

El Pleno del Tribunal Constitucional, compuesto por don Juan José González Rivas, Presidente, doña Encarnación Roca Trías, don Andrés Ollero Tassara, don Fernando Valdés Dal-Ré, don Santiago Martínez-Vares García, don Juan Antonio Xiol Ríos, don Pedro González-Trevijano Sánchez, don Antonio Narváez Rodríguez, don Alfredo Montoya Melgar, don Ricardo Enríquez Sancho, don Cándido Conde-Pumpido Tourón y doña María Luisa Balaguer Callejón, Magistrados, ha pronunciado.

EN NOMBRE DEL REY

la siguiente

SENTENCIA

En el recurso de inconstitucionalidad núm. 5284-2017 interpuesto por el Presidente del Gobierno contra la Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña. Han comparecido y formulado alegaciones el Parlamento y el Gobierno de la Generalidad de Cataluña. Ha sido ponente la Magistrada doña Encarnación Roca Trías, quien expresa el parecer del Tribunal.

I. Antecedentes.

1. El 31 de octubre de 2017 tuvo entrada en el registro de este Tribunal el recurso de inconstitucionalidad interpuesto por el Abogado del Estado, en representación del Presidente del Gobierno, contra la Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña. El Abogado del Estado invocó los arts. 161.2 CE y 30 LOTC, a fin de que se produjera la suspensión de la aplicación de la Ley 15/2017.

El recurso se basa en los motivos que, sucintamente, se exponen a continuación:

El Abogado del Estado comienza señalando que se recurre la Ley 15/2017 en su conjunto en atención no sólo a la asunción de competencias estatales por parte de la Agencia, sino también a la unidad de sentido de la Ley por su carácter de "estructura de estado". La impugnación tiene

un motivo fundamentalmente competencial, en cuanto la Ley vulnera la competencia exclusiva del Estado en materia de seguridad pública del art. 149.1.29 CE, dentro de la cual se integra la ciberseguridad, en conexión con las competencias estatales en materia de defensa y telecomunicaciones.

La norma impugnada parte de una concepción de la ciberseguridad, como materia integral, de modo que entiende que la Generalidad de Cataluña tiene competencias al tratarse, según dice, de una materia que afecta al régimen de autoorganización (art. 150 EAC), la competencia ejecutiva en materia de comunicaciones electrónicas (art. 140.7 EAC) y la competencia exclusiva en materia de comercio electrónico conforme al art. 121.1 a) del EAC.

De acuerdo con esa concepción, la Ley 15/2017 establece una completa regulación de la ciberseguridad en todos sus ámbitos y en todo el territorio de Cataluña. El precepto central de la norma es el art. 2 que define el objeto y funciones de la Agencia de Ciberseguridad, siendo el resto meramente instrumentales para la creación de esa Agencia o para adaptar su creación a la actual organización administrativa de la Generalidad. La inconstitucionalidad de la Ley en su conjunto deriva, no solo de constituir una "estructura de estado", sino también de tener un objeto y asumir unas funciones que inciden, al interpretarlas conjuntamente, en la competencia exclusiva del Estado en materia de seguridad pública conforme al art. 149.1.29 CE, en conexión con las atribuciones estatales en materia de defensa, telecomunicaciones y régimen general de comunicaciones. El art. 2, después de definir como objeto de la Agencia "garantizar la ciberseguridad en el territorio de Cataluña" (art. 2.1), fija como su finalidad "la ejecución de las políticas en materia de ciberseguridad" (art. 2.2) para desglosar en cuatro apartados lo que se entiende por ejecución. A su vez, el apartado 3 del art. 2 dispone que la Agencia "para la ejecución de los objetivos" puede ejercer sus funciones en relación con las personas físicas y jurídicas situadas en Cataluña y establecer la colaboración necesaria con los prestadores de servicios de la sociedad de la información y de comunicaciones electrónicas que actúen o tengan infraestructuras en Cataluña. El art. 2.4 desglosa las funciones que asume la Agencia para el cumplimiento de sus objetivos, entre las que se destaca por su relevancia, el apartado f). El art. 2.5 desarrolla las funciones de la Agencia en el ámbito de la Generalidad, aludiendo específicamente la demanda al apartado b) que atribuye competencia a la Generalidad para "informar preceptivamente" de las disposiciones normativas estatales sobre ciberseguridad, sin que ninguna competencia autonómica pueda sustentar esta atribución.

La demanda analiza a continuación las competencias del Estado en materia de seguridad pública del art. 149.1.29 CE y su relación con los títulos competenciales estatales en materia de defensa y de telecomunicaciones. Así indica que el art. 149.1.29 CE atribuye al Estado competencia exclusiva en materia de seguridad pública y dentro de ella se integra la ciberseguridad. No se discute que la Generalidad pueda ejercer determinadas funciones en el ámbito de la ciberseguridad, referida a su autoprotección, pero la Ley 15/2017 obvia las competencias estatales afectadas por la norma, en tanto que la ciberseguridad es uno de los aspectos imprescindibles a tener en cuenta a la hora de configurar la estrategia en materia de Seguridad Nacional. De hecho, diversas normas estatales se refieren a esta cuestión, como la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas; la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, o la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. Igualmente, se ha de tener en cuenta que las infraestructuras de telecomunicaciones pueden constituir infraestructuras críticas, ámbito al que se refiere la STC 128/2016.

El Abogado del Estado recuerda la doctrina constitucional en torno a la delimitación de competencias en materia de seguridad pública (cita STC 86/2014) y concluye que es doctrina consolidada del Tribunal Constitucional que esta es una competencia exclusiva del Estado ex art. 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 (por todas, STC 148/2000, FJ 5). Sin embargo, estima que las funciones atribuidas a la Agencia de Ciberseguridad de Cataluña desbordan el ámbito competencial de la Comunidad Autónoma.

Alude específicamente al art. 2.4.f) que atribuye a la Agencia la función de “Investigar y analizar tecnológicamente los ciberincidentes y ciberataques sobre infraestructuras tecnológicas, sistemas de información, servicios de tecnologías de la información y la comunicación o la propia información en los que la Agencia intervenga por razón de su competencia”. Señala el Abogado del Estado que este precepto fue considerado inconstitucional por el propio Consejo de Garantías Estatutarias, cuando se pronunció en relación con el texto de la ley en fase de proyecto. El Consejo valoró que el objeto de estas funciones de respuesta forma parte de manera clara de las policiales de preservación de la seguridad pública, que sobrepasan las que corresponden a la Agencia de Ciberseguridad de Cataluña, ya que la potestad de investigar y analizar los ciberincidentes y ciberataques, se proyecta sobre hechos que son constitutivos de

delitos informáticos, y permite entender que va más allá de la capacidad de respuesta en el orden técnico y organizativo ante estas situaciones.

Para el Abogado del Estado es notorio que, en un campo novedoso y en plena expansión como es el afectado por la ciberseguridad, no cabe sostener que la intervención pública en materia de seguridad se limite al ámbito penal. De hecho, si se trata de sancionar conductas antijurídicas, la ciberseguridad operará también como bien jurídico protegido en las infracciones administrativas que se establezcan para preservarla. Pero es evidente que la ciberseguridad no puede tener solo esta dimensión punitiva, sino que debe existir también una intervención pública promotora de la ciberseguridad y tendente a prevenir cualquier quiebra o peligro para la misma, en tanto que bien jurídico de relevancia esencial en la sociedad de la información. Por lo tanto, el art. 2.4.f) excede los límites competenciales autonómicos por cuanto el contenido de esta atribución se enmarca en las funciones estatales sobre seguridad pública relativa a la capacidad de investigar y analizar ciberataques e incidentes informáticos, sean o no delito.

A continuación, el Abogado del Estado plantea los motivos por los que a su parecer, la Ley en su conjunto resulta inconstitucional. Destaca que la Ley 15/2017 establece, en su art. 2.1, que "La Agencia de Ciberseguridad de Cataluña tiene por objeto garantizar la ciberseguridad en el territorio de Cataluña, entendida como la seguridad de las redes de comunicaciones electrónicas y de los sistemas de información". Esta previsión se considera inconstitucional pues es susceptible de afectar a infraestructuras situadas fuera del territorio catalán; afecta también a las competencias estatales ya reseñadas, y específicamente a aquellas que se refieren a la protección de la seguridad nacional y las telecomunicaciones. La Ley 15/2017 atribuye a la mencionada Agencia el ejercicio de amplias funciones en materia de ciberseguridad, sin que contenga ningún mandato ni previsión de coordinación y colaboración con los organismos, estrategias, planes y autoridades nacionales. Esta conclusión se ve reforzada si se atiende a las especificaciones de los apartados siguientes de este art. 2. El Abogado del Estado alude específicamente a los apartados 2 y 3, así como, citando el dictamen del Consejo de Estado, a los arts. 2.4, letras b), e) y f) y 2.5, letras a) y d) y, finalmente, al art. 2.5.b), al que ya había hecho referencia anteriormente.

Las consideraciones anteriores de la demanda se completan con una referencia a la Agencia de Ciberseguridad como "estructura de estado". A tal efecto, se destaca la relación teleológica que la Ley 15/2017 guarda con otras leyes catalanas aprobadas poco después y que

se enmarcan dentro del conjunto de actuaciones llevadas a cabo por la Generalidad en su propósito declarado de construir estructuras de Estado con virtualidad sustitutoria de las actualmente vigentes en el sistema estatal. Además de la doctrina de la STC 52/2017, de 10 de mayo, se citan las Leyes 17/2017, de 1 de agosto, del Código Tributario de Cataluña y de aprobación de los libros primero, segundo y tercero, relativos a la Administración Tributaria de la Generalidad, y 21/2017, de 20 de septiembre, de la Agencia de Protección Social de Cataluña, ambas impugnadas ante el Tribunal Constitucional, que ha admitido a trámite los recursos mediante Providencias de 12 de septiembre y 17 de octubre de 2017.

Concluye la demanda señalando que la Ley 15/2017 está redactada en unos términos ambiguos, incluye algunas previsiones que podrían entenderse indistintamente aplicables dentro del orden de distribución de competencias diseñado por la Constitución de 1978 o al margen de él, pero tampoco oculta que la Agencia que crea dicha Ley constituye, en su propio ámbito, una estructura organizativa idónea para actuar de forma autónoma en un eventual Estado catalán independiente. Su creación, de hecho, se encuentra prevista en el "Informe sobre la seguridad interna e internacional de Cataluña", elaborado por el ya mencionado Consejo Asesor para la Transición Nacional de Cataluña, que tiene por objeto analizar los principales retos y actuaciones de Cataluña en el ámbito de la seguridad interna e internacional durante el periodo de transición nacional y, más concretamente, los primeros meses de construcción de un eventual nuevo Estado catalán.

2. Por providencia de 28 de noviembre de 2017, el Pleno, a propuesta de la Sección Tercera, acordó admitir a trámite el recurso de inconstitucionalidad promovido por el Presidente del Gobierno y, en su representación y defensa, por el Abogado del Estado, contra la Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña; dar traslado de la demanda y documentos presentados, conforme establece el art. 34 de la Ley Orgánica del Tribunal Constitucional (LOTC), al Congreso de los Diputados y al Senado, por conducto de sus Presidentes, así como al Gobierno de Cataluña y al Parlamento de Cataluña, por conducto de sus Presidentes, al objeto de que, en el plazo de quince días, puedan personarse en el proceso y formular las alegaciones que estimaren convenientes. Con el fin de evitar un conflicto en la defensa de los intereses del Estado y de la Comunidad Autónoma de Cataluña, se suspendió el plazo para que el Gobierno de Cataluña pueda personarse y formular alegaciones, en tanto el Consejo de Ministros, de conformidad con el art. 5 del Real Decreto 944/2017, de 27 de octubre, ejerza las funciones y competencias que corresponden al Consejo de Gobierno de la Generalidad

de Cataluña. Asimismo, se tuvo por invocado por el Presidente del Gobierno el art. 161.2 de la Constitución, lo que, a su tenor y conforme dispone el art. 30 LOTC, produce la suspensión de la vigencia y aplicación de la Ley impugnada, desde la fecha de interposición del recurso -31 de octubre de 2017- para las partes del proceso y desde el día en que aparezca publicada la suspensión en el Boletín Oficial del Estado para los terceros, lo que se comunicará a los Presidentes del Gobierno de Cataluña y Parlamento de Cataluña. Finalmente, se acordó publicar la incoación del recurso en el Boletín Oficial del Estado y en el Diari Oficial de la Generalidad de Cataluña.

