AHOLKU BATZORDE JURIDIKOA
COMISIÓN JURÍDICA ASESORA
EUSKADI

SR. VICEPRESIDENTE PRIMERO Y CONSEJERO DE SEGURIDAD

El Pleno de la Comisión Jurídica Asesora de Euskadi, en la sesión del día 18 de mayo de 2023, con la asistencia de los miembros que al margen se expresan, ha examinado su **consulta**, registrada con el nº 88/2023, relativa al **anteproyecto de Ley de creación de la Agencia Vasca de Ciberseguridad** (**Ref.: DNCG_LEY_3728/22_02**).

Tras su deliberación, ha emitido por unanimidad el siguiente dictamen. Expresa el parecer de la Comisión el vocal Sr. Beitia Ruiz de Arbulo.

PRESIDENTE:
D. Sabino Torre Díez.

VICEPRESIDENTE:
D. Xabier Unanue Ortega.

VOCALES:
D.ª M.ª Teresa Astigarraga Goenaga.
D. Iñaki Beitia Ruiz de Arbulo.
D. Iñaki Calonge Crespo.
D.ª M.ª Jesús Urkiola Mendibil.
D.ª M.ª Lourdes Pérez Ovejero.
D.ª Mirari Erdaide Gabiola.
D.ª Jaione Juaristi Sánchez.

SECRETARIO:
D. Jesús M.ª Alonso Quilchano.

DICTAMEN N.º 85/2023

ANTECEDENTES

1. Por Orden de 4 de abril de 2023 del Vicelehendakari Primero y Consejero de Seguridad se solicita, de forma urgente, dictamen de la Comisión Jurídica Asesora de Euskadi acerca del anteproyecto de ley señalado en el encabezamiento, que tuvo entrada en esta Comisión ese mismo día.

2. Por Resolución de 5 de abril de 2023, el Presidente de la Comisión, de acuerdo con el artículo 26.3 de la Ley 9/2004, de 24 de noviembre, de la Comisión Jurídica Asesora de Euskadi (LCJA), estima la solicitud.

3. El expediente remitido comprende, además de la orden acordando la consulta, la siguiente documentación:

   a) Resolución de 11 de julio de 2022 de la Directora de Régimen Jurídico, Servicios y Procesos Electorales de apertura del plazo para la consulta previa.

   b) Orden de 3 de agosto de 2022 del Vicelehendakari Primero y Consejero de Seguridad por la que se acuerda el inicio del procedimiento para la elaboración del anteproyecto de ley.

   c) Memoria justificativa de 3 de agosto de 2022.

   d) Memoria económica de 3 de agosto de 2022.

   e) Informe justificativo de la ausencia de relevancia desde el punto de vista de género de 3 de agosto de 2022.

   f) Orden de 4 de agosto de 2022 del Vicelehendakari Primero y Consejero de Seguridad por la que se acuerda la aprobación previa del anteproyecto de ley.

   g) Informe de la Asesoría Jurídica de 16 de agosto de 2022.

h) Escrito de 16 de agosto de 2022 de la Directora de Servicios del Departamento de Trabajo y Empleo comunicando la no realización de observaciones.

i) Informe de organización de la Dirección de Atención a la Ciudadanía y Servicios Digitales de 17 de agosto de 2022.

j) Escrito de 18 de agosto de 2022 de la Dirección de Servicios del Departamento de Planificación Territorial, Vivienda y Transportes comunicando la no realización de observaciones.

k) Publicación en el BOPV de la Resolución de 4 de agosto de 2022, de la Directora de Régimen Jurídico, Servicios y Procesos Electorales, por la que se somete a información pública el anteproyecto de Ley de creación de la Agencia Vasca de Ciberseguridad.

l) Escrito de 30 de agosto de 2022 de la Directora de Servicios del Departamento de Cultura y Política Lingüística comunicando la no realización de observaciones.

m) Informe de la Dirección de Normalización Lingüística de las Administraciones Públicas de 2 de septiembre de 2022.

n) Escrito de 8 de septiembre de 2022 de la Directora de Servicios del Departamento de Igualdad, Justicia y Políticas Sociales comunicando la no realización de observaciones.

o) Informe de la Dirección de Tecnologías de la Información y la Comunicación de 8 de septiembre de 2022.

p) Alegaciones de la Diputación Foral de Álava de 14 de septiembre de 2022.

q) Alegaciones del Departamento de Salud de 15 de septiembre de 2022.

r) Alegaciones del Departamento de Gobernanza Pública y Autogobierno de 19 de septiembre de 2022.

s) Alegaciones de la Diputación Foral de Álava de 19 de septiembre de 2022.

t) Informe 12/2022, de 19 de septiembre, del Pleno de la Junta Asesora de Contratación Pública.

u) Alegaciones de la Diputación Foral de Bizkaia de 22 de septiembre de 2022.

v) Informe de la Dirección de Presupuestos de 23 de septiembre de 2022.

w) Dictamen de la Agencia Vasca de Protección de Datos de 26 de septiembre de 2022.

x) Escrito de 28 de septiembre de 2022 de la Dirección de Servicios del Departamento de Turismo, Comercio y Consumo comunicando la no realización de observaciones.

y) Informe de Emakunde de 4 de octubre de 2022.

z) Memoria sucinta de 8 de noviembre de 2022.

aa) Informe de la Comisión de Gobiernos Locales de Euskadi de 22 de noviembre de 2022.

bb) Memoria justificativa para la Oficina de Control Económico de 1 de diciembre de 2022.

cc) Informe de la Dirección de Patrimonio y Contratación de 13 de enero de 2023.

dd) Plan de actuación inicial relativo a la creación del ente público de derecho privado, Agencia Vasca Ciberseguridad–Euskadiko Zibersegurtasun Agentzia de 15 de marzo de 2023.

ee) Informe 3/2023, de 24 de marzo de 2023, de la Dirección de Función Pública.

ff) Informe del Consejero de Economía y Hacienda de 30 de marzo de 2023.

gg) Informe control económico-normativo de la Oficina de Control Económico de 30 de marzo de 2023.

hh) Informe de la Dirección de Función Pública de 30 de marzo de 2023 acerca de las previsiones de recursos humanos necesarios para el funcionamiento de la Agencia.

ii) Memoria sucinta de 4 de abril de 2023 para la Comisión Jurídica Asesora de Euskadi.

DESCRIPCIÓN DEL ANTEPROYECTO

4. El anteproyecto de ley sometido a nuestra consideración tiene por objeto la creación de la Agencia Vasca de Ciberseguridad-Euskadiko Zibersegurtasun Agentzia, como ente público de derecho privado del sector público de la Comunidad Autónoma de Euskadi, con personalidad jurídica propia, que ajusta su actividad al ordenamiento jurídico privado, con plena capacidad de obrar para el cumplimiento de sus fines y con autonomía orgánica y funcional, adscrita al departamento competente en materia de seguridad a través de la persona titular de la Viceconsejería de Seguridad.

5. Consta de una exposición de motivos, tres capítulos, en los que se encuadran trece artículos, una disposición adicional, una disposición transitoria y dos disposiciones finales.

6. La exposición de motivos alude al enorme desarrollo de las tecnologías de la información y la comunicación (TIC) y su conversión en elementos esenciales para el desarrollo económico y el progreso de la sociedad.

7. Pero se reseñan los riesgos que provoca un entorno hiperconectado y en constante evolución, por este motivo, la protección de las infraestructuras y servicios de comunicación frente a amenazas en el ámbito de la ciberseguridad se ha convertido en los últimos tiempos en un pilar básico para diferentes sectores y administraciones.

8. Por ello, sigue diciendo la exposición de motivos, la creación de un organismo público específico para impulsar la ciberseguridad puede constituir un importante instrumento técnico de apoyo a las actividades que desarrollan las diferentes administraciones públicas de la Comunidad Autónoma para proteger sus servicios, especialmente desde los organismos que prestan servicios informáticos al Gobierno Vasco, a las diputaciones forales y a las principales entidades locales. Asimismo, existen diferentes planes y acciones para apoyar al tejido empresarial y a la ciudadanía en su propia protección, llevados a cabo a través de los órganos que materializan el desarrollo y la promoción económica dentro de sus competencias, tanto a nivel de la Comunidad Autónoma Vasca como en los distintos territorios históricos.

9. Entre tales organismos constituye un referente el Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre o BCSC), que fue puesto en marcha por el Gobierno Vasco para promover la ciberseguridad en Euskadi, dinamizando la actividad económica relacionada con la aplicación de la ciberseguridad y fortalecer dicho sector. Desde 2017, el Centro Vasco de Ciberseguridad ha

venido promoviendo y desarrollando de manera exitosa una cultura de ciberseguridad en la sociedad vasca. El centro lidera y apoya iniciativas dirigidas a elevar el nivel de madurez y concienciación sobre la ciberseguridad en el País Vasco, a través de proyectos englobados en el ámbito de prevención y respuesta a incidentes de ciberseguridad (CERT, Computer Emergency Response Team) e iniciativas orientadas a la promoción del ecosistema vasco de ciberseguridad, en colaboración con el sector empresarial, y todo ello con la finalidad de atraer inversión y talento.

10. No obstante, el Centro Vasco de Ciberseguridad, por su forma jurídica, no puede ejercer las funciones ni prestar el servicio público de ciberseguridad en Euskadi. En este contexto surge la necesidad de desarrollar una iniciativa común en el sector público de Euskadi que articule y refuerce la coordinación de los recursos ya disponibles y permita elevar el nivel de madurez de ciberseguridad, así como la resiliencia en el conjunto de la Comunidad Autónoma Vasca.

11. Un organismo integrador y transversal de la ciberseguridad en Euskadi, continua la exposición de motivos, que proporcione seguridad y estabilidad a la sociedad frente a las amenazas derivadas del uso de Internet y las nuevas tecnologías, así como un punto único de relación con agentes externos. Y que responda a la imprescindible necesidad de coordinación entre las diferentes entidades competentes en materia de información y comunicaciones, así como con aquellos organismos responsables de los distintos ámbitos de la seguridad física y de las personas, en línea con la estrategia seguida en otros ámbitos competenciales como el estatal y con las iniciativas adoptadas en el ámbito europeo, fruto del interés y la consideración de la ciberseguridad como esencial a efectos de cumplir con los objetivos estratégicos de la Unión Europea.

12. Por este motivo, la finalidad de la presente ley es la creación de un ente público de derecho privado, la Agencia Vasca de Ciberseguridad-Euskadiko Zibersegurtasun Agentzia (en lo sucesivo, la Agencia), con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines. De este modo, se garantiza que el Gobierno Vasco disponga de las herramientas y recursos necesarios para afrontar las amenazas y riesgos en el ámbito de la ciberseguridad que se plantean en la actual sociedad de la información.

13. A continuación, se señala el fundamento competencial de la regulación y se explicita resumidamente el contenido de la ley.

14. El capítulo I ("Disposiciones generales") contempla la creación, naturaleza jurídica y régimen jurídico de la Agencia (artículo 1), su objeto y funciones (artículo 2).

15. El capítulo II ("Estructura orgánica") establece sus órganos de gobierno (artículo 3), diseña el Consejo de Administración (artículo 4), las funciones del Consejo de Administración (artículo 5), la Dirección General de la Agencia (artículo 6), el Consejo Consultivo (artículo 7), los recursos contra las resoluciones de los órganos de gobierno (artículo 8) y la atribución al Gobierno Vasco de la aprobación de sus estatutos mediante decreto (artículo 8).

16. El capítulo III ("Régimen de personal, económico-financiero, patrimonial y de contratación") regula el personal de la Agencia (artículo 10), el régimen económico-financiero y patrimonial (artículo 11), el régimen de contratación (artículo 12) y su posible extinción y disolución (artículo 13).

17. Finalmente, la disposición adicional se ocupa de la cesión a la Agencia por parte del ente público de derecho privado SPRI- Agencia Vasca de Desarrollo Empresarial, en cuanto responsable del Basque Cybersecurity Centre-Centro Vasco de Ciberseguridad, de los activos materiales y de personal y subrogación en los contratos y convenios.

18. La disposición transitoria prevé que el Basque Cybersecurity Centre-Centro Vasco de Ciberseguridad siga ejerciendo sus funciones hasta la constitución de la Agencia.

19. La disposición final primera establece que la fecha de puesta en marcha e inicio de las actividades de la Agencia será la que se establezca en el decreto que apruebe sus Estatutos, y en todo caso antes de un año desde la entrada en vigor de la presente ley.

20. Asimismo, contempla el caso de que el inicio de las actividades no coincida con la entrada en vigor de la correspondiente Ley de presupuestos.

21. La disposición final segunda autoriza al Gobierno para que realice las modificaciones presupuestarias y patrimoniales necesarias para traspasar a la Agencia los recursos a que se refiere la disposición adicional.

22. La disposición final segunda determina su entrada en vigor el día siguiente al de su publicación en el Boletín Oficial del País Vasco.

INTERVENCIÓN DE LA COMISIÓN

23. El presente dictamen tiene carácter preceptivo y se emite de conformidad con el artículo 3.1 de la Ley 9/2004, de 24 de noviembre, de la Comisión Jurídica Asesora de Euskadi, que incluye en su apartado a), dentro del ámbito de la

función consultiva de la Comisión, los "anteproyectos de Ley cualquiera que sea la materia y objeto de los mismos", sin que el que somete a consulta se encuentre incluido entre las excepciones de dicho apartado.

CONSIDERACIONES

I PROCEDIMIENTO DE ELABORACIÓN

24. Al iniciarse el procedimiento con posterioridad a la entrada en vigor de la Ley 6/2022, de 30 de junio, de procedimiento de elaboración de las disposiciones de carácter general (LPEDG), resulta de aplicación esta ley.

25. Es por tanto la LPEDG el parámetro de contraste para examinar el proceso de elaboración del texto sometido a dictamen.

26. Ahora bien, dicho análisis debe tener en cuenta dos aspectos que lo condicionan.

27. En primer lugar, un condicionante genérico, consustancial a este producto normativo, pues se trata de un anteproyecto de ley, por lo que es obligado recordar la radical diferencia entre el ejercicio de la iniciativa legislativa y la iniciativa reglamentaria del Gobierno, que se proyecta sobre los contornos que adquiere la intervención de la Comisión, expuestos por ejemplo en el Dictamen 116/2021 o en los recientes dictámenes 56 y 61/2023.

28. A modo de síntesis, salvo en los casos en que la Constitución (CE), el Estatuto de Autonomía (EAPV) o, en ocasiones, las leyes orgánicas prevean algún trámite específico excepcional —Sentencia del Tribunal Constitucional (STC) 35/ 1984, de 13 de marzo, o STC 176/2011, de 8 de noviembre—, la valoración del iter seguido para preparar en el ejecutivo los anteproyectos de ley difiere de la que corresponde en el caso de los reglamentos. Mientras en estos, por ejemplo, la falta de audiencia o de participación de intereses públicos y privados o la ausencia de informes preceptivos puede llegar a incidir en la validez del futuro producto normativo, con los anteproyectos de ley no sucede lo mismo ya que sólo en los indicados casos pueden ver comprometida su validez, junto a aquellos otros en los que la carencia afecte limitativamente a la formación de la voluntad parlamentaria (por todas, SSTC 108/1986, de 28 de julio, y 84/2015 , de 30 de abril).

29. Esta sustancial diferencia hace que el examen por la Comisión de los procedimientos de elaboración de los anteproyectos de ley se concrete esencialmente en contribuir al acierto de la regulación proyectada, esto es, a su racionalidad —entendida como utilidad para alcanzar los objetivos propuestos y

la corrección de la regulación en términos de adecuación a la realidad que se pretende normar—.

30. La precedente especificidad de la función consultiva en relación a los anteproyectos de ley no ha impedido, sin embargo, que con un ánimo de estricta colaboración con el órgano consultante la Comisión formule observaciones sobre el procedimiento de elaboración del anteproyecto y de la memoria que lo acompaña, en aras a su mejora. Pero siempre sin olvidar que la valoración del procedimiento de elaboración por el órgano consultivo no se adentra en el terreno de la validación jurídica del texto y no permite fundar objeciones a la constitucionalidad del producto normativo final.

31. En segundo lugar, un condicionante material, al ser característico del anteproyecto que nos ocupa su contenido organizativo, al tener por objeto la creación de un ente público de derecho privado, lo que también tiene una incidencia directa sobre su tramitación.

32. Tal naturaleza permitirá en ciertos aspectos modular los requerimientos y en otros acrecentarlos en la fase de elaboración del anteproyecto.

33. Con los criterios indicados iniciamos a continuación el examen del procedimiento que ha desembocado en el texto del anteproyecto de la Ley de creación de la Agencia Vasca de Ciberseguridad-Euskadiko Zibersegurtasun Agentzia.

34. El primer paso del itinerario procedimental es la **consulta pública,** cuya realización se acuerda por Resolución de 11 de julio de 2022 de la Directora de Régimen Jurídico, Servicios y Procesos Electorales.

35. Se abre el trámite para interactuar con la ciudadanía, de forma previa a la aprobación del texto jurídico normativo y con tal fin se plantean, de forma sucinta, los problemas que se quieren solucionar, la necesidad de la nueva norma, su oportunidad y los objetivos a conseguir, junto a las soluciones alternativas regulatorias o no regulatorias.

