INFORME DE LEGALIDAD SOBRE EL PROTOCOLO GENERAL DE ACTUACIÓN ENTRE LOS GOBIERNOS DE NUEVA-AQUITANIA, NAVARRA Y EUSKADI PARA EL FOMENTO CONJUNTO DE LA CIBERSEGURIDAD.

70/2022 IL – DDLCN
NBNC_PRO_3149/22_04

I. INTRODUCCIÓN.

La Dirección de Tecnologías de la Información y la Comunicación solicita, a la Dirección de Desarrollo Legislativo y Control Normativo, el informe de legalidad sobre el proyecto de Protocolo General enunciado. Se incluye en el expediente la siguiente documentación:

1. Memoria justificativa del mismo.
2. Borradores en euskera y castellano del texto del proyecto de Protocolo General.
3. Propuesta de Acuerdo del Consejo de Gobierno de toma de conocimiento.

Se emite el presente informe en virtud de lo dispuesto en el artículo 5.1 b) y f) de la Ley 7/2016, de 2 de junio, de Ordenación del Servicio Jurídico del Gobierno Vasco y el artículo 13.2 del Decreto 144/2017, de 25 de abril, del Servicio Jurídico Central del Gobierno Vasco.

Igualmente, hay que tener en cuenta lo dispuesto en el artículo 7.1. i) 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 15.1 a) 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.

Se echa en falta en el expediente alguna documentación relevante, incluyendo algunos informes preceptivos tales como el Informe justificativo de la ausencia de contenido económico, el Informe Jurídico departamental, el pronunciamiento de la Dirección de Acción Exterior o documentación referente a la capacidad y legitimidad de las otras partes signatarias, entre otras.

- Conviene recordar que, en los últimos años, tanto el Tribunal Supremo han insistido en la importancia de las memorias para explicar el contenido y efectos de las normas y actos, especialmente en su dimensión económica. Desde la sentencia de 27 de noviembre de 2006 (recurso número 51/2005), la jurisprudencia explica que las memorias sirven para proporcionar al titular de la potestad reglamentaria u órgano decisor «información sobre los costes que las medidas adoptadas puedan

suponer a fin de que, contraponiendo estos con las ventajas que aquellas han de representar, evidenciadas en la memoria justificativa, la decisión se adopte con conocimiento de todos los aspectos, tanto negativos como positivos". Por este motivo, se ha llegado a anular normas y convenios por insuficiencia de las memorias que las acompañaban [entre otras, sentencias de diciembre de 2011 (rec. 6507/2009); 18 de junio de 2012 (rec. 6513/2009); 2 de diciembre de 2016 (rec. 903/2014); 22 de marzo de 2018 (rec. 458/2016); 15 de marzo de 2019 (rec. 618/2017)], siendo por tanto muy recomendable que la documentación indicada se incorpore lo antes posible al expediente.

II. LEGALIDAD

1.- Ciberseguridad. Concepto y competencia.

El Estatuto de Autonomía de la Comunidad Autónoma del País Vasco nada refiere en lo que respecta a la ciberseguridad, siendo ésta, como es, una materia relativamente reciente y muy dependiente de avances tecnológicos de corta data. Lo cual no implica que dicha materia no tenga cabida entre las competencias autonómicas, en función de la interpretación y adaptación de las normas competenciales al tiempo en que han de ser aplicadas.

Para analizar el sistema competencial de la ciberseguridad en nuestro ordenamiento, una referencia ineludible es el pronunciamiento del Pleno del Tribunal Constitucional en su *Sentencia 142/2018, de 20 de diciembre de 2018, en el Recurso de inconstitucionalidad nº 5284/2017 e interpuesto contra la Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña.*

Así en el Fundamento Jurídico 4º, tras relacionar diversas definiciones posibles de ciberseguridad, y en especial la establecida en la Directiva (UE) 2016/1148, de 6 de julio, del Parlamento Europeo y del Consejo, y luego de exponer también diversa normativa de ámbito estatal, y respecto de su posible subsunción por vía interpretativa en diversos títulos estatales, en su párrafo final viene a manifestar que: «*Atendiendo a lo que se ha expuesto, puede concluirse que la ciberseguridad se incluye en materias de competencia estatal en cuanto, al referirse a las necesarias acciones de prevención, detección y respuesta frente a las ciberamenazas, afecta a cuestiones relacionadas con la seguridad pública y la defensa, las infraestructuras, redes y sistemas y el régimen general de telecomunicaciones.*»

Corolario de esto, concluye también la Sentencia del Tribunal Constitucional que el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, se dicta «al amparo de las competencias estatales de los artículos 149.1.21 y 149.1.29 CE (disposición final primera)».

