SECCIÓN DEL TRIBUNAL CONSTITUCIONAL

TRIBUNAL CONSTITUCIONAL

10045 *Pleno. Sentencia 20/2023, de 23 de marzo de 2023. Conflicto positivo de competencia 5253-2021. Planteado por el Consejo de Gobierno de la Comunidad Autónoma del País Vasco, en relación con diversos preceptos del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo. Competencias sobre seguridad pública, autoorganización y régimen jurídico de las administraciones públicas: extinción del conflicto constitucional por pérdida sobrevenida de su objeto.*

ECLI:ES:TC:2023:20

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 conflicto positivo de competencia núm. 5253-2021, promovido por el Consejo de Gobierno de la Comunidad Autónoma del País Vasco, en relación con los artículos 15.3 a), 26.2 c), 28.2 y 29.4, y la disposición adicional novena del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por Real Decreto 203/2021, de 30 de marzo. Ha sido parte el abogado del Estado, en la representación que ostenta. Ha sido ponente la magistrada doña María Luisa Segoviano Astaburuaga.

I. Antecedentes

1. Mediante escrito presentado en el registro general de este tribunal el 28 de julio de 2021, el Consejo de Gobierno de la Comunidad Autónoma del País Vasco promovió conflicto positivo de competencia en relación con los arts. 15.3 a), 26.2 c), 28.2 y 29.4, así como con la disposición adicional novena del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por Real Decreto 203/2021, de 30 de marzo.

Inicia su demanda mediante la exposición de los términos en los que se dio cumplimiento al trámite previo del requerimiento de incompetencia. Asimismo, da cuenta de que el Gobierno Vasco ha interpuesto el recurso de inconstitucionalidad núm. 1220-2021 contra, entre otros, los arts. 9 y 10 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (LPACAP), en la redacción dada por el art. 3 del Real Decreto-ley 14/2019, de 31 de octubre. Añade que tales artículos modificados son reproducidos por los preceptos reglamentarios contra los que se reacciona en este conflicto, siendo coincidente su objeto, pues en ambos casos se discute la autorización, previo informe vinculante, que se ha reservado el

cve: BOE-A-2023-10045
Verificable en https://www.boe.es

Estado para la admisión de determinados sistemas de identificación y firma electrónica de los ciudadanos ante las administraciones públicas.

A continuación, la demanda justifica el cumplimiento de los requisitos temporales y formales exigidos en la Ley Orgánica del Tribunal Constitucional (LOTC), y, tras identificar los preceptos impugnados, solicita que se declare la incompetencia del Estado para adoptar las disposiciones impugnadas y su consiguiente inconstitucionalidad, así como la nulidad de los preceptos que contienen la autorización y el informe vinculante que dos órganos de la Administración General del Estado han de emitir de forma previa, necesaria –dada la previsión del silencio desestimatorio–, y favorable para la implantación por las administraciones públicas autonómicas de los sistemas de identificación y firma para los ciudadanos que se dirijan a ellas por vía electrónica, basados en sistemas de clave concertada y otros sistemas de identificación y firma distintos de los sistemas de certificados de firma electrónica y certificados de sellos electrónicos avanzados y cualificados expedidos por prestadores incluidos en la «lista de confianza de prestadores de servicios de certificación».

El Gobierno demandante considera que el conflicto afecta a dos ámbitos esenciales de la correcta prestación del servicio público por las administraciones públicas vascas en sede digital: la identificación de los ciudadanos ante estas administraciones y la firma de los ciudadanos en sus escritos a ellas dirigidos. De los tres sistemas de identificación, centran el conflicto positivo en el previsto en los arts. 9.2 c) y 10.2 c) LPACAP, sobre identificación y firma respectivamente. Es el conocido como «sistema de clave concertada», y es la forma en la que los ciudadanos pueden identificarse para realizar trámites administrativos y firmar sus escritos ante las administraciones públicas sin disponer de certificado electrónico cualificado. Tras describir su sistema de funcionamiento, más cómodo en su uso que los basados en certificados electrónicos cualificados, expone la necesidad de seguridad de estos sistemas frente a los ciberataques.

Destaca que el legislador ha regulado el esquema nacional de seguridad como el instrumento nuclear con el que establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de las administraciones públicas, con naturaleza de norma básica, conforme al art. 149.1.18 CE (disposición final primera del Real Decreto 3/2010, de 8 de enero), y expone la finalidad y contenido del esquema nacional de seguridad (arts. 1.1, 31 y 33 del Real Decreto 3/2010), así como su complemento a través de las guías de seguridad e instrucciones técnicas de seguridad (art. 29 del Real Decreto 3/2010), de obligado cumplimiento. Añade a ello la cita de las medidas de organización en materia de seguridad adoptadas por el Gobierno Vasco: Orden de 26 de febrero de 2010, de la consejera de Justicia y Administración Pública; acuerdo del Consejo de Gobierno Vasco de 30 de junio de 2015, mediante el cual se aprobó la estructura organizativa y asignación de roles de seguridad para la administración electrónica del Gobierno Vasco; y los Decretos 21/2012, de 21 de febrero, de administración electrónica, y 36/2020, de 10 de marzo, que regula el modelo de gestión de las tecnologías de la información y la comunicación en el sector público de la Comunidad Autónoma de Euskadi.