3. Mediante escrito registrado el día 7 de diciembre de 2017, la Presidenta del Congreso de los Diputados comunicó al Tribunal el Acuerdo de la Mesa de la Cámara por el que se persona en el procedimiento y ofrece su colaboración a los efectos del art. 88.1 LOTC. Lo mismo hizo el Presidente del Senado por escrito que tuvo entrada en este Tribunal el día 13 de diciembre.

4. Por escrito registrado el día 15 de diciembre de 2017, el Letrado del Parlamento de Cataluña se personó en el procedimiento y solicitó una prórroga por el máximo legal, siendo atendida dicha petición por providencia de este Tribunal de 16 de diciembre de 2017, por la que se prorrogó en ocho días más el plazo concedido por la anterior providencia de 28 de noviembre.

5. Las alegaciones del Parlamento de Cataluña, interesando la desestimación del recurso, se registraron en este Tribunal Constitucional el día 15 de enero de 2018.

Defiende en primer lugar que se trata de un recurso preventivo incompatible con el principio de presunción de constitucionalidad de la ley. El recurso de inconstitucionalidad se dirige indiscriminadamente contra toda la Ley, sin hacer selección alguna de sus preceptos a efectos de impugnación. Esta falta de criterio selectivo “sorprende aún más cuando observamos que, aunque el objeto y las funciones de la Agencia se concentran prácticamente en un único precepto (el art. 2), se trata de un precepto notablemente amplio y extenso cuya lectura nos permite observar también la distinta naturaleza de algunas de las funciones de la Agencia y las consecuencias que ello debería suponer a los efectos de los diferentes títulos competenciales que hay que considerar para resolver adecuadamente el presente recurso”. Por otra parte, el recurso tiene interés en destacar que su fundamentación jurídica es esencialmente competencial por cuanto considera que la Ley vulnera la competencia exclusiva del Estado en materia de seguridad pública (art. 149.1 .29 CE).

Sin embargo, se evidencia claramente que la impugnación obedece al carácter de “estructura de estado” que, a juicio del recurrente, tiene la Agencia creada por la Ley impugnada. Se trata de un juicio de valor sobre el riesgo que podría suponer la creación de la Agencia de Ciberseguridad de Cataluña, porque la misma pudiera ser utilizada en el futuro como una “estructura de estado”. Juicio preventivo o prospectivo que no tiene cabida en el marco de un recurso de inconstitucionalidad, sobre todo cuando se admite que las previsiones de la Ley pueden desarrollarse dentro del sistema de distribución de competencias. Estas consideraciones deben ponerse en relación con las exigencias mínimas que la jurisprudencia constitucional ha establecido para la viabilidad de un recurso de inconstitucionalidad, que tienen que ver con la naturaleza de dicho recurso, con su finalidad no preventiva y con el principio de constitucionalidad de las leyes. La aplicación de lo anterior lleva necesariamente a la conclusión de que el presente debate no puede ser influido de ninguna manera por juicios de valor sobre las intenciones del legislador o por la voluntad de obtener declaraciones preventivas para ponerse a cubierto de eventuales aplicaciones inconstitucionales de la norma. Por el contrario, la resolución del recurso ha de fundamentarse solo en el contraste objetivo de la ley impugnada con la Constitución en el contexto competencial que le corresponde y sin olvidar el juego del principio de presunción de constitucionalidad de la ley.

El Letrado del Parlamento de Cataluña sostiene a continuación que, dado el carácter genérico e impreciso de la impugnación, el recurso tampoco cumple con la carga que tiene el recurrente de argumentar y fundamentar de manera suficiente los motivos que lo sustentan. Las alegaciones del recurso se centran en lo dispuesto en el art. 2, precepto que presenta diversos contenidos que no pueden ser tratados bajo una única perspectiva, es decir, sin tomar en consideración las distintas finalidades a las que responden las también distintas atribuciones que la Ley confiere a la Agencia. Se trata, en cualquier caso, de funciones de distinta naturaleza y con implicaciones competenciales más complejas que la relativa a la seguridad pública, que constituye la única base de la impugnación. Por tanto, una impugnación global de la ley debería tenerlo en cuenta y obligar al recurrente a fundamentar jurídicamente las razones por las cuales se impugnan todas las atribuciones de la Agencia, sin excepción o matiz alguno derivados de su diferente naturaleza y sin que se haga un contraste mínimamente argumentado entre los contenidos del art. 2 de la Ley con las reglas de reparto competencial, para así justificar la vulneración que se denuncia, lo que solo se hace respecto a dos puntos concretos del art. 2, la letra f) del apartado 4 y la letra b) del apartado 5. Por ello, la representación procesal del

Parlamento de Cataluña entiende que los fundamentos del recurso “adolecen de los mínimos exigibles por la jurisprudencia constitucional en cuanto a la obligación de precisar los motivos de la impugnación y de fundamentar, de forma pormenorizada, las razones de la supuesta inconstitucionalidad”. La conclusión es que “Más allá de la motivación concreta que se hace respecto de la letra f) del apartado 4 del art. 2, no existe en el recurso ningún análisis mínimamente detallado de los motivos que podrían justificar la inconstitucionalidad de todas las demás funciones de la Agencia. Respecto de las demás funciones de la Agencia solamente se aportan, a modo de comodín y en contraposición a lo que exigiría el análisis de cada caso en concreto, los argumentos genéricos e imprecisos que antes se han expuesto. La gravedad de este defecto procesal es tal que por este solo motivo la mayor parte del recurso debería ser rechazada”.

Se argumenta a continuación que la Ley impugnada tiene cobertura en las competencias que la Constitución y el Estatuto de Autonomía atribuyen a la Generalidad. En especial, en las competencias en materia de autoorganización y régimen jurídico, seguridad pública y telecomunicaciones. El recurso parte del principio que la ciberseguridad queda circunscrita al título competencial en materia de seguridad pública, aunque admite que pueda también conectarse con las competencias estatales en materia de defensa y telecomunicaciones. Aun aceptando la tesis de que la competencia principal es la seguridad pública, en este ámbito material la Generalidad tiene reconocidas competencias que amparan la Ley impugnada y también hay otros títulos competenciales que dan cobertura a la Ley, entre los que hay que señalar de manera especial los relativos a la organización de la administración de la Generalidad o a las funciones ejecutivas sobre las telecomunicaciones. La ciberseguridad tiene un marcado carácter instrumental que le permite proyectarse sobre distintos ámbitos materiales y cumplir también diversas funcionalidades. Puede identificarse con la defensa o la seguridad nacionales en los supuestos de mayor gravedad y 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 la protección de los derechos de los ciudadanos cuando se relacionan con la Administración por medios electrónicos.

La misma legislación estatal que se cita en el recurso reconoce a las Comunidades Autónomas facultades en materia de ciberseguridad, especialmente sobre la capacidad para organizar medios y dar respuesta a actuaciones que puedan comprometer la seguridad de las redes y de los sistemas de información. El Letrado del Parlamento de Cataluña destaca que se trata de

una norma de alcance marcadamente organizativo, como evidencia su contenido y la naturaleza de los objetivos y funciones que se atribuyen a la Agencia de Ciberseguridad. Desde ese punto de vista, es indiscutible que la ciberseguridad de sus redes y sistemas de información y comunicación constituye una competencia que forma parte de la capacidad de autoorganización de la Generalidad y que resulta indisociable de su régimen jurídico y de los aspectos procedimentales. Dicha conclusión también se desprende de determinadas normas estatales como la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, o la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, o de la normativa específica en la materia (Ley 11/2017, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y Real Decreto 3/2010, de 8 de enero). De dichas normas estatales se infieren dos conclusiones: la primera es la imbricación existente entre la ciberseguridad con la organización y el funcionamiento de las administraciones públicas, dado que los sistemas electrónicos forman parte del operativo normal de actuación pública y su seguridad es tema que atañe a todas ellas; la segunda es que la normativa estatal reseñada es una normativa básica dictada al amparo del art. 149.1.18 CE que, como tal, presupone que las Comunidades Autónomas disponen de la capacidad necesaria para adaptarla y desarrollarla en su propio espacio a partir del ejercicio de sus competencias. De acuerdo con el art. 150.b) EAC, la Generalidad tiene competencia exclusiva para determinar las diversas modalidades organizativas e instrumentales para la actuación administrativa. Y, de acuerdo con el art. 159.1 y 2 EAC, corresponden a la Generalidad, respectivamente, la competencia exclusiva sobre los medios necesarios para ejercer sus funciones administrativas y la competencia compartida de desarrollo de las bases estatales en materia de régimen jurídico y de procedimiento administrativo. Estas dos competencias darían cobertura a la creación de la creación de la Agencia de Ciberseguridad y a buena parte de sus funciones.

El contenido de las actividades que puede comprender la ciberseguridad tiene especial relación con la preservación de la seguridad pública. El recurso centra la controversia competencial sobre esta cuestión y entiende que existe una competencia exclusiva del Estado, derivada del art. 149.1.29 CE, que integra la ciberseguridad, en conexión con otras competencias, como las de defensa o las de telecomunicaciones. De esa reconducción de la ciberseguridad a la materia de seguridad pública, el recurso deduce la inexistencia de competencia alguna de la Generalidad para intervenir en la misma, ni siquiera mediante un instrumento con funciones ejecutivas como es la Agencia de Ciberseguridad de Cataluña. El Letrado autonómico destaca que, en esta materia, el ámbito competencial correspondiente a la creación de las policías

autonómicas comporta no solo una referencia orgánica, sino también funcional que incluye, además de la organización de la policía autonómica y del ejercicio de las funciones o servicios policiales no estatales, las potestades administrativas que son complementarias o inherentes a la actividad propiamente policial. Examina a continuación el marco de actuación que deriva de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, y de la Ley 8/2011, de 28 de abril, por las que se establecen medidas para la protección de las infraestructuras críticas, que son las dos leyes que el recurso toma como referencia para incardinar la ciberseguridad en la materia de seguridad pública. Sin embargo, de estas normas se deduciría que la ciberseguridad y las cuestiones que afectan a la seguridad nacional y las infraestructuras estratégicas son responsabilidades que atañen a todas las administraciones públicas de acuerdo con sus respectivas competencias. Ambas normas presuponen la actuación de las Comunidades Autónomas en las medidas relacionadas con la prevención de la ciberseguridad, y asumen que se desarrollen y se integren dentro de los mecanismos de protección y coordinación general establecidos por ambas leyes.

Por ello, el Letrado del Parlamento de Cataluña concluye que en este caso se da la relación de inherencia o complementariedad respecto de las facultades que son propias de las funciones policiales. La creación de la Agencia de Ciberseguridad de Cataluña puede integrarse así, con la misma naturalidad, como una medida organizativa que el legislador catalán ha considerado adecuado adoptar para poder cumplir integralmente junto con otras más propias de la autoprotección de sus sistemas, funciones de apoyo relacionadas con el ámbito más específico de la protección de personas y bienes y el mantenimiento del orden público que corresponden a la policía autonómica. Finalmente, se alude a la competencia ejecutiva en materia de telecomunicaciones del art. 140.7 EAC, la cual serviría para reforzar los títulos competenciales mencionados anteriormente en la medida en que la controversia afecta a funciones ejecutivas (las del art. 2 de la ley impugnada) y puede considerarse que se cumple el requisito estatutario de ejercerse de acuerdo con la normativa del Estado.