36. Mediante la inserción de la información en el Tablón de anuncios de la Sede Electrónica del Gobierno Vasco se invita a la ciudadanía y entidades que puedan verse afectadas potencialmente por el futuro marco legal a que se pronuncie sobre tales cuestiones.

37. El procedimiento de elaboración propiamente dicho se inicia mediante la Orden de 3 de agosto de 2022 del Vicelehendakari Primero y Consejero de Seguridad.

38. La **orden de iniciación** expresa sucintamente el objeto y finalidad de la norma, su viabilidad jurídica y material, la repercusión que tendrá en el ordenamiento jurídico, la incidencia económica y presupuestaria, y los trámites e informes que es preciso seguir antes de su aprobación y su sistema de redacción.

39. En principio, con ese contenido puede darse por debidamente cumplimentado lo dispuesto en el artículo 13 de la LPEDG, aunque no responde con exactitud a las exigencias establecidas por dicho artículo, que obliga a un examen preliminar bastante minucioso.

40. Consta una **memoria justificativa** del anteproyecto que analiza en primer lugar su objeto. A continuación, aborda la necesidad y oportunidad de la ley, la competencia, señalando la regulación y recursos de ámbito autonómico, la regulación y recursos de ámbito foral, la regulación y recursos de ámbito local y los precedentes jurisprudenciales. Después, se ocupa del rango normativo, del contenido de la regulación, la urgente necesidad de la creación y puesta en funcionamiento de la entidad y finaliza con la idoneidad de la naturaleza jurídica elegida para la Agencia.

41. En particular, la elección se fundamenta, partiendo de la previsión contenida en el artículo 43.2.c) de la Ley 3/2022, de 12 de mayo, del sector público vasco (LSPV), de la siguiente forma:

> En la medida en que, al nuevo ente, la Agencia Vasca de Ciberseguridad, se le van a otorgar potestades administrativas, la forma jurídica de la sociedad pública, la fundación y el consorcio se han descartado. Asimismo, y en la medida en que es poco frecuente que un organismo autónomo tenga por objeto la realización de actividades prestacionales o de mercado, las cuales se pretende igualmente que la futura Agencia ejerza, se ha escogido la forma jurídica de ente público de derecho privado.
>
> Los motivos de la elección se fundamentan, principalmente en la proximidad de esta figura con la de los organismos autónomos, que se configuran como el tipo de entidad que con mayor naturalidad puede ejercitar potestades administrativas o públicas (i.e. potestad de investigación en colaboración con la Ertzaintza, potestad de informar con carácter preceptivo en el seno de un procedimiento de elaboración de disposiciones normativas o reglamentarias, representación oficial de la CAE ante organismos estatales y regionales). Así, se ha optado por la figura del ente público de derecho privado, en la medida en que por su naturaleza jurídica puede ejercer potestades administrativas, y que

al mismo tiempo y a diferencia de los organismos autónomos, puede asumir con mayor asiduidad prestaciones de servicios que no necesariamente son de carácter público (i.e. prestaciones de servicios a la red empresarial vasca y a la ciudadanía).

De este modo el ente público de derecho privado se considera la forma jurídica idónea por las competencias, tanto públicas como privadas que asumirá, entre las cuales cabe destacar, a título de ejemplo, en el plano público: el impulso de estándares, directrices y normas técnicas de seguridad; la emisión de informe preceptivo en los procedimientos de elaboración de disposiciones normativas autonómicas en materia de ciberseguridad; la prevención y detección de incidentes de ciberseguridad en Euskadi, o la investigación y análisis tecnológico de los ciberincidentes y ciberataques, entre otras; y en el plano privado: el apoyo e impulso de la capacitación en materia de ciberseguridad y el desarrollo digital seguro en el ámbito empresarial.

42. Se redacta asimismo una **memoria económica**, en la que se expone la fundamentación del anteproyecto, la cuantificación de gastos e ingresos de explotación que ocasiona la creación de la Agencia, la cuantificación de inversiones y de recursos de capital que origina la creación de la Agencia, la financiación, la estructura orgánica y de personal, un resumen de explotación y capital y de rendimiento de servicios prestados, la identificación de aspectos que incidan o repercutan en materias propias de la hacienda general del País Vasco, descripción del programa económico-presupuestario en el que se inserta la disposición propuesta, y la incidencia económico-presupuestaria en la Administración, en otras administraciones públicas vascas y en la ciudadanía o en la empresa privada. Se adjunta como anexo I un Presupuesto de explotación.

43. Dados los servicios planteados para la puesta en marcha de la Agencia se establece una financiación anual de 8.500.000 euros, estableciéndose un presupuesto para 2023 de 5.378.435 euros. Considerando las necesidades de la Comunidad Autónoma de Euskadi y otras referencias existentes, se considera que el presupuesto podría ascender hasta los 12.000.000 euros anuales en una fase de madurez en la prestación del servicio. El presupuesto de 5.378.435 euros para el año 2023 se ha estimado considerando una incorporación paulatina del personal y equipos y los servicios a prestar. Los gastos de adecuación de la nueva sede del Parque Tecnológico de Miñano corresponderán al legado cedido por el Centro Vasco de Ciberseguridad, por lo que serán asumidos desde el Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente. Los

gastos correspondientes al uso de la sede actual serán asumidos por parte del presupuesto ordinario de la Agencia. En cuanto a las necesidades de personal, además del alto cargo para la Dirección General, se estima en unas 39 personas que deberán ser integradas de manera progresiva. En el despliegue inicial se dispondrá de 28 personas y una adicional con consideración de alto cargo. Los costes para 2023 del personal ascenderán a 2.199.995 euros.

44. En informe de 3 de agosto de 2022 se justifica que la naturaleza organizativa del anteproyecto y la ausencia de relevancia desde el punto de vista de género sobre la situación de mujeres y hombres permite eludir la exigencia de la elaboración del **informe de impacto en función del género** —regulado por los artículos 19 y 20 de la Ley 4/2005, de 18 de febrero, para la igualdad de mujeres y hombres y vidas libres de violencia machista contra las mujeres —, a tenor de las Directrices aprobadas por el Gobierno y publicadas mediante Resolución 40/2012, de 21 de agosto, de la Directora de la Secretaría del Gobierno y Relaciones con el Parlamento. Emakunde, por su parte, ha verificado que está exento del informe de impacto en función del género.

45. A continuación, el anteproyecto fue objeto de la **orden de aprobación inicial**, en sus dos versiones, castellano y euskera, conforme a las previsiones de la LPEDG, en concreto de su artículo 15. Según se explicita, posteriormente el anteproyecto se remite al Parlamento Vasco, en virtud de lo establecido en el apartado 1 del artículo 56 de la Ley 7/1981, de 30 de junio, de Gobierno, tras la modificación introducida por la Ley 8/2016, de 2 de junio, y la orden de aprobación previa, junto con el proyecto normativo, se hacen públicos en el espacio colaborativo Legesarea, así como en Legegunea.

46. Ahora bien, no se acompaña a la referida orden la **memoria de análisis de impacto normativo** que, según el artículo 15.3 de la LPEDG, debe contener los siguientes apartados:

> a) Oportunidad de la propuesta y alternativas de regulación estudiadas, lo que deberá incluir una justificación de la necesidad de la nueva norma frente a la alternativa de no aprobar ninguna regulación.
>
> b) Contenido y análisis jurídico, con referencia al derecho comparado y al de la Unión Europea, que incluirá el listado pormenorizado de las normas que quedarán derogadas como consecuencia de la entrada en vigor de la norma.
>
> c) Análisis sobre la adecuación de la norma propuesta al orden de distribución de competencias.

d) Impacto económico y presupuestario, que evaluará las consecuencias de su aplicación sobre los sectores, colectivos o agentes afectados por la norma, incluido el efecto sobre la competencia y la competitividad y su encaje con la legislación vigente en cada momento sobre estas materias.

e) Las cargas administrativas que conlleva la propuesta y el coste de su cumplimiento para la Administración y para los obligados a soportarlas, con especial referencia al impacto sobre las pequeñas y medianas empresas.

f) Informe sobre el impacto en función del género, en el que se ha de hacer constar una explicación detallada de los trámites llevados a cabo, de sus resultados con relación al cumplimiento de los preceptos de la Ley 4/2005 y de las medidas incorporadas para promover la igualdad.

g) Informe que analice la perspectiva de normalización del uso del euskera en el procedimiento de elaboración de disposiciones de carácter general, en el que se emitirá un pronunciamiento respecto a la adecuación a la normativa vigente en materia lingüística, sin perjuicio de las funciones que puedan corresponder a otros órganos informantes, y se propondrán medidas dirigidas a la normalización del uso del euskera en el ámbito objetivo de la disposición que se tramite.

h) Evaluación de impacto sobre la infancia y la adolescencia, en la que se haga constar una explicación detallada de los trámites llevados a cabo y su impacto previsto sobre la infancia y la adolescencia, que permita medir y contrastar el cumplimiento del principio del interés superior de la infancia.

i) Una descripción de la tramitación, con referencia a los informes o dictámenes preceptivos o facultativos evacuados y a los resúmenes de las principales aportaciones recibidas en el trámite de consulta previa a la ciudadanía, con carácter previo a la elaboración del texto, y de las recibidas en los trámites de audiencia, información pública y negociación colectiva. En todo caso, dicha descripción contendrá el resultado y el reflejo de aquellos en el texto del proyecto, así como, en su caso, las razones por las que se prescindió de aquellos o la justificación de la reducción de los plazos mínimos previstos.

j) Evaluación de impacto sobre la juventud, en la que se haga constar una explicación detallada de los trámites llevados a cabo y su impacto previsto sobre

la juventud, que permita medir y contrastar el cumplimiento del impulso y la transversalización de la política integral de juventud, en relación con proteger y facilitar el ejercicio por parte de las personas jóvenes de sus derechos, cualquiera que sea su naturaleza o condición; fomentar su participación activa en el desarrollo político, social, económico, sostenible y cultural de la sociedad; y generar las condiciones que posibiliten su autonomía y emancipación, como culminación de un proceso continuo iniciado en la infancia.

k) Un análisis de la accesibilidad tanto de los instrumentos técnicos que contemple la normativa como de la implementación de la propia norma en aquellos aspectos que tengan una especial incidencia sobre el derecho a la accesibilidad universal de la ciudadanía, tomando en especial consideración los elementos que plantea la Ley 20/1997, de 4 de diciembre, para la Promoción de la Accesibilidad, así como el resto de la normativa que emana de aquella.

l) Evaluación de otros impactos que pudieran ser relevantes, prestando especial atención al impacto de carácter ambiental y sus efectos para la mitigación del cambio climático y al impacto social, así como un análisis sobre el coste-beneficio, que recoja todos aquellos aspectos directos e indirectos que justifican la aprobación del proyecto.

m) Previsión de su evaluación ex post, indicando la sistemática que se va a utilizar en la evaluación de los resultados de la aplicación de la norma y la entidad u órgano que se considera idóneo para llevarla a cabo.

47. La LPEDG requiere que tales valoraciones se formulen conjuntamente. Ahora bien, si se cumplimentan en diversos documentos, previos o posteriores, en los que se estudian los temas relevantes a los que alude dicho precepto, cabe concluir que tal omisión no resulta relevante.

48. En este caso, a la vista del contenido del anteproyecto, organizativo y enfocado a una cuestión puramente técnica, puede soslayarse una memoria de análisis de impacto normativo que cubra los aspectos relacionados en las letras e), g), h), j), k) y l), al tener un efecto nulo o inapreciable.

49. Por el contrario, existe un estudio suficiente de los demás impactos, aunque lo sean en la memoria justificativa y en la memoria económica, obrando también en el expediente el informe jurídico específico al que alude el artículo 15.4 de la LPEDG.

50. Respecto a este **informe jurídico**, tras recoger los antecedentes y formular unas consideraciones específicas sobre la falta de inclusión del anteproyecto en el plan normativo anual del Gobierno Vasco aprobado para el año 2022, sin que ello tenga efecto invalidante, si bien exige la correspondiente justificación, a tenor del artículo 8.4 de la LPEDG, refiere el marco normativo en el ámbito europeo, estatal y autonómico, así como el fundamento objetivo del anteproyecto. Sobre el contenido del anteproyecto, analiza la competencia, el rango de la norma, el contenido del anteproyecto y su adecuación a la ley y al derecho, formulando una serie de observaciones a su articulado. Concluye su enjuiciamiento con la tramitación y la técnica legislativa.

51. Contiene un apartado dedicado al impacto en la empresa con el que se da cumplimiento al artículo 6 de la Ley 16/2012, de 28 de junio, de apoyo a las personas emprendedoras y a la pequeña empresa del País Vasco.

52. La Dirección de Atención a la Ciudadanía y Servicios Digitales ha emitido el **informe de organización** previsto en el artículo 12.1.d) del Decreto 8/2021, de 19 de enero, por el que se establece la estructura orgánica y funcional del Departamento de Gobernanza Pública y Autogobierno. Cabe destacar del mismo que no se aconseja la inclusión de un informe preceptivo en los procedimientos de elaboración de disposiciones normativas y que comparte los motivos para la elección de la personalidad jurídica de la Agencia señalados en la memoria justificativa.

> En efecto, la personalidad jurídica de "ente público de derecho privado" dota a la Agencia de capacidad para ejercer potestades administrativas (como el impulso de estándares, directrices y normas técnicas de seguridad; la emisión de informe preceptivo en los procedimientos de elaboración de disposiciones normativas autonómicas en materia de ciberseguridad; la prevención y detección de incidentes de ciberseguridad en Euskadi; o la investigación y análisis tecnológico de los ciberincidentes y ciberataques, entre otras) y asumir, también, prestaciones de servicios de carácter privado (como, por ejemplo, el apoyo e impulso de la capacitación en materia de ciberseguridad y el desarrollo digital seguro en el ámbito empresarial)".
>
> Las funciones asignadas a la Agencia se consideran adecuadas para la consecución de los fines.

53. Ha informado igualmente la **Dirección de Normalización Lingüística de las Administraciones Públicas**, al amparo del Decreto 233/2012, de 6 de

noviembre, por el que se establece el régimen de inclusión de la perspectiva de normalización del uso del euskera en el procedimiento de elaboración de disposiciones de carácter general, desde la doble perspectiva del cumplimiento de la normativa lingüística y de su incidencia en la normalización del uso del euskera.

54. Así como la **Junta Asesora de Contratación Pública** a la luz de las competencias atribuidas por el artículo 27. 1 a) del Decreto 116/2016, de 27 de julio, sobre el régimen de la contratación del sector público de la Comunidad Autónoma de Euskadi. En su Informe 12/2022, de 19 de septiembre, la junta recomienda que se realice una mención específica expresa sobre la aplicabilidad a la Agencia de la legislación en materia de contratación pública, así como su normativa de desarrollo. En el presente caso, la legislación aplicable es la Ley 9/2017, de 8 de noviembre, de contratos del sector público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (LCSP).

55. Se refiere asimismo a la calificación de la Agencia como medio propio, con la que se quiere cumplir con lo dispuesto en el artículo 32.2 de la LCSP y en la sección 1ª del título IV del Decreto 116/2016. Al respecto, tras consultar el Registro de Contratos (REVSCON) de la Plataforma de Contratación Pública en Euskadi y comprobar que hasta la fecha no ha existido relación contractual alguna entre el Basque Cybersecurity Centre-Centro Vasco de Ciberseguridad y poderes adjudicadores, al carecer este de personalidad jurídica, se plantea "hasta qué punto tiene sentido considerar como medio propio al ente de nueva creación Agencia Vasca de Ciberseguridad, sabiendo que dicha Entidad actuará, como ha venido haciendo hasta la fecha su 'antecesora', en el cumplimiento de sus funciones y no bajo una relación contractual".

56. Sobre la disposición adicional primera, relativa a la "Cesión a la Agencia de los activos materiales y de personal y subrogación en los contratos y convenios", recuerda que la SPRI es la actual responsable del Centro Vasco de Ciberseguridad y considera que, no solo debe procederse a la cesión de los activos materiales y de personal, sino que también procede la subrogación en los contratos y convenios suscritos, de manera que "se recomienda buscar alguna vía o mecanismo para garantizar su continuidad".

57. La **Dirección de Presupuestos** sugiere reformular el párrafo segundo de la disposición final primera y, en cuanto a la repercusión presupuestaria en el 2023 y ejercicios futuros, considera que los costes económicos derivados de su aplicación deberán ser asumidos anualmente con las dotaciones económicas que tenga asignadas en los presupuestos la Agencia Vasca de Ciberseguridad,

las cuales se ajustarán anualmente a las directrices económicas que apruebe el Gobierno.

58. Añade a su vez que:

> En cuanto a lo que se refiere al ejercicio 2023, se consignará en el presupuesto inicial del Departamento de Seguridad o, en su defecto, se procederá a la realización de las modificaciones presupuestarias oportunas a lo largo de dicho ejercicio a dicho Departamento, para dotar del crédito necesario a la partida o partidas destinadas a transferir los fondos que precise la Agencia una vez que se constituya e inicie las actividades. En todo caso, parte de dicho crédito ya está incluido en las dotaciones correspondientes del actual Centro Vasco de Ciberseguridad, dentro de la SPRI, adscrita al Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente, que para el año 2022 asciende a 2.224.759,43 euros.
>
> Lo mismo cabe decir respecto a las dotaciones de personal, parte de los cuales provendrán del actual Centro Vasco de Ciberseguridad.
>
> Por último, señalar que esta Dirección de Presupuestos no estima necesaria, en principio, la creación de un nuevo programa presupuestario en el Departamento de Seguridad, en el cuál únicamente se incluirían la partida o partidas destinadas a transferir fondos a la Agencia Vasca de Ciberseguridad.