También este mismo Fundamento Jurídico 4º de la Sentencia refiere, por lo que se refiere a las competencias de las Comunidades Autónomas lo siguiente:

a) Que es competencia de las Comunidades Autónomas la relacionada con la adopción de medidas ordinarias de prevención o seguridad de la red y, en general, de las

tecnologías de la información. En particular, respecto a la administración electrónica, garantizando la protección de las redes de comunicaciones electrónicas que esta genere y la protección de los derechos de los administrados en sus relaciones con las administraciones públicas a través de medios electrónicos. No discute el Abogado del Estado, que las Comunidades Autónomas pueden, al amparo de las competencias que sus Estatutos de Autonomía les reconocen, adoptar determinadas medidas dirigidas a garantizar la protección de sus infraestructuras y la seguridad de las tecnologías de la información y la comunicación. Medidas en este ámbito que, en muchas ocasiones, vienen reclamadas por las propias normas estatales (así, por ejemplo, el Real Decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad en el ámbito de la Administración electrónica, dictado en desarrollo del derogado artículo 42.2 de la Ley 11/2007).

Es decir, las Comunidades Autónomas tienen competencia para adoptar medidas en materia de ciberseguridad en tanto en cuanto se aplican a las relaciones que tiene con sus administrados y con otras administraciones, así como respecto de las infraestructuras tecnológicas, que pertenezcan a la estructura de la Administración autonómica y a su sector público.

b) La Estrategia de Seguridad Nacional 2017, aprobada por Real Decreto 1008/2017, de 1 de diciembre, que es el marco de referencia para un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, en la colaboración público-privada, y en la participación de la ciudadanía, fija seis objetivos específicos, el primero de los cuales y dirigido a las administraciones públicas es el de garantizar que los sistemas de información y telecomunicaciones utilizados poseen el adecuado nivel de seguridad y resiliencia;

c) Finalmente, y en aras de la brevedad, el Fundamento Jurídico 7º de la STC nº 142/2018, de 28 de diciembre interpreta el bloque constitucional en relación con las posibles competencias de las Comunidades Autónomas en materia de ciberseguridad «*entendida como la seguridad de las redes de comunicaciones electrónicas y de los sistemas de información*», al entender que las propias normas estatales *«… presuponen facultades autonómicas en ámbitos relacionados con la ciberseguridad, [así, por ejemplo, artículos 5 d), 10 y 15 de la Ley 8/2011 y artículos 6, 11, 27.3 y disposición adicional tercera de la Ley 36/2015],,,,»*

Y aun concreta más, estas competencias en el apartado i) este Fundamentos Jurídicos 7º.b)

Así, considera que las Comunidades Autónomas sí tienen competencia, tanto en lo que respecta a las funciones de asesoramiento a sus Gobierno en materia de ciberseguridad, como en la elaboración y ejecución de planes de ciberseguridad «*en relación con sus propias redes y sistemas de telecomunicaciones teniendo presente la necesidad de proteger sus comunicaciones electrónicas*», pues se relacionan con la competencia autonómica relativa a los medios necesarios para el ejercicio de las facultades de autoorganización y de su propia gestión administrativa, todo más si estas están relacionadas con funciones de administración electrónica. Son expresión de la aplicación de previsiones contenidas en normas estatales en materia de administración electrónica (arts. 1.2, 5, 12 a 30, 33 y 34 del Real Decreto 311/2022, de 3 de mayo), de seguridad nacional (arts.