Considera que el control estatal al que se someten los sistemas de identificación y firma basados en clave concertada, esto es, a una autorización otorgada por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio de Interior, no aparece justificado, por lo que no es posible saber a qué obedecen estas medidas tan extraordinarias que afectan a un aspecto tan puntual de la administración electrónica, ya que no se han adoptado medidas similares en ninguna otra faceta de dicha administración. Indica que no se encuentra su justificación en brechas de seguridad específicas en estos sistemas que requieran de medidas tan excepcionales. Señala que tampoco se cumple en este sentido con el principio de proporcionalidad en su triple vertiente, ni obedecen estas medidas a un canon de justo equilibrio o

cve: BOE-A-2023-10045
Verificable en https://www.boe.es

razonabilidad con los objetivos perseguidos. Afirma el representante del Gobierno Vasco que nos encontramos ante una intervención de la Administración General del Estado absolutamente genérica e indeterminada y donde los preceptos cuestionados solo indican que cabe la denegación exclusivamente «por motivos de seguridad pública». Y entiende que la afirmación del título competencial tal y como se recoge en el art. 149.1.29 CE (disposición final primera del Real Decreto 203/2021), aboca a una absoluta falta de seguridad jurídica y, en su conjunto, supone la vulneración de la competencia autonómica vasca en su capacidad de autoorganización (art. 10.2 del Estatuto de Autonomía para el País Vasco: EAPV).

Se alega también que el marco competencial adecuado de los preceptos impugnados se corresponde con el del art. 149.1.18 CE, al encontrarnos ante una cuestión de organización y procedimiento de las administraciones públicas. Se trata de la regulación de los sistemas de identificación y firma de los ciudadanos ante aquellas, en donde la seguridad de estos sistemas se ve integrada como un aspecto más de su diseño y configuración (STC 100/2019). En tal sentido, tras referirse al fundamento jurídico 9 de la STC 55/2018, de 24 de mayo, sostiene que la STC 142/2018, de 20 de diciembre, encuadró las políticas de ciberseguridad de las redes y sistemas de información de la Generalitat de Cataluña en materia de administración electrónica en el ámbito de la competencia autonómica de los arts. 150 y 159 EAC, y en el marco del art. 149.1.18 CE.

Esa misma conclusión se alcanza, a juicio del Gobierno Vasco, a partir de la contestación del Consejo de Ministros al requerimiento efectuado por el Consejo de Gobierno demandante, donde se insiste en que esa autorización e informe tienen por objetivo «únicamente verificar si el sistema validado tecnológicamente por parte de la administración y organismo público del que se trate puede o no producir afecciones o riesgos a la seguridad pública»; y también se deduce de la intervención de la ministra de Economía y Empresa en funciones, señora Calviño Santamaría, en el debate de convalidación del Real Decreto-ley 14/2019. Por esta razón, esta autorización previa y este informe preceptivo constituyen controles de ciberseguridad del sistema de identificación y firma que han de situarse en la materia régimen jurídico de las administraciones públicas (art. 149.1.18 CE).

A continuación, se detiene en el análisis de la STC 142/2018, que definió la ciberseguridad, como el «conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno» (FJ 4), por tanto, como una materia transversal, no reconducible a un único título, y que «afecta a cuestiones relacionadas con la seguridad pública y la defensa, las infraestructuras, redes y sistemas y el régimen general de telecomunicaciones». En relación con el pronunciamiento referido a la Agencia de Ciberseguridad de Cataluña, indica la demanda que, según el art. 2.2 de la Ley del Parlamento de Cataluña 15/2017, de 25 de julio, «tiene por objetivo la ejecución de las políticas públicas en materia de ciberseguridad», y que la mencionada sentencia abogó por la constitucionalidad de este precepto «entendido en el sentido de que el objetivo que persigue la agencia [autonómica] se relaciona con la necesidad de proteger las redes y sistemas de información de la administración de la Generalitat y de su sector público y los de los particulares y otras administraciones públicas que se relacionan por medios electrónicos con dicha administración, no es contrario al orden constitucional de distribución de competencias» [FJ 7 b) i)]. Sostiene, asimismo, que, en relación con la atribución a la Generalitat de la función de garantizar la ciberseguridad en la prestación de los servicios de identificación electrónica y de identidad, se validó su constitucionalidad [FJ 7 d)], al referirse a funciones circunscritas al «ámbito del Gobierno y de la administración de la Generalitat y de su sector público dependiente». De modo que se admitió la constitucionalidad de la garantía de la ciberseguridad en la prestación de los servicios de identificación electrónica y de identidad en los sistemas públicos circunscritos a la administración autonómica.

cve: BOE-A-2023-10045
Verificable en https://www.boe.es

Descarta el Gobierno Vasco que la seguridad de los sistemas de identificación y firma de los ciudadanos ante las administraciones públicas sea materia de seguridad pública (art. 149.1.29 CE), dada la necesidad de interpretar de modo restrictivo el aspecto material de la seguridad pública y de situar en el mismo de modo predominante las organizaciones y los medios instrumentales, en especial, los cuerpos de seguridad a que se refiere el art. 104 CE (STC 59/1985, de 6 de mayo, FJ 2 *in fine*). El Estado no puede invocar de forma vacua la seguridad pública para arrogarse competencias de control en las competencias de autoorganización vascas sobre su administración electrónica, y en sentido análogo lo ha rechazado este tribunal en la STC 33/1982, sobre seguridad alimentaria, o en la STC 313/1994, sobre seguridad industrial. Ambas sentencias negaron la prevalencia del art. 149.1.29 CE.