59. Desde la perspectiva del contenido de la futura norma se ha recabado informe de la **Dirección de Tecnologías de la Información y la Comunicació**n, del Departamento de Gobernanza Pública y Autogobierno, que suscribe la conveniencia y oportunidad del anteproyecto y formula una serie de sugerencias.

60. También el informe de la **Agencia Vasca de Protección de Dato**s, que formula una serie de consideraciones acerca de su intervención y relativas al articulado, con mención de las obligaciones establecidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. Se estima esencial su participación en el órgano consultivo.

61. Los demás departamentos de la Administración General no han formulado observaciones, salvo en el caso del **Departamento de Salud**, que solicita se den a conocer las razones por las que se incluyen en el Consejo Consultivo a representantes de los departamentos de Educación y de Salud, y del **Departamento de Gobernanza Pública y Autogobierno**, que cuestiona determinadas referencias competenciales de la exposición de motivos, sugiere una mención a las funciones y áreas de actuación contenidas en el Decreto 18/2020, de 6 de septiembre, del Lehendakari, de creación, supresión y modificación de los Departamentos de la Administración de la Comunidad Autónoma del País Vasco y de determinación de funciones y áreas de actuación de los mismos, y propone un reajuste en la composición del Consejo de Administración a la vista de las competencias que ostentan el Departamento de Seguridad y el Departamento de Gobernanza Pública y Autogobierno, y que la composición del Consejo Consultivo se determine en los Estatutos de la Agencia.

62. La participación y consulta a otras administraciones prevista por el artículo 18 de la LPEDG se ha materializado con la remisión del anteproyecto a las instituciones forales y a la Asociación de Municipios Vascos-Euskadiko Udalen Elkartea (EUDEL). Han formulado consideraciones dos diputaciones.

63. La **Diputación Foral de Álava**, en escritos de 14 y 19 de septiembre de 2022. En el primero solicita la incorporación al Consejo Consultivo de tres representantes de las sociedades públicas de servicios informáticos de las diputaciones forales; en el segundo, remite una sugerencia técnica sobre la delimitación del ámbito de la ley.

64. La **Diputación Foral de Bizkaia**, en escrito de 22 de septiembre de 2022, ha formulado diecisiete alegaciones, distinguiendo si son de adición, de reconsideración/corrección, y de adición y reconsideración, así como los artículos o disposiciones afectados por la alegación, y su texto correspondiente.

65. De forma resumida, además de propuestas de mejora técnica, fundamentalmente sugiere tener en cuenta que en el ámbito del sector público es de aplicación el Real Decreto 311/2022, de 3 de mayo, por el que se aprueba el Esquema Nacional de Seguridad (ENS), y solicita una aclaración sobre el encaje que tendrá este nuevo marco impulsado por la Agencia respecto al marco normativo y técnico vigente, en particular, ENS y las Guías y herramientas aprobadas y publicadas por el CCN-CERT, en materias como evaluaciones, rol a desempeñar en las funciones de prevención y detección, recogida de datos, notificación de incidentes, coordinación de los equipos de respuesta a incidentes de ciberseguridad (CSIRT) y equipos de respuesta a emergencias (CERT).

También se plantea si existe un engarce entre la estrategia de seguridad y los planes de seguridad de las entidades forales y locales y si estos son obligatorios. Se propone delimitar el alcance de los conceptos de coordinación y colaboración, el significado de lo que supone la representación oficial de la Comunidad Autónoma, el alcance funcional y organizativo de los conceptos prevención y detección, así como la puesta a disposición de servicios materiales y técnicos.

66. Desde el punto de vista organizativo, se propone en la composición del Consejo de Administración, sustituir la mención a los "Tres vocales provenientes de cada una de las sociedades públicas de servicios informáticos de las Diputaciones Forales. Todos o todas ellas, con rango de presidente o presidenta del Consejo de Administración de dichas sociedades públicas" por "Tres vocales provenientes de cada uno de los Territorios Históricos a nombrar [por] el Consejo de Gobierno de las Diputaciones Forales", e incluir en la representación municipal un vocal adicional proveniente de la Fundación BiscayTIK, ya que presta servicios informáticos a los entes locales del Territorio Histórico de Bizkaia. Reconsiderar la inclusión en el citado Consejo de Administración como vocal de la Dirección General de la Agencia, teniendo en cuenta que el Consejo de Administración es un órgano con funciones, entre otras, de asistencia, dación en cuenta y control de asuntos a la dirección. Completar la referencia al secretario o secretaria, con indicación del perfil o puesto de entre los que designará el Consejo de Administración. Así como la inclusión en el Consejo Consultivo de un representante de cada diputación foral experto en el ámbito de la ciberseguridad, a determinar por cada una de ellas.

67. En aplicación del artículo 17 de la LPEDG se ha descartado la realización del trámite de audiencia, pero no el de **información pública**, con la publicación en el Boletín Oficial del País Vasco (BOPV) de la Resolución de 4 de agosto de 2022, de la Directora de Régimen Jurídico, Servicios y Procesos Electorales, lo cual estaría justificado por la afección general que tiene la norma sobre el conjunto de la ciudadanía y no existir unos destinatarios directos, sin que conste que haya habido ninguna aportación.

68. Como consecuencia de la tramitación seguida hasta ese momento y a la vista de las alegaciones formuladas por los distintos intervinientes, se ha redactado una memoria del procedimiento de fecha 8 de noviembre de 2022.

69. En ella se recogen las observaciones y las modificaciones introducidas en el texto del anteproyecto, con expresión de las razones por las que algunas han sido estimadas y otras rechazadas.

70. El informe preceptivo de la **Comisión de Gobiernos Locales** de Euskadi (CGLE) de 30 de noviembre de 2022, previsto en el artículo 90.1 de la Ley 2/2016, de 7 de abril, de instituciones locales de Euskadi, y al que alude el artículo 21 de la LPEDG, constituye el siguiente hito procedimental. La CGLE, tras examinar la iniciativa, formula las siguientes conclusiones:

> El Anteproyecto de Ley no produce merma o vulneración en la autonomía de los entes locales vascos. En el ordenamiento jurídico no se atribuyen competencias y funciones específicas a los entes locales en materia de ciberseguridad.
>
> La seguridad en las redes informáticas es un ámbito de actuación novedoso que se integra en la noción general de «seguridad pública» cuya coordinación es competencia exclusiva de la Comunidad Autónoma. La Agencia Vasca de Ciberseguridad, aunque adscrita al Gobierno Vasco, sirve a todas las Administraciones del sector público vasco.
>
> El Anteproyecto prevé la participación de los municipios en el Consejo de Administración de la Agencia a través de vocales representantes de las entidades u organizaciones municipales de servicios informáticos de las tres capitales de territorio histórico de la CAE y de EUDEL.
>
> En términos generales, se considera positiva la creación de una entidad de referencia especializada en ciberseguridad en el sector público vasco.

71. Habiéndose recabado informe de la **Dirección de Patrimonio y Contratació**n, dicha dirección lo emite el 1 de enero de 2023, analizando la adecuación de diversos preceptos recogidos en el anteproyecto al régimen jurídico contenido en el Texto refundido de la Ley del patrimonio de Euskadi (TRLPE), aprobado por el Decreto Legislativo 2/2007, de 6 de noviembre. Por los motivos que reseña, se propone matizar la redacción del apartado h) del artículo 5 del anteproyecto, ajustar la redacción del artículo 11.3 del anteproyecto, así como la del artículo 11.4.d), para que resulten acordes con el TRLPE, y modificar la redacción del artículo 11.a) para dar cabida a los bienes adscritos al ente. En cuanto a la disposición adicional, se menciona la necesidad de suprimir la referencia global e indeterminada a "los activos materiales" del cedente, por una redacción en la que se diferencie entre los bienes y derechos del artículo 6.1 y los bienes y derechos del artículo 6.2 del TRLPE al objeto de concretar que solo estos últimos podrán ser cedidos a la Agencia Vasca de Ciberseguridad, y añadir respecto a la subrogación en los contratos y convenios suscritos por el Centro Vasco de

Ciberseguridad que se llevará a cabo *"*de acuerdo con lo establecido en la normativa de contratación pública".

72. El 3 de marzo de 2023 se aprueba el **Plan de Actuación Inicial** (PAI) para dar cumplimiento a lo dispuesto en el artículo 43.3 de la LSPV, que establece la necesidad de elaborar un plan de actuación inicial en el marco del procedimiento para la creación y constitución de entidades distintas de la Administración General de la Comunidad Autónoma de Euskadi.

73. Cabe recordar que, como requerimientos específicos en el procedimiento de tramitación de un proyecto de ley para la constitución de un ente público de derecho privado, como es el caso, el artículo 43.2 de la LSPV dispone que será imprescindible acreditar: "a) La necesidad de constituir un nuevo ente para el cumplimiento de las finalidades públicas pretendidas; b) La adecuación del nuevo ente desde la perspectiva de la organización institucional del conjunto del sector público de la Comunidad Autónoma de Euskadi, garantizando la inexistencia de reiteraciones orgánicas o funcionales así como, en su caso, la adopción de las medidas de reestructuración y extinción de entidades preexistentes; c) La idoneidad de la forma de personificación jurídica elegida de entre la tipología establecida en esta ley, a la luz de las funciones o actividad que vaya a desarrollar la nueva entidad y de conformidad con los criterios establecidos en esta ley para cada una de ellas; d) El procedimiento y las técnicas de control que ejecutará la Administración General de la Comunidad Autónoma de Euskadi sobre la nueva entidad; y e) La viabilidad económico financiera de la nueva entidad".

74. Debe ponerse esta última exigencia en relación con el contenido del artículo 43.3 de la LSPV relativo al PAI que ha de redactarse obligatoriamente.

75. Consta el PAI elaborado por la Viceconsejería de Seguridad el 15 de marzo de 2023, en el que se incluyen, tras una introducción, una declaración expresa del objeto o la finalidad del ente, una memoria acreditativa de la conveniencia y oportunidad de su creación, la forma jurídico-organizativa propuesta, la estructura organizativa propuesta, fundamentación de la estructura organizativa elegida, el plan estratégico, las previsiones sobre los recursos humanos necesarios, las previsiones sobre recursos de tecnologías de la información, el estudio económico-financiero, con un anexo I sobre el presupuesto de explotación para el año 2023 y una previsión para los cuatro años siguientes y un anexo II que contiene un extracto de reflexión de la ciberseguridad como servicio público de Euskadi.

76. Con fecha 24 de marzo de 2023 emite informe la **Dirección de Función Pública** en virtud de lo dispuesto en el artículo 18.2 a) de la Ley 11/ 2022, de 1 de diciembre, de empleo público vasco —en relación con el artículo 7.1.e) del

Decreto 18/2020, de 6 de septiembre, del Lehendakari, de creación, supresión y modificación de los Departamentos de la Administración de la Comunidad Autónoma del País Vasco y de determinación de funciones y áreas de actuación de los mismos, y el artículo 18 del Decreto 8/2021, de 19 de enero, por el que se establece la estructura y funciones del Departamento de Gobernanza Pública y Autogobierno—.

77. Sus conclusiones son las siguientes:

> 1. Habría que analizar qué puestos de trabajo deberían reservarse a personal funcionario, por ejercitar funciones públicas. El personal que ocuparía estos puestos sería personal funcionario de la Administración General de la CAE.
>
> 2. El régimen jurídico del personal funcionario será el que corresponda al personal funcionario de la Administración General de la CAE. En concreto, el acceso al empleo público, los requisitos y las características de las pruebas de selección, así como la convocatoria, gestión y resolución de los procedimientos de provisión de puestos de trabajo y promoción profesional son competencia del Departamento competente en empleo público, en la actualidad el Departamento de Gobernanza Pública y Autogobierno.
>
> 3. La persona titular de la dirección general de la Agencia será alto cargo y se le aplicará el régimen jurídico del personal alto cargo.
>
> 4. El personal cedido por SPRI mantiene los derechos y las obligaciones laborales que haya consolidado y adquirido. No obstante, este personal no tendrá la condición de personal empleado público de la Administración de la CAE.

78. Dicho informe se completa con otro emitido el 30 de marzo de 2023, que hace suyo la Consejera de Gobernanza Pública y Autogobierno, ya que el artículo 43.3.f) de la LSPV alude al informe vinculante de la persona titular de la consejería competente en materia de función pública, acerca de las previsiones sobre los recursos humanos necesarios para el funcionamiento del ente contenida en el PAI.

79. La conclusión es favorable:

> Sin entrar a valorar la conveniencia o no de la creación de un ente público de derecho privado y su adscripción al departamento de Seguridad, y como por otro lado la ley exige una previsión de plantilla global y a largo plazo, de entrada

cabe señalar que llama la atención la necesidad de una estructura tan amplia y con tantos puestos de responsabilidad. Ahora bien, como su puesta en marcha se va a llevar a cabo únicamente con 10 puestos y pretenden incorporar los puestos estructurales del BCC se considera procedente, ya que sólo deberían crearse inicialmente 4 nuevos puestos: - Director/a general (Alto cargo) - Secretaria/o alto cargo - Jefe/a área respuesta a incidentes críticos, y – Secretaria.

Por lo tanto, una vez puesta la Agencia en funcionamiento, se irá analizando la procedencia de continuar con los incrementos de plantilla previstos en cada momento.

80. Además, a tenor del artículo 43.4 de la LSPV el plan de actuación inicial y el estudio económico-financiero han de contar con el informe preceptivo de la persona titular de la consejería competente en materia de hacienda y presupuestos, que puede solicitar los informes adicionales que considere oportunos.

81. A tal fin, el **Consejero de Economía y Hacienda** emite su informe el 30 de marzo de 2023, expresando que el plan de actuación se ajusta al contenido mínimo que dispone el artículo 43.3 de la LSPV, sin perjuicio del control económico normativo que corresponde realizar a la Oficina de Control Económico (OCE). En relación al estudio económico-financiero, a la vista de la previsión presupuestaria que se adjunta, hasta el año 2027, que se inicia con un presupuesto de gastos para 2023 de 1.488.471 euros —estimando la entrada en funcionamiento del nuevo ente para el último trimestre del ejercicio—, para 2024 de 8.480.172 euros, con un incremento anual paulatino hasta alcanzar los 11.979.198 euros en 2027, una vez desplegado en su totalidad el servicio público de ciberseguridad, con un impacto presupuestario próximo a los 12.000.000 de euros anuales —de los que habría que descontar el coste económico actual del Centro Vasco de Ciberseguridad para determinar el incremento neto de coste— y dado que los ingresos de la entidad tienen su origen en transferencias de la Administración General, deberán preverse las dotaciones oportunas destinadas a financiar su actividad en los futuros presupuestos de la Administración General.

82. La **Oficina de Control Económico** (**OCE)** ha emitido su informe ejerciendo el control económico-normativo previsto, con carácter preceptivo, previsto en el Texto refundido de la Ley de control económico y contabilidad de la Comunidad Autónoma de Euskadi, aprobado por el Decreto Legislativo 2/2017, de 19 de octubre.

83. La OCE analiza en primer lugar el procedimiento y la tramitación seguida, concluyendo que se han cumplimentado, con carácter general, los requisitos que, para la elaboración de las disposiciones de carácter general, exige la LPEDG, así como las exigencias establecidas en la LSPV para la creación de entes públicos de derecho privado (artículos 6.4, 43 y 44). No obstante, se menciona que no se ha dado cumplimiento a lo previsto en el artículo 43.1 de la LSPV, conforme al cual, el anteproyecto debería haber sido promovido como de tramitación conjunta entre el departamento de Seguridad y el de Economía y Hacienda.

84. En segundo lugar, la incidencia organizativa, haciendo hincapié en los principios enunciados por el artículo 6 de la LSPV y las características que reúnen los entes públicos de derecho privado a tenor del artículo 39 de la LSPV, realizándose la siguiente valoración a partir de la justificación incluida en la memoria:

> Por tanto, como argumento fundamental para sostener la opción de crear un EPdDP, se alega la intención de que la nueva entidad desempeñe funciones tanto de carácter público como privado, mencionando expresamente en la Memoria la prestación de servicios a la red empresarial vasca y a la ciudadanía, como una de las funciones que se ejercerán conforme al derecho privado.
>
> Sin embargo, de la relación de funciones que se le atribuye en el artículo 2 del anteproyecto de ley, la gran mayoría tienen naturaleza pública incluyendo la descrita en la letra q) que es una actuación propia del ejercicio de la potestad administrativa pública subvencional. Es precisamente la sujeción al derecho privado de su funcionamiento ordinario el que habría de tenerse en cuenta para decantarse por la opción de crear un EPDP, que ha de ser, según la Ley 3/2022, elegido subsidiariamente respecto del organismo autónomo. La realización de "actividades prestacionales o de mercado" que se menciona en el expediente, así como aquellas actuaciones propiamente empresariales a las que poder aplicar criterios de gestión empresarial, como funciones a desempeñar por la Agencia, deberán contemplarse con claridad en el listado funcional del artículo 2.