10, 11, 27.3 y disposición adicional tercera de la Ley 36/2015) y de infraestructuras críticas [arts. 2 d), e) y f); 10 y 15.2 de la Ley 8/2011].

El propio Tribunal Constitucional reconoce que la ciberseguridad no es un concepto o materia reconducible a un único título competencial, sino que «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)

Estas medidas de organización y protección no se discutieron en el recurso de inconstitucionalidad, sino que quedaron expresamente excluidas, lo que ha provocado algunas dudas sobre los exactos márgenes del concepto de «seguridad pública» que, en principio, resulta de competencia exclusiva del Estado, pero que concurre con el reconocimiento de las competencias autonómicas en materia de ciberseguridad vinculadas a la competencia en materia de seguridad pública estatutariamente reconocida a la Comunidad Autónoma Vasca, y que van más allá de la creación de la policía de seguridad propia. Nos estamos refiriendo, por ejemplo, a aquellas competencias normativas autonómicas (vascas y navarras) necesarias para regular la investigación y el análisis de los ciberataques, por tratarse de una función directamente conectada con la protección de la seguridad de las tecnologías de la información y la seguridad pública, como funciones que han de realizar, por ejemplo, la Ertzaintza o la Policía Foral.

Asimismo, las competencias de coordinación con otros organismos en el *desarrollo de los planes de ciberseguridad y la organización de actividades de difusión, formación y concienciación dirigidas a diferentes colectivos* son medidas de fomento que las Comunidades Autónomas pueden llevar a cabo en su propio ámbito de competencias, y que «*no puede entenderse que perturben o menoscaben el ejercicio de las competencias estatales en materia de seguridad pública o de telecomunicaciones*».

Entendido en este contexto de carácter técnico u organizativo y orientado a garantizar la protección de sus infraestructuras y la seguridad de las tecnologías de la información y la comunicación de las Administraciones Publicas en el ámbito competencial funcional y territorial de cada Comunidad Autónoma, consideramos que nada obsta desde una perspectiva competencial para que la Comunidad Autónoma de Euskadi pueda promover la firma del protocolo que se pretende suscribir.

2.- *Objeto, justificación y marco normativo*.

Tal y como se expone en la documentación adjunta, la Región de Aquitania, Euskadi y Navarra son comunidades limítrofes y con intereses comunes en numerosos sectores, lo que conlleva que, en determinadas materias, la colaboración sea imprescindible.

Fruto de esa cooperación es la creación de la Euroregión Nueva-Aquitania Euskadi Navarra, entidad con personalidad jurídica propia, que adopta la forma de una Agrupación Europea de Cooperación Territorial (AECT), de acuerdo con el mencionado Reglamento (CE) 1082/2006, con el

fin de profundizar en la cooperación entre las regiones que la constituyen y contribuye a la creación de un gran espacio de relaciones, de intercambios y proyectos comunes en Europa.[1]

Dentro de este marco y en referencia a la ciberseguridad, tal y como se expone en la exposición del proyecto de Protocolo General, resulta conveniente aunar esfuerzos para la realización de actuaciones comunes, para analizar y determinar la estrategia de ciberseguridad en el sector público de dichas regiones

El proyecto de protocolo analizado pretende aunar estos esfuerzos en la elaboración y ejecución de esas estrategias de ciberseguridad, así como el diseño de cómo organizar la coordinación o la gestión de la respuesta que pueda resultar necesaria ante crisis de ciberseguridad en tales casos.

Todo ello, siempre, en el marco jurídico de las competencias de cada una de ellas y para el conjunto del sector público de dichas comunidades, siendo la directriz de su ejecución la cooperación y colaboración en el análisis y diseño de estrategia y sistemas organizativos de sus servicios públicos, en un concepto amplio y trasversal de la ciberseguridad.

Este objeto esta descrito en la estipulación Primera del proyecto de Protocolo y es conforme al marco jurídico competencial y normativo antes expuesto.

3.- *Naturaleza jurídica del protocolo*.

Hemos de reiterar que el proyecto de Protocolo General tiene marco institucional dentro de la Euroregión Nueva-Aquitania Euskadi Navarra.

