad pública y la seguridad nacional.

En ningún caso esta intervención podrá suponer una vulneración de los derechos fundamentales y libertades públicas reconocidas en el ordenamiento jurídico.

Asimismo, en el caso de incumplimiento de las obligaciones de servicio público a las que se refiere el título III, el Gobierno, previo informe preceptivo de la Comisión Nacional de los Mercados y la Competencia, e igualmente con carácter excepcional y transitorio, podrá acordar la asunción por la administración general del Estado de la gestión directa de los correspondientes servicios o de la explotación de las correspondientes redes. En este último caso, podrá, con las mismas condiciones, intervenir la prestación de los servicios de comunicaciones electrónicas.

Los acuerdos de asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refieren los párrafos anteriores se adoptarán por el Gobierno por propia iniciativa o a instancia de una administración pública competente. En este último caso, será preciso que la administración pública tenga competencias en materia de seguridad o para la prestación de los servicios públicos afectados por el anormal funcionamiento del servicio o de la red de comunicaciones electrónicas. En el supuesto de que el procedimiento se inicie a instancia de una Administración distinta de la del Estado, aquella tendrá la consideración de interesada y podrá evacuar informe con carácter previo a la resolución final.

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

Los acuerdos de asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refiere este apartado deberán ser comunicados por el Gobierno en el plazo de veinticuatro horas al órgano jurisdiccional competente para que, en un plazo de cuarenta y ocho horas, establezca si los mismos resultan acordes con los derechos fundamentales y libertades públicas reconocidas en el ordenamiento jurídico, procediendo a su anulación en caso negativo.»

Se observa, tras la lectura atenta del precepto, que en la nueva redacción ha desaparecido la alusión al orden público como causa justificativa de la asunción de la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicos por parte de la administración general del Estado. Siendo esta alusión, contenida en la anterior redacción del precepto, la que sustentaba la queja de inconstitucionalidad contenida en el escrito de demanda, al entender los recurrentes que dicha mención a un término impreciso suponía una injerencia en las competencias de la Generalitat de Cataluña, su eliminación hace desaparecer asimismo el objeto del recurso de inconstitucionalidad en este punto.

(iv) El artículo 6.2 del Real Decreto-ley 14/2019 modifica el art. 6.3 LGTel respecto de los «requisitos exigibles para la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas». En la nueva Ley general de telecomunicaciones, de 28 de junio de 2022, aquel precepto pasa a ser el art. 6 («Requisitos exigibles para el suministro de las redes y la prestación de los servicios de comunicaciones electrónicas»), en su apartado séptimo, con la siguiente dicción:

«7. Las administraciones públicas comunicarán al Ministerio de Asuntos Económicos y Transformación Digital toda instalación o explotación de redes de comunicaciones electrónicas en régimen de autoprestación que haga uso del dominio público, tanto si dicha instalación o explotación se realiza de manera directa, a través de cualquier entidad o sociedad dependiente de ella o a través de cualquier entidad o sociedad a la que se le haya otorgado una concesión o habilitación al efecto.

El régimen de autoprestación en la instalación o explotación de dicha red puede ser total o parcial, y por tanto dicha comunicación deberá efectuarse aun cuando la capacidad excedentaria de la citada red pueda utilizarse para su explotación por terceros o para la prestación de servicios de comunicaciones electrónicas disponibles al público.

En el caso de que se utilice o esté previsto utilizar, directamente por la administración pública o por terceros, la capacidad excedentaria de estas redes de comunicaciones electrónicas en régimen de autoprestación, el Ministerio de Asuntos Económicos y Transformación Digital verificará el cumplimiento de lo previsto en el artículo 13. A tal efecto, la administración pública deberá proporcionar al Ministerio de Asuntos Económicos y Transformación Digital toda la información que le sea requerida a efecto de verificar dicho cumplimiento.

Mediante real decreto podrán especificarse aquellos supuestos en que, en atención a las características, la dimensión de la instalación o la naturaleza de los servicios a prestar, no resulte necesario que las administraciones públicas efectúen la comunicación a que se refiere este apartado sobre la instalación de redes de comunicaciones electrónicas en régimen de autoprestación que haga uso del dominio público.»

La innovación legislativa, en este caso, se centra en el último párrafo del precepto, en el que prevé un desarrollo reglamentario que contemple eventuales excepciones a la comunicación a que se refiere el apartado. En todo caso, la causa de inconstitucionalidad asociada al precepto en la versión que introduce el art. 6.2 del Real Decreto-ley 14/2019, esto es la mera existencia de la obligación de comunicación de las redes en régimen de autoprestacion, no ha dejado de ser objeto del recurso, por cuando la obligación sigue existiendo sin perjuicio del futuro reconocimiento reglamentario de algunas excepciones a dicha obligación.

(v) Por último, el art. 6.5 del Real Decreto-ley 14/2019, da nueva redacción al art. 81.1 de la Ley general de telecomunicaciones, que pasa a ser el art. 111.1 de la Ley

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

general de telecomunicaciones de 2022. La nueva redacción de este precepto, referido a la suspensión cautelar de la actividad infractora antes de incoarse el procedimiento sancionador, es la siguiente:

«1. Previamente al inicio del procedimiento sancionador, podrá ordenarse por el órgano competente del Ministerio de Asuntos Económicos y Transformación Digital o de la Comisión Nacional de los Mercados y la Competencia, mediante resolución motivada sin audiencia previa, el cese de la presunta actividad infractora cuando existan razones de imperiosa urgencia basada en alguno de los siguientes supuestos:

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 de la supuesta actividad infractora puedan producirse perjuicios graves al funcionamiento de los servicios de seguridad pública, protección civil y de emergencias;
d) cuando se interfiera gravemente a otros servicios o redes de comunicaciones electrónicas;
e) cuando cree graves problemas económicos u operativos a otros proveedores o usuarios de redes o servicios de comunicaciones electrónicas o demás usuarios del dominio público radioeléctrico.»

La innovación legislativa en este precepto viene dada por la previsión expresa de que la resolución que adopta la suspensión cautelar deba ser motivada. La ausencia de motivación era objeto del recurso de inconstitucionalidad en relación con la eventual vulneración de los arts. 9.3 y 25 CE, pero tratándose estas de quejas ajenas a la eventual lesión de las competencias autonómicas, la mera modificación de la norma acarrea la pérdida de objeto del recurso en este punto. En cambio, los argumentos vinculados al hecho de que la medida cautelar es contraria a las competencias autonómicas, en cuanto puede suponer la intervención sobre redes públicas de comunicación y recursos que soportan las prestaciones digitales de la administración autonómica y en régimen de autoprestación, se mantienen activas como argumentos impugnatorios, de modo que el recurso no pierde objeto en este concreto punto.

De lo expuesto se deduce que, en el presente recurso de inconstitucionalidad, la modificación o derogación de las disposiciones a las que se refieren los artículos 2, 3 y 6 impugnados supone:

(i) La desaparición sobrevenida del objeto del recurso en lo que se refiere a las impugnaciones basadas en motivos sustantivos del art. 6 del Real Decreto-ley, por vulneración de los arts. 18 y 20 CE [antecedente 1 C)], así como la relativa a la impugnación específica del art. 6.5 por infracción de los arts. 9.3 y 25 CE [antecedente 1 B) c) (iii) parcial].

(ii) La desaparición sobrevenida del objeto del recurso allí donde el conflicto competencial ha sido superado con las nuevas previsiones normativas, lo que se proyecta a la impugnación del art. 3.1 y 2 del Real Decreto-ley, en cuanto modifica los arts. 9.2 c) y 10.2 c) de la Ley 39/2015 [antecedente 1 B) a) (ii)]; y al art. 6.1 impugnado, que modifica el art. 4.6 de la Ley 9/2014 [antecedente 1 B) c) (i)].

(iii) El mantenimiento del objeto del recurso en relación con la impugnación de la totalidad del Real Decreto-ley 14/2019 por falta de concurrencia del presupuesto habilitante *ex* art. 86.1 CE [antecedente 1 A)], así como el mantenimiento de las quejas relativas a la alteración del régimen constitucional de reparto de competencias respecto de los preceptos que no se han visto modificados o que han sido modificados manteniéndose vivo el conflicto competencial identificado en la demanda [antecedente 1 B), apartados a) (i); a) (iii); b) (i); b) (ii); b) (iii); c) (i); c) (iii) parcial y c) (iv)]

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

3. Control de constitucionalidad de la definición explícita y razonada de la situación de «extraordinaria y urgente necesidad» (art. 86.1 CE).

A la hora de dar respuesta a las tachas de inconstitucionalidad que se han expuesto, debemos comenzar por la pretensión impugnatoria vinculada a la utilización del instrumento normativo de urgencia, ya que, conforme a doctrina reiterada (por todas, STC 105/2018, de 4 de octubre, FJ 3, y las que allí se citan), el examen de las infracciones que se refieren al art. 86 CE ha de ser prioritario en el orden de nuestro enjuiciamiento, toda vez que la infracción denunciada incide directamente sobre la validez de los preceptos impugnados, ya que se cuestiona la legitimidad constitucional de su inclusión en una norma de urgencia. Por tanto, si se estimaran las alegaciones relativas al art. 86 CE, resultaría innecesario el examen de las restantes alegaciones.

El recurso sostiene que, del análisis de la exposición de motivos y del debate parlamentario de su convalidación en la Diputación Permanente del Congreso de los Diputados, no se infiere que concurra una necesidad extraordinaria que justifique el uso de la potestad legislativa excepcional en el caso del Real Decreto-ley 14/2019. Se hacen referencias genéricas a la necesidad de adaptación a la aceleración en el empleo de nuevas tecnologías por parte de la administración, que se complementan con consideraciones que, por un lado, se fundamentan en referencias a los desafíos de las nuevas tecnologías, a su carácter estratégico para la seguridad nacional y su mayor exposición a nuevas amenazas del desarrollo tecnológico. Por otro lado, se añaden consideraciones más específicas, como serían las referencias a «los recientes y graves acontecimientos acaecidos en parte del territorio español», que no se definen y respecto a los que se considera que demandan una respuesta inmediata para evitar que se reproduzcan, estableciendo un marco preventivo con el objetivo de proteger los derechos y libertades constitucionalmente reconocidos y garantizar la seguridad pública de todos los ciudadanos. Para la demanda, el Gobierno se limita a realizar una mera declaración formal de la necesidad de la aprobación rápida e inminente de la norma, y no aporta la motivación de las razones que imposibilitan la consecución de la eficacia de las medidas pretendidas mediante su tramitación y aprobación parlamentarias.