A continuación, en el escrito del Parlamento de Cataluña se analiza el contenido del art. 2 de la Ley 15/2017. El apartado 1 establece que la Agencia de Ciberseguridad de Cataluña tiene por objeto garantizar la ciberseguridad en el territorio de Cataluña, entendida como la seguridad de las redes de comunicación electrónicas y de los sistemas de información. Este objeto no puede ser entendido como una afirmación o voluntad de residenciar en la Agencia la exclusividad de esta función. Este resultado no se desprende de la lectura integral del art. 2, pues el resto del

precepto permite concretar su alcance de acuerdo con las competencias que corresponden a la Generalidad. El apartado 2 define los objetivos que tiene la Agencia de Ciberseguridad de Cataluña como principal ejecutor de las políticas de la Generalidad en materia de ciberseguridad. Todos estos objetivos tienen perfecto encaje con las funciones que corresponden a la Generalidad relacionadas con la administración electrónica y también con las que derivan de la necesidad de proteger las redes y sistemas de información propios, así como de los particulares que se relacionan por medios electrónicos con la administración. En el apartado 3 no se atribuye a la Agencia potestades de intervención o regulación sobre el sector privado, sino funciones de tipo prestacional o de puesta a disposición de servicios en beneficio de los administrados. Las funciones descritas en el apartado 4 deben ponerse en conexión con las políticas de seguridad que la legislación sobre administración electrónica impone a las administraciones públicas. Estas políticas de seguridad pueden concretarse en planes y otras determinaciones y su alcance abarca la gestión de los riesgos y la respuesta a los incidentes de ciberseguridad. Otras de las funciones previstas en dicho apartado 4 pueden tener relación con los requerimientos y actuaciones de ciberseguridad que derivan de la administración electrónica, pero plantean cuestiones que van más allá y entran dentro de la esfera de intervenciones que resultan más propias de la seguridad pública. Sin embargo, esto no significa su inconstitucionalidad, pues la Generalidad dispone de competencias que le permiten actuar en este ámbito, reconocidas además por las normas estatales antes citadas.

Todas las funciones del apartado 5 tienen un marcado e inequívoco carácter interno, es decir, relacionado con las políticas de ciberseguridad de las redes y sistemas de información de la Generalidad y de las relaciones que pueden establecerse con los mismos. El recurso solo hace una objeción específica a la letra b) que carece de fundamento, por cuanto afirma que dicha letra atribuye a la Generalidad la competencia para informar preceptivamente de las disposiciones normativas estatales sobre ciberseguridad, cosa que no se desprende en modo alguno del precepto, que deja bien claro que la función de informe solo alcanza a las disposiciones normativas que elabore la propia Administración de la Generalidad. El apartado 6 establece que la Agencia de Ciberseguridad ha de colaborar con los organismos judiciales y policiales de acuerdo con la normativa vigente y ha de coordinarse también con los cuerpos policiales a los efectos de las competencias que dichos cuerpos tienen reconocidas en esta materia. Este apartado debe ponerse en conexión con la letra e) del apartado 4 y también con la letra c) del apartado 2. Este conjunto de previsiones demuestra claramente la voluntad del legislador de situar la Agencia de Ciberseguridad dentro de un modelo interactivo entre todas las administraciones públicas y

las autoridades judiciales. Por último, el apartado 7 determina que la Agencia ha de establecer líneas de colaboración en el ámbito de la ciberseguridad con los entes locales de Cataluña. La razón de ser de esta colaboración puede encontrarse también en los requerimientos que los entes locales deben cumplir respecto a la administración electrónica y a la coordinación necesaria entre la policía autonómica y la local, en relación a las conductas ilícitas en el ámbito de la ciberseguridad.

Mediante otrosí solicita el levantamiento inmediato de la suspensión por los motivos que se resumen a continuación.

Alude, en primer lugar, al carácter excepcional de la medida de suspensión, lo que casa mal con una impugnación basada en argumentos genéricos y razones inconcretas, según los cuales las funciones que se atribuyen a la Agencia resultarían contrarias al orden constitucional. El Letrado del Parlamento de Cataluña reclama al Tribunal que valore estas circunstancias, pues entiende que el recurrente no solo tiene la carga de demostrar los perjuicios que puede suponer el mantenimiento de la vigencia de la Ley impugnada, sino de cumplir también los requerimientos mínimos que debe cumplir formal y materialmente la acción procesal interpuesta a la que ha anudado el poder de suspensión.

Por otra parte, se sostiene que el mantenimiento de la suspensión de la Ley puede producir perjuicios graves para la Administración de la Generalidad y para terceros, perjuicios derivados de la inexistencia de un instrumento que ha sido creado para garantizar la ciberseguridad en las redes y servicios de información, especialmente los de la propia administración. La suspensión de la Ley priva de un instrumento básico para la prevención y lucha frente a las actuaciones ilícitas en materia de ciberseguridad, con lo que sus efectos, caso de prolongarse, determinan que las fuerzas y cuerpos de seguridad, en especial los de la Generalidad, no dispongan en este momento de un mecanismo de apoyo técnico para el mejor desarrollo de su función de protección de personas y bienes y de mantenimiento del orden público.

6. Próximo a finalizar el plazo de los cinco meses que señala el art. 161.2 CE desde que se produjo la suspensión de los preceptos impugnados en este recurso de inconstitucionalidad, el Pleno, por providencia de 7 de febrero de 2018, acordó oír a las partes personadas-Abogado del Estado- para que, en el plazo de cinco días, exponga lo que considere conveniente acerca del mantenimiento o levantamiento de dicha suspensión.

El Abogado del Estado interesó el mantenimiento de la suspensión de los preceptos impugnados conforme a las alegaciones presentadas el día 14 de febrero de 2018.

7. El Pleno, por ATC 29/2018, de 20 de marzo, acordó mantener la suspensión de la Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña.

8. El Pleno, por providencia de 5 de junio de 2018, acordó que, perdida la vigencia del Real Decreto 944/2017, de 27 de octubre, conforme a lo previsto en su disposición adicional segunda, procedía alzar la suspensión del plazo acordado, para presentar alegaciones, según se expone en el antecedente 2 en atención a lo dispuesto en su art. 5, en el presente proceso constitucional. En consecuencia, se dio traslado al Gobierno de la Generalidad de Cataluña, por conducto de su Presidente, al objeto de que, en el plazo de quince días, pueda personarse en el proceso y formular las alegaciones que estime convenientes.

9. Las alegaciones del Gobierno de la Generalidad de Cataluña, interesando la desestimación íntegra del recurso, tuvieron entrada en el registro del Tribunal Constitucional el día 12 de junio de 2018.

Comienza señalando que el recurso tiene un carácter preventivo que se funda en un juicio acerca de la intencionalidad de la Ley, por su supuesto carácter a naturaleza de “estructura de estado”, que es ajeno a su contenido dispositivo. La consideración de la Agencia de Ciberseguridad de Cataluña como “estructura de estado” no aparece en el texto de la Ley y esa calificación no pasa de ser un juicio de intenciones y una valoración en términos políticos, carente de toda eficacia jurídica. Además, tal pretensión choca frontalmente con el principio de presunción de constitucionalidad de las leyes y de su debida interpretación conforme con la Constitución. Se trata, por el contrario, de una norma puramente organizativa, que crea nuevo organismo - una agencia gubernamental - en su sector público, para sustituir y suceder a la Fundación que viene ejerciendo en el ámbito de Cataluña las funciones de seguridad de la sociedad de la información, planificación, y la gestión y el control de la seguridad de las tecnologías de la información de la Administración de la Generalidad y de su sector público. Por tanto, la Generalidad no ha pretendido arrogarse con esta Ley la competencia para hacer una regulación general de la ciberseguridad. Además, la pretensión de enjuiciar la Ley 15/2017 en función de su supuesta intencionalidad política resulta totalmente improcedente dentro de un

procedimiento de recurso de inconstitucionalidad, que sólo permite un control jurídico y en abstracto de la norma recurrida, como tiene reiteradamente establecido el Tribunal Constitucional (cita STC 139/2017, de 29 de noviembre). Ese carácter preventivo de la demanda la hace incompatible con el objeto propio de un recurso de inconstitucionalidad, lo que debería llevar, por sí solo, a la desestimación íntegra.

A continuación, el Abogado de la Generalidad de Cataluña indica que el recurso se ha planteado contra la totalidad de la Ley, si bien en el escrito de demanda se dice que el artículo central de la Ley impugnada es el 2, siendo el resto de sus preceptos meramente instrumentales o accesorios, y se imputa la inconstitucionalidad al conjunto de la Ley por constituir una “estructura de estado” y por invadir las competencias del Estado. Sin embargo, según la representación procesal de la Generalidad, la demanda tan sólo formula algún razonamiento específico al referirse a la supuesta inconstitucionalidad por incompetencia del art. 2.1, y cuestiona la determinación del ámbito de actuación de la Agencia por referencia al territorio de Cataluña, así como la supuesta inconstitucionalidad del art. 2.4.f), relativo a la investigación y análisis tecnológico de los ciberincidentes y ciberataques, y del art. 2.5.b), sobre el informe preceptivo de la Agencia en la elaboración de disposiciones normativas tramitadas por la Administración de la Generalidad. Por ello considera que la parte demandante no ha aportado la debida argumentación que pueda fundar la impugnación de los demás preceptos de la Ley 15/2017.

Seguidamente señala, aludiendo al dictamen del Consejo de Estado, que el Estado no dispone de un título competencial específico referido a la materia de la ciberseguridad, por lo que, dando prevalencia al componente tuitivo de la ciberseguridad o seguridad informática, ha optado por encajarla en el título competencial relativo a la seguridad pública, recogido en el art. 149.1.29 CE. Sin embargo, esa competencia normativa estatal no impide que las Comunidades Autónomas puedan adoptar determinadas medidas que coadyuven a garantizar la protección de sus infraestructuras y la seguridad de las tecnologías de la información y la comunicación, lo que deriva de que la ciberseguridad es una técnica instrumental inherente a todo uso de las tecnologías de la comunicación y a múltiples actividades en la sociedad de la información. Del mismo modo, las actuaciones en materia de ciberseguridad conforman también un elemento inescindible de los recursos materiales, del soporte técnico e instrumental que requiere toda administración para actuar, ya sea ejerciendo sus potestades o prestando los servicios públicos.

En el marco de la legislación estatal, la ciberseguridad ha tenido diversos tratamientos que van desde unos relacionados estrictamente con la defensa militar y la seguridad nacional, en los supuestos de más gravedad, hasta otros relacionados con la seguridad pública para la protección de determinadas infraestructuras de telecomunicaciones, incluyendo los aspectos más técnicos. Pero, también, ha previsto la adopción de medidas ordinarias de seguridad respecto a la red y, en general, a las tecnologías de la información, entre otras, respecto a la Administración electrónica. Dicho enfoque tiene su reflejo en diversas leyes estatales como la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, la Ley 8/2011, de 28 de abril, de medidas para la protección de las infraestructuras críticas, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, o, más recientemente, las Leyes 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones públicas, y 40/2015, de 1 de octubre, de régimen jurídico del sector público. Desde el punto de vista del sistema de distribución de competencias entre el Estado y las Comunidades Autónomas, la ciberseguridad es una técnica instrumental de diversas competencias y, por tanto, una materia de naturaleza compleja. Incluso en el supuesto que la ciberseguridad quiera encuadrarse en una parte relevante en los ámbitos competenciales de la seguridad pública y de la defensa, ese encuadramiento no puede entenderse de modo excluyente de las actuaciones de ciberseguridad se han de desarrollar desde cada administración pública y que se enmarcan en sus potestades de organización y régimen jurídico, además de incidir también en otras competencias sectoriales. Corolario imprescindible de todo ello es que la Generalidad de Cataluña, como las demás administraciones públicas, ha de llevar a cabo actuaciones de prevención, de análisis y de investigación tecnológica, y de reacción ante incidencias y ciberataques.