En este orden de cosas, conviene traer a colación el artículo 47.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece lo siguiente en su párrafo segundo:

> *«No tienen la consideración de convenios, los Protocolos Generales de actuación o instrumentos similares que comporten meras declaraciones de intención de contenido general o que expresen la voluntad de las Administraciones y partes suscriptoras para actuar con un objetivo común, siempre que no supongan la formalización de compromisos jurídicos concretos y exigibles».*

En el mismo sentido, el artículo 54.2 del Decreto 144/2017, de 25 de abril, del Servicio Jurídico del Gobierno Vasco, reitera que:

> *"En todo caso, no tienen la consideración de Convenios, los Protocolos Generales de Actuación o instrumentos similares que comportan meras declaraciones de intención de contenido general o que expresen la voluntad de*

[1] Sobre el régimen jurídico de esta Euroregión, competencias y funciones nos remitimos al informe emitido por esta Dirección referido a la Adhesión de la Comunidad Foral de Navarra a ella 27/2016 IL - DDLCN

las Administraciones y partes suscriptoras para actuar con un objetivo común, siempre que no supongan la formalización de compromisos jurídicos concretos y exigibles".

Acorde con su naturaleza, la *Cláusula Séptima* del proyecto de Protocolo, reguladora de su régimen jurídico, recoge en su párrafo segundo que *«… es un instrumento que comporta meras declaraciones de* intención *de contenido general y que expresa la voluntad de las Administraciones y partes suscriptoras para actuar con un objetivo común.»*

4.- Estructura y contenido.

En cuanto a su estructura, el protocolo de colaboración que se somete a nuestra consideración consta de un encabezamiento (en el que se identifican los firmantes del protocolo); seis clausulas expositivas; y siete cláusulas operativas: «*Objeto», «Intenciones de las partes», «Servicios», «Duración de protocolo general de actuación», «Comité de seguimiento», «Modificación y resolución»* y *«Régimen jurídico legal».*

Por lo demás, teniendo en cuenta los objetivos planteados en el protocolo, resulta evidente la capacidad legal de las partes para suscribirlo, así como la existencia de un fin común de interés público que vincula a las partes en su formal y expreso deseo de colaboración.

Desde la perspectiva material, analizado el contenido del protocolo, debemos destacar las siguientes propuestas, que, en ningún caso, suponen una tacha de legalidad.

La *Cláusula Tercera*, lleva por título «*Servicios*», lo cual resulta un tanto desajustado o críptico, pues esta *Cláusula* comienza refiriendo «*Se procurará poner en marcha las siguientes actuaciones…».*

Sin embargo, en esta misma *Cláusula Tercera* el párrafo segundo dice: «*Los servicios de seguridad necesarios y prioritarios para hacer frente a las amenazas de la situación actual son los siguientes: ...»,* lo cual da una apariencia de incongruencia o corte en el relato.

Por ello, quizás sería conveniente sustituir tales redacciones por las siguientes:

«TERCERA.- Áreas de actuación y Servicios de interés».

Y el párrafo segundo antes referido, quizás pudiera ser redactado con un contenido parecido a lo siguiente:

«Se considerarán servicios de seguridad necesarios y prioritarios sobre los que cooperar para hacer frente a las amenazas a la ciberseguridad los siguientes:

Respecto de la *Cláusula Cuarta* «Duración del protocolo general de actuaciones», se ha de señalar que ni en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ni en el Decreto 144/2017, de 25 de abril, del Servicio Jurídico del Gobierno Vasco, por lo tanto, establecen

un límite temporal a la duración de los protocolos, como sí se hacen en los convenios. Por lo cual, y si ponemos esto en relación con la *Cláusula Sexta* referida a «*Modificación y resolución*» y al propio carácter no obligacional del Protocolo General, tal precepto, aunque perfectamente posible, resulta extraño. Su conclusión o prórroga sólo depende de la voluntad manifestada de una o todas las partes. Esta Cláusula (quizás fruto de la costumbre de las redacciones de los Convenios de Cooperación) reflejando término no resulta relevante en el contenido del proyecto de Protocolo.