El abogado del Estado defiende, por su parte, que ha quedado acreditado que los riesgos para los ciudadanos y para la propia administración pública, derivados de la aceleración de la transformación digital de las administraciones públicas, justifican la adopción de medidas de prevención como urgente respuesta a los riesgos para la seguridad pública y el adecuado ejercicio de los derechos y libertades de los ciudadanos.

En numerosas sentencias este tribunal ha resumido la doctrina constitucional elaborada en relación con el presupuesto que habilita al Gobierno para aprobar normas provisionales con rango de ley, lo que nos dispensa de reiterarla una vez más (por todas, STC 156/2021, de 16 de septiembre, FJ 4).

Bastará recordar que los términos «extraordinaria y urgente necesidad» no constituyen una cláusula o expresión vacía de significado dentro de la cual el margen de apreciación política del Gobierno se mueve libremente sin restricción alguna, sino un verdadero límite jurídico a la actuación mediante decretos-leyes; que la apreciación de la concurrencia de la extraordinaria y urgente necesidad constituye un juicio político que corresponde efectuar al Gobierno (titular constitucional de la potestad legislativa de urgencia) y al Congreso de los Diputados (titular de la potestad de convalidar, derogar o tramitar el texto como proyecto de ley), incumbiéndole a este tribunal controlar que ese juicio político no desborde los límites de lo manifiestamente razonable, sin suplantar a los órganos constitucionales que intervienen en la aprobación y convalidación de los decretos-leyes; y que ese control externo se concreta en la comprobación de que el Gobierno haya definido, de manera explícita y razonada, una situación de extraordinaria y urgente necesidad que precise de una respuesta normativa con rango de ley, y de que, además, exista una conexión de sentido entre la situación definida y las medidas adoptadas para hacerle frente (en este sentido, STC 20/2021, de 18 de febrero, FJ 2).

En cuanto a la definición de la situación de urgencia, nuestra doctrina ha precisado que no es necesario que la misma se contenga siempre en el propio decreto-ley, sino

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

que tal presupuesto cabe deducirlo igualmente de una pluralidad de elementos que son, básicamente, los que quedan reflejados en la exposición de motivos de la norma, a lo largo del debate parlamentario de convalidación, y en el propio expediente de elaboración de la misma (STC 152/2017, de 21 de diciembre, FJ 3, y las que allí se citan). Respecto de la conexión de sentido entre la situación de urgencia definida y las medidas adoptadas, deben valorarse el contenido y la estructura de las disposiciones incluidas en el decreto-ley controvertido [por todas STC 61/2018, de 7 de junio, FJ 4 e)].

(i) La exposición de motivos del Real Decreto-ley 14/2019 comienza su apartado I indicando que «(l)a 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». Posteriormente, indica que la Ley 36/2015, de 28 de septiembre, de seguridad nacional, «describe los riesgos asociados a las nuevas tecnologías como uno de los principales desafíos de la sociedad actual», siendo la ciberseguridad uno de los ámbitos prioritarios de actuación de la estrategia de seguridad nacional 2017, aprobada mediante Real Decreto 1008/2017, de 1 de diciembre, en cuanto «identifica las ciberamenazas y el espionaje como amenazas que comprometen o socavan la seguridad nacional». Continúa afirmando que «(e)l 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». En esa línea, se indica que «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». Se alude a continuación al «proceso de transformación digital de la administración», señalando que «[l]a 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».

A lo anterior se añade que «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».

Más adelante, el apartado III de la exposición de motivos vuelve a referirse al requisito de la extraordinaria y urgente necesidad, indicando que «el real decreto-ley constituye un instrumento constitucionalmente lícito, siempre que el fin que justifica la legislación de urgencia, sea, tal como reiteradamente ha exigido nuestro Tribunal Constitucional (sentencias 6/1983, de 4 de febrero, FJ 5; 11/2002, de 17 de enero, FJ 4, 137/2003, de 3 de julio, FJ 3, y 189/2005, de 7 julio, FJ 3), subvenir a un situación concreta, dentro de los objetivos gubernamentales, que por razones difíciles de prever exige una acción normativa inmediata en un plazo más breve que el requerido por la vía normal o por el procedimiento de urgencia para la tramitación parlamentaria de las leyes», mencionando luego la doctrina constitucional en torno a la concurrencia de los

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

presupuestos habilitantes de la extraordinaria y urgente necesidad y a la necesaria conexión de sentido entre la situación de necesidad definida y las medidas adoptadas.

Se sostiene también que «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». Se concluye afirmando que «los motivos que acaban de exponerse justifican ampliamente la concurrencia de los requisitos constitucionales de extraordinaria y urgente necesidad, que habilitan al Gobierno para aprobar el presente real decreto-ley dentro del margen de apreciación que, en cuanto órgano de dirección política del Estado, le reconoce el artículo 86.1 de la Constitución (STC 142/2014, FJ 3 y STC 61/2018, FFJJ 4 y 7). Concurren también las notas de excepcionalidad, gravedad y relevancia que hacen necesaria una acción normativa inmediata en un plazo más breve que el requerido para la tramitación parlamentaria de una ley, bien sea por el procedimiento ordinario o por el de urgencia (STC 68/2007, FJ 10 y STC 137/2011, FJ 7)». A lo que se añade que «en el supuesto abordado por este real decreto-ley ha de subrayarse que para subvenir a la situación de extraordinaria y urgente necesidad descrita es necesario proceder a la reforma de varias normas con rango de ley, lo que de por sí exige “una respuesta normativa con rango de ley” [STC 152/2017, de 21 de diciembre, FJ 3 i)]».

En el debate de convalidación del Real Decreto-ley 14/2019, de 27 de noviembre de 2019, ante la Diputación Permanente del Congreso de los Diputados (debate que se transcribe en «Diario de Sesiones. Congreso de los Diputados», XIII Legislatura, núm. 14, págs. 13-31), la ministra de Economía y Empresa en funciones asumió su defensa en nombre del Gobierno señalando que la revolución digital «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 emplea para fines legítimos que no comprometan los derechos y libertades de los ciudadanos». Esta idea se reitera posteriormente cuando afirma que «es imprescindible garantizar a los ciudadanos un nivel de seguridad y protección de sus derechos en el ámbito digital exactamente igual al que tienen en el ámbito analógico, y este, y no otro, es el objetivo que se persigue con este real decreto-ley, señorías, que incluye medidas en los ámbitos de la documentación nacional de identidad, la identificación electrónica ante la administración y datos en poder de las administraciones públicas, la contratación pública, las telecomunicaciones y la seguridad en las redes y sistemas de información».

Y sostiene que «[e]l real decreto-ley que se somete hoy a convalidación es coherente con los principios de urgente y extraordinaria necesidad que se exigen a esta figura jurídica. Se trata de una norma urgente, habida cuenta de la celeridad con la que se están produciendo los avances en esta materia y dada la situación política actual, con el Gobierno en funciones y las cámaras disueltas. Esperar a la constitución de las nuevas Cortes Generales y tramitar un proyecto de ley habría impedido contar con la suficiente celeridad con un marco jurídico preventivo que sirva para proteger los derechos y libertades constitucionalmente reconocidos».

Por último, debemos examinar el expediente de elaboración de la norma impugnada. En concreto, el documento aportado a los autos por el abogado del Estado, cuyo nombre completo es «Memoria abreviada del análisis de impacto normativo del proyecto de Real Decreto-ley por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones», elaborado conjuntamente por siete departamentos ministeriales con fecha 30 de octubre de 2019. Los contenidos de este documento han sido trasladados en gran parte a la exposición de motivos del Real Decreto-ley 14/2019 y reitera, al abordar la motivación de la propuesta, las referencias a los graves acontecimientos acaecidos en parte del territorio español, que hacen necesario adoptar medidas urgentes con el fin de preservar la seguridad pública de todos los ciudadanos.

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

Se afirma que «resulta necesario articular una respuesta inmediata para evitar que se reproduzcan sucesos de esta índole. Ha de establecerse un marco jurídico preventivo a tal fin, cuyo objetivo último sea proteger los derechos y libertades constitucionalmente reconocidos». Posteriormente, se alude a la intensidad del desarrollo de la administración electrónica y su dependencia de las tecnologías de la información, lo que incrementa «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», con la consecuencia de que se entiende obligado «establecer sin demora un marco jurídico que garantice el interés general y, en particular, la seguridad pública. Solo de este modo podrá asegurarse que la administración digital se emplea para fines legítimos que no comprometan los derechos y libertades de los ciudadanos».

En el apartado denominado «Análisis de alternativas» se indica que «se consideró la alternativa de introducir estas medidas mediante un proyecto de ley; sin embargo, dada la urgencia requerida para su aprobación y habida cuenta de que las Cámaras se encuentran disueltas, dilatar estas medidas hasta la constitución de las Cortes Generales, y aun utilizándose entonces el trámite de urgencia, no habría permitido reaccionar a tiempo».

(ii) Expuestos y analizados todos estos motivos, debemos valorar si dan cuenta de la existencia de una justificación razonable de la situación de extraordinaria y urgente necesidad, para comprobar luego si las medidas aprobadas son congruentes con esa situación. En la realización de este examen son necesarias dos precisiones. La primera es que, aunque no se impugnan todos los preceptos del Real Decreto-ley 14/2019, las alegaciones de la demanda cuestionan la falta del presupuesto habilitante en los preceptos impugnados de forma global o común, con lo que las razones alegadas para justificar la concurrencia de la extraordinaria y urgente necesidad se pueden examinar conjuntamente. La segunda es que, en ese examen, debe tenerse en cuenta el necesario «margen de apreciación» que debe reconocerse al Gobierno como órgano de dirección política cuando de decisiones de esta naturaleza se trata.

Teniendo en cuenta lo expuesto, el Tribunal aprecia que las razones que llevaron al Gobierno a dictar los preceptos del Real Decreto-ley 14/2019 aquí cuestionados tienen que ver con la necesidad de garantizar un adecuado nivel de protección de los derechos de los ciudadanos en un entorno en constante transformación como es el digital, evitando con ello los riesgos que, en dicho entorno, pueden plantearse para la seguridad pública. Consideración esta última fundada en la mención a determinados acontecimientos acaecidos que, en la consideración del Gobierno, hacían preciso introducir modificaciones tanto en el régimen jurídico aplicable a la utilización de medios electrónicos en las relaciones entre la administración y los ciudadanos como en el ámbito de las telecomunicaciones, incrementando el estándar de protección de la seguridad pública en ambos ámbitos.