En consecuencia, según el Abogado de la Generalidad, es lógico reconocer a la Ley 15/2017 su encaje esencialmente en las competencias asumidas en materia de organización de la Administración de la Generalidad (art. 150 EAC), en materia de régimen jurídico y procedimiento de las Administraciones públicas catalanas (art. 159 EAC), que comprende los medios necesarios para el ejercicio de las funciones administrativas y también en la competencia en materia de la competencia ejecutiva en materia de comunicaciones electrónicas, en los términos del art. 140.7 EAC, así como en las competencias asumidas en materia de ordenación administrativa del comercio electrónico (art. 121.1.a EAC). El encaje de la Ley catalana en esas competencias es perfectamente razonable si se atiende al carácter autoorganizativo de esta Ley, cuyo objeto es meramente la creación de la Agencia para el desarrollo de funciones ejecutivas en esta materia.

A mayor abundamiento, no puede desconocerse que la creación de la Agencia constituye una modificación orgánica para suceder, dar continuidad y desarrollo a las funciones que desde el año 2009 desempeñaba el Centro de Seguridad de la Información de Cataluña (CESICAT), ahora mediante una forma organizativa más ágil, eficiente y adecuada a los requerimientos de la gestión que tiene encomendada.

El Abogado de la Generalidad de Cataluña reconoce que la ciberseguridad presenta un aspecto directamente relacionado con cuestiones que inciden en ámbitos conectados a la seguridad pública, pero no admite que esa incidencia determine su exclusión respecto de las actuaciones de ciberseguridad que deban llevarse a cabo en Cataluña. De hecho alega que la legislación estatal relativa a la seguridad nacional y a la protección de las infraestructuras críticas no solo presupone la actuación en Cataluña de la Generalidad, adoptando las medidas relacionadas con la ciberseguridad, sino que asume que estas se desarrollen y se integren dentro de los mecanismos de protección y coordinación general establecidos por ambas leyes. Concluye que la Ley 15/2017, además de tener cobertura competencial en las competencias asumidas por la Generalidad de Cataluña en materia de autoorganización y régimen jurídico y procedimiento de las Administraciones de Cataluña, tiene igualmente cobertura en la competencia asumida en materia de seguridad pública, puesto que se da la relación instrumental, de inherencia o complementariedad respecto de las facultades que son propias de las funciones policiales.

Tras lo expuesto, y con carácter subsidiario a la alegación de falta de carga argumental del recurso, el escrito de la Generalidad de Cataluña examina los preceptos de la Ley 15/2017 en los términos que a continuación se exponen.

Respecto al art. 1, indica que se limita a crear la Agencia de Ciberseguridad de Cataluña y a determinar su naturaleza jurídica y su régimen jurídico. En el art. 2 se examinan por separado cada uno de sus apartados. Sobre el apartado 1 señala que no define a la Agencia como la única entidad que vela por la ciberseguridad en Cataluña, ni dispone que vaya a excluir la actuación que corresponde a las instancias estatales en ejercicio de sus propias competencias. El apartado 2 define el objetivo de la Agencia como "la ejecución de las políticas públicas en materia de seguridad", añadiendo a continuación que ese objetivo se concreta en las actuaciones que se enumeran en los cinco subapartados que integran el precepto. Estos objetivos se corresponden con las funciones de la Generalidad respecto de la administración electrónica y también con las que derivan de la necesidad de proteger las redes y sistemas de información propios, así como

los de los particulares que se relacionan por medios electrónicos con la Administración de la Generalidad. Sobre el apartado 3, destaca que nada impide a la Agencia ofrecer la prestación de servicios de ciberseguridad al sector privado, ya que esa oferta se aviene perfectamente con su propia naturaleza de Agencia, en tanto que entidad de derecho público que ajusta su actuación al derecho privado. La Ley no atribuye a la Agencia potestades públicas de regulación ni de intervención sobre el sector privado, sino tan solo funciones de tipo promocional y prestacional, poniendo sus servicios a disposición de los administrados.

Acerca del apartado 4, relativo a las funciones de la Agencia, señala, en primer lugar, que la legislación estatal obliga a las Comunidades Autónomas a disponer de sistemas, medios e instrumentos dentro de su organización para vigilar, prevenir y actuar, así como para coordinarse con el Estado y otras Administraciones a fin de garantizar el normal funcionamiento de los servicios y recursos básicos que se consideran de especial interés para la seguridad nacional, entre los que se encuentra la ciberseguridad. Las funciones previstas en las letras a), b), e) y d) del apartado 4, forman parte de las necesarias medidas de protección que la legislación estatal exige a todas las administraciones públicas. Por lo que se refiere a la función de actuar como apoyo, en materia de ciberseguridad, de cualquier autoridad competente para el ejercicio de sus funciones públicas, de la letra e) es la concreción, en esta materia, de la debida colaboración interadministrativa y del deber de colaborar con Jueces y Tribunales y con el Ministerio Fiscal, que resultan del cumplimiento del ordenamiento vigente. En cuanto a la letra f) señala que la investigación a la que se alude no es policial ni penal, sino relacionada con la necesidad de que la Generalidad ejerza sus funciones de análisis, investigación y respuesta para restablecer sus propios servicios y garantizar su seguridad. Las funciones de las letras g) y h) han de ser interpretadas en términos similares.

Las funciones a las que se refiere el apartado 5 han de entenderse en clave interna, es decir, circunscritas a las políticas de ciberseguridad de las redes y sistemas de información de la propia Generalidad y de las relaciones que pueden establecerse con los mismos. En particular, respecto a la letra b), única mencionada en la demanda, señala que se refiere a las normas que elabore la Generalidad de Cataluña en el ámbito de sus competencias. El art. 2.6 establece que la Agencia de Ciberseguridad de Cataluña ha de colaborar con los organismos judiciales y policiales, de acuerdo con la normativa vigente y ha de coordinarse también con los cuerpos policiales a los efectos de las competencias que dichos cuerpos tienen reconocidas en esta materia. Ello hace patente la voluntad del legislador de que la Agencia actúe coordinadamente y

en colaboración con los demás organismos y autoridades públicas. Lo mismo sucede con el apartado 7 en relación con los entes locales de Cataluña.

Sobre los arts. 3 a 11, las dos disposiciones adicionales, la disposición transitoria y las cinco disposiciones finales, la contestación a la demanda, resalta la falta de argumentación sobre su pretendida inconstitucionalidad así como que se trata de preceptos con un alcance estrictamente organizativo.

10. Por providencia de 18 de diciembre de 2018 se señaló para deliberación y fallo de esta Sentencia el día 20 del mismo mes y año.

II. Fundamentos Jurídicos.

1. El presente proceso constitucional tiene por objeto resolver el recurso de inconstitucionalidad que el Presidente del Gobierno ha interpuesto contra la Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña.

La Ley 15/2017 crea la Agencia de Ciberseguridad de Cataluña como entidad de derecho público con personalidad jurídica propia y sometida al derecho privado, a la que corresponde desarrollar y liderar el servicio público de ciberseguridad necesario para la protección del territorio de Cataluña, gestionar los incidentes de carácter global que afecten a Cataluña y a sus instituciones y coordinar los esfuerzos de los diferentes equipos que puedan tener conocimiento de ellos. La norma regula la naturaleza jurídica y el régimen que se aplica a la Agencia y define, entre otras cuestiones, su objeto y funciones, estructura orgánica, régimen económico y financiero, de contratación, de personal y de control y relaciones con el departamento de adscripción.

Como se ha expuesto en los antecedentes, la impugnación tiene un motivo fundamentalmente competencial porque la Ley 15/2017 vulneraría la competencia exclusiva del Estado en materia de seguridad pública del art. 149.1.29 CE, dentro de la cual se integra la ciberseguridad, en conexión con las competencias estatales en materia de defensa (art. 149.1.4 CE) y telecomunicaciones (art. 149.1.21 CE). La demanda articula, además, un segundo motivo de impugnación relativo al carácter de “estructura de estado” de la Agencia creada por la Ley 15/2017, en función de la relación que dicha Ley 15/2017 guardaría con otras leyes catalanas

aprobadas poco después y que se enmarcan dentro del conjunto de actuaciones llevadas a cabo por la Generalidad en su propósito declarado de construir “estructuras de estado”, con virtualidad sustitutoria de las actualmente vigentes en el sistema estatal.

Por el contrario, el Letrado del Parlamento y el Abogado de la Generalidad de Cataluña han considerado, con argumentos similares, que el recurso tiene una finalidad meramente preventiva, siendo una impugnación genérica e imprecisa, sin que la norma recurrida incurra en ninguna de las vulneraciones constitucionales que la demanda denuncia.

2. Expuesto el objeto de este recurso y las posiciones de las partes, es preciso, atendiendo a lo planteado por las representaciones procesales del Parlamento de Cataluña y del Gobierno de la Generalidad, primero, hacer unas consideraciones en torno al carácter cautelar o preventivo del recurso, y, segundo, acerca de la necesidad de argumentar o fundamentar de manera suficiente los motivos que lo sustentan.

a) En cuanto a lo primero, la naturaleza del recurso, debe concluirse que la impugnación no es preventiva, ni cautelar, y no merece, por tanto, el reproche que en tal sentido se hace por parte del Letrado del Parlamento de Cataluña y del Abogado del Gobierno de la Generalidad.

Este Tribunal se ha pronunciado sobre la dificultad de valorar con carácter general y previo el carácter preventivo de un recurso. Verificar si dicho rasgo concurre requiere examinar cada una de las impugnaciones (STC 110/2011, de 22 de junio, FJ 3, con cita de la STC 31/2010, de 28 de junio, FJ 2). El Tribunal tiene declarado que “es constante la doctrina que insiste en que no será legítima la utilización del recurso de inconstitucionalidad con la finalidad de obtener declaraciones preventivas o previsoras ante eventuales agravios competenciales o interpretativas que pongan a cubierto de aplicaciones contrarias al orden de competencias establecidas en la [Constitución] y, dentro del marco constitucional, en los Estatutos de Autonomía (STC 49/1984, de 5 de abril, FJ 2)” (SSTC 110/2011, FJ 3, y 31/2010, FJ 2). Sin embargo, en las mismas Sentencias se declara también que estos defectos “solo podrán ‘verificarse’ caso por caso, con ocasión del examen de cada una de las impugnaciones” por lo que en ellas se rechaza el motivo de oposición al recurso cuando se plantea con carácter general en estos términos.