Se añade, igualmente, que ni el Real Decreto-ley 14/2019 ni el reglamento impugnado permiten deducir motivo alguno que justifique una intervención estatal, amparada en este título, sobre la ordinaria actividad de las administraciones públicas vascas en la autoorganización de su administración electrónica.

Una vez que se ha determinado que la materia de que se trata debe insertarse en el art. 149.1.18 CE, la demanda denuncia que los controles establecidos por las normas impugnadas suponen una vulneración del principio de autoorganización del art. 10.2 EAPV y del principio de autonomía de los arts. 2 y 137 CE, pues los informes y autorizaciones estatales previstos en los preceptos impugnados conllevan, a la postre, una posición jerárquica de control estatal sobre la actividad administrativa ordinaria de las comunidades autónomas, no derivada de la propia Constitución o de previsiones legales perfectamente legítimas (SSTC 215/2014 y 55/2018), teniendo carácter genérico o indeterminado, en contra de lo que ha destacado el Tribunal Constitucional [SSTC 154/2015, FJ 6 b), y 14/2018, FJ 10 c)]. Asimismo, es un control innecesario, al existir normativa básica, dictada en virtud del art. 149.1.18 CE, sobre seguridad de los sistemas públicos (esquema nacional de seguridad y las instrucciones técnicas de seguridad), y desproporcionado, no solo por no justificar que existan medidas menos restrictivas, sino por carecer de cualquier explicación.

Subsidiariamente, y para el caso de que se considere que estos controles se insertan en el art. 149.1.29 CE, defiende la demanda que, con fundamento en el art. 17 EAPV, la comunidad autónoma tiene competencias ejecutivas en materia de seguridad pública, invocando al efecto la doctrina establecida, entre otras, en las SSTC 86/2014, FJ 4, y 59/1985, FJ 2 *in fine*. Se aduce que, aunque las competencias en algunos aspectos de la ciberseguridad fueran reconducidas a los títulos de la seguridad pública del art. 149.1.29 CE o de las telecomunicaciones del art. 149.1.21 CE, ello no comporta que el Estado pueda desarrollar funciones de ejecución excluyendo a las comunidades autónomas. La Comunidad Autónoma del País Vasco tiene competencias de ejecución en materia de seguridad sobre las redes y sistemas públicos, que han sido expresamente reconocidas por el Estado. En tal sentido, se menciona la estrategia de seguridad nacional de 2017, que constituye el marco de referencia para la política de seguridad nacional, y que adopta una concepción amplia de la seguridad, en la que las comunidades autónomas desempeñan un importante papel activo. Por su parte, la estrategia de ciberseguridad nacional (2019), insiste aún más en el papel ejecutivo que desempeñan las comunidades autónomas, contemplando que dispongan de sus CSIRT (por sus siglas en inglés *Computer Security Incident Response Team*), con competencias propias y con capacidad de reacción ante incidentes de seguridad, en el marco del Real Decreto-ley 12/2018 y del Real Decreto 43/2021, y con multitud de servicios relacionados con esta seguridad pública de los sistemas. Todo ello sin perjuicio de las funciones de coordinación y colaboración entre todas ellas y con instancias estatales e internacionales. Del mismo modo, a las comunidades autónomas se les reconocen funciones ejecutivas en materia del art. 149.1.29 CE en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

En suma, una autorización y un informe de control como los que se imponen en los preceptos impugnados, amparados en el art. 149.1.29 CE, relegan absolutamente las

cve: BOE-A-2023-10045
Verificable en https://www.boe.es

competencias vascas del art. 17 EAPV, y, con vulneración de los principios de colaboración y coordinación, establecen un control jerárquico estatal sobre competencias ejecutivas autonómicas.

Finalmente, se alega en la demanda el carácter genérico e indeterminado de los controles establecidos en los preceptos impugnados, proscritos por el Tribunal Constitucional [STC 14/2018, FJ 10 b)], que, a juicio del Gobierno Vasco, no superan el test de proporcionalidad en sus tres escalones (STC 172/2020). Y el mismo resultado se obtiene si se someten al «canon de justo equilibrio, razonabilidad o adecuación de las medidas al objetivo perseguido» (STC 112/2011, FJ 6).

En conclusión, estos mecanismos de control estatal son exorbitantes y desproporcionados, y desbordan el justo equilibro entre los medios empleados y la finalidad pretendida, ya que se somete a autorización previa (incluso con silencio negativo) e informe preceptivo la legítima elección de todas las administraciones públicas del Estado (arts. 9.2 y 10.2 LPACAP) por este sistema de identificación y firma por clave concertada.

La demanda concluye solicitando que se tenga por promovido conflicto positivo de competencia contra los arts. 15.3 a), 26.2 c), 28.2 y 29.4, así como contra la disposición adicional novena, del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por Real Decreto 203/2021, de 30 de marzo, y que se dicte sentencia por la que declare la incompetencia del Estado para adoptar estas disposiciones por vulneración de las competencias de la Comunidad Autónoma del País Vasco, y de los principios y cánones constitucionales, y su consiguiente declaración de inconstitucionalidad y nulidad.