A eso debe añadirse que, cuando el Gobierno aprobó la norma, las posibilidades de que la situación de urgente necesidad que debía ser atendida pudiera solventarse a través del procedimiento legislativo era remota. Cuando se dicta el Real Decreto-ley 14/2019 recurrido en este proceso constitucional, el Gobierno llevaba más de medio año en funciones, concretamente 185 días. Las Cortes Generales fueron disueltas en virtud de lo dispuesto en el art. 99.5 CE y convocadas elecciones generales para el día 10 de noviembre de 2019 (en virtud del Real Decreto 551/2019, de 24 de septiembre, de disolución del Congreso de los Diputados y del Senado y de convocatoria de elecciones). La disolución automática de las cámaras y la correspondiente convocatoria de nuevas elecciones generales prolongó de un modo inevitable la situación de interinidad del Gobierno, iniciada originariamente con la convocatoria de elecciones de 28 de abril de 2019 (Real Decreto 129/2019, de 4 de marzo, de disolución del Congreso de los Diputados y del Senado y de convocatoria de elecciones generales). Durante el dilatado periodo de interinidad gubernamental, el Gobierno no pudo presentar proyectos de ley por establecerlo así el art. 21.5 de la Ley 50/1997, de 27 de noviembre, del Gobierno. Y, dado el breve plazo transcurrido desde la constitución de las cámaras y

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

sus órganos hasta su disolución como consecuencia del transcurso de dos meses, a contar desde la primera votación de investidura, sin que el Congreso de los Diputados invistiera a un nuevo presidente del Gobierno (art. 99.5 CE), no era previsible que una proposición de ley pudiera culminar la tramitación parlamentaria hasta convertirse en ley. En esta situación, de prolongada interinidad del Gobierno, unida a la convocatoria de elecciones generales, que resultaba incierto el ejercicio de la potestad legislativa de las cámaras, encuentra justificación el recurso al instrumento de la legislación de urgencia para atender a la situación antes descrita.

El Tribunal estima que las situación descrita por el Gobierno, aun cuando no explicitada como es deseable la carga de que concurre el presupuesto habilitante, se mantiene dentro de los márgenes de apreciación que deben reconocérsele para hacer uso de la potestad legislativa excepcional del art. 86.1 CE.

La acreditada de manera suficiente en este proceso reúne las características del art. 86.1 CE, que legitiman al Gobierno para revertirla o corregirla con una urgencia que no permitiría la aprobación de una ley formal en el parlamento. La necesidad justificadora de los decretos-leyes supone una valoración esencialmente política de ordenación de prioridades de actuación respecto de situaciones concretas y objetivos gubernamentales que, por razones difíciles de prever, requieren una acción normativa inmediata en un plazo más breve que el requerido por la vía normal o incluso por el procedimiento de urgencia para la tramitación parlamentaria de las leyes. En este caso, el Gobierno ha definido «la situación de necesidad de modo explícito y razonado», por referencia a la situación que trata de atender y a la imposibilidad de resolverla por el procedimiento legislativo, sin necesidad de que «se refiera expresamente a todos y cada uno de los elementos determinantes de la misma, lo que no sería coherente con que la citada doctrina constitucional califique la decisión gubernativa de dictar un decreto-ley de "juicio político o de oportunidad" y defina la verificación de esta decisión que atañe al Tribunal como "control externo" a realizar mediante una "valoración conjunta de todos aquellos factores que determinaron al Gobierno a dictar la disposición legal excepcional"» (STC 93/2015, FJ 5).

Por tanto, y como consecuencia de todo ello, no es posible apreciar un exceso en el margen de apreciación del Gobierno o un uso arbitrario de la potestad del art. 86.1 CE.

En cuanto al segundo elemento de nuestro canon, atendiendo al control que corresponde a este tribunal, que debe respetar el margen de discrecionalidad política que en la apreciación de este requisito corresponde al Gobierno, podemos considerar que no se ha vulnerado la conexión de sentido entre la medida adoptada y la situación de extraordinaria necesidad y urgencia definida. Las modificaciones normativas se ajustan a los objetivos que la exposición de motivos de la norma de urgencia afirma perseguir en cuanto que todas ellas tienen que ver con la garantía de los derechos de los ciudadanos y de la seguridad pública en un entorno digital. Desde esta perspectiva, las medidas contenidas en los preceptos impugnados son coherentes con la situación de necesidad definida. Por otro lado, se modifica de manera inmediata la regulación existente, lo cual también es acorde con la situación de urgencia definida. No es obstáculo para ello, el hecho de que, respecto a algunas de las medidas se otorgue un plazo para su cumplimiento (disposiciones adicional única, transitoria primera.2 y transitoria segunda.1), pues la obligación ha quedado ya fijada y el ordenamiento modificado en el momento en que la norma de urgencia se aprueba. A este respecto, la STC 237/2012, de 13 de diciembre, FJ 6, señala que «no debe confundirse eficacia inmediata de la norma provisional con la ejecución instantánea de la misma. Solo aquella es un requisito ínsito en la definición constitucional del decreto-ley establecida en el art. 86.1 CE […] en tanto que la celeridad de la completa ejecución estará en función de la naturaleza y complejidad de las propias medidas adoptadas en cada decreto-ley para hacer frente a la situación de urgencia».

En suma, el Tribunal aprecia que las circunstancias reflejadas en la exposición de motivos del decreto-ley impugnado y puestas de manifiesto durante la fase de convalidación y en el expediente de elaboración de la norma reflejan, más allá de una

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

mera conveniencia política, una situación de hecho que permite concluir, en el ámbito del control externo que compete realizar a este tribunal, que existen razones suficientes para apreciar la existencia de una situación de extraordinaria y urgente necesidad.

4. Examen de las quejas competenciales derivadas de la reforma de la Ley Orgánica 4/2015, de protección de la seguridad ciudadana; la Ley 59/2003, de firma electrónica, y la Ley 39/2015, de procedimiento administrativo común de las administraciones públicas.

Descartada la concurrencia del primer motivo de inconstitucionalidad alegado, debemos abordar ahora el enjuiciamiento de los concretos preceptos impugnados por razones competenciales, empezando por la impugnación de los preceptos que reforman la Ley Orgánica 4/2015 y las leyes 59/2003 y 39/2015, impugnados por introducir regulaciones a las que se imputa que restringen la potestad de autoorganización autonómica en relación con la administración digital, contraviniendo con ello los arts. 150 y 159 EAC.

Tales tachas se formulan: (i) a las medidas relativas al documento nacional de identidad establecidas en los arts. 1 y 2 del Real Decreto-ley 14/2019, por los que se modifican el art. 8.1 LOPSC y el art. 15.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica; (ii) al régimen de autorización previa para el empleo de sistemas de identificación y de firma electrónica de clave concertada u otros que cuenten con un registro previo como usuario que permita garantizar su identidad y que las administraciones consideren válido, previsto en el art. 3.1 y 2 del Real Decreto-ley 14/2019, en la redacción que da a los artículos 9.2 c) y 10.2 c) de la Ley 39/2015 y (iii) a la restricción del uso de las denominadas tecnologías de registro distribuido que deriva del art. 3.3 del Real Decreto-ley 14/2019, en cuanto añade una nueva disposición adicional sexta a la citada Ley 39/2015.

Sobre el segundo bloque de quejas de los citados, no nos pronunciaremos por haber desaparecido sobrevenidamente el objeto del recurso en este punto, tal y como se expone extensamente en el fundamento jurídico 2.

Tampoco lo haremos sobre otra serie de argumentos que guarda relación con las quejas anteriores. Nos referimos a aquellos que se plantean la inconstitucionalidad del art 3.1 y 2 del Real Decreto-ley 14/2019, en la obligación que incorpora a los arts. 9.3 y 10.3 de la Ley 39/2015, de situar «en territorio español» los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de los sistemas previstos en los artículos 9.2 c) y 10.2 c) de la citada ley, así como, por conexión, la disposición transitoria primera, apartado 2, del propio Real Decreto-ley 14/2019. Sin embargo, la tacha formulada respecto a estos tres preceptos no se relaciona con la infracción del orden constitucional de distribución de competencias, en la medida en que lo que realmente se alega es que no se ajustan a lo previsto 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 (RGPD), apreciación en la que descansa la denuncia de vulneración competencial construida, en todo caso, en torno a lo que se entiende como una infracción directa de una norma de Derecho de la Unión Europea, el ya referido Reglamento general de protección de datos.

Por tanto, teniendo en cuenta el modo en que se formula, esta tacha no puede ser atendida en sede de recurso de inconstitucionalidad, ya que es consolidada la doctrina recordada en la STC 81/2020, de 15 de julio, FJ 2, según la cual «el Derecho de la Unión Europea no es en sí mismo canon directo de constitucionalidad en los procesos constitucionales, de modo que la eventual infracción de las normas de la Unión Europea por leyes estatales o autonómicas constituye un conflicto de normas que ha de resolverse en el ámbito de la jurisdicción ordinaria y, en su caso, por el Tribunal de Justicia de la Unión Europea (entre otras muchas, SSTC 28/1991, de 14 de febrero,

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

FJ 5; 128/1999, de 1 de julio, FJ 9; 173/2005, de 23 de junio, FJ 9; 135/2012, de 19 de junio, FJ 2; 64/2013, de 14 de marzo, FJ 4, y 76/2019, de 22 de mayo, FJ 3)».

Lo propio sucede también con la limitación a las transferencias de datos contenidas en el último párrafo de los nuevos arts. 9.3 y 10.3 de la Ley 39/2015, respecto a los que no hay propiamente denuncia de vulneración competencial, pues lo que en realidad se alega es que se trata de un régimen más restrictivo que el previsto en el Reglamento general de protección de datos, cuestión que, por lo que se acaba de exponer, no puede ser valorada en esta sede.

(i) Dicho lo anterior, nos centraremos, en primer lugar, en la impugnación de los arts. 1 y 2 del Real Decreto-ley 14/2019, relativos a la regulación del DNI y del DNI electrónico.

El art. 1 da nueva redacción al apartado 1 del art. 8 LOPSC, que queda redactado en los siguientes términos:

«1. Los españoles tienen derecho a que se les expida el Documento Nacional de Identidad.

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.»

Por su parte, el art. 2 modifica el apartado 1 del art. 15 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, en los siguientes términos:

«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.»

Siendo, como se expone en el fundamento jurídico 2, la literalidad actual de eta previsión la siguiente, contenida en la disposición adicional tercera de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza:

«[E]l Documento Nacional de Identidad electrónico es el Documento Nacional de Identidad que permite acreditar 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, así como la firma electrónica de documentos.»

La modificación introducida en el art. 8.1 LOPSC ha consistido en añadir que el DNI es «el único documento» con suficiente valor por sí solo para acreditar «a todos los efectos» la identidad del titular y sus datos personales. La reforma del art. 15.1 de la Ley de firma electrónica es consecuencia de lo anterior, en cuanto se limita a incorporar una remisión al citado art. 8.1 LOPSC.

