FACULTAD DE DERECHO

LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS EN LA UE: ¿CIBERSEGURIDAD AL RESCATE?

Autor: Isabel Marco Clement
5º E-3 B
Derecho Internacional Público

Tutor: Susana De Tomás Morales

Madrid
Abril 2017

RESUMEN

La protección de las infraestructuras críticas se constituye en pieza angular de las políticas nacionales y supranacionales de la Era de la Información, toda vez que proveen los servicios esenciales para la subsistencia de las sociedades. En este contexto, el presente trabajo aborda las previsiones europeas encaminadas a la identificación de estas infraestructuras, en la medida en que esta etapa es condición necesaria para la aplicación de las medidas protectoras. En vista de las fallas que presenta la normativa en materia de infraestructuras críticas, el trabajo pone de manifiesto cómo la reciente directiva dirigida a la seguridad de las redes y sistemas de información viene a complementar, *de facto*, la protección de aquellas entidades que prestan servicios esenciales para la población. La amenaza que supone la pertenencia de las infraestructuras a la Era Digital se torna, gracias a la nueva directiva, en fuente de garantías adicionales.

Palabras clave: Infraestructuras Críticas, Ciberseguridad, Unión Europea, Directiva 2008/114/CE, Directiva NIS.

ABSTRACT

Protecting critical infrastructures is a cornerstone of national and supranational policies of the Information Era. In fact, critical infrastructures are known for providing the most essential services of our societies. In this context, the present paper examines the European legal provisions aimed at identifying critical infrastructures, for this stage is a necessary condition for the implementation of security measures. In view of the shortcomings identified in critical infrastructures' regulation, this paper goes on revealing how the recent European directive on network and information security has proven to complement, in practice, the protection of those entities that provide essential services. The inherent threat of belonging to the Digital Era has become, thanks to the new directive, a source of further guarantees for critical infrastructures.

Key words: *Critical Infrastructures, Cybersecurity, European Union, Directive 2008/114/CE, Directive NIS.*

ÍNDICE DE CONTENIDOS

LISTADO DE ABREVIATURAS

CSIRT	Equipos de respuesta a incidentes
ENISA	Agencia Europea de Seguridad de las Redes y de la Información
IC	Infraestructura(s) Crítica(s)
ICE	Infraestructura(s) Crítica(s) Europea(s)
PEPIC	Programa Europeo de Protección de las Infraestructuras Críticas
RSI	Redes y sistemas de información
TIC	Tecnologías de la Información y Comunicación
TJ	Tribunal de Justicia
TJUE	Tribunal de Justicia de la Unión Europea
TUE	Tribunal de la Unión Europea
UE	Unión Europea

1. INTRODUCCIÓN

1.1. Objeto de estudio

"Los servicios esenciales para la sociedad son proporcionados en su mayor parte por instalaciones, redes o sistemas que se han dado en llamar por la comunidad internacional infraestructuras críticas (IC)"[1].

Tal y como subraya SÁNCHEZ GÓMEZ, las infraestructuras críticas han cobrado un protagonismo sin precedentes en las sociedades del siglo XXI. Ciertamente, los recientes ataques y sucesos catastróficos a los que se han visto sometidas han puesto de manifiesto su inmensa dependencia de una serie de servicios considerados esenciales. Los ataques contra el *World Trade Center* en septiembre de 2001 o los atentados de 2004 contra la red de Cercanías de Madrid atestiguan de la necesidad de protegerse con instrumentos fuertes y eficaces[2]. En consecuencia, tanto los gobiernos como las organizaciones supranacionales vienen desarrollando, en los últimos años, estrategias de seguridad enfocadas a la protección de estas infraestructuras críticas (en adelante, IC) y, en el mismo sentido, florece abundante legislación en la materia[3].

Pues bien, a la hora de abordar la protección de las infraestructuras críticas, resulta esencial tener presente el contexto en que éstas se desenvuelven.

El término "ciberespacio" fue acuñado por WILLIAM GIBSON, escritor de ciencia ficción, en el contexto de un relato breve que vio la luz en el año 1982. Su creación literaria resultó sorprendentemente profética, erigiéndose hoy como la forma con que se designa al conjunto de aparatos informáticos, redes, cables de fibra óptica, y demás infraestructuras que llevan el internet a miles de millones de personas de todo el mundo[4].

---

[1] SÁNCHEZ GÓMEZ, F.J., "Las políticas de protección de infraestructuras críticas en España", *Seguridad y Ciudadanía: Revista del Ministerio del Interior*, n.11, 2014, p.15 (disponible en http://www.interior.gob.es; última consulta 6/02/2017).

[2] MIRANZO, M. y DEL RÍO, C., "La protección de infraestructuras críticas", *UNISCI Discussion Papers,* n.35, 2014, pp.339-340 (disponible en https://www.ucm.es/data/cont/media/www/pag-72481/UNISCIDP35-17DELRIO-MIRANZO.pdf; última consulta 2/02/2017).

[3] SÁNCHEZ GÓMEZ, F.J., *op. cit.*, nota 1.

[4] GILES, M., "Defending the digital frontier", *The Economist (Special Report on Cyber-Security)*, pp.1-2 (disponible en http://www.economist.com/sites/default/files/20140712_cyber-security.pdf; última consulta 8/03/2017).