Lo mismo sucede aquí. El objeto de este recurso es la creación por la Ley 15/2017 de una nueva estructura organizativa autonómica en un ámbito material concreto, el de la

ciberseguridad, creación a la que se le imputan vicios de inconstitucionalidad sustantivos y competenciales, que, caso de ser estimados, determinarían que el Parlamento de Cataluña habría incurrido en una inconstitucionalidad actual y efectiva, pues habría llevado a cabo una actuación legislativa y una afirmación competencial que constituirían un ilícito constitucional consumado (SSTC 71/1982, de 30 de noviembre, FJ 5; 101/1995, de 26 de junio, FJ 7, y 128/2016, de 7 de julio, FJ 5). En suma, se pone en duda la viabilidad del recurso con argumentos que no inciden sobre la corrección procesal de la vía emprendida al interponerlo, sino sobre lo mal fundado de la pretensión que incorpora [en el mismo sentido, STC 52/2017, de 10 de mayo, FJ 2.b)].

b) Respecto al incumplimiento por el Abogado del Estado de su carga alegatoria, que también esgrimen el Letrado del Parlamento de Cataluña y el Abogado del Gobierno de la Generalidad, el Tribunal tiene declarado que la obligación de levantar la carga alegatoria en todos los procesos seguidos ante él supone una exigencia de colaboración con la justicia, además de una condición inexcusable inherente a la presunción de constitucionalidad de las normas con rango de ley, que no puede desvirtuarse sin un mínimo de argumentación (por todas, STC 184/2016, de 3 de noviembre, FJ 2). En efecto, “cuando lo que está en juego es la depuración del ordenamiento jurídico, es carga de los recurrentes no sólo la de abrir la vía para que el Tribunal pueda pronunciarse, sino también la de colaborar con la justicia del Tribunal en un pormenorizado análisis de las graves cuestiones que se suscitan. Es justo, pues, hablar... de una carga del recurrente y en los casos en que aquélla no se observe, de una falta de diligencia procesalmente exigible, que es la diligencia de ofrecer la fundamentación que razonablemente es de esperar (STC 11/1981, de 8 de abril, FJ 3, reiterada en las SSTC 43/1996, de 15 de abril, FJ 3; 36/1994, de 10 de febrero, FJ 1, y 61/1997, de 20 de marzo, FJ 13)” (STC 86/2017, de 4 de julio, FJ 2).

A fin de verificar si el recurrente ha satisfecho la diligencia procesal exigible para justificar la existencia de las infracciones constitucionales que denuncia es obligado analizar el contenido del recurso. Atendiendo al mismo, cabe constatar que en la demanda hay una argumentación específica en cuanto al carácter de “estructura de estado” que se imputa a la Agencia creada por la Ley 15/2017, lo que implica que debemos pronunciarnos al respecto.

Sobre la vulneración del orden de distribución de competencias que se reprocha a la norma, el Abogado del Estado denuncia que “la regulación completa que realiza la Ley desborda las competencias autonómicas”. La queja es que se establece una completa regulación de la ciberseguridad en todos sus ámbitos y en todo el territorio de Cataluña, pero esa queja, concretada

en que las funciones atribuidas a la Agencia de Ciberseguridad de Cataluña superan el ámbito competencial autonómico, solo se desarrolla respecto a un precepto de la norma. Como hemos expuesto con más detalle en los antecedentes, el iter discursivo del recurso arranca con la descripción del contenido de la norma, con especial detenimiento en su art. 2, a lo que sigue la exposición de la doctrina constitucional sobre el régimen de distribución de competencias entre el Estado y las Comunidades Autónomas en relación con la seguridad pública. Dicha exposición es insuficiente por sí misma para satisfacer la diligencia procesal que permita soportar la impugnación de los concretos preceptos de la Ley 15/2017, pues es exigible que la parte recurrente proyecte la doctrina que expone sobre los mismos mediante un razonamiento que justifique el exceso competencial denunciado (en el mismo sentido, STC 118/2017, de 19 de octubre, FJ 2).

En efecto, esta exposición no va seguida de la fundamentación necesaria para permitir el pronunciamiento de este Tribunal acerca de la totalidad de los preceptos de la Ley 15/2017, con lo que el recurrente no cumple la carga alegatoria exigible que le incumbe (STC 92/2017, de 6 de julio, FJ 2, entre muchas otras). La argumentación de la demanda se ciñe exclusivamente al art. 2 relativo al objeto y funciones de la Agencia de Ciberseguridad de Cataluña. La demanda describe los contenidos de los diferentes apartados de este precepto, si bien las razones de la inconstitucionalidad que se solicita aparecen únicamente concretadas respecto al apartado 1 y, por relación con él, a los apartados 2 y 3. También se denuncia que la Ley 15/2017 atribuye a la Agencia una serie de facultades y funciones que exceden de las competencias autonómicas, pero este exceso competencial únicamente se argumenta específicamente respecto a la letra f) del apartado 4 y a la letra b) del apartado 5, así como, ya por remisión al dictamen del Consejo de Estado, respecto a las letras b) y e) de ese mismo apartado 4 y de las letras a) y d) del apartado 5. Sobre el resto de preceptos de la Ley 15/2017 no es posible, atendiendo a lo que la demanda plantea, dilucidar las objeciones genéricas de inconstitucionalidad formuladas en el recurso, al no exponer el mismo las razones por las que tales preceptos habrían excedido las competencias autonómicas, con la consiguiente vulneración de las estatales que se afirma en la demanda.

Ese modo de articular el recurso, unido a la reiterada doctrina de este Tribunal, por la que no podemos “reconstruir de oficio la demanda ni suplir las razones de los recurrentes, cuando éstas no se aportan en su recurso” (STC 85/2016, de 28 de abril, FJ 2), lleva a entender que únicamente concurre la carga argumental mínima exigible en relación con la vulneración de las competencias estatales que se denuncian en la demanda respecto al apartado 1, en relación con

los apartados 2 y 3; al apartado 4, letras b), e) y f) y a la letras a), b) y d) del apartado 5, todos ellos del art. 2 de la Ley 15/2017.

3. Señalado lo anterior se puede ya iniciar el enjuiciamiento de la Ley 15/2017.

Comenzaremos por el examen de la queja relativa al carácter de “estructura de estado” que se imputa a la Ley 15/2017 en cuanto crea la Agencia de Ciberseguridad de Cataluña.

El Abogado del Estado argumenta, por referencia al dictamen del Consejo de Estado, que la Ley 15/2017 puede relacionarse con el proceso de creación de estructuras de estado acometido por la Generalidad, sobre el que ya se ha pronunciado la STC 52/2017. Añade que la norma está redactada en unos términos ambiguos, incluyendo algunas previsiones que podrían entenderse indistintamente aplicables dentro del orden de distribución de competencias diseñado por la Constitución o al margen de él, pero tampoco oculta que la Agencia que crea dicha Ley constituye, en su propio ámbito, una estructura organizativa idónea para actuar de forma autónoma en un eventual Estado catalán independiente. Los Letrados autonómicos han negado el carácter de “estructura de estado” que la demanda atribuye a la Agencia, alegando que la norma ha de ser examinada atendiendo al sentido propio y al contenido literal de sus términos.

La Ley 3/2015, de 11 de marzo, de medidas fiscales, financieras y administrativas de Cataluña, vino a materializar propuestas contenidas en los informes del Consejo Asesor para la Transición Nacional de Cataluña, en los que se diseñó la denominada “hoja de ruta” para la constitución de un Estado catalán y se abordaron diversas cuestiones estrechamente relacionadas con la pretensión de crear estructuras de estado, dotadas de características precisas para operar la sustitución del sistema estatal en el momento en que se produjera la pretendida independencia de Cataluña. Dicha norma fue declarada parcialmente inconstitucional en la STC 128/2016. La creación de la Agencia de Ciberseguridad de Cataluña no se encontraba mencionada en la referida Ley 3/2015, como una de las actuaciones encomendadas a la Generalidad de Cataluña dentro del llamado proceso de transición nacional para la “desconexión” del Estado.

Este Tribunal ha rechazado ya en ocasiones anteriores pretensiones similares a la que ahora se formula [SSTC 139/2017, de 29 de noviembre, FJ 2.c); 90/2017, de 5 de julio, FJ 2, y 128/2016, FJ 5.A)]. En los tres casos, el Tribunal ha destacado que el control que desarrolla “es exclusivamente de constitucionalidad, de carácter jurídico, no político, ni de oportunidad, ni de

calidad técnica, ni de idoneidad. De modo que las intenciones del legislador, su estrategia política o su propósito último no constituyen, como es evidente, objeto de nuestro enjuiciamiento, que ha de circunscribirse a contrastar los concretos preceptos impugnados y las normas y principios constitucionales que integran en cada caso el parámetro de control” [por todas, STC 185/2016, de 3 de noviembre, FJ 7.a)]. Por ello, la norma impugnada, cuya supuesta inconstitucionalidad se ventila debe ser interpretada y enjuiciada en atención a su propio sentido y tenor literal, no a partir del contexto que la demanda trae a colación referido a su utilización como una eventual “estructura de estado”, pues esa apreciación se basa en la intención que se atribuye a la norma catalana (STC 54/2018, de 24 de mayo, FJ 4), no en la literalidad de la disposición. Sentido y tenor literal de las disposiciones impugnadas que fueron las que llevaron a este Tribunal a apreciar, en la STC 128/2016 la inconstitucionalidad y nulidad de las disposiciones adicionales vigésima segunda, vigésima cuarta y vigésima sexta de la mencionada Ley 3/2015.

En este caso, dicho carácter, como explícitamente reconoce el Abogado del Estado, no se deduce indubitadamente del tenor de la norma impugnada. Tampoco la alegación se formula de modo concluyente, sino en términos marcadamente hipotéticos, ya que la propia demanda admite que algunas previsiones de la Ley 15/2017 “podrían entenderse indistintamente aplicables dentro del orden de distribución de competencias diseñado por la Constitución de 1978 o al margen de él”. Resulta también de aplicación la consolidada doctrina acerca de que la eventualidad de un uso desviado de la norma no puede servir de fundamento para su anulación. Como señaló la STC 238/2012, de 13 de diciembre, FJ 7, “la mera posibilidad de un uso torticero de las normas no puede ser nunca en sí misma motivo bastante para declarar la inconstitucionalidad de éstas, pues aunque el Estado de Derecho tiende a la sustitución del gobierno de los hombres por el gobierno de las leyes, no hay ningún legislador, por sabio que sea, capaz de producir leyes de las que un gobernante no pueda hacer mal uso (STC 58/1982, de 27 de julio, FJ 2, en el mismo sentido SSTC 132/1989, de 18 de julio, FJ 14; 204/1994, de 11 de julio, FJ 6; 235/2000, de 5 de octubre, FJ 5, y 134/2006, de 27 de abril, FJ 4)”.

Consecuentemente, este primer motivo de inconstitucionalidad ha de ser desestimado.

4. Se debe analizar ahora la vulneración de las competencias estatales que la demanda denuncia.

Denuncia que, como ya se ha expuesto, se imputa al apartado 1, en relación con los apartados 2 y 3; al apartado 4, letras b), e) y f) y a la letras a), b) y d) del apartado 5, todos ellos del art. 2 de la Ley 15/2017.

Para ello es preciso hacer una breve referencia a la ciberseguridad, a fin de insertar los preceptos impugnados en el contexto que les es propio, atendiendo también a lo discutido entre las partes.

La Unión Internacional de Telecomunicaciones define 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” (Recomendación de la Unión Internacional de Telecomunicaciones UIT-T X.1205). Por su parte, en la Directiva (UE) 2016/1148, de 6 de julio, del Parlamento Europeo y del Consejo, se define la “seguridad de las redes y sistemas de información” como “la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información accesibles a través de ellos” (art. 4.2). Con esta finalidad, y según la propia Directiva, los Estados pueden adoptar medidas de “prevención, detección, respuesta y mitigación de los incidentes y riesgos que afecten a las redes y sistemas de información” (considerando 34).

Dado el contenido de los diversos aspectos que configuran el concepto de la ciberseguridad, es posible considerar que ésta puede tener varias acepciones y comprender varias actividades. Ese carácter de la ciberseguridad ha sido también destacado en las alegaciones de los letrados autonómicos.