85. En cuanto al análisis del articulado, la OCE formula una serie de observaciones acerca del artículo 1.1, artículo 1.2, artículo 1.4, artículo 7, artículo 10, artículo 11.5 y artículo 13.

86. En relación con la incidencia económico-presupuestaria, la OCE constata que el plan económico-financiero que realiza una estimación del coste de

funcionamiento de la Agencia para el primer quinquenio de su existencia, coste que se desglosa en gastos globales de personal y gastos globales de funcionamiento, prevé como único ingreso previsto para la financiación de los gastos estimados las transferencias y subvenciones para operaciones corrientes de la Administración General, sin que se prevean ingresos propios por prestación de servicios o realización de actividad. Asimismo, no se realiza estimación alguna de las inversiones a realizar en cada ejercicio presupuestario ni, en consecuencia, sus fuentes de financiación. Se afirma que no serán necesarias inversiones específicas en el inicio de actividad de la Agencia dada la previsión de la disposición adicional de la norma, de subrogación de la Agencia en los contratos y convenios vigentes a la fecha de su entrada en vigor, en el ámbito de la SPRI y concernientes al BCSC. Ello no obstante, en los ejercicios presupuestarios posteriores sí será necesario realizar inversiones que deberían haberse estimado. Por otro lado, debe tenerse en cuenta que el artículo 1.2 de la norma prevé la posible apertura de delegaciones en los territorios históricos de Bizkaia y Gipuzkoa, cuya razonabilidad no se ha argumentado en el expediente y cuya apertura, en su caso, implicaría necesidad de inversión.

87. Con respecto a los gastos de personal, se recogen las previsiones del PAI que se corresponden con un plan de despliegue de recursos humanos: en el año 2023 serán 10 los puestos operativos, en el año 2024 se añadirán otros 10 y en el año 2025 se prevé que se incorpore toda la plantilla, que se conformaría con un alto cargo y 38 empleados.

88. Por último, se recoge la incidencia económica que trasladan tanto la memoria económica como el PAI en otras administraciones públicas —"La creación de la Agencia no afecta a otros niveles institucionales como las Diputaciones Forales o los ayuntamientos, aunque parte de su actividad estará orientada a la prestación de servicios a las mismas dentro de las atribuciones de seguridad que corresponden al Departamento matriz"—, en la ciudadanía y en la empresa privada —"La creación de la Agencia impactará de manera directa en la ciudadanía y en las empresas de Euskadi. //Además de los beneficios que les puede suponer contar con una administración pública más resiliente ante los riesgos de ciberseguridad y con una estrategia común, la propia agencia tiene entre sus funciones la provisión de servicios hacia la ciudadanía y las empresas que les permitan mejorar su madurez y protección en el ámbito de la ciberseguridad de manera individual y colectiva.//En el caso de las empresas, además, la Agencia, a través de su apoyo y coordinación al Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente y a la SPRI (perteneciente al mismo), será un dinamizador del talento de manera tanto directa como indirecta que permitirá dotar al sector privado de un sector con mayor potencial al existente actualmente y continuar con su posicionamiento de referencia en el ámbito internacional"—.

89. Se ha redactado una **memoria sucinta** sobre el procedimiento de elaboración a fin de dar cumplimiento al mandato del artículo 24.2 de la LPEDG, en la que se exponen los antecedentes, los trámites practicados y su resultado y las modificaciones realizadas en el texto del proyecto para adecuarlo a las observaciones y sugerencias de los diferentes informes evacuados. En dicho documento se exponen de forma razonada los motivos por los que algunas han sido estimadas y otras rechazadas, aunque no se distinguen las que se corresponden con aquellas contenidas en informes preceptivos, en cuyo caso la ley requiere que la no aceptación venga precedida de una justificación con "suficiente detalle".

90. Tales antecedentes permiten valorar de forma positiva el procedimiento seguido en la elaboración del anteproyecto, si bien se hace preciso añadir lo siguiente.

91. El artículo 24.3 de la LPEDG contempla que la memoria sucinta analizará igualmente la congruencia de la iniciativa con el resto del ordenamiento jurídico, del vigente en Euskadi y de la Unión Europea, y con otras que se estén elaborando en los distintos departamentos del Gobierno Vasco o que vayan a elaborarse de acuerdo con el plan anual normativo, así como con las que se estén tramitando en el Parlamento Vasco, y la necesidad de incluir la derogación expresa de otras normas, así como de refundir en la nueva otras existentes en el mismo ámbito.

92. Aunque se afirma en la misma que la entrada en vigor de la ley no supondrá la derogación ni modificación de ninguna disposición de igual o inferior rango, se echa en falta un análisis de su repercusión y, sobre todo, del encaje de las funciones atribuidas a la Agencia a la vista de la regulación actual en materia de ciberseguridad aplicable a las administraciones públicas.

II LA CIBERSEGURIDAD

93. La ciberseguridad constituye una fuente de preocupación a nivel europeo, al igual que otros graves riesgos, y la normativa europea ha buscado armonizar las legislaciones de los estados miembros para dar una respuesta común.

94. En ese sentido, es preciso citar en primer lugar la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

95. La directiva ya señalaba (considerando 5) que constituye un primer paso en el proceso de identificación y designación de las infraestructuras críticas europeas

y de evaluación de la necesidad de mejorar su protección. Como tal, la directiva se concentra en los sectores de la energía y de los transportes y debe revisarse con el fin de evaluar su incidencia y la necesidad de incluir en su ámbito de aplicación otros sectores como el de las tecnologías de la información y de las comunicaciones (TIC).

96. Su trasposición se produjo con la aprobación de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (LPIC), con un enfoque más amplio, incluyendo como sectores estratégicos la Administración y las tecnologías de la Información y las comunicaciones (TIC).

97. Su exposición de motivos señalaba que la seguridad de las infraestructuras críticas exige contemplar actuaciones que vayan más allá de la mera protección material contra posibles agresiones o ataques, razón por la cual resulta inevitable implicar a otros órganos de la Administración General del Estado, de las demás administraciones públicas, de otros organismos públicos y del sector privado. Estas infraestructuras críticas dependen cada vez más de las tecnologías de la información, tanto para su gestión como para su vinculación con otros sistemas, para lo cual se basan, principalmente, en medios de información y de comunicación de carácter público y abierto. Es preciso contar, por tanto, con la cooperación de todos los actores involucrados en la regulación, planificación y operación de las diferentes infraestructuras que proporcionan los servicios esenciales para la sociedad, sin perjuicio de la coordinación que ejercerá el Ministerio del Interior en colaboración con las comunidades autónomas.

98. La LPIC declara que el Sistema de Protección de Infraestructuras Críticas se compone de una serie de instituciones, órganos y empresas, procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos (artículo 5.1), entre los que se incluyen, las comunidades autónomas (artículo 5.2 d).

99. En particular, el artículo 10.1 de la ley reconoce a las comunidades autónomas que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, el ejercicio, sobre las infraestructuras ubicadas en su demarcación territorial, de las facultades que reglamentariamente se determinen respecto a su protección, sin perjuicio de los mecanismos de coordinación que se establezcan.

100. Importa destacar que la ley invoca la competencia atribuida al Estado en virtud del artículo 149.1.29.ª de la CE en materia de seguridad pública (disposición final

1ª), y su contenido "se entiende sin perjuicio de lo que establezca la normativa autonómica en materia de protección civil, de acuerdo con las competencias correspondientes a cada territorio en virtud de lo dispuesto en los correspondientes Estatutos de Autonomía" (disposición final 2ª).

101. En su desarrollo se dictó el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, que completó en su artículo 10 la remisión de la LPIC, "dada la existencia en ellas de Cuerpos policiales autonómicos, y sin perjuicio de que las respectivas Delegaciones del Gobierno en dichas Comunidades Autónomas tengan conocimiento de la información sensible y de los planes a que se refiere el presente reglamento".

102. En el campo específico de las redes y sistemas de información, finalmente se aprobó la Directiva 2016/1148, de 6 de julio de 2016, del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva NIS, por las siglas Network and Information Systems).

103. La citada directiva expresa que la responsabilidad de velar por la seguridad de las redes y sistemas de información recae en gran medida en los operadores de servicios esenciales y los proveedores de servicios digitales. Debe fomentarse una cultura de gestión de riesgos que implique una evaluación del riesgo y la aplicación de medidas de seguridad adecuadas a los riesgos que hay que afrontar, y esta se debe desarrollar a través de requisitos normativos adecuados y prácticas sectoriales voluntarias. Asimismo, es indispensable sentar unas condiciones de igualdad dignas de confianza para garantizar el funcionamiento efectivo del Grupo de cooperación y la red de CSIRT y, por ende, la cooperación efectiva de todos los estados miembros (considerando 44).

104. También establece que se aplica únicamente a las administraciones públicas que hayan sido identificadas como operadores de servicios esenciales. Por consiguiente, es responsabilidad de los estados miembros garantizar la seguridad de las redes y sistemas de información de las administraciones públicas que no estén incluidas en el ámbito de aplicación de la esta directiva (considerando 45).

105. Como señala su artículo 2.1, la directiva: a) establece obligaciones para todos los estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información; b) crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los estados miembros y desarrollar la confianza y seguridad entre ellos; c) crea una red de equipos de respuesta a incidentes de seguridad informática —en lo

sucesivo, «red de CSIRT», por sus siglas en inglés de «computer security incident response teams»— con el fin de contribuir al desarrollo de la confianza y seguridad entre los estados miembros y promover una cooperación operativa rápida y eficaz; d) establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales; y e) establece obligaciones para que los estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información.

106. En este caso, la trasposición fue llevada a cabo, una vez vencido el plazo, por el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Tiene por objeto, a tenor de su artículo 1, 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. Así mismo, establece un marco institucional para la aplicación del real decreto-ley y la coordinación entre autoridades competentes y los órganos de cooperación relevantes en el ámbito comunitario

107. 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, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y a los servicios digitales.

108. Y debe ser entendido, según el artículo 5, sin perjuicio de las acciones emprendidas para salvaguardar la seguridad nacional y las funciones estatales esenciales, incluyéndose las dirigidas a proteger la información clasificada o cuya revelación fuere contraria a los intereses esenciales del Estado, o las que tengan como propósito el mantenimiento del orden público, la detección, investigación y persecución de los delitos y el enjuiciamiento de sus autores

109. Lo importante es que el artículo 9 no incluye entre las autoridades competentes a las comunidades autónomas, ni el artículo 11 les reconoce la condición de equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia en materia de seguridad de las redes y sistemas de información.

110. Es el Centro Criptológico Nacional (CCN), *ex* artículo 11.3, el que ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del sector público comprendido en la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, y en la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.

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

112. El CCN ejercerá la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las administraciones públicas con los CSIRT internacionales, en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan.

113. Por su parte, el artículo 13 atribuye al Consejo de Seguridad Nacional la condición de punto de contacto único, que ejercerá, a través del Departamento de Seguridad Nacional, una función de enlace para garantizar la cooperación transfronteriza de las autoridades competentes designadas conforme al artículo 9, con las autoridades competentes de otros estados miembros de la Unión Europea, así como con el grupo de cooperación y la red de CSIRT.

114. Por último, se dicta en virtud de las competencias exclusivas atribuidas al Estado en materia de régimen general de telecomunicaciones y seguridad pública por el artículo 149.1. 21.ª y 29.ª de la CE (disposición final 1ª).

115. En su desarrollo se ha aprobado el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de noviembre, de seguridad de las redes y sistemas de información, con el mismo fundamento competencial, en el que se abordan nuevamente el marco estratégico e institucional, las medidas de seguridad, de gestión y notificación de incidentes.

116. Confluyen en la materia, asimismo, otras tres leyes que se ocupan de la ciberseguridad desde distintas perspectivas y que casi coinciden en el tiempo.

117. Por un lado, la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, entre otras razones para la trasposición de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. Entre los delitos contra el patrimonio y contra el orden socio económico se incluyen específicamente las conductas tipificadas por el artículo 264 y artículo 264 bis.

118. De otro lado, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, considera a la ciberseguridad como un ámbito de especial interés de la Seguridad Nacional, tal como señala su artículo 10, y que, por ello, requiere una atención

específica por resultar básica para preservar los derechos y libertades y el bienestar de los ciudadanos y para garantizar el suministro de los servicios y recursos esenciales.

119. Dicha ley se dicta al amparo de lo dispuesto en el artículo 149.1.4.ª y 29.ª de la CE que atribuyen al Estado la competencia exclusiva en materia de defensa y Fuerzas Armadas y en materia de seguridad pública (encaje validado por la STC 184/2016).

120. De acuerdo con las previsiones de su artículo 4.3, se aprobó el Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017, y posteriormente, el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021.

121. En el ámbito de las administraciones públicas, la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público (LRJSP), amplió el ámbito de aplicación del Esquema Nacional de Seguridad (ENS) a todo el sector público, estableciendo en su artículo 3, que regula los principios generales, la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por dichos medios, señalando al ENS como instrumento fundamental para el logro de dichos objetivos en su artículo 156.

122. Esta ley se dicta al amparo de lo dispuesto en el artículo 149.1. 18.ª de la CE, que atribuye al Estado competencia exclusiva sobre las bases régimen jurídico de las administraciones públicas.

123. Asimismo, la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, incluye en el artículo 13 entre los derechos de las personas en sus relaciones con las administraciones públicas el relativo a la protección de los datos personales y, en particular, el derecho a la seguridad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas. Esta ley se aprueba al amparo asimismo de lo dispuesto en el artículo 149.1. 18.ª de la CE.

124. En desarrollo de las dos leyes anteriores, el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, concreta en diferentes preceptos la obligación del cumplimiento de las medidas de seguridad previstas en el ENS,

como los referidos al intercambio electrónico de datos en entornos cerrados de comunicación, los sistemas de clave concertada y otros sistemas de identificación de las personas interesadas, el archivo electrónico único o los portales de internet, entre otros.

125. También se cita el artículo 149.1.18 de la CE, pero la disposición final primera .2 explicita que "los artículos 15, 16, 23, 26, 28.2, 28.3 y 29.4 y la disposición adicional tercera del Reglamento que aprueba este real decreto, en cuanto a su relación con la ciberseguridad y su impacto en la seguridad de las redes y sistemas de información se dictan, además, de acuerdo con lo dispuesto en los artículos 149.1.21.ª y 149.1.29.ª de la CE, que atribuyen al Estado la competencia exclusiva en materia de telecomunicaciones y en materia de seguridad pública, respectivamente".

126. Dicho ENS, establecido originariamente en 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, fue modificado por el Real Decreto 951/2015, de 23 de octubre, y en la actualidad se encuentra vigente el aprobado por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que se dice dictado al amparo de lo establecido en los artículos 149.1.18.ª, 149.1.21.ª y 149.1.29.ª de la CE, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, las telecomunicaciones y la seguridad pública, respectivamente (disposición final primera).

127. El ENS es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la LRJSP, así como a las entidades del sector privado, incluida la obligación de contar con la política de seguridad cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

128. El artículo 12.2 prevé que cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente. No obstante, la totalidad o una parte de los sujetos de un sector público institucional podrán quedar incluidos en el ámbito subjetivo de la política de seguridad aprobada por la Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización.

129. En el caso de los municipios "podrán disponer de una política de seguridad común elaborada por la entidad local comarcal o provincial que asuma la responsabilidad de la seguridad de la información de los sistemas municipales".

130. Según el artículo 12.6, la política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los siguientes requisitos mínimos: a) Organización e implantación del proceso de seguridad; b) Análisis y gestión de los riesgos; c) Gestión de personal; d) Profesionalidad; e) Autorización y control de los accesos; f) Protección de las instalaciones; g) Adquisición de productos de seguridad y contratación de servicios de seguridad; h) Mínimo privilegio; i) Integridad y actualización del sistema; j) Protección de la información almacenada y en tránsito; k) Prevención ante otros sistemas de información interconectados; l) Registro de la actividad y detección de código dañino; m) Incidentes de seguridad; n) Continuidad de la actividad; ñ) Mejora continua del proceso de seguridad.

131. A la luz del artículo 12.7, los requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28, alguno de los cuales podrá obviarse en sistemas sin riesgos significativos.

132. En esa idea de adecuación cabe mencionar que el artículo 29 contempla que la utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto. Los supuestos concretos de utilización de estas infraestructuras y servicios serán determinados por cada administración pública.

133. Asimismo, en relación a la proporcionalidad para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios, el artículo 30 permite implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad.

134. En el ámbito autonómico, ni la Ley 15/2012, de 28 de junio, de ordenación del Sistema de seguridad pública de Euskadi (LOSS), ni el Texto refundido la Ley de gestión de emergencias, aprobado por Decreto Legislativo 1/2017, de 27 de abril, mencionan específicamente la ciberseguridad.

135. Aunque la primera señala en su artículo 2.2 que el sistema de seguridad pública de Euskadi comprende la policía y seguridad ciudadana, la seguridad vial y la gestión de emergencias y protección civil, regulados en sus normativas específicas, así como otras políticas públicas sectoriales destinadas a garantizar la seguridad de personas y bienes y el libre ejercicio de los derechos y libertades.

136. Por el contrario, el Plan General de Seguridad Pública de Euskadi 2020-2025, aprobado conforme al artículo 11 de la LOSS, sí que alude a la ciberseguridad y entre sus iniciativas figura: "Junto con el Basque Cibersecurity Center (BCSC), definir políticas preventivas y de respuesta ante incidentes de ciberseguridad, formando un grupo de actuación de máximo nivel en la Ertzaintza para investigar los incidentes críticos".