La demanda cuestiona el posible efecto restrictivo que la concreta regulación que ahora se efectúa pueda tener sobre las competencias de la Generalitat para determinar los sistemas de identificación de los interesados ante las administraciones públicas, incidiendo en las competencias previstas en los arts. 150 y 159 EAC. Concretamente, se critica que la principal consecuencia de dicha modificación es que la creación de sistemas de identificación y firma deba ir precedida de una identificación personal que solo podrá realizarse a través del DNI. El abogado del Estado, por el contrario, ha defendido que la regulación impugnada no impide, como parece entender la demanda, la utilización de otros sistemas de identificación, sino que veta únicamente la creación de sistemas de identificación a los que se pretendiera otorgar la misma consideración y eficacia que al DNI.

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

El DNI se regula en el capítulo II LOPSC, (arts. 8 a 11), preceptos en los que se establece el derecho de los españoles a la expedición del DNI y el valor de dicho documento para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular. Se determina el régimen de obligaciones y derechos, señalando que ningún español puede ser privado del DNI, ni siquiera temporalmente, salvo en los casos y en la forma establecidos por las leyes según las cuales deba ser sustituido por otro documento y se fija la exigencia de exhibirlo a requerimiento de los agentes de la autoridad de conformidad con lo dispuesto en la ley. El DNI también permite a los españoles mayores de edad que gocen de plena capacidad de obrar y a los menores emancipados la identificación electrónica de su titular, así como la firma electrónica de documentos, en los términos previstos en la legislación específica (en este caso, disposición adicional tercera de la Ley 6/2020).

Tratándose de una controversia competencial hemos, en primer lugar, de encuadrar la regulación cuestionada en el ámbito que le sea propio.

A este respecto la disposición final primera del Real Decreto-ley 14/2019, relativa a los títulos competenciales, afirma que «los artículos 1 y 2 de este real decreto-ley se dictan al amparo del artículo 149.1.29 de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública». Efectivamente, este encuadre es el adecuado en cuanto que la acreditación de la identidad de los ciudadanos es una premisa para que los poderes públicos puedan cumplir su función de perseguir los delitos y garantizar a la vez la seguridad ciudadana y la paz social. De hecho, garantizar el cumplimiento de los fines que persigue la Ley Orgánica de protección de la seguridad ciudadana es el sentido al que responde toda la regulación tanto sobre la documentación e identificación personal de los ciudadanos españoles, como acerca de los deberes de sus titulares y de la incorporación de las posibilidades de acreditación electrónica de la identidad y la exigencia de exhibirlos a requerimiento de los agentes de la autoridad en los supuestos y con las garantías que prevé la ley.

En dicha materia, el Estado ostenta, *ex* art. 149.1.29 CE, competencias sobre seguridad pública «sin perjuicio de la posibilidad de creación de policías por las comunidades autónomas en la forma que se establezca en los respectivos estatutos en el marco de lo que disponga una ley orgánica». Por tanto, las comunidades autónomas no pueden asumir estatutariamente más competencias que las previstas, para la creación de cuerpos propios de policía, en el artículo 149.1.29 CE. Competencias que la Generalitat ostenta con los contenidos funcionales definidos en el artículo 164 EAC y —para determinados efectos— «de acuerdo con lo dispuesto en la legislación estatal» o «en el marco de la legislación estatal» (funciones contempladas, respectivamente, en los números 1 y 3 de dicho artículo).

Tal y como se recoge en el fundamento jurídico 6 a) de la STC 142/2018, de 20 de diciembre, sobre la Agencia de Ciberseguridad de Cataluña, la materia «seguridad pública» es, en principio, competencia exclusiva del Estado *ex* artículo 149.1.29 CE, y solamente se encuentra limitada por las competencias que las comunidades autónomas hayan asumido respecto a la creación de su propia policía (con la cita, por todas, de la STC 148/2000, de 1 de junio, FJ 5). En la misma STC 142/2018 se dice que, «[s]in embargo, la seguridad pública no se agota en la actividad policial (STC 86/2014, FJ 4), de modo que la falta de identificación absoluta entre la materia seguridad pública y el ámbito propio de los servicios policiales tiene consecuencias en el plano de la delimitación de competencias en la materia, de manera que a las comunidades autónomas con competencias asumidas corresponde la organización de sus propios servicios policiales y el ejercicio de las funciones o servicios policiales no estatales, así como la necesaria inherencia o complementariedad (SSTC 104/1989, FJ 6, y 175/1999, FJ 5) de determinadas funciones o potestades no estrictamente policiales» [FJ 6 a)].

Examinada la regulación del DNI y encuadrada la cuestión discutida en el ámbito de la seguridad pública, hemos de constatar ahora que el recurso parte, en este punto, de un inadecuado entendimiento de la regulación que cuestiona, lo que condiciona toda su argumentación. Atendiendo a las finalidades a las que el DNI sirve, se relaciona

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

estrechamente con la competencia estatal en materia de seguridad pública del art. 149.1.29 CE. Pero la atribución al DNI del carácter de único documento válido para acreditar a todos los efectos la identidad y los datos personales de su titular (recuperando un rasgo que ya le atribuía el art. 1 del Decreto 196/1976, de 6 de febrero, por el que se regula el documento nacional de identidad) no va, como también ha señalado el abogado del Estado, en detrimento de la utilización de otros posibles sistemas de identificación que puedan utilizar las administraciones públicas.

La reforma de la regulación del DNI convive con el mantenimiento de las reglas prescritas por la legislación estatal en materia de procedimiento administrativo común. Conforme a tales reglas, las administraciones públicas pueden verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación del nombre y apellidos que consten en el DNI o documento identificativo equivalente (art. 9.1 Ley 39/2015). Pero se mantiene igualmente la posibilidad de que los interesados se identifiquen ante las administraciones públicas a través de sistemas basados en certificados electrónicos, de clave concertada o de cualquier otro sistema que las administraciones consideren válido (art. 9.2), como por ejemplo el conocido como sistema Cl@ve. Se constata entonces que la regulación impugnada no impide, como dice la demanda, la utilización de otro sistema de identificación, posibilidad abierta por la norma estatal en materia de procedimiento administrativo común en el referido art. 9 de la Ley 39/2015, a la que luego habrá oportunidad de referirse en detalle.

Lo que sí queda vedado con esta regulación, sin que ello plantee problema competencial alguno, dado el carácter exclusivo del título estatal en los términos que resulta de la doctrina constitucional, es, como la propia demanda reconoce, que se regulen otros sistemas de identificación a los que se les otorgue la misma consideración y eficacia descrita en el art. 8.1 LOPSC. En otros términos, las normas cuestionadas lo único que hacen es cercenar la posibilidad de introducir un nuevo documento de acreditación de la identidad que pudiera sustituir al DNI.

Respetando tal límite, impuesto por las competencias estatales en materia de seguridad pública, en nada se afecta a la posibilidad, abierta por las propias normas estatales y confirmada por la doctrina constitucional (STC 55/2018, de 24 de mayo, FJ 9), de que las administraciones públicas establezcan sistemas de identificación electrónica, con lo que la reforma llevada a cabo por el Real Decreto-ley 14/2019 no afecta a la competencia de la Generalitat de Cataluña para organizar su propia administración (art. 150 EAC), ni a la que le corresponde en materia de régimen jurídico y procedimiento de las administraciones públicas catalanas (art. 159 EAC).

Por tanto, habiendo sido desechada la premisa sobre la descansaba la queja competencial que se formulaba, no queda sino desestimar esta impugnación.

(ii) Por lo que hace a la impugnación de la disposición adicional sexta de la Ley 39/2015, introducida por el art. 3.3 del Real Decreto-ley 14/2029, esta presenta el siguiente tenor literal:

«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.»

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

Para la demanda, impedir a una administración pública el uso de una tecnología por no disponer aún de un marco normativo específico, es una limitación desproporcionada y preventiva de sus competencias para el establecimiento de los sistemas de identificación. La existencia de riesgos no debe ser un obstáculo para el uso de tecnologías de tratamiento de datos personales, si se dispone de las debidas garantías, lo que se asegura mediante la aplicación del Reglamento general de protección de datos. Por tanto, la recurrente entiende que se vulneran los arts. 150 y 159 EAC. Por el contrario, el abogado del Estado sostiene que el uso de esta tecnología en la administración electrónica debe hacerse con cautela, para garantizar la seguridad de los datos, de forma que se eviten riesgos de lesión de derechos fundamentales. La restricción cautelar y temporal a estas tecnologías, en tanto la Unión Europea no desarrolle una normativa para su uso compatible con el citado Reglamento, se justifica en razones de seguridad pública del art. 149.1.29 CE.

El precepto alude a las denominadas tecnologías de registro distribuido o DLT (*distributed ledger technologies*, en inglés). A los efectos que ahora interesan el registro distribuido se define como una tecnología que se fundamenta en almacenes de información, en forma de bases de datos digitales descentralizadas, en las cuales existen copias de la información distribuidas entre diversos participantes que se comparten, actualizan y sincronizan de forma descentralizada y por acuerdo de los usuarios. De manera que la información digital se certifica por varios participantes distintos que la registran, actualizan y validan mediante consenso mayoritario sin intermediación de una autoridad central o certificadora, a diferencia de los sistemas de bases de datos centralizadas. También puede servir para desarrollar sistemas de la denominada gestión de identidad, en la medida en que en la red descentralizada se contienen todos los atributos o características que permiten la identificación de la persona, sin que sea así necesaria la intervención de un sistema centralizado de acreditación de la identidad.

Según la disposición final primera del Real Decreto 14/2019, el art. 3.3 del Real Decreto-ley 14/2019 se dicta al amparo de las competencias estatales de los arts. 149.1.18 y 149.1.29 CE.

El precepto aquí discutido, en la medida en que tiene relación con los posibles sistemas de identificación a utilizar por los interesados en sus relaciones con las administraciones, ha de encuadrarse preferentemente en el art. 149.1.18 CE, tal como se desprende de la doctrina constitucional (por todas, STC 55/2018, FJ 9) que considera que los sistemas de identificación electrónica y, en general, la disciplina sobre la identidad electrónica que fijen las normas estatales cumple una función típica de las normas de procedimiento administrativo común como es la de garantizar un tratamiento asimismo común de los administrados ante todas las administraciones públicas.

Por tanto, aunque no pueda descartarse en esta cuestión la incidencia del art. 149.1.29 CE, en atención a la doctrina que se ha citado, la cuestión que aquí se plantea ha de ser analizada a efectos de su encuadramiento competencial bajo el prisma del art. 149.1.18 CE, en tanto que título más específico.