En lo que a efectos del presente proceso interesa, hay que mencionar, en primer lugar, la relacionada con la adopción de medidas ordinarias de prevención o seguridad de la red y, en general, de las tecnologías de la información. En particular, respecto a la administración electrónica, garantizando la protección de las redes de comunicaciones electrónicas que esta genere y la protección de los derechos de los administrados en sus relaciones con las administraciones públicas a través de medios electrónicos. No discute el Abogado del Estado,

que las Comunidades Autónomas pueden, al amparo de las competencias que sus Estatutos de Autonomía les reconocen, adoptar determinadas medidas dirigidas a garantizar la protección de sus infraestructuras y la seguridad de las tecnologías de la información y la comunicación. Medidas en este ámbito que, en muchas ocasiones, vienen reclamadas por las propias normas estatales (así, por ejemplo, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, dictado en desarrollo del derogado art. 42.2 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos).

De acuerdo con ello, la Generalidad debe adoptar medidas en materia de ciberseguridad en tanto en cuanto se aplican a las relaciones que tiene con sus administrados y con otras administraciones, así como respecto de las infraestructuras tecnológicas, que pertenezcan a la estructura de la Administración de la Generalidad y a su sector público. Cabe mencionar, como ejemplo de lo anteriormente expuesto, la aprobación, mediante Acuerdo del Gobierno GOV/50/2009, de 17 de marzo, del Plan de Seguridad de la Información de Cataluña. Posteriormente, por Acuerdo del Gobierno de 22 de diciembre de 2009, se autorizó la constitución de la Fundación Centro de Seguridad de la Información de Cataluña (CESICAT), a la que se encomendó la consecución de los objetivos perseguidos por el referido Plan; por Acuerdo del Gobierno GOB/103/2012, de 16 de octubre, se encargó al CESICAT la planificación, gestión y control de la seguridad de las TIC de la Administración de la Generalidad de Cataluña y de su sector público. La Agencia de Ciberseguridad de Cataluña, creada al amparo de dicha competencia, pretende sustituir a este organismo autonómico, que deberá iniciar el procedimiento de disolución en el momento de constitución de aquella y cederle sus bienes, derechos y obligaciones (disposición final tercera de la Ley 15/2017). A la Agencia se le encomiendan funciones mucho más amplias, como son las de “prestar el servicio público de ciberseguridad”, según se reconoce en la exposición de motivos, desarrollando y liderando tal servicio, coordinando la ciberseguridad en el ámbito de Cataluña y garantizando la ciberseguridad de la Administración de la Generalidad.

La 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 conceptualización 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.

En el ATC 29/2018, de 20 de marzo, FJ 5, ya se constató la conexión existente entre ciberseguridad y seguridad nacional “incluida como dice expresamente la Ley 36/2015, en los títulos competenciales de las materias 4 y 29 del art. 149.1 CE” (STC 184/2016, FJ 3), pues la Ley 36/2015, de 28 de septiembre, de seguridad nacional, identifica en su art. 10 la ciberseguridad como uno de los “ámbitos de especial interés de la seguridad nacional ... que requieren una atención específica, por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales”. También la Ley 8/2011, de 28 abril, de medidas para la protección de las infraestructuras críticas, dictada al amparo de la competencia atribuida al Estado en virtud del art. 149.1.29 CE, hace referencia a la ciberseguridad. El art. 2 de esta Ley define las infraestructuras estratégicas como “las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales”. Tales servicios esenciales son los necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas. La Ley 8/2011 también define las infraestructuras críticas como aquellas de las infraestructuras estratégicas “cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales”. Y en su anexo se incluyen las tecnologías de la información y las comunicaciones como sector estratégico. Las instalaciones, redes, sistemas y equipos de tecnología de la información tienen la consideración, en los casos previstos en dicha norma, bien de instalaciones estratégicas o, incluso, de instalaciones críticas.

A mayor abundamiento, el mantenimiento de la ciberseguridad es una de las funciones propias del Centro Nacional de Inteligencia, según establece el art. 4.b) de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. Además, la ciberseguridad es uno de sus objetivos, conforme a la Estrategia de Seguridad Nacional 2017, aprobada por Real Decreto

1008/2017, de 1 de diciembre, a fin de “Garantizar un uso seguro de las redes y los sistemas de información y comunicación a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques, potenciando y adoptando medidas específicas para contribuir a un ciberespacio seguro y fiable”. Este objetivo se desarrolla a través de líneas estratégicas de acción igualmente definidas en la norma, tendentes a mejorar los desarrollos normativos, organizativos y técnicos y los mecanismos de prevención y respuesta frente a posibles agresiones que redunden en un entorno digital seguro y fiable, tanto en el ámbito del sector público como en el empresarial o el de los ciudadanos.

Esta relación entre ciberseguridad y seguridad nacional se confirma en la Orden PCI/870/2018, de 3 de agosto, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba el procedimiento para la elaboración de una nueva Estrategia de Ciberseguridad Nacional que sustituya a la actualmente vigente. Esa Estrategia de Ciberseguridad Nacional data del año 2013 y sienta las prioridades, objetivos y medidas adecuadas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información. Dicha Estrategia es el marco de referencia de un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, en la colaboración público-privada, y en la participación de la ciudadanía. Según se afirma, es el documento estratégico que sirve de fundamento al Gobierno de España para desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas.

La Estrategia fija seis objetivos específicos: 1) para las administraciones públicas, garantizar que los Sistemas de Información y Telecomunicaciones utilizados poseen el adecuado nivel de seguridad y resiliencia; 2) para las empresas y las infraestructuras críticas, impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular; 3) en el ámbito judicial y policial, potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio; 4) en materia de sensibilización, concienciar a los ciudadanos, profesionales, empresas y administraciones públicas españolas de los riesgos derivados del ciberespacio; 5) en capacitación, alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad; y 6) en lo que se refiere

a la colaboración internacional, contribuir en la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales, así como colaborar en la capacitación de Estados que lo necesiten a través de la política de cooperación al desarrollo. Estos objetivos se concretan en unas líneas de acción que son las siguientes: 1) capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas; 2) seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas; 3) seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas; 4) capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia; 5) seguridad y resiliencia de las TIC en el sector privado; 6) conocimientos, competencias e i+d+i; y 7) cultura de ciberseguridad y compromiso internacional.

Finalmente, ha de aludirse al Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico 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. Esta norma 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. 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. Se afirma dictado al amparo de las competencias estatales de los arts. 149.1.21 y 149.1.29 CE (disposición final primera).

En suma, puede afirmarse que la evolución de las tecnologías de la información y de la comunicación ha hecho que las redes y sistemas de información desempeñen actualmente un papel crucial en nuestra sociedad, siendo su fiabilidad y seguridad aspectos esenciales para el desarrollo de las actividades económicas y sociales. Prueba de ello es que los operadores de redes

y servicios de comunicaciones electrónicas disponibles al público están obligados a gestionar “adecuadamente los riesgos de seguridad que puedan afectar a sus redes y servicios a fin de garantizar un adecuado nivel de seguridad y evitar o reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y en las redes interconectadas” (art. 44.1 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones). Atendiendo a lo que se ha expuesto, puede concluirse 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.

5. Como ha indicado el Parlamento de Cataluña en sus alegaciones, 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.

Tal y como ha quedado expuesto, la Ley catalana tiene por objeto la creación de una Agencia de Ciberseguridad como entidad de derecho público de la Administración de la Generalidad (art. 1) a la que corresponde "garantizar la ciberseguridad en el territorio de Cataluña, entendida como la seguridad de las redes de comunicaciones electrónicas y de los sistemas de información" (art. 2.1).

Dicha creación pretende ampararse, según precisa la exposición de motivos de la Ley 15/2017, en la competencia exclusiva de la Generalidad de Cataluña en materia de organización de su Administración, así como en la competencia ejecutiva en materia de comunicaciones electrónicas y en la competencia exclusiva en materia de comercio [arts. 150, 140.7 y 121.1.a) EAC].

Se constata así que no existe, en este caso, título competencial autonómico alguno específicamente referido a la ciberseguridad, sobre la que se proyectan las funciones encomendadas a la Agencia.

En lo que respecta al encuadramiento material de la norma, a efectos de resolver la impugnación planteada, debe partirse del carácter transversal e interconectado de las tecnologías de la información y las comunicaciones y de su conceptualización como conjunto de mecanismos dirigidos a la protección de las infraestructuras informáticas y de la información digital que albergan los sistemas interconectados. Componente tuitivo al que se ha aludido ya y que determina que las cuestiones discutidas en el presente recurso deban resolverse a partir de su encuadramiento material en el ámbito de la seguridad pública en relación con las telecomunicaciones y la seguridad nacional. El Abogado del Estado no ha cuestionado, antes al contrario, que las diferentes administraciones públicas son competentes para la adopción de medidas de autoprotección en relación con sus infraestructuras y la seguridad de las tecnologías de la información y la comunicación, por lo que esta dimensión de la ciberseguridad no se ve aquí concernida.

En consecuencia, lo que hay que determinar es si la Ley 15/2017, en aquellos de sus preceptos sobre los que el recurso ha proporcionado una adecuada fundamentación de la impugnación, ha pretendido regular la ciberseguridad como un ámbito material relacionado con la seguridad pública, que es lo que el recurso denuncia, o bien se trata de una regulación que persigue dar una respuesta adecuada a las amenazas que puedan afectar a las redes de comunicación electrónica y sistemas de información de las Administraciones Públicas de Cataluña.

6. Se deben mencionar ahora, en primer lugar, los preceptos del bloque de la constitucionalidad que delimitan la distribución de competencias en la materia de “seguridad pública” y, en segundo lugar, a los términos en los que la doctrina constitucional se ha referido a dicha materia, en particular en lo relativo a las competencias estatales y autonómicas sobre la misma. Aludiremos también a la doctrina constitucional sobre la materia telecomunicaciones y régimen general de comunicaciones, así como acerca de los restantes títulos invocados por los Letrados autonómicos, la potestad relativa a la organización de su propia administración pública de la Comunidad Autónoma y las competencias autonómicas en materia de comercio electrónico.

a) Procede recordar que la materia “seguridad pública” hace referencia a la “protección que se lleva a cabo, preferentemente, mediante la actividad policial propiamente dicha y las funciones no policiales inherentes o complementarias a aquellas” (SSTC 104/1989, de 8 de junio,

FJ 6, y 175/1999, de 30 de septiembre, FJ 5). Pero también “puede ir más allá de la regulación de las intervenciones de la ‘policía de seguridad’, es decir, de las funciones propias de las fuerzas y cuerpos de seguridad” (STC 86/2014, de 29 de mayo, FJ 4), de tal suerte que “la actividad policial es una parte de la materia más amplia de la seguridad pública” (SSTC 175/1999, FJ 7). La seguridad pública es, en principio, competencia exclusiva del Estado ex art. 149.1.29 CE, precepto constitucional que pone de manifiesto que ya en él se establecen salvedades (“sin perjuicio de...”) que, en cierto sentido, vienen a modular la exclusividad de la competencia estatal, proclamada en el párrafo inicial del art. 149 CE. De esas salvedades pueden derivarse, en su caso, límites, en razón del contenido de los Estatutos de las diferentes Comunidades Autónomas y de la Ley Orgánica a la que la norma constitucional confía la regulación del marco al que ha de ajustarse la creación de policías por las Comunidades Autónomas. Así se ha declarado que “la competencia exclusiva del Estado en materia de seguridad pública no admite más excepción que la que derive de la creación de las policías autónomas” (STC 104/1989, de 8 de junio, FJ 3). Es pues doctrina consolidada de este Tribunal que la seguridad pública es una competencia exclusiva del Estado ex art. 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 (por todas, STC 148/2000, de 1 de junio, FJ 5).