137. De otro lado, la LSPV, dedica el capítulo III del título V, a la Administración electrónica y atención ciudadana. Entre los principios de la Administración electrónica el artículo 68.e) prevé el principio de seguridad en la implantación y utilización de los medios electrónicos, por el sector público de la Comunidad Autónoma de Euskadi, en cuya virtud se exigirá al menos el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos y el artículo 68.f) el principio de proporcionalidad, en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones. Asimismo, sólo se requerirán a las ciudadanas y ciudadanos aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten.

138. En materia de Administración electrónica, el artículo 69.2.e) de la LSPV reconoce a todos los ciudadanos y ciudadanas en su relación con el sector público de la Comunidad Autónoma de Euskadi el derecho a la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones del sector público de la Comunidad Autónoma de Euskadi.

139. Por su parte, el artículo 42 del Decreto 21/2012, de 21 de febrero, de Administración electrónica, que se aplica a la Administración General de la Comunidad Autónoma de Euskadi y a su sector público, así como a las personas físicas, jurídicas y entes sin personalidad en sus relaciones con las entidades incluidas en el ámbito de aplicación del decreto, regula la política de gestión de documentos electrónicos, que cumplirá los requisitos establecidos en los Esquemas Nacionales de Interoperabilidad y de Seguridad y sus normas de desarrollo.

140. Este panorama no estaría completo si no citáramos, en primer lugar, la existencia a nivel europeo de la Agencia de la Unión Europea para la ciberseguridad (ENISA). El Reglamento (CE) 460/2004 del Parlamento Europeo y del Consejo creó ENISA

con el objetivo de contribuir al establecimiento de un elevado y efectivo nivel de seguridad de las redes y de la información en la Unión y al desarrollo de una cultura de la seguridad de las redes y de la información en beneficio de los ciudadanos, los consumidores, las empresas y las administraciones públicas. En la actualidad se encuentra regulada en el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 («Reglamento sobre la Ciberseguridad»).

141. Entre los objetivos de la ENISA el artículo 4.4 contempla el de fomentar "la cooperación, en particular el intercambio de información, y la coordinación a nivel de la Unión entre los Estados miembros, las instituciones, órganos y organismos de la Unión y las partes interesadas pertinentes, públicas y privadas, sobre las cuestiones relacionadas con la ciberseguridad".

142. Como señala el Considerando 5 del reglamento, mientras que los ciberataques a menudo son transfronterizos, las competencias de las autoridades de ciberseguridad y policiales, así como las respuestas políticas de las mismas, son predominantemente nacionales. Los ciberincidentes a gran escala podrían perturbar la prestación de servicios esenciales en toda la Unión. Esta situación requiere una respuesta efectiva y coordinada y una gestión de crisis a escala de la Unión, basadas en políticas específicas y en instrumentos más amplios que propicien la solidaridad y la asistencia mutua en Europa.

143. En segundo lugar, la reciente aprobación de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2), así como la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo.

144. Los estados miembros han de proceder y publicar las disposiciones necesarias para la trasposición de las dos directivas a más tardar el 17 de octubre de 2024.

145. La segunda ya advierte en su Considerando 9 que, "dada la importancia de la ciberseguridad para la resiliencia de las entidades críticas y en aras de la coherencia, debe garantizarse, siempre que sea posible, un enfoque coherente entre la presente Directiva y la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo. Teniendo en cuenta la mayor

frecuencia y las características particulares de los riesgos cibernéticos, la Directiva (UE) 2022/2555 impone unos requisitos exhaustivos a un amplio conjunto de entidades para garantizar su ciberseguridad. Dado que la ciberseguridad se trata de manera suficiente en la Directiva (UE) 2022/2555, las materias reguladas por dicha Directiva deben quedar excluidas del ámbito de aplicación de la presente Directiva, sin perjuicio del régimen particular aplicable a las entidades del sector de las infraestructuras digitales".

146. En cuanto a la Directiva (UE) 2022/2555, de su larga relación de considerandos preliminares es suficiente con referir que su objetivo principal es el de eliminar las divergencias detectadas entre los estados miembros, concretamente mediante la definición de normas mínimas relativas al funcionamiento de un marco regulador coordinado, el establecimiento de mecanismos para que las autoridades competentes de cada estado miembro cooperen de manera eficaz, la actualización de la lista de sectores y actividades sujetos a las obligaciones de ciberseguridad y la disponibilidad de vías de recurso y medidas de ejecución eficaces que son fundamentales para garantizar el cumplimiento efectivo de dichas obligaciones.

147. De esta amplia exposición de los elementos que condicionan la regulación del anteproyecto, consideramos importante destacar que la ciberseguridad se concibe de formas distintas y con diferentes facetas, desde una multiplicidad de enfoques.

148. Por un lado, estarían las actuaciones y ataques cibernéticos que pueden llegar a incidir en la seguridad nacional, habiéndose canalizado la respuesta desde ese ámbito, o las que constituyen actividades de ciberdelincuencia, que han de ser perseguidas por las fuerzas y cuerpos de seguridad, sin perjuicio del deber genérico impuesto a cualquier ciudadano o ciudadana por el artículo 259 de la Ley de enjuiciamiento criminal, y el específico del artículo 262 de la Ley de enjuiciamiento criminal a los que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, que estarán obligados a denunciarlo inmediatamente al Ministerio fiscal, al tribunal competente, al juez de instrucción y, en su defecto, al municipal o al funcionario de policía más próximo al sitio si se tratare de un delito flagrante.

149. La ciberseguridad queda fuera del ordenamiento administrativo cuando se refiere a actividades delictivas, pero no toda protección de la seguridad de las redes requiere una actuación policial y judicial penal.

150. Incluso un grave incidente de ciberseguridad podría provocar una catástrofe, calamidad pública o situación de grave riesgo colectivo, por lo que su prevención y gestión debe ser objeto de la política de protección civil, a través de sus

instrumentos y con arreglo a las competencias de las diversas autoridades, pero lo será cuando deba ser gestionado desde ese campo de actuación.

151. Por último, estaría la ciberseguridad que, tomando en cuenta el soporte, se despliega de forma ordinaria, esto es, la que se ocupa de la seguridad de las redes y sistemas de información, para prevenir incidentes y gestionarlos, y, dentro de ella, como una subcategoría, la seguridad aplicable al ámbito del sector público, para una protección adecuada de la información tratada y los servicios prestados, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos.

152. En ese sentido, también el Estado tiene proyectado constituir el Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus organismos públicos, previsto en el Plan de Digitalización de las Administraciones Públicas 2021-2025 —en concreto en la Medida 9 "Centro de Operaciones de Ciberseguridad" del Eje 1 "Transformación digital de la Administración General del Estado")—. Este centro, según consta en la documentación a la que ha tenido acceso esta Comisión, contribuirá a mejorar la situación de seguridad (del orden de 90 entidades) y actuará como elemento facilitador para el cumplimiento de la regulación del ENS.

III ASPECTOS COMPETENCIALES

153. En tanto que el objeto de la ley es la creación de la Agencia Vasca de Ciberseguridad-Euskadiko Zibersegurtasun Agentzia, cabe decir que constituye expresión de la competencia autoorganizativa que reconoce el artículo 10.2 del EAPV.

154. La doctrina constitucional considera que la competencia relativa a la libre organización de la propia Administración autonómica es algo inherente a la autonomía —STC 50/1999 (FJ 3), reiterada en las SSTC 251/2006, de 25 de julio y 137/2013 de 6 junio—.

155. En la medida en que la STC 142/2018, de 20 de diciembre, resuelve el recurso de inconstitucionalidad interpuesto respecto de la Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña, necesariamente nos vemos abocados a hacer referencia a dicha sentencia y utilizarla, sin duda, como canon de análisis del proyecto remitido.

156. De momento, resulta oportuno recordar que:

> 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).

157. Esto es, estamos ante una competencia instrumental para el adecuado ejercicio de una competencia sustantiva.

A) Respecto al Estado

158. El anteproyecto, además de justificar la creación de la Agencia en lo dispuesto en el artículo 10.2 del EAPV, invoca la competencia reconocida por el artículo 17 del EAPV en materia de seguridad pública, en policía y seguridad ciudadana. Competencia que ha de entenderse integrada, a su vez, con otras, tales como las competencias en materias de emergencias y protección civil. Todas estas competencias configuran un sistema general de seguridad propio, si bien participado por otras administraciones que también ostentan competencias sobre dichas materias.

159. La memoria y exposición de motivos alegan también que dentro de la competencia en seguridad pública de la Comunidad Autónoma de Euskadi se integran las materias de planificación y coordinación del sistema de seguridad pública de Euskadi. La finalidad de dicha organización competencial, cuyas autoridades y órganos autonómicos competentes se regulan en la Ley 15/2012, de 28 de junio, de ordenación del Sistema de seguridad pública de Euskadi, es

la de proporcionar a la ciudadanía la protección frente a toda clase de riesgos y garantizar el libre y pacífico ejercicio de derechos y libertades de forma integral.

160. Tal enfoque, a juicio de la Comisión, requiere ser reconsiderado porque la citada STC 142/2018 ha entendido que el encaje de la ciberseguridad en ese ámbito trasciende el campo de las competencias autonómicas, pues lo ha restringido a las actuaciones relacionadas con las administraciones y sus sistemas de información y comunicaciones.

161. Respecto a la ciberseguridad, la sentencia citada acoge para el encuadramiento competencial su definición técnica, 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), y la que plasma la Directiva (UE) 2016/1148, de 6 de julio, del Parlamento Europeo y del Consejo, que 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).

162. De ello se extrae una primera conclusión: "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" (FJ 4).

163. Y consecuentemente, "no es un concepto o materia reconducible a un único título competencial. Puede, como allí se recalca, identificarse con la seguridad nacional o con la seguridad pública cuando se trata de la protección ordinaria de las redes y las infraestructuras de telecomunicaciones. Pero también puede proyectarse sobre otros planos, como es el caso de la administración electrónica, que abarca la organización de medios y previsión de medidas de protección de la administración y, por extensión, la protección de los derechos de los ciudadanos cuando se relacionan con la administración por medios electrónicos" (FJ 5).

164. En particular, esa acepción conectada con la autoprotección, que tiene como finalidad última prevenir las amenazas y vulnerabilidades inherentes a sus redes interdependientes e infraestructuras de la información, tanto internamente como

en sus relaciones con los administrados y con otras administraciones o entidades públicas, ha sido expresamente reconocida como un componente fundamental de las competencias de autoorganización administrativas.

165. Ello por cuanto 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).

166. Cuando las facultades atribuidas a la agencia autonómica no se limitaban a proteger las redes y sistemas de información de la Administración de la Generalitat y de su sector público y los de los particulares y otras administraciones públicas que se relacionan por medios electrónicos con dicha administración, ha entendido que se infringía el orden constitucional porque la ciberseguridad se integra en las competencias estatales en materia de seguridad pública (149.1.29 CE) y de telecomunicaciones y régimen general de comunicaciones (art. 149.1.21 CE), lo que impide atribuir a la agencia potestades de intervención o regulación sobre el sector privado.

167. Dicho de otra forma, la ciberseguridad tiene, de una u otra forma, una indudable conexión con el mantenimiento de la tranquilidad u orden ciudadanos, que es en lo que consiste la seguridad pública (SSTC 33/1982, FJ 3; 117/1984, FJ 4; 104/1989, FJ 3; 148/2000, entre otras). Pero, a juicio del alto tribunal, 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.

168. De un lado, por lo que se refiere a la materia de seguridad pública:

> es, en principio, competencia exclusiva del Estado ex artículo 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 artículo 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).

(…)

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 artículo 149.1.29 CE contempla a la exclusiva competencia estatal sobre seguridad pública.

169. Cabe señalar que dicha doctrina es coincidente con la expuesta en la STC 86/2014, de 29 de mayo de 2014, que resolvió el recurso de inconstitucionalidad interpuesto, en relación con diversos preceptos de la Ley del Parlamento Vasco 15/2012, de 28 de junio, de ordenación del Sistema de seguridad pública de Euskadi, de suerte que corresponden al Estado, "además de los servicios policiales que en todo caso han quedado reservados a las fuerzas y cuerpos de seguridad del Estado, las restantes potestades o facultades administrativas que, siendo relevantes para la seguridad pública, no sean sin embargo propias ni inherentes de las funciones o servicios policiales, según han sido definidos por la Ley Orgánica de Fuerzas y Cuerpos de Seguridad y por la Ley Orgánica a que se remite el artículo 104.2 CE".

170. Y su conclusión: "no ha de confundirse (es) la competencia específica relativa al 'régimen de la policía autónoma, para la protección de las personas y bienes y el mantenimiento del orden público dentro del territorio autónomo', prevista en el artículo 17 EAPV, que se proyecta sobre el sistema de autoridades territoriales y servicios policiales propios en los términos ya expuestos con la más genérica y, por tanto, de contenido más amplio –en tanto que abarca un amplio espectro de actuaciones administrativas (STC 104/2005, FJ 5)– en materia de seguridad pública que el artículo 149.1.29.ª CE reserva, con los límites ya examinados, al Estado".

171. De otro lado, por lo que respecta a la competencia exclusiva estatal del artículo 149.1.21 CE, en materia de telecomunicaciones y régimen general de comunicaciones:

> 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 artículo 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 artículo 140 EAC atribuye a la Generalitat «de acuerdo con la normativa del Estado, la competencia ejecutiva en materia de comunicaciones electrónicas», citando a continuación las potestades que incluye, potestades que la doctrina constitucional ha relacionado preferentemente con la materia relativa a los medios de comunicación social. Dicha competencia no puede menoscabar ni perturbar la competencia estatal en materia de régimen general de comunicaciones que tiene por objeto ordenar normativamente y asegurar la efectividad de las comunicaciones, ni tampoco la dimensión técnica vinculada al uso del dominio público radioeléctrico que está en manos del Estado, que es su titular (art. 149.1.21 CE; STC 31/2010, de 28 de junio, FJ 85).

172. En definitiva, las funciones atribuidas a la Agencia no pueden afectar a la dimensión de la ciberseguridad relacionada con la seguridad pública —que no sea la propiamente policial— en el ámbito material de las redes e infraestructuras informáticas —salvo en el caso de la autoprotección de la Administración—.

173. Lo que no impide que la Agencia, como señala la Ley catalana, pueda 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, ni que pueda colaborar en la investigación y represión de ilícitos penales, 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.

174. La STC 142/2018 confirma su constitucionalidad porque:

> 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 Generalitat (art. 164.5 EAC), bien de las autoridades judiciales competentes, en los términos previstos en la legislación procesal.

175. Así pues, lo que legitima y fundamenta la actuación, en este caso, de la Agencia Vasca de Ciberseguridad es la preservación de la seguridad en la Administración electrónica de la Administración General de la Comunidad Autónoma y las redes de comunicaciones electrónicas del resto de administraciones públicas vascas, tanto a nivel interno como externo, en su relación con el resto de entidades públicas y los administrados.

176. Ahora bien, esa competencia también obliga a tener en cuenta que se encuentra limitada por la del Estado prevista en el artículo 149.1.18 de la CE.

177. La jurisprudencia constitucional, sintetizada en la STC 141/2014, de 11 de septiembre (FJ 5.D), delimita el alcance de la potestad autoorganizativa autonómica en relación con las competencias del Estado para fijar las bases del régimen jurídico de las administraciones públicas (art. 149.1.18 CE), recordando que «para determinar el régimen jurídico de la organización y funcionamiento de su propia Administración, no tiene carácter exclusivo, sino que debe respetar y, en su caso, desarrollar las bases establecidas por el Estado» (STC 50/1999, de 6 de abril, FJ 3).

178. No obstante, la intensidad de estas bases fijadas por el Estado es diversa. El Tribunal Constitucional afirma que no procede atribuir a las bases estatales la misma extensión e intensidad cuando se refieren a aspectos meramente organizativos internos, que no afectan directamente a la actividad externa de la Administración y de los administrados, que en el resto de aspectos en los que sí que se da esta afectación (STC 50/1999, FJ 3).

179. Como ha quedado expuesto anteriormente, el Estado también ha incidido en este ámbito de la ciberseguridad interna de las administraciones públicas, invocando una triada de títulos competenciales, principalmente, el citado de las bases del régimen jurídico de las administraciones públicas (artículo 149.18 CE), pero también los de seguridad pública (artículo 149.1. 29 CE) y telecomunicaciones y régimen general de comunicaciones (artículo 149.1.21 CE).

180. Puede decirse que es indudable la capacidad de las administraciones públicas vascas y su sector público para prevenir y dar respuesta a las amenazas derivadas de la ciberseguridad, pero, igualmente, deben hacerlo respetando las bases establecidas por el Estado, materializadas en el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, y sobre todo en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

B) Respecto a los territorios históricos y entidades locales

181. Parece conveniente citar las competencias exclusivas atribuidas a la Comunidad Autónoma por el artículo 10.2 del EAPV en materia de organización, régimen y funcionamiento de sus instituciones de autogobierno dentro de las normas del presente Estatuto, artículo 10.4 del EAPV en materia de régimen local y artículo 10.24 del EAPV en materia de sector público propio del País Vasco.