El Tribunal estima que puede considerarse básica la decisión en torno a la eventual utilización de una determinada tecnología en el concreto ámbito discutido. Los sistemas para acreditar la identidad de los ciudadanos constituyen uno de los instrumentos clave para el despliegue de la administración electrónica y resultan un requisito previo para la implementación de cualquier tipo de procedimiento con plenas garantías. La previsión impugnada se relaciona, por tanto, con una de las finalidades que las medidas estatales adoptadas al amparo del art. 149.1.18 CE pueden cumplir, como es la de garantizar un tratamiento común a los ciudadanos en sus relaciones con las administraciones públicas. No cabe, por lo mismo, entender que concurra la vulneración de las alegadas competencias autonómicas de los arts. 150 y 159 EAC, en cuanto que dichas competencias no son ilimitadas sino que han de ajustarse al marco previamente definido por la norma estatal cuando actúa legítimamente en el ámbito competencial que le es propio. De hecho, el art. 9.2 c) de la Ley 39/2015 (tanto en la versión derivada del Real

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

Decreto-ley 14/2019 como en la actual) permite que los interesados se identifiquen mediante sistemas de clave concertada y cualquier otro sistema que las administraciones públicas consideren válido, «en los términos y condiciones que se establezcan» y el art. 10.2 c) permite la firma electrónica de los interesados mediante «cualquier otro sistema que las administraciones públicas consideren válido, en los términos y condiciones que se establezcan», cláusula que, evidentemente, habilita al legislador estatal a tomar decisiones que delimiten el ámbito en el que hacer posible la utilización de esos sistemas alternativos, como pueden ser los basados en tecnologías de registro distribuido.

La restricción cobra su sentido en cuanto se refiere a la posible utilización de un determinado sistema de identificación y firma de los interesados respecto del que todavía es preciso valorar sus implicaciones desde el punto de vista de la necesaria protección en el acceso a los sistemas de información de las administraciones públicas y de los derechos de los ciudadanos que con ellas se relacionan, en la medida en que en este tipo de sistemas todos los participantes disponen de igual información en tiempo real y los datos están interconectados y, por tanto, disponibles. Resulta posible entonces que el Estado, al amparo de sus competencias en materia de procedimiento administrativo común, proyectadas al ámbito específico de los sistemas de administración electrónica, establezca prevenciones al respecto a fin de garantizar la seguridad jurídica de las relaciones electrónicas entre la administración y los ciudadanos.

Por otro lado, frente a lo que la demanda argumenta, la limitación impuesta no es, en términos de la exposición de motivos del Real Decreto-ley 14/2019, una prohibición general. Se persigue restringir de forma puntual y provisional su uso, en tanto no exista un marco regulatorio *ad hoc* de carácter estatal o europeo que haga frente a las necesarias adaptaciones que implican las peculiaridades de la tecnología de registro para hacer posible su utilización, desde el punto de vista de las normas aplicables a la imprescindible identificación y autenticación de usuarios así como para la seguridad de las propias redes. Algo que también se recoge en el precepto impugnado, que remite a una posterior regulación estatal en el marco del Derecho de la Unión Europea.

De hecho, la propia demanda advierte del hecho de que no ha sido objeto de regulación el uso de estas tecnologías de registro distribuido para usarse en sistemas de identificación, con lo que no se dispone del instrumento normativo que prevea las condiciones y garantías específicas para utilizarlo en el ámbito de los sistemas de identificación ante las administraciones públicas. Y la consideración de la demanda de que dicha circunstancia no resulta suficiente para justificar la limitación por considerar que existían otras alternativas posibles, no deja de ser la expresión de una discrepancia en torno a la cierta prevención con que el legislador estatal ha afrontado la cuestión. Lo aquí relevante es que, dejando a un lado consideraciones de oportunidad y técnica legislativa, la normativa efectivamente establecida y sometida a nuestro enjuiciamiento es un ejercicio de la libertad de configuración legislativa constitucionalmente garantizada que no desborda los límites del art. 149.1.18 CE y, por tanto, no invade las competencias autonómicas en materia de organización y procedimientos administrativos [en un sentido similar, STC 55/2018, FJ 9 b)].

5. Examen de las quejas competenciales derivadas de la reforma de la Ley 40/2015 de régimen jurídico del sector público

Se aborda ahora el examen de las medidas previstas en el art. 4 del Real Decreto-ley 14/2019, en cuanto que introduce un nuevo art. 46 *bis* y modifica el art. 155 de la Ley 40/2015, así como la disposición transitoria segunda, apartado 1, que se refiere al régimen transitorio de tales modificaciones.

El apartado primero del art. 4 del Real Decreto-ley 14/2019 introduce un nuevo art. 46 *bis* en la Ley 40/2015 en cuya virtud se establece la obligación de ubicar y prestar dentro del territorio de la Unión Europea, los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión de determinadas bases de datos como son el censo electoral, los padrones municipales de habitantes y otros

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

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. En relación con lo anterior, la disposición transitoria segunda prevé un plazo de seis meses a partir de la entrada en vigor del Real Decreto-ley 14/2019 para que las entidades pertenecientes al sector público adopten las medidas necesarias para dar cumplimiento a estas nuevas obligaciones.

Con respecto a ambas previsiones ocurre algo similar a lo que ya se ha apreciado en el fundamento jurídico anterior, pues lo que se alega es la contradicción con el Reglamento general de protección de datos, contradicción que no puede, por las razones que ya se han expuesto anteriormente, dirimirse ante la jurisdicción constitucional (en el mismo sentido, STC 76/2019, de 22 de mayo, FJ 3).

Por el contrario, sí debe examinarse la queja que se plantea respecto al nuevo art. 155 de la Ley 40/2015 según el cual:

«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 garantía de los derechos digitales y su normativa de desarrollo, cada administración deberá facilitar el acceso de las restantes administraciones públicas a los datos relativos a los interesados que obren en su poder, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad.

2. En ningún caso podrá procederse a un tratamiento ulterior de los datos para fines incompatibles con el fin para el cual se recogieron inicialmente los datos personales. De acuerdo con lo previsto en el artículo 5.1 b) del Reglamento (UE) 2016/679, no se considerará incompatible con los fines iniciales el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.

3. Fuera del caso previsto en el apartado anterior y siempre que las leyes especiales aplicables a los respectivos tratamientos no prohíban expresamente el tratamiento ulterior de los datos para una finalidad distinta, cuando la administración pública 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 pública cedente a los efectos de que esta pueda comprobar dicha compatibilidad. La administración pública cedente podrá, en el plazo de diez días oponerse motivadamente. Cuando la administración cedente sea la administración general del Estado podrá en este supuesto, excepcionalmente y de forma motivada, suspender la transmisión de datos por razones de seguridad nacional de forma cautelar por el tiempo estrictamente indispensable para su preservación. En tanto que la administración pública cedente no comunique su decisión a la cesionaria esta no podrá emplear los datos para la nueva finalidad pretendida.

Se exceptúan de lo dispuesto en el párrafo anterior los supuestos en que el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales esté previsto en una norma con rango de ley de conformidad con lo previsto en el artículo 23.1 del Reglamento (UE) 2016/679.»

Para la representación procesal de la Generalitat de Cataluña, la obligación de comunicación previa a la administración cedente es una medida de control inconstitucional impuesta a la administración autonómica. Según el Reglamento general de protección de datos los responsables del tratamiento deben ajustarse a las reglas previstas en él, especialmente en el art. 6.4. Pero el nuevo art. 155.3 de la Ley 40/2015 alteraría este régimen de cesión de datos entre administraciones públicas, incorporando

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

un procedimiento de comprobación que equivale a una tutela cautelar que se considera contraria a las competencias autonómicas. El abogado del Estado sostiene que es una medida de régimen jurídico de las administraciones públicas, no de regulación de la protección de datos y que se ajusta a lo previsto en el Reglamento general de protección de datos, tanto en cuanto a la prohibición de tratamiento incompatible como a la suspensión por afección de la seguridad nacional.

Conforme al Reglamento general de protección de datos, los datos que se han recogido para fines determinados, explícitos y legítimos, no pueden tratarse con posterioridad de forma incompatible con estos fines. La norma europea establece la presunción general de que son actividades compatibles con otra anterior los tratamientos con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. El tratamiento posterior para otros fines se permite previa determinación de si ese tratamiento posterior es o no compatible con el fin por el que se recogieron inicialmente los datos personales, atendiendo a las condiciones previstas por los arts. 6.4 y 23.1 RGPD. Así, la cesión de datos entre administraciones es, en principio, posible cuando sea necesaria para el ejercicio de poderes públicos conferidos al responsable del tratamiento [art. 6.1 e) RGPD], siempre que el ejercicio de tales poderes de tratamiento de datos derive de «una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal» (art. 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales).

La controversia se traba respecto al número 3 de este precepto de la Ley 40/2015, por cuanto los números 1 y 2 se limitan a trasladar la regulación del Reglamento general de protección de datos al ámbito de las transmisiones de datos entre administraciones públicas. El apartado 3 regula el procedimiento que tiene por finalidad comprobar si la finalidad ulterior a la que se quiere destinar los datos es o no compatible con la que inicialmente legitimó su tratamiento. Se establece una obligación adicional de consulta a la administración que comunica los datos, a resultas de la cual la destinataria, responsable del nuevo tratamiento, no podrá llevarlo a cabo hasta que lo haya comunicado a la administración que los recogió inicialmente. Y esta, puede comprobar que se da la citada compatibilidad, pudiendo oponerse, en caso contrario, en un plazo de diez días. Concretamente lo discutido es la posibilidad que el precepto otorga a la administración general del Estado para suspender la transmisión de datos por razones de seguridad nacional de forma cautelar por el tiempo estrictamente indispensable para su preservación.

Ya hemos expuesto que no procede aquí examinar la conformidad o no del precepto estatal con el Derecho de la Unión Europea, lo que, pese a lo alegado por las partes, nos exime de valorar la regulación cuestionada a la luz de lo dispuesto por el Reglamento general de protección de datos, pues el Derecho de la Unión Europea no es en sí mismo canon o parámetro directo de constitucionalidad [STC 152/2020, de 22 de octubre, FJ 2 b) y las que cita], especialmente cuando el motivo de inconstitucionalidad que pretende hacerse valer atañe a la vulneración de las reglas constitucionales y estatutarias de distribución de competencias. El Derecho de la Unión Europea no altera el orden constitucional y estatutario de reparto de competencias entre el Estado y las comunidades autónomas (por todas, STC 45/2001, de 15 de febrero, FJ 7), por lo que la ejecución del Derecho europeo presenta carácter neutro en cuanto que no «predetermina el reparto de competencias dentro de nuestro ordenamiento interno» (STC 100/2019, de 18 de julio, FJ 5).

Atendiendo a las reglas de reparto competencial, puede, en principio, considerarse que la regulación del art. 155 de la Ley 40/2015 tiene amparo en las competencias estatales en materia de régimen jurídico de las administraciones públicas del art. 149.1.18 CE, en cuanto contribuye a determinar las garantías en torno a los datos de los ciudadanos cuando son objeto de transmisión o cesión entre las respectivas administraciones públicas, con la doble finalidad de facilitar el ejercicio de las funciones y

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

competencias propias de aquellas y, al propio tiempo, asegurar los derechos de los administrados en este concreto ámbito material.