2. Por providencia del Pleno de este tribunal de 7 de octubre de 2021, a propuesta de la Sección Segunda, se acordó admitir a trámite el presente conflicto positivo de competencia; dar traslado de la demanda y documentos presentados al Gobierno de la Nación, por conducto de su presidente, al objeto de que en el plazo de veinte días y, por medio de la representación procesal que determina el art. 82.2 LOTC, aporte cuantos documentos y alegaciones considere convenientes; comunicar la incoación del conflicto a la Sala de lo Contencioso-Administrativo del Tribunal Supremo, por si ante la misma estuvieran impugnados o se impugnaren los citados preceptos, en cuyo caso se suspenderá el curso del proceso hasta la decisión del conflicto, según dispone el art. 61.2 LOTC; y publicar la incoación del conflicto en el «Boletín Oficial del Estado» y en el «Boletín Oficial del País Vasco».

La publicación tuvo lugar en el «Boletín Oficial del Estado» núm. 247, de 15 de octubre de 2021, y en el «Boletín Oficial del País Vasco» núm. 212, de 25 de octubre de 2021.

3. En fecha 12 de noviembre de 2021 tuvo entrada en este tribunal escrito de alegaciones del abogado del Estado, en el que solicita que se tenga por evacuado el trámite y, en su día, se dicte sentencia en la que se desestime íntegramente el conflicto planteado.

Tras sintetizar el contenido del conflicto positivo, dedica una primera parte de las alegaciones a encuadrar competencialmente el recurso planteado por el Gobierno del País Vasco, y, una segunda parte, al examen concreto de los preceptos impugnados.

a) En primer lugar, considera que el conflicto guarda identidad de razón y fundamento con el recurso de inconstitucionalidad núm. 1220-2021, en lo que se refiere a la impugnación de los art. 9 y 10 de la Ley 39/2015, en la redacción dada por el art. 3 del Real Decreto-ley 14/2019. Señala que este, del que traen causa los preceptos de la Ley 39/2015 desarrollados por el real decreto impugnado, contiene medidas cuya finalidad es incrementar el estándar de protección de la seguridad pública frente a las crecientes amenazas que plantea el uso de las nuevas tecnologías, y a la luz siempre de los últimos sucesos producidos en territorio español. Abunda en el concepto de seguridad pública a través de la cita de las SSTC 235/2001, de 13 de diciembre, FJ 6; 25/2004, de 26 de

cve: BOE-A-2023-10045
Verificable en https://www.boe.es

febrero, FJ 6, y 86/2014, de 29 de mayo, FFJJ 2 y 4. Y, circunscribiéndose dentro de la seguridad pública a la ciberseguridad, la considera materia incardinada en la competencia estatal sobre seguridad pública *ex* art. 149.1.29 CE, que es el título competencial prevalente en los incisos de los artículos y la disposición impugnados por motivos competenciales.

Con la finalidad de justificar el indicado encuadre competencial destaca: (i) que la ciberseguridad es uno de los aspectos imprescindibles a tener en cuenta al configurar la estrategia en materia de seguridad nacional, y la Ley 8/2011, de 28 de abril, que establece medidas para la protección de las infraestructuras críticas se dicta de conformidad con el art. 149.1.29 CE; (ii) que el art. 10 de la Ley 36/2015, de 28 de septiembre, de seguridad nacional –que se dicta al amparo del art. 149.1.4 y 29 CE–, incluye la ciberseguridad en los ámbitos de especial interés para la seguridad nacional; (iii) la ciberseguridad es una de las funciones propias del Centro Nacional de Inteligencia, tal y como resulta de la letra b) del art. 4 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia; (iv) la Orden PCI/870/2018, de 3 de agosto, confirma la relación entre ciberseguridad y seguridad nacional; (v) la disposición final primera del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, afirma que dicha norma, que 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 esos servicios, se dicta al amparo de las competencias estatales del art. 149.1.21 y 29 CE.

Destaca el abogado del Estado que las tareas de prevención de actividades delictivas forman parte de la seguridad pública, que alcanza a la sociedad de la información (SSTC 104/1989, de 8 de junio, y 142/2018, de 20 de diciembre). De modo que la regulación de los sistemas y de las medidas de protección relativos a la administración digital no forma parte de las competencias que corresponden a la Comunidad Autónoma del País Vasco en materia de autoorganización, ya que, a través de dicha regulación, el Estado ejerce sus funciones en materia de seguridad pública para la prevención de actividades delictivas y, en particular, de todas aquellas que pueden afectar gravemente al interés general, tal y como se indica al vincularlas a la seguridad nacional, al orden público y a la protección de las telecomunicaciones; medidas de protección que, por su propia finalidad, exceden del ámbito territorial de una comunidad autónoma.