Por tanto, en esta materia las Comunidades Autónomas no pueden asumir estatutariamente más competencias que las previstas, para la creación de cuerpos propios de policía, en el art. 149.1.29 CE. Competencias que la Generalidad ostenta con los contenidos funcionales definidos en el art. 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).

Sin 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.

De este modo, en los términos de nuestra doctrina, no basta únicamente la conexión de una determinada función con la materia seguridad pública, para encuadrarla competencialmente en la esfera de responsabilidad del Estado, sino que, además del dato positivo de esa posible conexión, que se daría en todos los casos de funciones policiales, es necesario el negativo de la inexistencia de vinculación específica con la competencia derivada de la “creación” de la policía autonómica, cuyo ámbito competencial no comporta sólo una referencia orgánica, sino también funcional. Esta competencia autonómica se refiere a la función policial prestada por dicha policía autónoma, esto es, a la capacidad de los poderes autonómicos de organizar aquella y ejercer las funciones o servicios policiales no estatales, así como las potestades administrativas que puedan ser consideradas como complementarias o inherentes a las tareas de prevención e investigación de hechos delictivos y persecución de los culpables, del mantenimiento del orden ciudadano y otras análogas que se atribuyen a los cuerpos y fuerzas de seguridad (por todas, STC 104/1989, FJ 4).

Entendida en tales términos, competencias orgánicas y funcionales sobre la propia policía y potestades administrativas inherentes o complementarias a la actividad estrictamente policial, la competencia autonómica derivada de la creación de la policía de seguridad propia es la única excepción que el art. 149.1.29 CE contempla a la exclusiva competencia estatal sobre seguridad pública.

b) En segundo lugar, incide en esta materia la competencia exclusiva estatal en materia de telecomunicaciones y de régimen general de comunicaciones del art. 149.1.21 CE. La primera de ellas se conecta con los aspectos técnicos de la emisión relativos al uso de las ondas radioeléctricas o electromagnéticas (dominio público radioeléctrico), lo que justifica proceder a una “ordenación conjunta de todas las variantes de telecomunicación y radiocomunicación” [STC 78/2017, de 22 de junio, FJ 4.a), citando la STC 168/1993, de 27 de mayo, FJ 4]. Por su parte la competencia exclusiva estatal respecto del “régimen general de comunicaciones” “comprende, desde luego, la totalidad de las competencias normativas sobre la misma (SSTC 84/1982, FJ 4 y 38/1983, FJ 3); pero implica también un plus”, ya que “puede comportar la atribución de las competencias de ejecución necesarias para configurar un sistema materialmente unitario” (STC 195/1996, de 28 de noviembre, FJ 6).

Como recuerda la STC 8/2016, de 21 de enero, FJ 3: “Desde una última perspectiva, más global, se integra también en la materia de telecomunicaciones y de régimen general de

comunicaciones (y corresponde por tanto al Estado la competencia exclusiva conforme al 149.1.21 CE) la conformación, regulación o configuración del propio sector de telecomunicaciones (comunicaciones electrónicas) atendiendo a la convergencia tecnológica (y de servicios) y al marco regulador de las comunicaciones electrónicas de la Unión Europea para asegurar una regulación homogénea en todo el territorio español. Esta homogeneidad resulta necesaria, no solo para el desarrollo e innovación del sector, sino también para la garantía de los derechos de los ciudadanos en el marco de la sociedad de la información (o sociedad del conocimiento), si se tiene en cuenta que el desarrollo de las comunicaciones y de las nuevas tecnologías de la información constituye un factor esencial para lograr la cohesión social, económica y territorial necesarias para evitar, o al menos disminuir, la llamada fractura digital”.

A este respecto, el art. 3.b) del Real Decreto-ley 12/2018, dictado al amparo de las competencias exclusivas del Estado en materia de telecomunicaciones y régimen general de comunicaciones (art. 149.1.21 CE) y seguridad pública (art. 149.1.29 CE), define la seguridad de las redes y sistemas de información como: “la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos”.

El apartado 7 del art. 140 EAC atribuye a la Generalidad “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).

c) El otro título competencial que invoca la ley catalana, relativo al comercio [art. 121.1.a) EAC], no presta cobertura a esta regulación, cuyo objeto directamente no es el comercio electrónico. Y aunque indirectamente lo fuera, no trata de la actividad comercial a la que se refiere este título competencial, sino de las condiciones de seguridad en las que debe desenvolverse

cuando la actividad comercial se desarrolla por vía electrónica, lo cual reconduce al soporte –las redes y servicios de comunicación electrónica- que prevalentemente se encuadran en el ámbito del art. 149.1.21 CE.

d) Finalmente, puesto que las representaciones de las instituciones autonómicas han entendido que los preceptos impugnados responden a la capacidad de la Generalidad de Cataluña para organizar su propia Administración, procede recordar, siquiera brevemente, nuestra doctrina al respecto.

La “potestad de autoorganización” de la Comunidad Autónoma (STC 204/1992, de 26 de noviembre, FJ 5) supone la potestad para crear, modificar y suprimir los órganos, unidades administrativas o entidades que configuran la respectiva Administración autonómica o dependen de ella (STC 55/1999, de 6 de abril, FJ 3, y las que allí se citan) que nuestra doctrina ha identificado con la competencia autonómica en materia de régimen de organización de su autogobierno, esto es, de decidir cómo organizar el desempeño de sus propias competencias. Resulta de lo anterior que la Comunidad Autónoma puede “conformar libremente la estructura orgánica de su aparato administrativo” (STC 165/1986, de 18 de diciembre, FJ 6), creando los departamentos o unidades que estime convenientes en orden al adecuado ejercicio de las competencias que le han sido atribuidas, siempre y cuando con ello no interfiera en las que son propias del Estado. Así pues, tan indiscutible es esta competencia autonómica para la propia organización, como el que la misma solo podrá ejercerse sobre ámbitos que, materialmente, correspondan a la propia Comunidad Autónoma, “pues no son concebibles, en Derecho, órganos, servicios o agencias autonómicos cuyas funciones no sean reconducibles a unas u otras competencias estatutarias” (STC 52/2017, FJ 5).

La Generalidad ostenta competencias para la organización de su propia Administración (arts. 71.6 y 150 EAC), así como que 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). Sin embargo, la cuestión planteada no es ésta, sino la de las funciones que la Ley 15/2017 reconoce o atribuye a la Agencia que crea. La queja que ha planteado el Abogado del Estado se centra en que el objeto y funciones en que se inserta la actividad de la Agencia no se ciñe al ámbito de la protección de la seguridad de las redes de comunicación electrónicas de la Administración de la Generalidad, sino que, por el contrario, el abanico de actuaciones que desarrolla la Agencia, de naturaleza muy diversa, permite

deducir elementos que, según el caso, pueden incidir sobre las competencias en materia de seguridad pública (149.1.29 CE) y de telecomunicaciones y régimen general de comunicaciones (art. 149.1.21 CE).

7. Conforme a todo lo anterior puede ya abordarse el examen de los preceptos de la Ley 15/2017 impugnados por razones competenciales. Estos son el apartado 1, en relación con los apartados 2 y 3; el apartado 4, letras b), e) y f), y las letras a), b) y d) del apartado 5, todos ellos del art. 2 de la Ley 15/2017. Dado que la argumentación no es exhaustiva, tampoco habrá de serlo nuestra respuesta (STC 42/2018, de 26 de abril, FJ 5, y a las que se remite).

a) El art. 2.1 prescribe que “La Agencia de Ciberseguridad de Cataluña tiene por objeto garantizar la ciberseguridad en el territorio de Cataluña, entendida como la seguridad de las redes de comunicaciones electrónicas y de los sistemas de información”.

El Abogado del Estado ha planteado que, dada su redacción genérica, es susceptible de afectar a infraestructuras situadas fuera del territorio catalán. Los Letrados autonómicos han negado la vulneración denunciada.

Las propias normas estatales que ya se han mencionado presuponen facultades autonómicas en ámbitos relacionados con la ciberseguridad, [así, por ejemplo, arts. 5.d), 10 y 15 de la Ley 8/2011 y arts. 6, 11, 27.3 y disposición adicional tercera de la Ley 36/2015], de suerte que el precepto, en cuanto expresión de esas facultades, no podría ser considerado inconstitucional. Ahora bien, la definición del objeto que efectúa el precepto es muy extensa en su concepción, pues si hemos apreciado la ciberseguridad se integra en las competencias estatales en materia de seguridad pública y de telecomunicaciones, es claro que esa atribución incondicionada a la Agencia en el territorio de Cataluña desborda en su enunciación los márgenes en los que la ciberseguridad se incluye en las competencias autonómicas, tal como antes han quedado definidos. Esas competencias autonómicas no permiten amparar una pretensión de configurar una garantía general y omnicomprendiva de la ciberseguridad como la que contiene el precepto que examinamos. Pretensión de generalidad que, por lo demás, se ratifica a la vista de la exposición de motivos de la Ley 15/2017.

Por tanto, el art. 2.1 de la Ley 15/2017 es inconstitucional y nulo.

b) Respecto a los apartados 2 y 3, lo único que se alega es que su tenor literal reforzaría la conclusión de inconstitucionalidad que se le imputa al apartado 1.

i) La impugnación del apartado 2 no puede ser estimada, ya que se circunscribe a las actuaciones en relación con la Administración de la Generalidad y de su sector público. Este apartado define el objetivo de la Agencia como "la ejecución de las políticas públicas en materia de ciberseguridad", añadiendo a continuación que, en particular, ese objetivo se concreta en las actuaciones que se enumeran en los cinco subapartados, relativos a asesorar al Gobierno y prestarle apoyo en la elaboración de los planes de ciberseguridad; ejecutar los planes de ciberseguridad; coordinarse con otros organismos en el desarrollo de estos planes; organizar actividades de difusión, formación y concienciación dirigidas a los diferentes colectivos de destinatarios, haciendo especial énfasis en las situaciones de vulnerabilidad y facilitando instrumentos y programas al respecto; e impulsar un clima de confianza y seguridad que contribuya al desarrollo de la economía y de la sociedad digital en Cataluña.

Se trata, en unos casos, de actuaciones referidas a la ejecución de políticas públicas en materia de ciberseguridad, políticas cuya existencia, en tanto que referidas a la Administración de la Generalidad y su sector público, no ha sido discutida por el Abogado del Estado. Las tres primeras guardan relación con las actuaciones que la Generalidad puede poner en marcha en relación con sus propias redes y sistemas de telecomunicaciones teniendo presente la necesidad de proteger sus comunicaciones electrónicas. Se relacionan con la competencia autonómica del art. 159.1.a) EAC, relativa a los medios necesarios para el ejercicio de las facultades administrativas y con las funciones que corresponden a la Generalidad relacionadas con la administración electrónica. Son expresión, por otra parte, de la aplicación de previsiones de normas estatales en materia de administración electrónica (arts. 1.2, 11 a 30 y 36 del Real Decreto 3/2010), de seguridad nacional (arts. 10, 11, 27.3 y disposición adicional tercera de la Ley 36/2015) y de infraestructuras críticas [arts. 2.d), e) y f); 10 y 15.2 de la Ley 8/2011]. Las otras dos actuaciones se refieren a medidas de fomento que la Generalidad puede llevar a cabo en su propio ámbito de competencias y que, tal como se formulan, no puede entenderse que perturben o menoscaben el ejercicio de las competencias estatales en materia de seguridad pública o de telecomunicaciones.

Por tanto, el art. 2.2, entendido en el sentido de que el objetivo que persigue la Agencia se relaciona con la necesidad de proteger las redes y sistemas de información de la

Administración de la Generalidad 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. Esta interpretación se llevará al Fallo.

ii) El tenor literal del art. 2.3 permite diferenciar dos ámbitos en este precepto.