Sin embargo, la concreta excepción aquí discutida encuentra su fundamento, conforme al tenor del precepto, en consideraciones basadas únicamente en la preservación de la seguridad nacional, lo que enlaza con las competencias estatales exclusivas del art. 149.1.4 y 29 CE (STC 184/2016, de 3 de noviembre, FJ 3). Se trata de una medida de prevención que tiene por finalidad proporcionar al Estado capacidad de reacción ante situaciones que afectan a esa seguridad nacional, de indudable responsabilidad estatal. Atendiendo a las anteriores consideraciones, no cabe poner en duda la competencia estatal para realizar la actuación en cuestión, justificándose en el ejercicio de atribuciones propias relacionadas con la preservación de un ámbito de responsabilidad estatal, como es la seguridad nacional en el entorno de la sociedad de la información y de las nuevas tecnologías de la comunicación (STC 142/2018, FJ 4), sin que ello suponga una alteración del esquema competencial, ni tampoco, por la misma razón, el establecimiento de un inconstitucional mecanismo de tutela sobre la actuación autonómica, extremo en el que la recurrente ha centrado sus quejas.

Por otro lado, la excepción, fundada en motivos de seguridad nacional, al régimen general de comunicación de datos entre administraciones públicas no es incondicionada, sino que incorpora una serie de cautelas o garantías que contribuyen a delimitar su ejercicio. Por un lado, esta potestad de suspensión de la cesión de datos tiene carácter excepcional y se adopta de manera motivada y por el tiempo estrictamente indispensable para la preservación de la seguridad nacional. Por otro, atendiendo a su ubicación sistemática, no puede aplicarse a los supuestos en que el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales esté previsto en una norma con rango de ley, de conformidad con lo dispuesto en el art. 23.1 RGPD al que remite el precepto, esto es, cuando se fundamenta en una «medida necesaria y proporcional en una sociedad democrática» para salvaguardar fines como la seguridad del Estado; la defensa; la seguridad pública; la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales incluida la protección frente a amenazas a la seguridad pública y su prevención; otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social; la protección de la independencia judicial y de los procedimientos judiciales; la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; la supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública; la protección del interesado o de los derechos y libertades de otros y la ejecución de demandas civiles.

Procede, por tanto, desestimar la impugnación.

6. Quejas competenciales en relación con la modificación de la Ley 9/2014, de 9 de mayo, general de telecomunicaciones.

(i) El art. 6.2 introduce un nuevo apartado tercero en el art. 6 LGTel, que queda redactado como sigue:

«Las administraciones públicas deberán 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 vaya a realizarse de manera directa, a través de cualquier entidad o sociedad dependiente de ella o a través de cualquier entidad o sociedad a la que se le haya otorgado una concesión o habilitación al efecto.

El régimen de autoprestación en la instalación o explotación de dicha red puede ser total o parcial, y por tanto dicha comunicación deberá efectuarse aun cuando la

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

capacidad excedentaria de la citada red pueda utilizarse para su explotación por terceros o para la prestación de servicios de comunicaciones electrónicas disponibles al público.

En el caso de que se utilice o esté previsto utilizar, directamente por la administración pública o por terceros, la capacidad excedentaria de estas redes de comunicaciones electrónicas en régimen de autoprestación, el Ministerio de Economía y Empresa verificará el cumplimiento de lo previsto en el artículo 9. A tal efecto, la administración pública deberá proporcionar al Ministerio de Economía y Empresa toda la información que le sea requerida a efecto de verificar dicho cumplimiento.

La obligación establecida en este apartado se entiende sin perjuicio de la prevista en el artículo 7.3 de esta ley.»

Relacionada con la anterior se encuentra la disposición adicional única que prevé que la comunicación de las redes de comunicaciones electrónicas en régimen de autoprestación que hagan uso del dominio público que hayan sido instaladas o estén en proceso de instalación o explotación se lleve a cabo en el plazo de un mes contado a partir de la entrada en vigor del Real Decreto-ley 14/2019.

Según la demanda, la obligación de comunicar al Ministerio de Economía y Empresa las redes de comunicaciones en régimen de autoprestación de la Generalitat de Cataluña que hagan uso del dominio público es una medida redundante, en cuanto referida a un ámbito en el que la administración del Estado ya dispone de suficiente información, ya que esta obligación se añade a la ya existente de notificación al registro de operadores prevista en aquel momento en el art. 7.3 LGTel y al amplio elenco de obligaciones informativas que pesan sobre quienes exploten redes o presten servicios de comunicaciones electrónicas, conforme al art. 10 LGTel. Se considera, además, que incorpora un mecanismo de control inconstitucional y extralimita las competencias estatales del art. 149.1.21 CE, vulnerando la potestad de autoorganización autonómica. El abogado del Estado sostiene que una obligación de mera comunicación no puede vulnerar la competencia autonómica de autoorganización. El único fin de la norma es garantizar que el uso del excedente de redes en autoprestación no dé lugar a distorsiones en la competencia que puedan contravenir el Derecho de la Unión Europea por el que deba responder el Reino de España.

La adecuada comprensión del precepto impugnado requiere hacer una referencia al régimen de la Ley 11/2022, general de telecomunicaciones, en punto a la actuación de las administraciones públicas en esta materia.

La Ley 11/2022 contiene el régimen jurídico que regula la explotación de redes y prestación de servicios de comunicaciones electrónicas en régimen de libre competencia, diferenciando entre las redes y servicios que se explotan a terceros («al público») y las actividades de telecomunicaciones que se sujetan al régimen de autoprestación. Al respecto, la mencionada ley prevé dos tipos de intervenciones de las administraciones públicas en el ámbito de las comunicaciones electrónicas: por una parte, la instalación y explotación de redes públicas o la prestación de servicios de comunicaciones electrónicas en régimen de prestación a terceros por operadores controlados directa o indirectamente por administraciones públicas y, por otra parte, las actuaciones en régimen de autoprestación.

El primer supuesto es el previsto en el art. 13 de la Ley 11/2022 en el que la actividad «se realizará dando cumplimiento al principio de inversor privado, con la debida separación de cuentas, con arreglo a los principios de neutralidad, transparencia, no distorsión de la competencia y no discriminación, y cumpliendo con la normativa sobre ayudas de Estado a que se refieren los artículos 107 y 108 del Tratado de Funcionamiento de la Unión Europea» (art. 13.2 LGTel), actividad que está sometida a la previa comunicación al registro de operadores previsto en el art. 7 de la Ley 11/2022.

En el caso de autoprestación, esto es, «la explotación de redes y la prestación de servicios de comunicaciones electrónicas por una administración pública para la satisfacción de sus necesidades, esto es, las vinculadas al desempeño de las funciones propias del personal al servicio de la administración pública de que se trate y que contribuyan al cumplimiento de los fines que le son propios» (Circular 1/2010, de la

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

Comisión del Mercado de las Telecomunicaciones, por la que se regulan las condiciones de explotación de redes y la prestación de servicios de comunicaciones electrónicas por las administraciones públicas, publicada en el «Boletín Oficial del Estado» de 9 de agosto de 2010), la administración pública no está sometida al régimen general de libre competencia que, en cuanto que deriva del art. 5 de la Ley 11/2022, es inherente a la explotación de redes y a la prestación de servicios de comunicaciones electrónicas.

A las anteriores obligaciones, se añade ahora el deber de comunicar al Ministerio de Asuntos Económicos y Transformación Digital el proyecto de instalación o explotación de redes en régimen de autoprestación que hagan uso del dominio público, tanto si la actividad se realiza de forma directa como indirecta. Asimismo, se dispone que, en caso de que la citada red de comunicaciones electrónicas en régimen de autoprestación tenga capacidad excedentaria, pueda usarse para su explotación por terceros o para la prestación de servicios de comunicaciones electrónicas disponibles al público, el citado Ministerio verifique el cumplimiento de lo previsto en el art. 13 LGTel.

Señalado todo lo anterior, estamos ya en condiciones de abordar el enjuiciamiento de ambas disposiciones, comenzando por su encuadramiento competencial. Al respecto el Real Decreto-ley 14/2019, las considera dictadas al amparo de la competencia estatal del art. 149.1.21 CE en materia de régimen general de comunicaciones (disposición final primera.4).

A la vista del contenido y finalidad de ambos preceptos, es preciso convenir en que se trata de una materia que incide en el régimen de explotación de las redes y de prestación de los servicios de comunicaciones electrónicas, inserto en la materia del régimen general de comunicaciones (STC 8/2012, de 18 de enero, FJ 7), sobre la que corresponde al Estado la totalidad de la competencia normativa *ex* artículo 149.1.21, e incluso la función ejecutiva necesaria para configurar un sistema materialmente unitario [por todas, STC 142/2018, de 20 de diciembre, FJ 6 b)]. El apartado 7 del art. 140 EAC atribuye a la Generalitat «de acuerdo con la normativa del Estado, la competencia ejecutiva en materia de comunicaciones electrónicas», citando a continuación las potestades que incluye, potestades que la doctrina constitucional ha relacionado preferentemente con la materia relativa a los medios de comunicación social. Dicha competencia no puede menoscabar ni perturbar la competencia estatal en materia de régimen general de comunicaciones que tiene por objeto ordenar normativamente y asegurar la efectividad de las comunicaciones, ni tampoco la dimensión técnica vinculada al uso del dominio público radioeléctrico que está en manos del Estado, que es su titular (art. 149.1.21 CE; STC 31/2010, de 28 de junio, FJ 85).

En particular, la STC 8/2016, de 21 de enero, FJ 3, ya destacó que «el Estado es competente, en exclusiva, para: a) la caracterización del sector (mercado) de las telecomunicaciones —actualmente, definidas como servicios de interés general que se prestan en régimen de libre competencia (arts. 2 y 5 de la Ley general de telecomunicaciones) frente a su tradicional consideración de servicio público—; b) el establecimiento de las condiciones de explotación de las redes y de prestación de servicios de comunicaciones electrónicas así como el régimen jurídico de los operadores (STC 8/2012, FJ 7)», señalando posteriormente que «[s]e trata, en definitiva, de la atribución al Estado de la competencia para definir los elementos estructurales del sector a través tanto del establecimiento del marco institucional del mercado (regulación de la competencia) como de la intervención en los procesos del propio mercado (obligaciones de hacer o no hacer de los operadores del sector, en el ámbito del acceso a redes, interconexión o garantía de cobertura, por ejemplo».