La *Cláusula Séptima* «Régimen Jurídico» refiere que el Protocolo «no tiene naturaleza administrativa» algo que a nuestro parecer no es jurídicamente preciso.

En efecto, y sin entrar en honduras, el presente protocolo refiere declaraciones de intenciones de contenido general y no tiene «*compromisos jurídicos concretos y exigibles*», de ello deriva que no sea un Convenio administrativo de los establecidos en los artículos 47 a 53 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Pero ello no implica que no sea un acto de la Administración, y que por tanto tenga naturaleza administrativa. De hecho, se regula en dicha Norma, pero no se excluye de ella.

Por otra parte, y sólo es una cuestión de estilo, pero el considerar el Proyecto de Protocolo «*Simplemente un instrumento…*» y dado el rango de la y los signatarios y las instituciones que representan, en el parecer de quien esto suscribe no resulta cuando menos elegante.

Por ello, se propone reformular la redacción de esta Cláusula Séptimo por otra ya muy habitual en otros Protocolos redactados en esta Administración:

> *«El presente instrumento tiene naturaleza administrativa y expresa la voluntad de las partes suscriptoras para actuar con el objetivo común expresado en la cláusula primera, no suponiendo en ningún caso la formalización de compromisos jurídicos concretos y exigibles al amparo de lo dispuesto en el artículo 47 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público»*.

5.- Régimen de tramitación.

Tal y como relata la Memoria departamental, a la que me remito para evitar reiteraciones innecesarias, conforme a los artículos 55.3 y 57.2 del Decreto 144/2017, tanto el memorando, como los protocolos y acuerdos no normativos, no requieren de la autorización previa del Consejo de Gobierno, al que sólo le compete conocer del texto a suscribir (o ya suscrito, aunque sólo si estuviera en la excepción del 63.2 que permite la suscripción antes de pasar por Consejo de Gobierno).

Desde la perspectiva de que este proyecto de Protocolo puede afectar a la esfera internacional, procede advertir la incidencia que pueda tener en la iniciativa que informamos la regulación, de nivel estatal, contenida en la Ley 2/2014, de 25 de marzo, de la Acción y del Servicio Exterior del Estado; así como, fundamentalmente, en la Ley 25/2014, de 27 de noviembre, de Tratados y otros Acuerdos Internacionales.

Al respecto, entendemos, nos encontramos ante el supuesto recogido en el artículo 2 c) de la Ley 25/2014, así como en el artículo 11.4 de la Ley 2/2014. Esto es, puede calificarse sin dificultad el presente como un «*acuerdo internacional no normativo*», a celebrar por un órgano de una Comunidad Autónoma, en este caso de la CAPV, con un órgano análogo de otro sujeto de derecho internacional (la Euroregión y Nueva Aquitania), tratándose efectivamente de un acuerdo que no genera obligaciones jurídicas, para los Estados a los que pertenecen, en tal ámbito del Derecho internacional.

Consecuentemente con ello, y en el ámbito procedimental externo a la CAPV, también se habrá de proceder a la correspondiente tramitación ante el Ministerio de Asuntos Exteriores y Cooperación, conforme a las previsiones establecidas en el Título IV de dicha Ley 25/2014, de 27 de noviembre, entre las que se incluye la remisión del proyecto para su informe –que habrá de emitirse en el plazo de diez días–, así como la remisión de una copia ya firmada para su inscripción en el correspondiente registro administrativo.

No podemos finalizar sin señalar las obligaciones establecidas en el *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información,* con especial incidencia en referente a los CSIRT (Computer Security Incident Response Team)[2] de referencia y los operadores de servicios esenciales.

III. CONCLUSIONES

Siendo lo expuesto cuanto cabe informar respecto de la documentación remitida, se informa favorablemente el proyecto de protocolo objeto de este informe.

Este es el informe que emito y someto a cualquier otro mejor fundado en derecho,

En Vitoria-Gasteiz, a 22 de junio de 2022.

[2] El término protegido CERT (Computer Emergency Response Team) está registrado en EE.UU.