La STC 142/2018, de 20 de diciembre, que resuelve el recurso del presidente del Gobierno contra la Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña, declara dicha ley parcialmente inconstitucional precisamente por vulnerar la competencia exclusiva del Estado en materia de seguridad pública del art. 149.1.29 CE, remarcando que dentro de esta competencia se integra la ciberseguridad. De modo que el Tribunal Constitucional, al abordar la ciberseguridad, entiende que esta, como sinónimo de seguridad en la red, se integra en la seguridad pública (art. 149.1.29 CE), así como en las telecomunicaciones (art. 149.1.21 CE). El Tribunal cita en este sentido la conexión existente entre ciberseguridad y seguridad nacional (ATC 29/2018, de 20 de marzo). Y es que «debe partirse del carácter transversal e interconectado de las tecnologías de la información y las comunicaciones y de su conceptuación como un conjunto de mecanismos dirigidos a la protección de las infraestructuras informáticas y de la información digital que albergan los sistemas interconectados».

b) En segundo lugar, alega el abogado del Estado que el Gobierno Vasco, al afirmar que los preceptos impugnados establecen un control jerárquico que desconoce la potestad autoorganizatoria de la comunidad autónoma, asumiendo el Estado una función ejecutiva no amparada en el art. 149.1.18 CE, omite de forma significativa en su examen la justificación de la autorización desde el punto de vista de la ciberseguridad. Considera que la potestad organizativa de la comunidad autónoma se respeta al ser amplio el abanico de posibilidades para el acceso a los servicios públicos online, y que por ello el establecimiento de un régimen de verificación es plenamente compatible con dicha

cve: BOE-A-2023-10045
Verificable en https://www.boe.es

potestad, que únicamente aparece limitada por motivos de seguridad pública, titulo competencial que habilita al Estado para establecer la cuestionada autorización.

Aduce que estas cuestiones fueron abordadas en la STC 55/2018, al referirse al Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, conocido como Reglamento eIDAS (acrónimo de su denominación en lengua inglesa: *Regulation on electronic identification and trust services for electronic transactions in the internal market*). Alude a los requisitos exigidos para la expedición de un certificado cualificado conforme a la Ley 19/2003, de 19 de diciembre, de firma electrónica, y recuerda que, en España, el organismo de supervisión es el Ministerio de Asuntos Económicos y Transformación Digital, al que le corresponde, conforme al Reglamento (UE) 914/2014, en cumplimiento de las medidas de seguridad, verificar si el prestador de servicios de confianza y los servicios de confianza que presta cumplen los requisitos establecidos en el citado reglamento, y, en su caso, la inclusión en la lista de confianza prevista en su art. 22. Se refiere también a la exigencia que se impone a los prestadores cualificados de superar las auditorías al menos cada veinticuatro meses.

Entiende el abogado del Estado que existe una amplia habilitación para que cada administración pueda utilizar en su ámbito competencial sistemas de clave concertada y otros. Añade que las indicadas exigencias de seguridad no se aplican a estos sistemas de identificación que se prevén en los arts. 9.2 c) y 10.2 c) de la Ley 39/2015, y que desarrollan los incisos aquí impugnados del reglamento aprobado por el Real Decreto 203/2021, por lo que tales sistemas pasan a estar sujetos a una autorización previa meramente de verificación de su seguridad por parte de la Secretaría General de Administración Digital, previo informe de la Secretaría de Estado de Seguridad, y siempre que se garantice un registro previo. 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. Al respecto, la STC 55/2018 ya indicaba: «La Ley 39/2015 tampoco impone los sistemas de identificación electrónica en las relaciones del ciudadano con las administraciones públicas ni establece el régimen del registro previo ni fija requisitos mínimos de seguridad».

Mediante la cita de la STC 142/2018, sostiene que «la ciberseguridad se incluye en materias de competencia estatal en cuanto, al referirse a las necesarias acciones de prevención, detección y respuesta frente a las ciberamenazas, afecta a cuestiones relacionadas con la seguridad pública y la defensa, las infraestructuras, redes y sistemas y el régimen general de telecomunicaciones», sin perjuicio de que las comunidades autónomas puedan «dar una respuesta adecuada a las amenazas que puedan afectar a las redes de comunicación electrónica y sistemas de información de las administraciones públicas», que se circunscriben exclusivamente a las específicamente referidas al ámbito del Gobierno y de la administración de la comunidad autónoma y su sector público dependiente. Esto es, la competencia de las comunidades autónomas 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.

De este modo, las competencias de las comunidades autónomas que la propia STC 55/2018, de 24 de mayo, reconoce, no son incompatibles con la introducción de una autorización previa de la Administración General del Estado cuyo objetivo es únicamente verificar si el sistema validado tecnológicamente por parte de la administración u organismo público de que se trate puede o no producir afecciones o riesgos a la seguridad pública, de modo que, si así fuera y solo en este caso, la administración del Estado, tras la evaluación de la Secretaría de Estado de Seguridad del Ministerio del Interior, denegará la autorización con base en dichas consideraciones de seguridad pública. La existencia de mínimos de seguridad por parte del Estado se infería ya de la STC 55/2018, que habilitaba el establecimiento de determinadas condiciones o requisitos, como una verificación de cumplimiento de un nivel mínimo común de

cve: BOE-A-2023-10045
Verificable en https://www.boe.es

seguridad para el conjunto de las administraciones públicas, que es, en definitiva, lo que se realiza a través del Real Decreto-ley 14/2019.

Asimismo, descarta que el régimen de autorización cuestionado afecte a la autoorganización administrativa o a las competencias exclusivas de la comunidad recurrente. Y concluye que la regulación de un sistema de previa autorización es un ejercicio de la libertad de configuración legislativa constitucionalmente garantizada, que se basa en la competencia exclusiva del Estado sobre seguridad pública, reflejada en el art. 149.1.29 CE, que no desborda los límites del art. 149.1.18 CE, garantiza un tratamiento común de los administrados y, por tanto, no invade las competencias autonómicas en materia de organización y procedimientos administrativos.