Atendiendo a la doctrina que se acaba de exponer, no cabe apreciar el reproche competencial que se formula a los preceptos impugnados, pues esta exigencia de información se justifica en las competencias estatales en la materia, sin que implique una supervisión de la actuación autonómica incompatible con su autonomía. Lejos de establecer fórmula alguna de control o supervisión, el precepto impugnado regula un mecanismo de suministro de información que se incardina con naturalidad en el marco

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

de la colaboración y la lealtad institucional, implícitos en el correcto funcionamiento del sistema autonómico.

Estos mecanismos se justifican desde un doble punto de vista.

En primer término, la obligación de remisión de la información necesaria para el ejercicio de las competencias propias es un medio válido de cooperación entre administraciones públicas. Téngase en cuenta, además, que según el art. 142 de la Ley 40/2015, el deber de colaboración puede hacerse efectivo, entre otras, a través de la técnica del suministro de información, datos, documentos o medios probatorios que se hallen a disposición del organismo público o la entidad al que se dirige la solicitud y que la administración solicitante precise disponer para el ejercicio de sus competencias.

Más específicamente, esta comunicación permite, en última instancia, asegurar el cumplimiento de los requisitos para el uso de la capacidad excedentaria de estas redes, requisitos que los cuales tienen como finalidad salvaguardar los principios de inversor privado, neutralidad, transparencia, no distorsión de la competencia y no discriminación propios de un mercado liberalizado como es el de las telecomunicaciones, pero con fuerte intervención pública. Así pues, la verificación a la que se alude en el precepto tiene que ver, como así lo expresa con su referencia al art. 13 LGTel, con la necesidad de asegurar el respeto a las normas aplicables a la explotación de redes y de servicios de comunicaciones electrónicas en régimen de prestación a terceros por parte de las administraciones públicas y, por lo tanto, a través de operadores controlados por estas.

Como resaltó la STC 8/2016, FJ 6, el Estado, en ejercicio de la competencia exclusiva que le otorga el art.149.1.21 CE para regular las condiciones de explotación de redes y prestación de servicios, ha decidido caracterizarlo como un sector abierto a la libre competencia cuyas particulares características, sin embargo, determinan no solo una regulación más intensa por parte de los poderes públicos, sino también la posibilidad de establecer excepciones a aquel principio. Entre tales excepciones está la posibilidad de la instalación y explotación de redes públicas y prestación de servicios de comunicaciones electrónicas por operadores controlados directa e indirectamente por las administraciones públicas, excepción que también implica la de definir los servicios cuya prestación por los poderes públicos no supone una distorsión de la libre competencia del sector y que justifica la tarea de verificación que aquí se ha discutido. Tampoco se impide con ello que la comunidad autónoma, en su ámbito de competencias, pueda adoptar las medidas que considere adecuadas para garantizar la prestación de los servicios y las redes de comunicación electrónicas que sean de su responsabilidad.

En suma, por todo lo expuesto, esta impugnación debe ser desestimada.

(ii) b) El art. 6.5 da nueva redacción al apartado 1 del art. 81 LGTel que queda redactado en los términos siguientes:

«1. Previamente al inicio del procedimiento sancionador, podrá ordenarse por el órgano competente del Ministerio de Economía y Empresa, mediante resolución sin audiencia previa, el cese de la presunta actividad infractora cuando existan razones de imperiosa urgencia basada en alguno de los siguientes supuestos:

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 de la supuesta actividad infractora puedan producirse perjuicios graves al funcionamiento de los servicios de seguridad pública, protección civil y de emergencias.

d) Cuando se interfiera gravemente a otros servicios o redes de comunicaciones electrónicas.

e) Cuando cree graves problemas económicos u operativos a otros proveedores o usuarios de redes o servicios de comunicaciones electrónicas o demás usuarios del espectro radioeléctrico.»

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

La demanda argumenta que la medida cautelar consistente en el cese de la actividad presuntamente infractora, antes de iniciar un procedimiento sancionador, es contraria a las competencias autonómicas en materia de comunicaciones electrónicas del art. 140.7 EAC, así como a las relativas a la organización de sus propios recursos en materia de administración electrónica derivadas de los arts. 150 y 159 EAC. Se incide con esta previsión en el control de las infraestructuras de comunicación que la administración de la Generalitat de Cataluña utiliza para la prestación de las comunicaciones corporativas dentro del ámbito de sus competencias, constituyendo una intromisión en el ámbito de la ejecución de la infraestructura digital de la administración.

El abogado del Estado defiende que la modificación que se introduce en el art. 81.1 LGTel no tiene otro objetivo que reforzar las potestades del Gobierno para actuar en situaciones que puedan suponer una amenaza inmediata y grave para el orden público, la seguridad, la seguridad nacional o la salud pública y para ello amplía los supuestos habilitantes para la adopción de una medida cautelarísima previa al inicio del expediente sancionador sin audiencia del presunto infractor. Este instrumento y los supuestos habilitantes existen en todo ordenamiento jurídico y, en particular, en el art. 30.6 del Código europeo de las comunicaciones electrónicas. Y, todo ello, sin que se afecte a las garantías que la propia LGTel y la Ley 39/2015 otorgan al presunto infractor, ni altere el régimen de responsabilidad previsto en la Ley general de telecomunicaciones, ya se trate de un operador público o privado o de cualquier otro sujeto obligado a respetar lo establecido en la normativa de telecomunicaciones.

Pues, bien, la queja competencial, la única a la que nos referiremos por las razones expuestas en el fundamento jurídico 2, no puede prosperar. Se integra en la materia de telecomunicaciones y de régimen general de comunicaciones (y corresponde, por tanto, al Estado la competencia exclusiva conforme al art. 149.1.21 CE) la conformación, regulación o configuración del propio sector, en el que se incluye el establecimiento de las condiciones de explotación de las redes y de prestación de servicios de comunicaciones electrónicas, así como el régimen jurídico de los operadores (STC 8/2016, citando la STC 8/2012, de 18 de enero, FJ 7).

Por otro lado, ha de recordarse el carácter instrumental de la potestad sancionadora respecto a la competencia material de manera que la titularidad de la potestad sancionadora va ligada a la competencia sustantiva de que se trate (STC 34/2013, de 14 de febrero, FJ 19, entre muchas otras). Por ello, el titular de la competencia sustantiva lo es también de las potestades de naturaleza ejecutiva referidas a la inspección, vigilancia y control, a la adopción de medidas provisionales y a la instrucción de expedientes sancionadores; de esta suerte, al Estado le corresponde definir el régimen sancionador aplicable a la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas y los recursos asociados (art. 1.1 LGTel), determinando a quién corresponde la responsabilidad por las infracciones en materia de telecomunicaciones (art. 74 LGTel), tipificando las conductas (arts. 76 a 78 LGTel) y las sanciones correspondientes (arts. 79 y 80 LGTel). No hay, por tanto, previsión alguna de control de las infraestructuras de comunicaciones de competencia de la Generalidad de Cataluña, sin que la demanda tampoco explicite el modo en que el ejercicio de esas competencias sancionadoras puede suponer un control inconstitucional susceptible de afectar a la explotación de redes y prestación de servicios que, en régimen de autoprestación, realice la comunidad autónoma. Y tampoco se vulnera el art. 140.7 EAC, por cuanto ya tenemos declarado que «dicha competencia no puede menoscabar ni perturbar la competencia estatal en materia de régimen general de comunicaciones que tiene por objeto ordenar normativamente y asegurar la efectividad de las comunicaciones, ni tampoco la dimensión técnica vinculada al uso del dominio público radioeléctrico que está en manos del Estado, que es su titular (art. 149.1.21 CE; STC 31/2010, de 28 de junio, FJ 85)» (STC 142/2018, FJ 6).

Por tanto, esta impugnación ha de ser desestimada.

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

(iii) El art 7 del Real Decreto-ley 14/2019 modifica el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, introduciendo un apartado 3 en el art. 11 del siguiente tenor literal:

«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 comprendido en la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, y en la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.

Los CSIRT de las administraciones públicas consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellos en el ejercicio de sus respectivas funciones.

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 que les correspondan.»

En la demanda se argumenta que este precepto desconoce las competencias autonómicas en relación con los incidentes de seguridad que se refieran a servicios en el ámbito de competencias autonómico, con lo que se vulneran los arts. 150 y 159 EAC y se desconoce la doctrina de la STC 142/2018, de 20 de diciembre, en relación a la Agencia Catalana de Ciberseguridad. El abogado del Estado ha negado la vulneración denunciada señalando que esta coordinación ya se establecía tanto en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, como en el esquema nacional de seguridad en la administración electrónica aprobado en el año 2010, lo que encuentra justificación en las competencias exclusivas en materia de comunicaciones (art. 149.1.21 CE) y de seguridad pública (art. 149.1.29 CE), sin que menoscabe las competencias autonómicas para crear centros de soporte ante incidentes en el ámbito de su sector público.

El Real Decreto-ley 12/2018 ahora modificado tiene, entre otros objetivos, el de trasponer al derecho español la Directiva (UE) 2016/1148, del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva NIS, por las siglas *Network and Information Systems*). Esta norma persigue regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales y establecer un sistema de notificación de incidentes. Además, establece un marco institucional para su aplicación y la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario. El real decreto-ley se aplica a los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, así como a los servicios de la sociedad de la información en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. La norma identifica los sectores en los que es necesario garantizar la protección de las redes y sistemas de información, y establece procedimientos para identificar los servicios esenciales ofrecidos en dichos sectores, así como los principales operadores que prestan dichos servicios.

Conforme a su art. 1, tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes. En lo que a esto último respecta, desarrolla la red CSIRT (por sus siglas en inglés de *Computer Security Incident Response Team*) creada por la Directiva NIS, definiendo a dichos organismos como los equipos de respuesta a incidentes que analizan riesgos y supervisan incidentes a escala nacional (definido como suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información), difunden alertas sobre ellos y aportan soluciones para mitigar sus efectos (arts. 11 y 12). El art. 11.1 a) 1

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

del Real Decreto-ley 12/2018 declara que tiene la condición de CSIRT de referencia en materia de seguridad de las redes y sistemas de información respecto de la comunidad constituida por las entidades públicas incluidas en el ámbito de aplicación de la Ley 40/2015, el Centro Criptológico Nacional [CCN-CERT (*Computer Emergency Response Team*)] —que fue creado por el Real Decreto 421/2004, de 12 de marzo— adscrito al Centro Nacional de Inteligencia (Ley 11/2002, de 6 de mayo).

De lo expuesto se deduce que, en lo que resulta de relevancia para el presente proceso, los CSIRT son los responsables del desarrollo de las medidas preventivas y reactivas ante incidentes de seguridad en los sistemas de información y telecomunicaciones de los que se sirvan las administraciones públicas para así garantizar la seguridad de los sistemas de las tecnologías de la información que emplean.