182. Todas ellas limitadas por la competencia estatal del artículo 149.1.18 de la CE, como ampliamente argumentamos en el Dictamen 120/2014, que permite al

Estado establece principios y reglas básicas sobre aspectos organizativos y de funcionamiento de todas las administraciones públicas.

183. Pero lo que nos interesa analizar aquí es si es posible que el legislador autonómico puede llegar a incidir en la capacidad autoorganizativa de los territorios históricos y de los municipios, y en tal caso, con arreglo a qué fórmulas.

184. El artículo 37.3.a) del EAPV atribuye a los territorios históricos competencias exclusivas en materia de organización, régimen y funcionamiento de sus propias instituciones. Dicha competencia forma parte del núcleo intangible de la foralidad.

185. La Comisión ha defendido, a pesar de dicha atribución, que, bajo el prisma del artículo 10.2 del EAPV, la autonomía organizativa de los órganos forales no ha de concebirse como un esfera total y absolutamente resistente a cualquier mínima incidencia o afectación proveniente del legislador autonómico en cuanto institución que forma parte de los poderes del País Vasco, siempre que no cuestione sus rasgos organizativos ni desdibuje la imagen identificable de sus régimen foral tradicional, encuentre adecuado soporte en preceptos constitucionales y tenga carácter principial (dictámenes 105/2012, 120/2014, 138/2015, 127/2016 y 190/2020).

186. Por otro lado, el artículo 4.1 de la Ley 7/1985, de 2 de abril, reguladora de las bases del régimen local (LBRL), contempla como competencia de los municipios, en todo caso, la de autoorganización. Asimismo, el artículo 4.2.c) de la Ley 2/2016, de 7 de abril, de instituciones locales de Euskadi (LILE), enuncia entre los principios rectores del régimen local el principio de autoorganización, y el artículo 9.5 de la LILE prevé que la autonomía municipal comprende, en todo caso, la organización y gestión de sus propios órganos de gobierno y administración, siendo objeto de dicha potestad el artículo 10 de la LILE.

187. En la medida en que la autonomía constitucionalmente reconocida no impide que el Estado pueda, al establecer bases del régimen jurídico de las administraciones públicas, condicionar la competencia foral y municipal, también podrá hacerlo el legislador vasco al desarrollar tales bases al servicio de un modelo común de los poderes públicos vascos.

188. Cabe resaltar que parte de ese enfoque unitario la reciente LSPV, aunque con matices, a la luz del artículo 3.1 y disposición adicional primera.

189. Desde luego, los servicios de administración electrónica forman parte de la potestad de autoorganización inherente a la autonomía de los territorios históricos y administraciones locales.

190. Resulta de interés en esta exposición, referirnos al fundamento jurídico 11 de la STC 111/2016, de 9 de junio, que analiza la letra g) del art. 36.1 de la LBRL — en la redacción dada por el art. 1.13 de la Ley 27/2013, de 27 de diciembre, de racionalización y sostenibilidad de la Administración Local—, conforme a la cual, corresponde a la diputación provincial, como competencia propia, «la prestación de los servicios de administración electrónica y la contratación centralizada en los municipios con población inferior a 20.000 habitantes»:

> La previsión impugnada en modo alguno transfiere en bloque a la diputación provincial toda la prestación de servicios de administración electrónica y de la contratación de municipios de menos de 20.000 habitantes; una traslación semejante, general e indiscriminada, ni la pretende el legislador ni resultaría compatible con la potestad de autoorganización inherente a la autonomía constitucionalmente garantizada a todos los municipios (art. 137 CE), también a los de menores dimensiones. En realidad, el art. 36.1, letra g), LBRL, se ha limitado a incluir atribuciones nuevas que especifican la más general de «asistencia y cooperación jurídica, económica y técnica a los municipios, especialmente los de menor capacidad económica y de gestión», que estaba –y sigue– estando prevista como base del régimen local [art. 36.1, letra b), LBRL]. Hay que tener en cuenta, además, que el art. 31.2 a) LBRL dispone como fines propios y específicos de las diputaciones provinciales los de «garantizar los principios de solidaridad y equilibrio intermunicipales» y, de modo particular, el de «asegurar la prestación integral y adecuada en la totalidad del territorio provincial de los servicios de competencia municipal». Por ello, lo que pretende el precepto es dar efectividad a la prestación de unos servicios que exigen la aplicación de tecnología informática (en el caso de la administración electrónica) o técnico-jurídica (en el supuesto de la contratación centralizada) que los municipios de pequeña o mediana población (hasta 20.000 habitantes), pueden no estar en condiciones de asumir. En definitiva, se trata de que la diputación provincial cumpla su función institucional más característica prestando apoyo a estos municipios en las tareas que desempeñan relacionadas con la contratación y la llamada administración electrónica. Solo en este sentido, que se desprende naturalmente de interpretación conjunta de los citados artículos de la Ley

reguladora de las bases del régimen local, puede entenderse el precepto impugnado.

Hay que tener en cuenta, que el art. 149.1.18 CE autoriza una legislación básica estatal que desarrolle «el apoyo a los Municipios» como «núcleo» de la actividad de la provincia, «en cuanto entidad local determinada por la agrupación de Municipios (art. 141.1 CE)» con autonomía constitucionalmente garantizada (STC 109/1998, de 21 de mayo, FJ 2). A su vez, las tareas provinciales de cooperación con (o asistencia al) municipio, lejos de vulnerar la autonomía municipal, contribuyen a facilitar su desarrollo efectivo, por lo que no pueden entenderse infringidos los arts. 137 y 140 CE".

191. El artículo 17.1.30 de la LILE prevé como competencias propias de los municipios la de "Administración electrónica, racionalización y simplificación de procedimientos. En particular, la promoción en el término municipal de la participación de los ciudadanos en el uso eficiente y sostenible de las tecnologías de la información y las comunicaciones".

192. Ahora bien, en este caso no se trata de negar las competencias de los territorios históricos y municipios respecto a su propia Administración electrónica, sino de valorar, como venimos razonando, si es posible que el legislador vasco cree una Agencia con funciones fundamentalmente de apoyo y coordinación en materia de ciberseguridad.

193. La respuesta creemos que debe ser positiva visto el componente de seguridad propio de la ciberseguridad, que es ajeno a las competencias forales —artículo 6 de la Ley 27/1983, de 25 de noviembre, de relaciones entre las instituciones comunes de la Comunidad Autónoma y los órganos forales de sus territorios históricos (LTH)— y municipales (artículo 17.1 4 y 5 LILE), y que también ha sido destacado a la hora de encuadrar la competencia, en una suerte de yuxtaposición de títulos, aunque no se ejercite propiamente la competencia en materia de seguridad pública o, al menos, esta no resulte prevalente, a fin de que la Agencia diseñe el marco estratégico e institucional en materia de ciberseguridad a nivel autonómico, desarrolle una actividad de coordinación y, sobre todo, preste apoyo a tales administraciones en el ejercicio de sus funciones públicas y de forma particular en la prevención y resolución de los incidentes.

194. Desde esta perspectiva, constituirá una herramienta de garantía en la actuación coordinada de todas las administraciones públicas vascas y en el cumplimiento de las medidas de protección de la seguridad, de carácter ordinario y preventivo

necesarias, que han de adoptar, así como de las que requiera el restablecimiento de la normalidad de los sistemas.

195. A los efectos de este dictamen es suficiente con resaltar que los principios de colaboración, cooperación y coordinación son esenciales para lograr una actuación eficaz por parte de las administraciones públicas.

196. Según el Tribunal Constitucional, el principio general de colaboración no está precisado de justificación en preceptos concretos del orden constitucional por implícito —también en términos de cooperación— en la propia esencia de la forma de organización territorial del Estado. El principio de coordinación, por el contrario, está expresamente enunciado en el artículo 103.1 de la CE. Ambos aparecen mencionados en la legislación positiva [p. ej.: artículo 2 de la LTH, artículo 3.k) y 140 de la LRJSP o artículo 10.1 de la LBRL].

197. También la LSPV se hace eco de tales principios, se refiere al principio de colaboración en el artículo 5.2 y a ambos en el artículo 11.2, incluso como una especie de deber, una vez señalado que en su actuación —la Administración de la Comunidad Autónoma— se guiará por los principios de legalidad, objetividad, transparencia, publicidad, eficacia y eficiencia, "como garantía de su observancia, se promoverá y realizará la coordinación entre órganos y, en todo caso, con los órganos de los territorios históricos y de las administraciones locales, fomentando la colaboración con ellos". Y el capítulo IV del título II de la LSPV se refiere a la "colaboración y coordinación interadministrativas", indicando su artículo 31 que la Administración General e institucional de la Comunidad Autónoma de Euskadi actúa de conformidad con el deber de colaboración entre administraciones públicas y con los principios de cooperación y de lealtad institucional, utilizando para ello los instrumentos y las técnicas de colaboración, coordinación y cooperación previstas en las leyes.

198. En particular, el artículo 73 prevé instrumentos de cooperación para el impulso de la Administración electrónica, y su párrafo 1 indica que la Administración General de la Comunidad Autónoma de Euskadi promoverá la celebración de convenios de colaboración y demás instrumentos de cooperación con las entidades correspondientes de la Administración de los territorios históricos y entidades locales de la Comunidad Autónoma de Euskadi, para el impulso de la Administración electrónica. Asimismo, impulsará los citados convenios e instrumentos de cooperación con cualesquiera entidades de la Unión Europea, la Administración del Estado, de las comunidades autónomas y de sus entidades locales u otros organismos internacionales con competencias en la materia.

199. En suma, así como se ha visto la necesidad de una necesaria cooperación y coordinación a nivel europeo (ENISA) y a nivel nacional (Centro Criptológico

Nacional), la creación de la Agencia Vasca de Ciberseguridad mejorará la cooperación, el intercambio de información y la coordinación entre las administraciones vascas.

IV ANÁLISIS DEL OBJETO Y FUNCIONES DE LA AGENCIA VASCA DE CIBERSEGURIDAD

200. Con ese bagaje competencial, estamos en condiciones de analizar el objeto y funciones que se atribuyen a la Agencia.

201. Para ello, es esencial atender al contenido del artículo 2.1 del anteproyecto porque el mismo encuadra y sintetiza la actividad de la Agencia con dos proyecciones: una relativa al sector público vasco, consistente en "promover y coordinar la ciberseguridad en el sector público vasco delimitado en la Ley 3/2022, de 12, de mayo, en el ámbito de la seguridad de los sistemas de información y de las redes electrónicas de su competencia"; y una segunda al ámbito privado, consistente en "apoyar e impulsar la capacitación en ciberseguridad y el desarrollo digital seguro de la Comunidad Autónoma de Euskadi, de su ciudadanía y de su tejido empresarial".

202. Antes de abordar el contenido de las funciones asociadas a ambas perspectivas, cabe adelantar que es acorde con la configuración de la Agencia y su especialización la atribución de una facultad de asesoramiento preceptivo en los procedimientos de elaboración de disposiciones normativas tramitadas por la Administración de la Comunidad Autónoma de Euskadi en materia de ciberseguridad, prevista en el artículo 2.2 c) del anteproyecto.

203. Aunque se atribuye a la Agencia la representación oficial del sector público vasco ante organismos internacionales, estatales y regionales en materia de ciberseguridad, artículo 2.2 p) del anteproyecto, ello no quiere decir que las administraciones públicas vascas no puedan desarrollar actividades de interlocución sobre cuestiones de su competencia.

A) El sector público vasco

204. Desde la primera perspectiva, impulsa las actividades de ciberseguridad y coordina las actuaciones, fundamentalmente, de la Administración General de la Comunidad Autónoma de Euskadi, las administraciones forales de los territorios históricos y las administraciones locales, así como de su respectiva administración institucional y los demás entes instrumentales dependientes y adscritos a las mismas.

205. Parte el anteproyecto de la existencia de las tres instancias territoriales y de dos tipos de relaciones interinstitucionales, de cooperación y de coordinación, y,

aunque ambas derivan del ejercicio autónomo de competencias propias, tienen una distinta significación: la cooperación es voluntaria y la coordinación implica un cierto poder de dirección.

206. En la doctrina del Tribunal Constitucional quien ostenta facultades de coordinación está legitimado, en línea de principio, para establecer unilateralmente medidas armonizadoras destinadas a la más eficaz concertación de la actuación de todos los entes involucrados. Ahora bien, la coordinación no entraña la sustracción de competencias propias de las entidades coordinadas, sino que implica tan sólo un límite al ejercicio de las mismas (STC 27/1987 FJ 5.º).

207. A partir de tal delimitación, podemos avanzar que responden a la lógica de la colaboración entre administraciones las funciones incluidas en el artículo 2 consistentes en: (I) promover una estrategia de ciberseguridad para el conjunto de las administraciones públicas de Euskadi y potenciar y coordinar el alineamiento en la ciberseguridad en dicho conjunto (letra a); (II) impulsar un marco de estándares, directrices y normas técnicas de seguridad recomendables para el sector público vasco (letra b); (III) organizar actividades de difusión, promoción, formación y concienciación en materia de ciberseguridad (letra j); (IV) proponer medidas técnicas de ciberseguridad en la utilización de los recursos informáticos y de las comunicaciones existentes, y la formación en estas medidas al personal de la Administración de la Comunidad Autónoma de Euskadi y al propio personal de la Agencia (letra k); (v) 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 (letra l).

208. Las mismas son respetuosas con las competencias de las respectivas administraciones y, además, el artículo 2.5 del anteproyecto requiere que la Agencia establezca líneas de colaboración en el ámbito de la ciberseguridad con las diputaciones forales y entes locales de Euskadi.

209. Igualmente lo es la función atribuida por el artículo 2.2.d), "realizar evaluaciones anuales de las políticas públicas en materia de ciberseguridad desplegadas en el ámbito del sector público vasco". Tales evaluaciones pueden resultar complementarias del informe del estado de la seguridad contemplado en el artículo 32 del ENS, y servir para que las administraciones competentes impulsen las medidas oportunas para la mejora continua del estado de seguridad.

210. Así como la prevista en el artículo 2.2.f) del anteproyecto, consistente en recoger los datos pertinentes de las entidades que gestionan servicios públicos o esenciales en la Comunidad Autónoma de Euskadi en relación con el estado de la seguridad de la información, prestando especial atención a los sistemas considerados como críticos para el funcionamiento de los servicios públicos o la seguridad de las personas, con vistas a informar al Gobierno Vasco, así como a las administraciones públicas del territorio que intervengan en la prestación de dichos servicios críticos y esenciales, y proponer las medidas adecuadas llevando a cabo la gestión de riesgos en materia de ciberseguridad.

211. Viene a ser natural concreción del principio de colaboración, previsto en el artículo 141.1.c) y d) de la LRJSP y artículo 5.2.c) y d) de la LSPV, esto es, de la obligación de facilitar a las otras administraciones la información que precisen sobre la actividad que desarrollen en el ejercicio de sus propias competencias y prestar, en el ámbito propio, la asistencia que las otras administraciones pudieran solicitar para el eficaz ejercicio de sus competencias, con los límites del artículo 141.2 de la LRJSP y artículo 5.3 de la LSPV, que también serían aplicables en este caso.

212. Por el contrario, responden a la lógica de la coordinación dos funciones que se enuncian, sin embargo, de forma diferente, porque, el artículo 2.2.m) atribuye a la Agencia la de "Coordinar al sector público vasco en la elaboración de sus respectivos planes de ciberseguridad, así como en la consecución de los objetivos establecidos en los mismos", mientras que el artículo 2.2.o) la reconduce a la de "Impulsar la coordinación del sector público vasco en todo lo que se considere necesario para la consecución de los objetivos especificados en los planes de ciberseguridad, estableciendo para ello las líneas de colaboración que se entiendan necesarias".

213. Entiende la Comisión que, en este caso, la coordinación podría estar justificada, pues de lo que se trata básicamente es de garantizar la seguridad de la Administración electrónica, para la prestación integral y adecuada de las actividades de las entidades del sector público vasco, por existir un interés concurrente y complementario de ámbito autonómico, que trasciende el interés propio de tales administraciones.

214. Además, no se trata propiamente de una coordinación vertical porque las administraciones coordinadas participan de los órganos de gobierno de la Agencia y, por tanto, podrán deliberar y, en su caso, acordar las medidas.

215. No obstante, se toma como premisa que el sector público vasco debe elaborar "sus respectivos planes de seguridad", pero no nos consta que tales planes se encuentren regulados en una norma sustantiva que defina su contenido y

características. El artículo 12 del ENS menciona la "política de seguridad de la información" como el instrumento que recoge el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.