Por último, destaca que la medida prevista en los incisos de los artículos impugnados no es desproporcionada ni desequilibrada, ya que solo exige una previa autorización con un límite en cuanto a las causas de denegación, y la afectación a la seguridad pública es una opción del legislador que no se puede considerar ni excesiva ni desproporcionada.

4. Mediante escrito de 10 de febrero de 2023, el magistrado don Juan Carlos Campo Moreno comunicó su decisión de abstenerse de conocer del conflicto positivo de competencia núm. 5253-2021, por haber participado, en su condición de ministro de Justicia, en el Consejo de Ministros de 30 de marzo de 2021, en el que se aprobó el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, invocando a tal efecto la causa del art. 219.13 LOPJ. La abstención se estimó justificada por auto de 21 de febrero de 2023, en el que se acordó apartarle definitivamente del conocimiento del presente conflicto.

5. Por providencia de 21 de marzo 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 conflicto y posiciones de las partes

El Consejo de Gobierno de la Comunidad Autónoma del País Vasco promueve conflicto positivo de competencia contra los arts. 15.3 a), 26.2 c), 28.2 y 29.4, y contra la disposición adicional novena del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por Real Decreto 203/2021, de 30 de marzo. La demanda centra su impugnación en la exigencia de autorización previa por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital –que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior– para que se puedan implantar por las administraciones públicas autonómicas los sistemas de identificación y firma para los ciudadanos que se dirijan a ellas por vía electrónica, basados en sistemas de clave concertada y otros sistemas de identificación y firma electrónica distintos de los previstos en los arts. 9.2 a) y b) y 10.2 a) y b) de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, esto es, distintos de sistemas basados en certificados electrónicos cualificados de firma electrónica y sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación». La exigencia contenida en los preceptos reglamentarios que aquí se cuestionan trae causa de los arts. 9.2 c) y 10.2 c) de la Ley 39/2015, en la redacción dada a los mismos por el art. 3.1 y 2 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.

Como de modo más extenso se expone en los antecedentes de esta resolución, el Gobierno Vasco entiende que los preceptos reglamentarios impugnados vulneran sus competencias de autoorganización (art. 10.2 EAPV) y el principio de autonomía (arts. 2

cve: BOE-A-2023-10045
Verificable en https://www.boe.es

y 137 CE), como consecuencia del encuadre competencial de tales preceptos en el art. 149.1.29 CE, puesto que ello implica una competencia de control genérico y abstracto, que coloca a la comunidad autónoma en una posición de dependencia jerárquica respecto del Estado, que menoscaba sus competencias de autoorganización. Considera que el encuadre competencial correcto de dichas disposiciones se localiza en el 149.1.18 CE, en cuanto afectan a la organización de las administraciones públicas sobre su administración electrónica, invocando la STC 142/2018, de 20 de diciembre, para afirmar que corresponde a la comunidad autónoma la función de garantizar la ciberseguridad en la prestación de los servicios de identificación electrónica y de identidad en los sistemas públicos. Subsidiariamente, para el caso de que se considere que estos controles se insertan en el art. 149.1.29 CE, defiende que, con fundamento en el art. 17 EAPV, la comunidad autónoma tiene competencias ejecutivas en materia de seguridad sobre las redes y sistemas públicos, que han sido expresamente reconocidas por el Estado, y que son relegadas en virtud del sistema de control impuesto por los preceptos impugnados, con vulneración de los principios de colaboración y cooperación. Por último, estima, asimismo, que los preceptos impugnados suponen unos mecanismos de control exorbitantes y desproporcionados, y que desbordan el justo equilibrio entre los medios empleados y la finalidad pretendida.

El abogado del Estado, en los términos que se recogen más extensamente en los antecedentes, rechaza las vulneraciones denunciadas, defendiendo la incardinación de la normativa impugnada en la competencia estatal sobre seguridad pública del art. 149.1.29 CE, y que se respeta la potestad organizativa de las comunidades autónomas, pues existe una amplia habilitación para que cada administración utilice otros sistemas de identificación y firma, que están sujetos a una autorización previa de mera verificación de su seguridad por la Secretaría General de Administración Digital, ante la necesidad de salvaguardar la seguridad pública en el proceso de transformación digital de la administración. Por todo ello, solicita la desestimación íntegra del conflicto planteado.

2. Pervivencia del conflicto positivo de competencia: extinción por pérdida sobrevenida de objeto

De forma previa al enjuiciamiento de las cuestiones de fondo que se suscitan en el presente conflicto, es preciso determinar si permanece vigente la controversia competencial en los términos en los que ha sido planteada, a la vista de las alteraciones normativas producidas en el marco en el que se encuadran los preceptos que el Gobierno Vasco pone en tela de juicio por afectar a sus competencias estatutarias, según entiende, de manera incompatible con el orden constitucional de distribución de competencias.