El precepto impugnado atribuye al Centro Criptológico Nacional la coordinación estatal de todas las autoridades o equipos de respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información. Adicionalmente, obliga a todos los CSIRT de las administraciones públicas a colaborar en el ejercicio de las funciones respectivas y a consultar, cuando proceda, a los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal. Finalmente, atribuye al Centro Criptológico Nacional la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las administraciones públicas con los CSIRT internacionales, cuando se trate de la respuesta a los incidentes y la gestión de los riesgos de seguridad que les corresponden.

Es, por tanto, evidente, la relación que el precepto impugnado guarda con la materia ciberseguridad, respecto a la que nos pronunciamos en la ya citada STC 142/2018. Tal como allí se declaró «[l]a ciberseguridad, como sinónimo de la seguridad en la red, es una actividad que se integra en la seguridad pública, así como en las telecomunicaciones. A partir de su conceptuación como conjunto de mecanismos dirigidos a la protección de las infraestructuras informáticas y de la información digital que albergan, fácilmente se infiere que, en tanto que dedicada a la seguridad de las tecnologías de la información, presenta un componente tuitivo que se proyecta específicamente sobre el concreto ámbito de la protección de las redes y sistemas de información que utilizan los ciudadanos, empresas y administraciones públicas. El uso cotidiano de las tecnologías de la información y la comunicación ha provocado que se conviertan en un elemento esencial para el desarrollo económico y las relaciones sociales. No obstante, es también un hecho constatado que las amenazas a la seguridad de la red comportan un riesgo que afecta a los ámbitos más diversos, por cuanto pueden afectar a la disponibilidad, integridad y confidencialidad de la información» (FJ 4). También señalamos que «la ciberseguridad no es un concepto o materia reconducible a un único título competencial. Puede, como allí se recalca, identificarse con la seguridad nacional o con la seguridad pública cuando se trata de la protección ordinaria de las redes y las infraestructuras de telecomunicaciones. Pero también puede proyectarse sobre otros planos, como es el caso de la administración electrónica, que abarca la organización de medios y previsión de medidas de protección de la administración y, por extensión, la protección de los derechos de los ciudadanos cuando se relacionan con la administración por medios electrónicos» (FJ 5).

Constatamos así, el carácter «transversal e interconectado de las tecnologías de la información y las comunicaciones y de su conceptuación como conjunto de mecanismos dirigidos a la protección de las infraestructuras informáticas y de la información digital que albergan los sistemas interconectados» (STC 142/2018, FJ 5), lo que, a su vez, determinaba dos consecuencias. La primera, su encuadramiento material en el ámbito de las competencias estatales en materia de seguridad pública en relación con las relativas a las telecomunicaciones y a la seguridad nacional. La segunda era que, a partir del respeto a dichas competencias estatales a las que se acaba de hacer mención, las diferentes administraciones públicas son competentes para la adopción de medidas de

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

autoprotección en relación con sus infraestructuras y la seguridad de las tecnologías de la información y la comunicación, en la medida en que, como ya se ha mencionado, el diseño, creación y mantenimiento de «servicios de administración electrónica» es un aspecto central de la «potestad de autoorganización» inherente a la autonomía (STC 111/2016, de 9 de junio, FJ 11).

A la vista de la delimitación competencial en la materia, debe examinarse el precepto impugnado empezando por la función de coordinación nacional que asume el Centro Criptológico Nacional.

Respecto a la función de coordinación, la doctrina constitucional tiene declarado que «la coordinación persigue la integración de la diversidad de las partes o subsistemas en el conjunto o sistema, evitando contradicciones y reduciendo disfunciones que, de subsistir, impedirían o dificultarían respectivamente la realidad misma del sistema» (STC 33/2017, de 1 de marzo, FJ 4). La coordinación estatal sirve así para garantizar que no haya disfunciones, y «"presupone la existencia de competencias de las Comunidades Autónomas que deben ser coordinadas, y que el Estado debe respetar al desarrollar su función de coordinación […] la competencia de coordinación no otorga a su titular competencias que no ostente, especialmente facultades de gestión complementarias, de suerte que, implicando lógicamente su ejercicio la existencia de competencias autonómicas que deben ser coordinadas, en ningún caso puede aquel suponer la invasión y el vaciamiento de las mismas (STC 194/2004, FJ 8). En definitiva, la competencia en materia de coordinación no autoriza al Estado "para atraer hacia su órbita de actividad cualquier competencia de las Comunidades Autónomas por el mero hecho de que su ejercicio pueda incidir en el desarrollo de las competencias estatales sobre determinadas materias. La coordinación no supone "una sustracción o menoscabo de las competencias de las entidades sometidas a la misma: antes bien, presupone, lógicamente, la titularidad de las competencias en favor de la entidad coordinada" (STC 27/1987, de 27 de febrero); por lo que no puede servir de instrumento para asumir competencias autonómicas, ni siquiera respecto de una parte del objeto material sobre el que recaen" [STC 227/1988, de 29 de noviembre, FJ 20 e)]" (FJ 9)» [STC 71/2018, de 21 de junio, FJ 3 b)].

Conforme a dicha doctrina, ninguna objeción cabe formular al hecho de que la función de coordinación sea ejercida por un órgano estatal, sin que con ello se produzca detrimento o menoscabo de las competencias autonómicas. Esta previsión tampoco desconoce la doctrina de la STC 142/2018, por cuanto la atribución de dicha función coordinadora al órgano estatal en nada afecta a las competencias autonómicas, delimitadas en los términos que allí se expusieron, sino que responde a la necesidad de un funcionamiento armonizado del conjunto de instrumentos y mecanismos para la prevención y respuesta de los incidentes de seguridad en las redes.

Ningún reproche cabe formular tampoco al mecanismo de consulta al que alude el segundo párrafo del precepto impugnado, en tanto que manifestación de los principios de colaboración y cooperación que han de regir en las relaciones entre las administraciones públicas. No en vano el principio de cooperación entre el Estado y las Comunidades Autónomas está implícito en el correcto funcionamiento del Estado de las Autonomías; depende en buena medida de la estricta sujeción de uno y otras a las fórmulas racionales de cooperación, consulta, participación, coordinación, concertación o acuerdo previstas en la Constitución y en los estatutos de autonomía (por todas, STC 109/2017, de 21 de septiembre, FJ 4), sin que, tal como se diseña, presente el riesgo de usarse para «eludir responsabilidades propias ni para ejercer las competencias que el sistema constitucional ha atribuido a otras Administraciones» (STC 132/2018, de 13 de diciembre, FJ 10). Así pues, esta posibilidad de consulta («cuando proceda»), dirigido indistintamente a los CIRST de todas las administraciones públicas, respecto a los órganos con competencias específicas en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y de colaborar con ellos en el ejercicio de sus respectivas funciones, es conforme con el orden competencial.

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

Por último, la función de enlace atribuida al Centro Criptológico Nacional lo es para garantizar la cooperación transfronteriza con los CIRST internacionales lo que pone de relieve su vinculación con la competencia estatal del art. 149.1.3 CE, en relación con las competencias estatales en materia de ciberseguridad. Por otra parte, responde a una de las exigencias de la Directiva NIS, (art. 8.3 y 4) en cuanto que esta norma exige a cada Estado miembro la designación de un único punto de contacto en materia de seguridad de las redes y sistemas de información para garantizar la cooperación transfronteriza entre las autoridades de los estados miembros y con las autoridades competentes en otros estados miembros y con el grupo de cooperación y la red de CSIRT.

Respecto a esto último es preciso también recordar la consolidada doctrina según la cual «en el ámbito de la resolución de disputas competenciales, bien sea en conflictos de competencias o en procesos de inconstitucionalidad, el hecho de que una competencia suponga ejecución del Derecho comunitario no prejuzga cuál sea la instancia territorial a la que corresponda su ejercicio, porque ni la Constitución ni los estatutos de autonomía prevén una competencia específica para la ejecución del Derecho comunitario; si bien tampoco cabe ignorar la necesidad de proporcionar al Gobierno los instrumentos indispensables para desempeñar la función que le atribuye el artículo 93 CE […] esto es, para adoptar las medidas necesarias a fin de garantizar el cumplimiento de las resoluciones de los organismos internacionales en cuyo favor se han cedido competencias (del Derecho derivado europeo, en lo que ahora interesa), función que solo una interpretación inadecuada de los preceptos constitucionales y estatutarios puede obstaculizar» [STC 69/2018, de 21 de junio, FJ 5 c)].

Consecuentemente, la impugnación del art. 7 del Real Decreto-ley 14/2019 debe ser desestimada.

7. Desestimación de la impugnación de la disposición final primera del Real Decreto-ley 14/2019.

La disposición final primera explicita los títulos competenciales estatales que prestan amparo a las distintas regulaciones incluidas en el Real Decreto-ley 14/2019. Su impugnación no es autónoma. La demanda fundamenta el reproche competencial simplemente en la conexión que la referida disposición tiene con el resto de los contenidos impugnados del Real Decreto-ley 14/2019 por razones competenciales. De modo que la desestimación de las anteriores impugnaciones lleva consigo la de la disposición final primera (en el mismo sentido, entre otras, STC 101/2017, de 20 de julio, FJ 11).

FALLO

En atención a todo lo expuesto, el Tribunal Constitucional, por la autoridad que le confiere la Constitución de la Nación española, ha decidido:

1.º Declarar extinguido, por pérdida sobrevenida del objeto, el presente recurso de inconstitucionalidad núm. 718-2020, interpuesto por el Gobierno de la Generalitat de Cataluña contra 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, en relación con el art. 3.1 y 2 (respecto de la modificación de los arts. 9.2 c) y 10.2 c) de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas); en relación con el art. 6.1 (que modifica el art. 4.6 de la Ley 9/2014, de 9 de mayo, general de telecomunicaciones); y en relación con el art. 6.5 (que da nueva redacción al art. 81.1 de la Ley general de telecomunicaciones).

cve: BOE-A-2023-8217
Verificable en https://www.boe.es

2.º Desestimar el recurso en todo lo demás.

Publíquese esta sentencia en el «Boletín Oficial del Estado».

Dada en Madrid, a veintitrés de febrero de dos mil veintitrés.–Cándido Conde-Pumpido Tourón.–Inmaculada Montalbán Huertas.–Ricardo Enríquez Sancho.–María Luisa Balaguer Callejón.–Ramón Sáez Valcárcel.–Enrique Arnaldo Alcubilla.–Concepción Espejel Jorquera.–María Luisa Segoviano Astaburuaga.–César Tolosa Tribiño.–Laura Díez Bueso.–Firmado y rubricado.

cve: BOE-A-2023-8217
Verificable en https://www.boe.es