216. Más complejo resulta llegar a una respuesta segura en el caso de las siguientes funciones: (I) prevenir y detectar incidentes de ciberseguridad en la Comunidad Autónoma de Euskadi y responder a ellos, estableciendo criterios y promoviendo el despliegue de las medidas de protección pertinentes ante las ciberamenazas y los riesgos inherentes sobre las infraestructuras tecnológicas, los sistemas de información, los servicios de las tecnologías de la información y la comunicación, y la información que estos tratan, todo ello con respeto del marco competencial aplicable (letra e); (II) ejercer las funciones de equipo de respuesta a emergencias (CERT) dentro de las competencias de la Comunidad Autónoma de Euskadi, incluyendo la relación y coordinación con otros organismos de ciberseguridad nacionales e internacionales con el objetivo de minimizar los daños y el tiempo de recuperación en caso de ciberataque (letra g); (III) coordinar los equipos de respuesta a incidentes de ciberseguridad (CSIRT) y equipos de respuesta a emergencias o entidades equivalentes que actúen en su ámbito de actuación y de acuerdo a la legislación vigente, estableciendo modelos de colaboración con otros CSIRT nacionales e internacionales. Asimismo, la Agencia ejercerá funciones de alerta temprana y de ayuda en la respuesta ante amenazas, vulnerabilidades, ataques e incidentes de seguridad en el ámbito del sector público vasco (letra h); e (IV) investigar y analizar tecnológicamente los ciberincidentes y ciberataques sobre infraestructuras tecnológicas, sistemas de información y servicios de tecnologías de la información (letra i).

217. Aunque suscitan dudas por la forma en que son descritas, estas pueden ser solventadas atendido el objeto dispuesto por el artículo 2.1 del anteproyecto, que predetermina dicho elenco, y las acotaciones incluidas en algunos casos —"todo ellos con respeto del marco competencial aplicable", "dentro de las competencias de la Comunidad Autónoma de Euskadi", "que actúen en su ámbito de actuación y de acuerdo con la legislación vigente"—, de forma que cabe interpretar que las infraestructuras tecnológicas, los sistemas de información y los servicios de las tecnologías de la información a las que se refiere son de titularidad de las entidades integrantes del sector público vasco.

218. Cabe decir que, en una primera aproximación, lo establecido en el anteproyecto no cercena las competencias de cada administración pública cuando se trate de incidentes que solo afectan a cada una de ellas, ni es incompatible con las obligaciones que impone a cada Administración pública el ENS. Tampoco lesiona

las funciones que en el caso de incidentes de seguridad se atribuyen al CCN-CERT o a la ENISA porque la Agencia, como equipo de respuesta emergencias (CERT) o coordinador de los equipos de respuesta a los incidentes de seguridad informática (CSIRT), constituidos en cada Administración, canalizará las medidas preventivas y reactivas a escala de la comunidad autónoma, proporcionando o coordinando la prestación de asistencia operativa especializada, cuando el incidente no tenga una escala nacional o europea.

219. En cualquier caso, se echa en falta un documento en el que se analice la congruencia de las funciones atribuidas a la Agencia en el marco regulatorio fijado por el ENS.

B) La ciudadanía y el tejido empresarial

220. Por lo que se refiere al ámbito privado, se trata de una actividad típica de fomento, conectada con las competencias que tiene la comunidad autónoma en materia de promoción, desarrollo económico y planificación de la actividad económica del País Vasco de acuerdo con la ordenación general de la economía (artículo 10.25 EAPV). Podrían también mencionarse de forma residual, dada la transversalidad de la ciberseguridad, las de comercio (artículo 10.27 EAPV), defensa del consumidor (artículo 10.28 EAPV) o industria (artículo 10.30 EAPV), entre otras, que dotarían de adecuado fundamento a tal labor encaminada a promover la ciberseguridad por parte de los particulares.

221. Como es sabido, con arreglo a la tipología clásica —policía, fomento y servicio público—, estamos ante una actividad administrativa de fomento con la que se incentiva y estimula, mediante ayudas económicas, subvenciones u otras medidas, el ejercicio de la actividad privada con la finalidad de orientarla a la consecución de determinados fines públicos o de interés general.

222. Es importante destacar que la Agencia no desarrolla una actividad administrativa de policía, con la que se restringe, de una forma u otra, la libertad, los derechos o la actividad misma de los particulares; ni una actividad administrativa de servicio público, mediante la que se prestan a los ciudadanos concretos servicios esenciales para la comunidad, ya que no se fija el régimen jurídico básico de ese servicio de ciberseguridad, esto es, la normativa propia del servicio que presta.

223. En este caso, al reparar en el listado del artículo 2.2 del anteproyecto, se hace eco de tal función su letra q): "Apoyar e impulsar la capacitación en materia de ciberseguridad y el desarrollo digital seguro en el ámbito empresarial y en los sectores esenciales de Euskadi, como son el sector sanitario, el sector de emergencias y seguridad, el sector de servicios sociales y de intervención social, el sector educativo, el sector del

transporte y el sector de la energía y las telecomunicaciones, o cualquier otro sector que pudiera considerarse sensible".

224. Hay que pensar que esa tarea de apoyo e impulso tiene por destinatarias a entidades privadas incluidas en tales sectores esenciales, siendo su intervención distinta, como se ha razonado, en el campo de las entidades del sector público vasco.

225. Es preciso añadir que, con arreglo a la propia lógica del anteproyecto, que limita la actividad de la Agencia a la actividad de fomento, no resulta congruente que en la exposición de motivos se justifique su creación en que el Centro Vasco de Ciberseguridad, por su forma jurídica, "no puede ejercer las funciones ni prestar el servicio público de ciberseguridad en Euskadi".

226. Por último, como ya hemos señalado anteriormente, la STC 142/2018 avala la posible colaboración de la Agencia con los organismos judiciales y policiales de acuerdo con los establecido por la normativa vigente.

227. Sin embargo, el artículo 2.4 del anteproyecto añade un contenido cuyo alcance resulta difícil vislumbrar. Dice el precepto:

> En el ejercicio de sus funciones, la Agencia debe coordinarse con los cuerpos policiales y de seguridad pública, sin perjuicio de las funciones propias del departamento competente en esta materia. En especial, la Agencia debe coordinarse con los cuerpos policiales para la ciberseguridad y protección de los sistemas de información policiales, de acuerdo con las competencias que dichos cuerpos tienen reconocidas en esta materia.

228. Según la STC 142/2018, la actuación de la Agencia en este ámbito sería meramente auxiliar y requeriría la solicitud expresa, bien de los cuerpos policiales, bien de las autoridades judiciales competentes, en los términos previstos en la legislación procesal.

V CONTENIDO DEL ANTEPROYECTO

229. Estudiaremos el anteproyecto siguiendo el orden de sus respectivos capítulos, formulando aquellas observaciones jurídicas que consideremos de interés.

A) Capítulo I: disposiciones generales

230. Por lo que se refiere al propio ente, a partir de su constitución como ente público de derecho privado del sector público de la Comunidad Autónoma de Euskadi,

con personalidad jurídica propia, que ajusta su actividad al ordenamiento jurídico privado, con plena capacidad de obrar para el cumplimiento de sus fines y con autonomía orgánica y funcional, adscrito al departamento competente en materia de seguridad a través de la persona titular de la Viceconsejería de Seguridad (artículo 1.1), adquiere esa naturaleza por ser calificado como tal, de manera expresa, en la ley que establece su creación, como requiere el artículo 44.1 de la LSPV.

231. En cuanto al contenido de la ley, el artículo 44.2 de la LSPV prevé el mínimo que debe tener el proyecto de ley de constitución de la entidad correspondiente.

232. En ese sentido, el capítulo I responde a las exigencias establecidas por las letras a) —la expresión de su personificación, naturaleza jurídica e identificación del departamento de la Administración general al que se adscribe—, b) —la denominación de la entidad y su sede— y c) —la finalidad e interés general al que obedece su creación y las funciones que se le encomiendan, con indicación expresa de las potestades administrativas que pueda ejercer—. Otra cosa es que sea correcta su plasmación, por los motivos que pasamos a exponer.

233. En el expediente tramitado ha suscitado dudas en la OCE la forma jurídica que debe adoptar la Agencia, atendido el principio de subsidiariedad fijado por el artículo 6.1 de la LSPV, por el que la constitución de entidades optará preferentemente por organismos autónomos, en segundo lugar, por entes públicos de derecho privado y solo en última instancia por entidades de forma privada, y la regla del artículo 6.5 de la LSPV, conforme a la cual, las entidades de nueva constitución adoptarán la forma jurídica que resulte más adecuada a la actividad y funciones que justifiquen su existencia, conforme a los principios regulados para cada una de ellas en esta ley.

234. Con arreglo al artículo 39.1 de la LSPV

> 1. Los entes públicos de derecho privado son aquellos entes institucionales de la Comunidad Autónoma de Euskadi de naturaleza pública, a los que se encomienda la prestación o gestión de servicios públicos o la producción de bienes de interés público susceptibles de contraprestación. Pueden ejercer potestades administrativas, excepto la expropiatoria, cuando les sean encomendadas en su norma de creación, en la que deberán identificarse los órganos del ente a los que les son atribuidas.
>
> 2. Los entes públicos de derecho privado se rigen en sus relaciones con terceros y en el desarrollo de su actividad por el derecho privado. Se rigen por el derecho

administrativo en el ejercicio de potestades administrativas, en su funcionamiento interno y en la formación de la voluntad de sus órganos, en las obligaciones derivadas en materia de transparencia y participación ciudadana, así como en las demás materias establecidas en esta u otras leyes que les sean de aplicación.

3. Los entes públicos de derecho privado tienen personalidad jurídica pública diferenciada de la Administración general. Disponen de los ingresos propios que obtengan en el desarrollo de su actividad y de los que les sean asignados en los presupuestos generales. Y desarrollan las funciones que tienen atribuidas con autonomía de gestión y empleando criterios de gestión empresarial y de gestión por objetivos orientados al bien común y al interés general conforme a los principios de sostenibilidad social y ambiental, conforme a lo establecido en esta ley.

4. Las potestades administrativas atribuidas a los entes públicos de derecho privado sólo pueden ser ejercidas por aquellos órganos de estos a los que los estatutos les asignen expresamente esta facultad. No obstante, a los efectos de esta ley, los órganos de los entes públicos de derecho privado no son asimilables en cuanto a su rango administrativo al de los órganos de la Administración general de la Comunidad Autónoma de Euskadi, salvo las excepciones que, a determinados efectos se fijen, en cada caso, en sus estatutos.

235. Examinadas las funciones de la Agencia, desde el doble ámbito ya analizado, la Comisión también constata que no se le encomienda "la prestación o gestión de servicios públicos o la producción de bienes de interés público susceptibles de contraprestación", sin que en sus relaciones con las administraciones públicas y su sector público y en la actividad de fomento con el tejido industrial y la ciudadanía pueda regirse por el derecho privado.

236. Las relaciones interadministrativas estás sujetas a principios enunciados por normas administrativas y deben encauzarse con instrumentos públicos, en este caso, fundamentalmente, por la estrategia de ciberseguridad que coordine la actividad de las administraciones públicas vascas y los acuerdos de colaboración con las diputaciones forales y entes locales de Euskadi.

237. Por otro lado, no va a disponer de ingresos propios obtenidos en el desarrollo de su actividad, ni obviamente tiene sentido que emplee criterios de gestión empresarial y de gestión por objetivos. Aunque el artículo 11.4.c) del

anteproyecto así lo prevé, el PAI ha descartado que pueda percibir ingresos como consecuencia de sus actividades.

238. Cabe recordar que el artículo 2.1 de la Ley 38/2003, de 17 de noviembre, General de subvenciones, entiende por subvención, a los efectos de esa ley, toda disposición dineraria realizada por cualesquiera de los sujetos contemplados en el artículo 3 de esa ley, a favor de personas públicas o privadas, y que cumpla los siguientes requisitos: a) que la entrega se realice sin contraprestación directa de los beneficiarios; b) que la entrega esté sujeta al cumplimiento de un determinado objetivo, la ejecución de un proyecto, la realización de una actividad, la adopción de un comportamiento singular, ya realizados o por desarrollar, o la concurrencia de una situación, debiendo el beneficiario cumplir las obligaciones materiales y formales que se hubieran establecido; y c) que el proyecto, la acción, conducta o situación financiada tenga por objeto el fomento de una actividad de utilidad pública o interés social o de promoción de una finalidad pública.

239. En parecidos términos, el artículo 48.2 del Texto refundido de la Ley de principios ordenadores de la hacienda general del País Vasco, aprobado por el Decreto Legislativo 1/1997, de 11 de noviembre (LPOHGPV).

240. De otro lado, conviene reconsiderar el tenor literal del artículo 1.4, *in fine*, ya que contempla que "la Agencia, en sus relaciones con el departamento al que se adscribe, se somete al derecho administrativo, en concreto, aquellas contenidas en las letras d), e), f), g), h), i), l), m), n), o), p) y r) del artículo 2.2, cuando se refieran al Sector Público de la Comunidad Autónoma de Euskadi".

241. En primer lugar, las relaciones de la Administración General con las entidades del sector público de la Comunidad Autónoma de Euskadi se someten al derecho administrativo, y el capítulo IV del título IV de la LSPV aborda tales relaciones, en particular en sus artículos 58, 59 y 60, que deben completarse con las previsiones establecidas en la propia ley que crea la Agencia, que traducen tales relaciones en reglas relativas a la composición y funciones del Consejo de Administración, designación y funciones de la Dirección general, composición y funciones del Consejo consultivo, recursos contra las resoluciones de los órganos de gobierno y estatutos de la Agencia.

242. Como dijo la STC 14/1986, de 31 de enero, "la instrumentalidad de los entes que se personifican o que funcionan de acuerdo con el Derecho Privado, remiten su titularidad final a una instancia administrativa inequívocamente pública, como público es también el ámbito interno de las relaciones que conexionan dichos entes con la Administración de la que dependen, tratándose en definitiva de la utilización por la Administración de técnicas

ofrecidas por el Derecho Privado, como un medio práctico de ampliar su acción social y económica".

243. En segundo lugar, salvo la incluida en la letra q) del artículo 2.2, en tales funciones y con respecto a todas las entidades incluidas en el sector público vasco, no solo del sector público de la Comunidad Autónoma de Euskadi, se somete a lo dispuesto en la propia ley, que es una norma administrativa y que es la que, precisamente, le atribuye tales competencias, y que ha de ejercerlas en el marco normativo administrativo de la ciberseguridad del que hemos dado cumplida cuenta y el que, en su caso, se apruebe por la Administración de la Comunidad Autónoma, tal y como anuncia el artículo 2.2.c) del anteproyecto.

244. En relación con dicha letra q) del artículo 2.2, igualmente deberá regirse por las normas que regulan la actividad subvencional porque, en el caso de que la ley de creación o las normas estatutarias atribuyan la potestad administrativa de fomento a los entes públicos de derecho privado, el artículo 48.5 de la LPOHGPV señala que deberán sujetarse a "lo dispuesto en los párrafos 3, 10, 11 y 12 del artículo 49, los párrafos 1, 2 y 3 del artículo 50, el párrafo 1 del artículo 51 y los párrafos 1, 2 y 3 del artículo 53. La aprobación de las bases reguladoras y la concesión de ayudas corresponderá a los órganos competentes conforme a los estatutos sociales o norma de creación de la entidad, y se garantizará la difusión de las citadas bases a través del Boletín Oficial del País Vasco".

245. No parece existir, en suma, una clara congruencia entre el objeto y funciones de la Agencia y la previsión incluida en el artículo 1.4 del anteproyecto, según la cual, la actividad de la Agencia se ajusta en sus relaciones externas a las normas de derecho civil, mercantil y laboral que le son de aplicación, salvo los actos que implican el ejercicio de potestades públicas, que se someten al derecho administrativo.

246. En cualquier caso, respecto a esa personificación de la Agencia como ente público de derecho privado, interesa de manera singular comprobar que se ha seguido el procedimiento general previsto en el artículo 44 de la LSPV para la constitución, transformación y extinción de entidades de la Administración institucional, previo cumplimiento de lo dispuesto en el artículo 43 para la constitución de entidades distintas de la Administración General de la CAPV, en especial, la previa elaboración de un plan de actuación inicial con el contenido mínimo que se indica. A ese respecto, el expediente da noticia de que se ha dado cumplimiento a tales previsiones.

247. La opción por la personificación de la Agencia como ente público de derecho privado corresponde, como dijimos en el Dictamen 43/2023, al poder del

legislador en ejercicio de su libertad de conformación de la configuración del ente.

B) Capítulo II: estructura orgánica

248. En este caso, se ha de dar respuesta a otras dos de las exigencias dispuestas para la ley de creación por el artículo 44.2 de la LSPV: sus órganos de gobierno y, si los hubiere, los que tengan encomendadas funciones consultivas, con expresión de su naturaleza unipersonal o colegiada, su composición, el procedimiento de designación de sus miembros y la distribución de funciones correspondientes a cada uno de los existentes (letra d); y las bases de su estructura orgánica y administrativa, así como los puestos directivos de la entidad, especificando las funciones que les sean encomendadas, con expresión del valor jurídico de sus actos o resoluciones e indicación, en su caso, de cuáles de ellos agotan la vía administrativa (letra e).

249. En cuanto a la adscripción de la Agencia y respecto a la composición del Consejo de Administración, debe advertirse la conveniencia —si no exigencia— de que se refleje adecuadamente la base competencial y el ámbito en el que la Agencia desplegará sus funciones, tal y como ha sido delimitado por la jurisprudencia constitucional, y que, en resumen, pivota de manera principal en torno a la actividad que sobre la Administración electrónica desarrollan las administraciones públicas vascas y sus sectores respectivos, y en menor medida en materia de seguridad pública.

250. Ello permitirá afianzar la factibilidad de la norma en el proceso de toma de decisiones y, por tanto, la consecución de los objetivos perseguidos con la constitución del nuevo ente.