La cuestión ha de ser examinada a la luz de la reiterada doctrina que este tribunal tiene establecida en relación con los procesos de naturaleza competencial, conforme a la cual, «la eventual apreciación de la pérdida de objeto del proceso dependerá de la incidencia real que sobre el mismo tenga la derogación, sustitución o modificación de la norma y no puede resolverse apriorísticamente en función de criterios abstractos o genéricos, pues lo relevante no es tanto la expulsión de la concreta norma impugnada del ordenamiento, cuanto determinar si con esa expulsión ha cesado o no la controversia competencial, toda vez que poner fin a la misma a la luz del orden constitucional de reparto de competencias es el fin último al que sirven tales procesos [por todas, STC 149/2012, de 5 de julio, FJ 2 b)]. De modo que si la normativa en torno a la cual se trabó el conflicto resulta parcialmente modificada por otra que viene a plantear los mismos problemas competenciales la consecuencia será la no desaparición del objeto del conflicto (por todas, STC 133/2012, de 19 de junio, FJ 2)» [STC 65/2013, de 14 de marzo, FJ 2 b); en el mismo sentido, SSTC 88/2014, de 9 de junio, FJ 2; 112/2014, de 7 de julio, FJ 2, y 185/2021, de 28 de octubre, FJ 2].

Según se ha expuesto en el fundamento jurídico anterior, el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del

cve: BOE-A-2023-10045
Verificable en https://www.boe.es

sector público por medios electrónicos, se dicta, en lo que a los preceptos impugnados se refiere, en ejecución de los art. 9.2 c) y 10.2 c) de la Ley 39/2015, en la redacción dada por el Real Decreto-ley 14/2019 (que ha sido objeto, entre otros, del recurso de inconstitucionalidad núm. 1220-2021, planteado también por el Consejo de Gobierno de la Comunidad Autónoma del País Vasco), que exigían, para la utilización de cualquier otro sistema de identificación y firma electrónica de los interesados que las administraciones públicas consideraran válido (distinto de los sistemas basados en certificados electrónicos cualificados de firma electrónica y sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación»), la previa autorización de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital; autorización que solo podría ser denegada por motivos de seguridad pública y previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. El plazo máximo para emisión de la autorización era de tres meses y los efectos de la falta de resolución dentro del citado plazo eran desestimatorios.

La redacción de todos los preceptos del Reglamento de actuación y funcionamiento del sector público por medios electrónicos que el Gobierno Vasco impugna a través del presente conflicto positivo de competencia es plenamente tributaria de esa exigencia de los arts. 9.2 c) y 10.2 c) de la Ley 39/2015 (en cursiva, los incisos discutidos):

«Art. 15. Sistemas de identificación, firma y verificación.

[…]

3. Las personas interesadas podrán utilizar los siguientes sistemas de identificación y firma en sus relaciones electrónicas con las administraciones públicas:

a) De acuerdo con lo previsto en el artículo 9.2 de la Ley 39/2015, de 1 de octubre, los interesados podrán identificarse electrónicamente ante las administraciones públicas a través de los sistemas descritos en las letras a), b) y c) de dicho artículo. En este último supuesto los sistemas deberán ser autorizados previamente por la Secretaría General de Administración Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

[…]

Art. 26. Sistemas de identificación de las personas interesadas en el procedimiento.

2. En particular, de acuerdo con lo previsto en el artículo 9.2 de la Ley 39/2015, de 1 de octubre, serán admitidos los siguientes sistemas de identificación electrónica:

[…]

c) Sistemas de clave concertada y 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, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

[…]

cve: BOE-A-2023-10045
Verificable en https://www.boe.es

Artículo 28. Sistemas de clave concertada y otros sistemas de identificación de las personas interesadas.

[…]

2. Los sistemas de identificación a que se refiere el apartado anterior deberán ser autorizados previamente por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

[…]

Artículo 29. Sistemas de firma electrónica de las personas interesadas admitidos por las Administraciones Públicas y régimen de uso.

[…]

4. Los sistemas de firma electrónica previstos en la letra c) del apartado 1 deberán contar con la previa autorización de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. Asimismo, deberán cumplir con lo previsto en el Real Decreto 3/2010, de 8 de enero.

[…]

Disposición adicional novena. Autorización de los sistemas de identificación previstos en el artículo 9.2 c) y de los sistemas de firma previstos en el artículo 10.2 c) de la Ley 39/2015, de 1 de octubre.

1. Los sistemas de identificación a que se refiere el artículo 9.2 c) y los sistemas de firma a que se refiere el artículo 10.2 c) de la ley 39/2015, de 1 de octubre, que, en ambos casos, se hubieran puesto en servicio hasta el 6 de noviembre de 2019, fecha de entrada en vigor de la modificación de dichos artículos en virtud 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, no requerirán la autorización de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior, siempre y cuando no hayan sido modificados tras dicha fecha.

2. Los sistemas que, tras el 6 de noviembre de 2019, hayan sido autorizados en aplicación de las previsiones de los artículos 9.2 c) y 10.2 c) de la Ley 39/2015, de 1 de octubre, y sean modificados posteriormente, deberán ser objeto de una nueva autorización previa a su puesta en servicio».

Como el propio Consejo de Gobierno de la Comunidad Autónoma del País Vasco destaca en su demanda, ha promovido también el recurso de inconstitucionalidad 1220-2021 contra el Real Decreto-ley 14/2019, de 31 de octubre, dirigiendo su impugnación, entre otros aspectos, contra la modificación de los arts. 9 y 10 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, que lleva a cabo dicho real decreto-ley. Y reconoce la directa relación de esos dos preceptos con los que en este proceso se impugnan, al afirmar que «[e]stas dos normas modificadas son reproducidas por los preceptos reglamentarios contra los que se reacciona en este conflicto, por lo que existe una íntima conexión entre aquel recurso y este conflicto, toda vez que el objeto coincide en ambos casos, en concreto, una autorización, previo informe vinculante, que se ha reservado el Estado

cve: BOE-A-2023-10045
Verificable en https://www.boe.es

para la admisión de determinados sistemas de identificación y firma de los ciudadanos ante las administraciones públicas».