El primero establece que, en la ejecución de los objetivos fijados en el apartado 2, la Agencia “puede ejercer sus funciones” con relación a las personas físicas y jurídicas situadas en Cataluña. Nuevamente la referencia incondicionada a las personas físicas y jurídicas evidencia una pretensión de generalidad en la actuación de la Agencia que supera las atribuciones autonómicas en esta materia. Es, así, contraria al orden competencial por cuanto no se limita a objetivos relacionados con la necesidad de proteger las redes y sistemas de información propios y los de los particulares y de otras administraciones que se relacionan por medios electrónicos con la administración.

El segundo prevé que, para la ejecución de esos mismos objetivos, también puede “establecer la colaboración necesaria” con los prestadores de servicios de la sociedad de la información que actúen o tengan su infraestructura en Cataluña. En este punto, como señala el Letrado del Parlamento de Cataluña, la norma no atribuye a la Agencia potestades de intervención o regulación sobre el sector privado, sino funciones de tipo prestacional o de puesta a disposición de servicios en beneficio de los administrados, sin que, por lo demás, la demanda haya argumentado mínimamente en qué se vulnerarían o menoscabarían las competencias estatales en materia de seguridad pública.

Por tanto, el inciso “con relación a las personas físicas o jurídicas situadas en Cataluña” del art. 2.3 de la Ley 15/2017 es inconstitucional y nulo.

c) En el apartado 4 se deben examinar las letras b), e) y f).

i) La letra b) dispone que una de las funciones de la Agencia de Ciberseguridad es la siguiente: “b) Planificar, gestionar, coordinar y supervisar la ciberseguridad en Cataluña, estableciendo la capacidad preventiva y reactiva necesaria para paliar los efectos de los incidentes de ciberseguridad que afecten al territorio de Cataluña, así como las pruebas que puedan

organizarse en materia de ciberseguridad y continuidad. En el ámbito de la Administración de la Generalidad y su sector público, la Agencia debe ejercer estas funciones mediante la prestación de sus servicios, coordinando las actuaciones que requieran su apoyo con el Centro de Telecomunicaciones y Tecnologías de la Información”.

El Abogado de la Generalidad de Cataluña y el Letrado del Parlamento de Cataluña estiman que esta función forma parte de las necesarias medidas de protección que la legislación estatal exige a todas las Administraciones. Sin embargo, es posible apreciar que la función de este apartado b) trasciende, en su primer inciso, el ámbito estricto de la administración y su protección frente a ciberataques, ya que proyecta su ejercicio a la tarea de planificar, gestionar, coordinar y supervisar la ciberseguridad en Cataluña y no exclusivamente en relación a la Administración de la Generalidad y su sector público. Presupone así el diseño de un marco estratégico e institucional en esta materia que supera las competencias de la Generalidad en este ámbito, ya que no se refiere a la actuación de la administración y tampoco puede relacionarse con las competencias autonómicas derivadas de la creación de la policía de seguridad propia. Por el contrario, interfiere o menoscaba las competencias estatales en materia de seguridad pública, así como las del art. 149.1.21 CE en cuya virtud corresponde al Estado adoptar las previsiones necesarias para garantizar un tratamiento unitario de esta cuestión.

En consecuencia, el inciso “Planificar, gestionar, coordinar y supervisar la ciberseguridad en Cataluña, estableciendo la capacidad preventiva y reactiva necesaria para paliar los efectos de los incidentes de ciberseguridad que afecten al territorio de Cataluña, así como las pruebas que puedan organizarse en materia de ciberseguridad y continuidad” de la letra b) del apartado 4 del art. 2 de la Ley 15/2017 es inconstitucional y nulo.

El resto del precepto no infringe el orden constitucional de distribución de competencias. Por un lado, refiere dichas funciones al “ámbito de la Administración de la Generalidad y su sector público”. Por otro, la mención del precepto “al territorio de Cataluña” es una aplicación de lo previsto en el art. 115.1 del EAC, que circunscribe al ámbito de Cataluña el ejercicio de las competencias asumidas estatutariamente, competencias esta vez dirigidas a proteger y mejorar la seguridad de las redes y alertar ante la existencia de ciberamenazas relacionadas con la Administración de la Generalidad y sus sistemas de información y comunicaciones.

Por tanto, en el entendimiento de que las funciones de la Agencia a las que se alude en el primer inciso del precepto deben ser referidas exclusivamente a las actuaciones de la Administración de la Generalidad y su sector público en relación con la protección de sus sistemas de información y comunicación, este segundo inciso del art. 2.4.b) no es contrario al orden constitucional de delimitación de competencias.

ii) La función atribuida a la Agencia de Ciberseguridad por la letra e) tiene el siguiente tenor literal: “Actuar como apoyo, en materia de ciberseguridad, de cualquier autoridad competente para el ejercicio de sus funciones públicas y, en particular, en las tareas de lucha contra las conductas ilícitas, incluidas la intervención directa y la obtención de pruebas electrónicas. En la investigación y represión de ilícitos penales, la Agencia debe colaborar con los cuerpos policiales y las autoridades judiciales de acuerdo con lo establecido por la normativa vigente, previo requerimiento, actuando de forma coordinada, y preservando y poniendo a su disposición los elementos relevantes para la investigación y los que puedan constituir una prueba”.

La norma contiene un mandato de colaboración con el resto de autoridades con competencias en materia de ciberseguridad que no es sino concreción del principio general de cooperación que informa el Estado autonómico, así como del deber de colaborar con Jueces y Tribunales y con el Ministerio Fiscal que resulta del ordenamiento jurídico vigente. Más específicamente, acerca de la investigación y represión de ilícitos penales, que, evidentemente, no corresponden a la Agencia, el precepto no le atribuye una función directa en esas materias vinculadas a la seguridad pública. Su participación en las funciones propias de los cuerpos policiales y las autoridades judiciales, en particular en lo relativo a la “intervención directa y la obtención de pruebas electrónicas”, no se produce por iniciativa de la propia Agencia, sino que se condiciona a que haya sido requerida para hacerlo, así como que se actué de acuerdo con la normativa vigente. Su actuación en este ámbito es meramente auxiliar y requiere la solicitud expresa, bien de los cuerpos policiales, entre los que se encuentra la Policía de la Generalidad (art. 164.5 EAC), bien de las autoridades judiciales competentes, en los términos previstos en la legislación procesal.

Por tanto, el recurso debe desestimarse.

iii) La letra f) atribuye a la Agencia la función de “Investigar y analizar tecnológicamente los ciberincidentes y ciberataques sobre infraestructuras tecnológicas, sistemas de información, servicios de tecnologías de la información y la comunicación o la propia información en los que la Agencia intervenga por razón de su competencia”.

El Abogado del Estado alega que este precepto, en cuanto atribuye a la Agencia funciones de investigación de conductas que pudieran ser delictivas, vulnera las competencias estatales en materia de seguridad pública. El Abogado de la Generalidad de Cataluña sostiene, por el contrario, que se trata de una investigación tecnológica que no excluye otras que pudieran realizar otros órganos o entidades en el ejercicio de sus atribuciones. Por su parte, el Letrado del Parlamento de Cataluña defiende que el precepto ha de ser situado en el contexto de las funciones de apoyo y colaboración a que se refiere el apartado anterior.

La impugnación no puede ser estimada. Por un lado, el tenor literal del precepto circunscribe las labores de investigación y análisis de la Agencia a los aspectos tecnológicos de los ciberincidentes y ciberataques, lo que permite excluir cualquier interferencia en el plano de la detección, persecución e investigación de conductas ilícitas, funciones que corresponden a las Fuerzas y Cuerpos de Seguridad del Estado y también a la Policía de la Generalidad-Mossos d'Esquadra. Se trata de funciones dirigidas a prevenir y mitigar los efectos de los ciberataques, pues corresponde a la Generalidad la autoprotección de los servicios de su administración y de su sector público, para lo que ha de ejercer las funciones de análisis, investigación y respuesta necesarios para restablecer sus propios servicios y garantizar su seguridad. Por otro lado, esta función de investigación y análisis tecnológico que se encomienda a la Agencia solo se lleva a cabo respecto de los sistemas de información, servicios de tecnologías de la información y la comunicación "en los que la Agencia intervenga por razón de su competencia", esto es, los que acaban de mencionarse.

En conclusión, la función atribuida a la Agencia de Ciberseguridad de Cataluña por la letra f) del apartado 4 del art. 2 de la Ley 15/2017 no es inconstitucional.

d) Restan por enjuiciar las letras a), b) y d) del apartado 5, según las cuales son funciones de la Agencia de Ciberseguridad de Cataluña, específicamente referidas al ámbito del Gobierno y de la Administración de la Generalidad y su sector público dependiente las siguientes:

- “a) Impulsar y aprobar un marco de directrices y normas técnicas de seguridad de cumplimiento obligatorio para la Administración de la Generalidad y para los organismos y entidades vinculados o dependientes, para garantizar una protección eficaz, en particular ante el cibercrimen y los ciberataques. En el marco de las directrices y normas técnicas para la protección de los sistemas de información policiales, la Agencia debe coordinarse con el departamento competente en materia de policía y seguridad pública.
- b) Informar preceptivamente en los procedimientos de elaboración de disposiciones normativas tramitadas por la Administración de la Generalidad en materia de ciberseguridad y gobernanza de las tecnologías de la información y la comunicación.
- d) 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 Cataluña o que, en otro caso, ofrezcan servicios a la Administración de la Generalidad y a los organismos y entidades vinculados o dependientes.”

Los tres apartados impugnados se refieren a funciones circunscritas al “ámbito del Gobierno y de la Administración de la Generalidad y su sector público dependiente”. Así, conforme a su tenor literal, todas ellas han de entenderse vinculadas a las políticas de ciberseguridad de las redes y sistemas de información de la Generalidad que no han sido cuestionadas en el presente proceso. Se trata, por tanto, de funciones inherentes a las medidas de protección que resultan de la legislación en materia de Administración electrónica adoptadas al amparo de las competencias autonómicas de los arts. 150 y 159 EAC.

La demanda se refiere expresamente al apartado b) ya que considera contrario al orden competencial que se atribuya a la Agencia la función de informar preceptivamente las disposiciones normativas estatales sobre ciberseguridad. Sin embargo, el tenor literal del precepto desmiente dicha vulneración, ya que alude a “disposiciones normativas tramitadas por la Administración de la Generalidad”, lo que se concreta en disposiciones meramente organizativas en relación a sus propias funciones en materia de ciberseguridad (al respecto, STC 31/2010, FJ 61).

Consecuentemente, procede desestimar el recurso en este punto.

FALLO

En atención a todo lo expuesto, POR LA AUTORIDAD QUE LE CONFIERE LA CONSTITUCIÓN DE LA NACIÓN ESPAÑOLA,

Ha decidido

1) Estimar parcialmente el presente recurso de inconstitucionalidad y, en consecuencia, declarar que son inconstitucionales y nulos el apartado 1; el inciso “con relación a las personas físicas o jurídicas situadas en Cataluña” del apartado 3; el inciso “Planificar, gestionar, coordinar y supervisar la ciberseguridad en Cataluña, estableciendo la capacidad preventiva y reactiva necesaria para paliar los efectos de los incidentes de ciberseguridad que afecten al territorio de Cataluña, así como las pruebas que puedan organizarse en materia de ciberseguridad y continuidad” de la letra b) del apartado 4, todos ellos del art. 2 de la Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña.

2) Declarar que el art. 2.2 de la Ley 15/2017 no es contrario a la Constitución interpretado en los términos del fundamento jurídico 7.b.i) de la presente Sentencia.

3) Desestimar el recurso en todo lo demás.

Publíquese esta Sentencia en el “Boletín Oficial del Estado”.

Dada en Madrid, a veinte de diciembre de dos mil dieciocho.