251. Por otro lado, la determinación de los vocales representantes de las diputaciones forales y de las tres capitales de los territorios históricos no puede serlo en los términos recogidos por las letras d) y e) del artículo 4. En tanto que se trata de entidades adscritas, que dependen o vinculadas a la respectiva Administración territorial, es esta la que debe proponer o designar a los vocales que han de representarla, en ejercicio de sus potestades organizativas que conforman su autonomía institucional [disposición adicional primera CE y artículo 37.3.a) del EAPV y artículo 140 CE].

252. La ley no debe intervenir ni condicionar las funciones que, en el ámbito de la ciberseguridad, tales administraciones decidan atribuir a tales sociedades públicas o entidades de servicios informáticos, que están sujetas a las normas de creación correspondientes, ni menos, aún, reconocer una representación

oficial en tal materia a los directivos, presidentes o presidentas de sus consejos de administración.

253. En la relación de funciones del Consejo de Administración se echa en falta en el artículo 5 la de informar el proyecto de Estatutos con carácter previo a su aprobación por el Consejo de Gobierno en la primera sesión que celebre el referido órgano, tal y como señala el artículo 44.4 de la LSPV.

254. En cuanto a la evaluación, el artículo 5.g) atribuye al Consejo de Administración el seguimiento, supervisión y evaluación de la actuación de la Agencia y, en particular, el control de la gestión de la Dirección de la Agencia y la exigencia a esta de las responsabilidades que procedan. Por su parte, el artículo 6.3.f) incluye como funciones de la Dirección General de la Agencia la de presentar al Consejo de Administración las orientaciones generales de la planificación de la actividad de la Agencia, de su plan director y planes anuales, así como la propuesta de evaluación de sus resultados.

255. Parece oportuno recordar que resulta de aplicación a la Agencia el régimen de evaluación dispuesto por el capítulo II del título IV de la LSPV. En particular, con arreglo al procedimiento de evaluación que diseña el artículo 52 de la LSPV, cada una de las entidades del sector público de la Comunidad Autónoma de Euskadi deben elaborar anualmente un documento de evaluación, que ha de ser validado por la persona u órgano que desempeñe las funciones ejecutivas y de dirección superiores en la entidad y remitido al departamento de adscripción, que verificará su ajuste a las orientaciones generales que haya podido marcar respecto a la eficacia de las entidades dependientes del mismo.

256. Este, a su vez, lo remitirá al departamento competente en materia de administración pública para que, con el conjunto de la información recibida, elabore un informe general de evaluación del sector público, que será elevado al Consejo de Gobierno al efecto de su aprobación y remisión al Parlamento para su conocimiento.

257. En el artículo 6.1 del anteproyecto se dispone que la Dirección General de la Agencia será designada libremente por el Gobierno Vasco, a propuesta de la Presidencia del Consejo de Administración, que tendrá las potestades correspondientes para su contratación y separación, si procede.

258. Esa referencia final "que tendrá las potestades correspondientes para su contratación y separación, si procede" debe suprimirse al resultar equívoca, pues parece remitirse a un supuesto de relación laboral de carácter especial del personal de alta dirección, regulada por el Real Decreto 1382/1985, de 1 de agosto.

259. Con arreglo al artículo 13.4.d) de la LSPV, tienen la consideración de alto cargo de la Comunidad Autónoma de Euskadi: los presidentes y presidentas y los directores y directoras generales de organismos autónomos y de entes públicos de derecho privado.

260. Por su parte, el artículo 13.5 de la LSPV prevé que quienes sean altos cargos tendrán un régimen jurídico específico, iniciando su relación de servicio con el decreto de nombramiento y finalizando dicha relación por cese o dimisión, que producirán sus efectos a partir de la fecha de publicación del decreto correspondiente.

261. Con respecto al segundo contenido expuesto por el artículo 44.2.e) de la LSPV, no podemos sino constatar que se produce un cumplimiento insuficiente de dicha exigencia, pues deja sin precisar los órganos o puestos directivos de la entidad.

262. Según el artículo 14.1.c) de la LSPV, tiene la consideración de órganos directivos del sector público de la Comunidad Autónoma de Euskadi las direcciones generales, de área, de división o de cualquier otra denominación de la Administración General y entes institucionales, cuando expresamente tengan atribuida la consideración de órgano directivo o bien expresamente se califique a la persona titular de dicho órgano como personal directivo en la norma de creación del órgano.

263. En la estructura prevista, la nueva entidad integrará cuatro direcciones y todas ellas van ser operativas en el año 2023 —la Dirección de Estrategia de Ciberseguridad, la Dirección de Auditoria y Gobierno de Riesgo, la Dirección de Operaciones y Equipo de Respuesta y la Dirección de Ciudadanía y Empresas— , así como seis divisiones —de las que dos tendrán titular en este año—.

264. Sin que la ley los recoja, su catalogación como órganos directivos resultaría jurídicamente problemática porque a ese instrumento jurídico reserva la LSPV la determinación de las bases de su estructura orgánica y administrativa.

265. Se ha de puntualizar, asimismo, que esa determinación orgánica y asignación competencial correlativa no significa que no se puedan dar modificaciones, y ese es el sentido del artículo 44.4 de la LSPV, según el cual, "mediante decreto del Gobierno Vasco se podrán acometer todas aquellas reestructuraciones de la entidad, organismo autónomo o ente público de derecho privado que no alteren la naturaleza y finalidades legales establecidas en la ley de constitución, que recogerá expresamente esta posibilidad".

266. Esto es, el reglamento está autorizado a realizar tales reestructuraciones en los entes públicos de derecho privado, que pueden afectar a las atribuciones de competencias de los órganos que lo componen, pero precisamente esa flexibilización, la apertura a la regulación reglamentaria de los aspectos organizativos coyunturales, implica una previa fijación en la ley de su configuración organizativa básica y de las funciones esenciales de los órganos creados por aquella.

C) Capítulo III: régimen de personal, económico-financiero, patrimonial y de contratación, y disposición adicional

267. Las carencias iniciales del anteproyecto en esta materia han sido corregidas en la versión final, atendidas las sugerencias formuladas por los diferentes órganos que han intervenido en el procedimiento de elaboración del anteproyecto.

268. Lo mismo podemos decir respecto a la disposición adicional, que regula la cesión a la Agencia de los activos materiales y de personal y subrogación en los contratos y convenios.

269. Con ellos se da cumplimiento a otras dos exigencias establecidas por el artículo 44.2 de la LSPV, esto es, la identificación del régimen jurídico concreto que le resulte de aplicación en su caso en las materias relativas a su régimen económico-financiero y a sus recursos humanos (letra f), el personal y patrimonio que se adscribe a la entidad, así como los recursos económicos con que cuenta para el desarrollo de sus funciones (letra g).

270. A tenor del artículo 48 de la LSPV, las entidades integradas en el sector público de la Comunidad Autónoma de Euskadi se regirán por la presente ley, por las normas que les resulten de aplicación conforme a su naturaleza jurídica y por el conjunto normativo que forma el bloque de la legalidad que integra la hacienda general del País Vasco y el empleo público, con las especificidades que resulten necesarias según el tipo de entidad de que se trate.

271. Como dijimos en el Dictamen 132/2021, se encuentran disposiciones en materias propias de la hacienda general del País Vasco de expresa aplicación a los entes públicos de derecho privado en la LPOHGPV —artículo 29.2, sobre elaboración de anteproyecto de su presupuesto y 48.5, sobre actividad subvencional—; en la Ley 8/1996, de 8 de noviembre, de finanzas de la Comunidad Autónoma de Euskadi —artículos 35, sobre endeudamiento, y 51, sobre prestación de garantías—; en el Texto refundido de las disposiciones legales vigentes en materia de régimen presupuestario de Euskadi y se regula el régimen presupuestario aplicable a las fundaciones y consorcios del sector

público de la Comunidad Autónoma de Euskadi, aprobado por el Decreto Legislativo 1/2011, de 24 de mayo —artículos 51 y relacionados—; en el Texto refundido de la Ley de control económico y contabilidad de la Comunidad Autónoma de Euskadi, aprobado por el Decreto Legislativo 2/2017, de 19 de octubre (artículos 1.4 y 6.3, entre otros); y en el Texto refundido de la Ley de patrimonio de Euskadi, aprobado por el Decreto Legislativo 2/2007, de 6 de noviembre (artículo 1.1 y concordantes). Al contrario, la Ley 13/1998, de 29 de mayo, de tasas y precios públicos de la Administración de la Comunidad Autónoma del País Vasco (artículo 1.2), excluye de su ámbito los ingresos derivados de la prestación de servicios por este tipo de entes.

272. Y añadíamos que también se proyecta sobre su funcionamiento como norma transversal la Ley 10/1982, de 24 de noviembre, básica de normalización del uso del Euskera, y mencionábamos el Acuerdo de Consejo de Gobierno de 13 de abril de 2021, de los criterios de uso de las lenguas oficiales en la Administración General de la Comunidad Autónoma de Euskadi y en el resto de entidades que conforman el sector público adscrito a la misma (Resolución 22/2021, de 19 de abril, del Director de la Secretaría del Gobierno y de Relaciones con el Parlamento, BOPV nº 865, de 5 de mayo de 2021).

273. Ahora es preciso citar también la Ley 11/2022, de 1 de diciembre, de empleo público vasco, que es de aplicación al personal funcionario y, en lo que proceda, al personal laboral al servicio del sector público vasco.

274. Al margen de tales previsiones autonómicas, también son de aplicación las normas estatales que disciplinan la actividad de dichas entidades públicas cuando ejercen potestades administrativas, artículo 2.2.b) de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (LPAC), y artículo 2.2.b) de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público (LRJSP).

275. Así como las contenidas en la legislación de contratos del sector público, artículo 3.1.g) de la Ley 9/2017, de 8 de noviembre, de contratos del sector público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (LCSP).

276. Dicho esto, puede decirse que la Agencia debe ser considerada como un poder adjudicador a los efectos previstos en la legislación sobre contratación pública, circunstancia a la que se ve obligado a causa del artículo 3.3.d) de la LCSP.

277. A tenor del citado artículo 3.3.d) de la LCSP, son poder adjudicador "todas las demás entidades con personalidad jurídica propia distintas de las expresadas en las letras anteriores que hayan sido creadas específicamente para satisfacer necesidades de interés general que no tengan carácter industrial o mercantil, siempre que uno o varios sujetos que deban considerarse poder adjudicador de acuerdo con los criterios de este apartado 3, bien financien mayoritariamente su actividad; bien controlen su gestión; o bien nombren a más de la mitad de los miembros de su órgano de administración, dirección o vigilancia.".

278. En cuanto a la disposición adicional se refiere, podría sugerirse que en el caso del personal se recogiera expresamente, en un nuevo párrafo, que se integrará en las condiciones previstas en la Ley de presupuestos generales de la Comunidad Autónoma.

279. Esa remisión se vincula al contenido de la disposición adicional décima de la Ley 15/2022, de 23 de diciembre, por la que se aprueban los presupuestos generales de la Comunidad Autónoma de Euskadi para el ejercicio 2023 —previamente incluida también en ejercicios anteriores, p.ej., Ley 1/2021, de 11 de febrero, por la que se aprueban los Presupuestos Generales de la Comunidad Autónoma de Euskadi para el ejercicio 2021 o la Ley 11/2021, de 23 de diciembre, por la que se aprueban los Presupuestos Generales de la Comunidad Autónoma de Euskadi para el ejercicio 2022—.

280. Dicha disposición contempla lo siguiente:

> 1. En el supuesto de reorganizaciones administrativas que vengan producidas por cualesquiera planes, programas, actuaciones significativas, así como por disposiciones con rango de ley, el Gobierno podrá regular y disponer cuanto sea necesario en relación con la subrogación en las relaciones contractuales y en cuantos derechos y obligaciones de cualquier género se deriven de la creación, extinción o transformación de cualquier entidad del sector público y, en particular, sobre la adscripción e integración del personal a su servicio en otra entidad del sector público, de conformidad con la legislación laboral o de función pública que le sea aplicable.
>
> 2. A tales efectos, el Consejo de Gobierno, a propuesta de los departamentos competentes en materia de presupuestos y de función pública, podrá autorizar la modificación de las plantillas presupuestarias y la creación de nuevas dotaciones de personal en las entidades del sector público de la Comunidad Autónoma de Euskadi siempre que se proceda a la consiguiente amortización

de las dotaciones necesarias en otras entidades del sector público de manera que no represente superior coste anual bruto.

281. Por el contrario, la inclusión de dicha remisión en el artículo 13, que constituye el último precepto del capítulo III del anteproyecto, a la Ley de presupuestos no cumple lo previsto en el artículo 44.2.h) de la LSPV, que requiere otro contenido, pues forma parte del mínimo que debe incluir la ley de constitución del ente "el procedimiento de extinción y liquidación de la entidad".

282. Es cierto que sobre la extinción existen previsiones en el propio artículo 44.6 de la LSPV y sobre todo en el artículo 55 de la LSPV.

283. De un lado, conforme al artículo 44.6 de la LSPV, la extinción se realizará por ley o por decreto del Gobierno Vasco, siempre que se acredite que la misma ha cumplido la finalidad de su creación o que concurre cualquier otra causa tasada y así prevista expresamente en la ley.

284. De otro lado, el artículo 55.1de la LSPV parece decantarse únicamente por la Ley, "conforme al procedimiento y requisitos que se establezcan en la legislación aplicable", lo que induce a pensar en un régimen común y no en un régimen establecido en cada ley de creación del ente.

285. La ley de extinción, por otra parte, regulará "las medidas relativas al régimen de personal, patrimonio, sucesión en los derechos y obligaciones de la entidad y requisitos para su liquidación económico-financiera", y será en el procedimiento de elaboración de dicha ley en el que, "además de motivarse los aspectos específicos que concurran para la extinción de la entidad, habrán de analizarse sus efectos sobre el conjunto del sector público de la Comunidad Autónoma de Euskadi en cuanto a la racionalización y coherencia de su organización y estructura resultante, de conformidad con los principios generales de actuación como sujetos integrantes del sector público y principios aplicables para la creación de nuevas entidades o participación en otras ya existentes, establecidos en esta ley".

286. De todo ello cabe pensar que la ley podrá introducir reglas específicas respecto al ente que crea y, en todo caso, en el procedimiento de elaboración de la ley de extinción y liquidación del ente, además de esa exigencia de motivación y análisis de efectos, se deberán recabar los informes precisos para que pueda pronunciarse sobre tales medidas y requisitos, lo que podría precisar el anteproyecto que nos ocupa.

VI TÉCNICA NORMATIVA

287. De acuerdo con las Directrices para la elaboración de proyectos de Ley, decretos, órdenes y resoluciones, aprobadas por acuerdo del Consejo de Gobierno de 23 de marzo de 1993, y con otras consideraciones, convenientes a fin de mejorar la calidad del producto normativo, cabe efectuar las siguientes observaciones.

288. En la parte expositiva se recomendaría evitar incluir las referencias a la competencia en materia de seguridad o, cuando menos, hacerlo después de recoger las del artículo 10.2 EAPV, en materia de organización, régimen y funcionamiento de sus instituciones de autogobierno dentro de las normas del presente Estatuto, artículo 10.4 del EAPV en materia de régimen local y artículo 10.24 del EAPV en materia de sector público propio del País Vasco.

289. Incluso podría citarse la STC 142/2018, de 20 de diciembre, que reconoce las competencias de la Comunidad Autónoma en materia de autoprotección del sector público autonómico, de sus redes interdependientes e infraestructuras de la información, tanto internamente como en sus relaciones con los administrados y con otras administraciones o entidades públicas.

290. Para la labor de apoyo e impulso en la capacitación en ciberseguridad y el desarrollo digital seguro en el ámbito empresarial, podría resultar suficiente con citar el artículo 10.25 del EAPV, que reconoce la competencia autonómica en materia de promoción, desarrollo económico y planificación de la actividad económica del País Vasco de acuerdo con la ordenación general de la economía.

291. La cita de la LSPV debe ser completa en el artículo 2.1 del anteproyecto, con inclusión de la denominación oficial de la ley, "del sector público vasco".

292. La acotación final del artículo 6.h) del anteproyecto —"y demás normas relativas a su organización y funcionamiento"— resulta innecesaria porque precisamente es en los estatutos donde se regula tal contenido, como lo acredita el artículo 9 del anteproyecto.

293. El orden de los conceptos "extinción" y "disolución" debe ser el mismo en el nombre del artículo 13 y en su texto.

294. La disposición final segunda se refiere a la "disposición adicional primera", cuando la disposición adicional no tiene número.

CONCLUSIÓN

La Comisión dictamina que, una vez consideradas las observaciones formuladas en el cuerpo del presente dictamen, puede elevarse al Consejo de Gobierno para su aprobación el anteproyecto de ley de referencia.

Lo que certifico en Vitoria-Gasteiz, en la fecha de la firma, con el visto bueno del Presidente, para su conocimiento y consideración, recordándole la obligación prevista en el artículo 30.2 de la Ley 9/2004, de 24 de noviembre, de comunicar a esta Comisión la disposición o resolución que finalmente se adopte, en la forma y plazo que se establecen en el artículo 34 del Reglamento de organización y funcionamiento (aprobado por Decreto 167/2006, de 12 de septiembre).

	Vº Bº:
Jesús María Alonso Quilchano,	Sabino Torre Díez,
Secretario	**Presidente**

Firmado electrónicamente