Hay que precisar que los reseñados preceptos reglamentarios no han sufrido modificación alguna en su redacción tras la interposición del conflicto positivo de competencia por parte del Consejo de Gobierno de la Comunidad Autónoma del País Vasco, por lo que, formalmente, el conflicto positivo de competencia que nos ocupa subsistiría. Sin embargo, este tribunal ha de tomar en consideración (al igual que hizo en el FJ 2 de la sentencia de 23 de febrero de 2023, que resolvió el recurso de inconstitucionalidad núm. 718-2020, en el que también se impugnaban diversos preceptos del Real Decreto-ley 14/2019, de 31 de octubre) que los arts. 9.2 c) y 10.2 c) de la Ley 39/2015 (en la redacción que les dio el art. 3 del Real Decreto-ley 14/2019) han sido modificados por la disposición final primera, apartados primero y segundo, de la Ley 11/2022, de 28 de junio, general de telecomunicaciones, en un aspecto que resulta esencial a los efectos de este conflicto: se sustituye la necesidad de previa autorización de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital y el previo informe vinculante de la Secretaría de Estado de Seguridad para la implantación por parte de las administraciones públicas de otros sistemas de identificación y firma electrónica de los interesados ante ellas, por un sistema de comunicación previa a esa misma Secretaría General de Administración Digital, «acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente». Con carácter previo 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».

Por consiguiente, el aspecto que motivaba de manera exclusiva la impugnación de los preceptos del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, esto es, la necesidad de obtener la autorización previa de la administración del Estado para la implantación de clave concertada y de otros sistemas de identificación y firma electrónica de los interesados por parte de las administraciones públicas, ha desaparecido de las normas legales que servían de fundamento a los arts. 15.3 a), 26.2 c), 28.2 y 29.4, así como a la disposición adicional novena del referido reglamento, que son el objeto del presente conflicto positivo de competencia. Ello determina que, aunque formalmente el conflicto subsistiera, porque el Reglamento aprobado por el Real Decreto 203/2021, de 30 de marzo, no ha sido modificado para adaptarlo a la nueva regulación legal, sin embargo, hay que concluir que, materialmente, el conflicto ha perdido su objeto, porque se debe entender que el aspecto sobre el que se asentaba la impugnación y que fundamentaba las tachas competenciales articuladas por el Consejo de Gobierno de la Comunidad Autónoma del País Vasco ha desaparecido. En efecto, las previsiones reglamentarias que se discuten en el conflicto han de considerarse derogadas, al resultar incompatibles con el actual contenido de los arts. 9.2 c) y 10.2 c) de la Ley 39/2015, en la redacción dada por la disposición final primera de la Ley general de telecomunicaciones, sea por aplicación del párrafo c) de la disposición derogatoria de esta, sea en virtud del apartado 1 de la disposición derogatoria de la Ley 39/2015, al tratarse de normas de inferior rango que se oponen a lo establecido en esta última ley tras su modificación. Y, comoquiera que el problema competencial que planteaba el conflicto no subsiste tras esa modificación legal, en aplicación de la doctrina constitucional antes expuesta debemos colegir obligadamente que el presente conflicto de competencia ha perdido sobrevenidamente su objeto, en tanto que el marco normativo actual ya no establece la necesidad de obtener la autorización previa de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, ni el previo informe vinculante de la Secretaría de Estado de Seguridad, controvertidos en este proceso, para que las administraciones públicas puedan establecer cualquier otro sistema de identificación y firma electrónica de los interesados que consideren válido, distintos de los basados en

cve: BOE-A-2023-10045
Verificable en https://www.boe.es

certificados electrónicos cualificados de firma electrónica o sello electrónico a que se refieren los arts. 9.2 a) y b) y 10.2 a) y b) de la Ley 39/2015.

3. Conclusión

En consecuencia, debemos concluir que ha desaparecido de forma sobrevenida el objeto del conflicto positivo de competencia deducido contra los arts. 15.3 a), 26.2 c), 28.2 y 29.4, así como contra la disposición adicional novena, del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por Real Decreto 203/2021, de 30 de marzo, y, consiguientemente, el proceso ha quedado extinguido, lo que convierte en innecesario nuestro pronunciamiento sobre las cuestiones planteadas por el Gobierno Vasco en el suplico del escrito de interposición de este conflicto positivo de competencia.

FALLO

En atención a todo lo expuesto, el Tribunal Constitucional, por la autoridad que le confiere la Constitución de la Nación española, ha decidido declarar extinguido, por desaparición sobrevenida de su objeto, el conflicto positivo de competencia promovido por el Consejo de Gobierno de la Comunidad Autónoma del País Vasco contra los arts. 15.3 a), 26.2 c), 28.2 y 29.4, y la disposición adicional novena del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por Real Decreto 203/2021, de 30 de marzo.

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

Dada en Madrid, a veintitrés de marzo 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-2023-10045
Verificable en https://www.boe.es