Las miríadas de conexiones forjadas por estas tecnologías han aportado inmensos beneficios en muchos sentidos, pero este extraordinario invento también tiene un lado oscuro. Así, las violaciones de datos son cada vez más sustanciales y acontecen con mayor frecuencia. Entre las víctimas más recientes se encuentra el gigante minorista Target, que sufrió el robo de millones de ficheros digitales relativos a sus clientes, con el detalle de sus tarjetas de crédito y débito. El daño potencial, sin embargo, se extiende más allá de las incursiones comerciales. Tal y como revela el caso Snowden, los propios Estados y los organismos que de ellos dependen también están en el punto de mira de esta clase de ataques. La protección del ciberespacio –o ciberseguridad- es difícil, puesto que la arquitectura de internet fue concebida para promover la conectividad, no la seguridad. En un mundo en el que millones de personas encienden a diario sus ordenadores para hacer operaciones bancarias, comprar en comercios virtuales, intercambiar informaciones en las redes sociales y enviar todo tipo de datos delicados a través de la web, las amenazas crecen a pasos agigantados en número, formas y sofisticación. En este contexto, los gobiernos han comenzado a tomar conciencia de los peligros que imperan y, haciendo honor a la labor que se les ha encomendado, se han implicado activamente en la materia[5].

Sin ir más lejos, la Estrategia de Seguridad Nacional del gobierno español[6], afirma que "*el ciberespacio es hoy el ejemplo más claro de un ámbito accesible, poco regulado y de difícil control*", a la par que consagra la ciberseguridad como temática protagonista del documento. Asimismo, es tal la importancia que está cobrando la ciberseguridad en nuestras vidas que no sólo se erige en gran preocupación de las autoridades nacionales, sino también –y por su carácter transnacional- de los organismos supranacionales, entre ellos la Unión Europea. En una de sus comunicaciones[7], en efecto, la Comisión declara que "*los derechos fundamentales, la democracia y el Estado de Derecho deben ser protegidos en el ciberespacio*" así como que "*la libertad en línea requiere también protección y seguridad*". En este sentido, los organismos europeos vienen trabajando en materia de ciberseguridad desde hace ya varios años, habiéndose promulgado

---

[5] *Ibídem.*

[6] Presidencia del Gobierno, "Estrategia de Seguridad Nacional", 2013, (disponible en http://www.lamoncloa.gob.es; última consulta 2/04/2017)

[7] Unión Europea, "Comunicación conjunta de la Comisión y la Alta Representante al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 7 de febrero de 2013, sobre la Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro" (disponible en: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es; última consulta 2/03/17).

numerosas Comunicaciones, Informes, Conclusiones, un Libro Verde e incluso una Directiva.

En base a lo expuesto, el presente Trabajo de Fin de Grado adopta como objeto de estudio la compleja labor de la protección de las infraestructuras críticas en la Unión Europea, tanto desde el punto de vista de la normativa que le es propia como desde la legislación en materia de ciberseguridad, que se impone con fuerza en lo que podemos apodar la Era del Ciberespacio.

1.2. Antecedentes

En el marco de nuestro objeto de estudio, este trabajo analizará la normativa de referencia en materia de IC y de Ciberseguridad. Se trata, como tendremos ocasión de ver en detalle, de dos Directivas de la UE, una relativa a las IC dictada en el año 2008 y otra en materia de Ciberseguridad, del año 2016. A pesar de que se vaya a centrar el análisis en estos dos textos normativos, lo cierto es que el conjunto de organismos de la UE viene trabajando los últimos años en ambas materias, a lo largo de los cuales se han realizado numerosas propuestas y debates. Para tener una idea de este recorrido y de los esfuerzos que se han llevado a cabo, conviene hacer un breve repaso de las últimas actuaciones de la Unión tanto en relación con las IC como con la ciberseguridad.

1.2.1. Antecedentes en materia de IC

Las actuaciones para mejorar la protección de las IC comienzan en junio de 2004, cuando el Consejo Europeo solicita a la Comisión y al Alto Representante que elaboren una estrategia global para la protección de las infraestructuras críticas. En respuesta a este requerimiento, la Comisión dicta, con fecha 20 de octubre de 2004, una Comunicación dirigida al Consejo y al Parlamento Europeo sobre la protección de las infraestructuras críticas en la lucha contra el terrorismo, en la que aborda la prevención, preparación y respuesta de Europa a los ataques terroristas que afecten a las IC[8]. En diciembre de 2004, el Consejo dicta unas conclusiones relativas a la Comunicación de la Comisión, en las que respalda el propósito de lanzar un Programa Europeo de

[8] Unión Europea, "Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 20 de octubre de 2004, sobre la protección de las infraestructuras críticas en la lucha contra el terrorismo".

Protección de Infraestructuras Críticas (en adelante, PEPIC) y aprueba la creación, por parte de la Comisión, de una Red de información relativa a las alertas tempranas para las IC[9]. Asimismo, los días 6 y 7 de junio de 2005 tiene lugar el primer Seminario europeo relativo a esta materia. En él, participan todos los Estados miembros, que, finalizado el mismo, remiten a la Comisión sus planteamientos y observaciones al respecto. Igualmente, los días 12 y 13 de septiembre se celebra el segundo Seminario relativo a la protección de IC con el objetivo de continuar y profundizar el debate[10]. Concluidos ambos seminarios, el 17 de noviembre la Comisión presenta el Libro Verde sobre el PEPIC[11]. Este documento se propone recabar puntos de vista en relación con la creación del PEPIC y la CIWIN, procedentes de todos los agentes interesados. Con posterioridad a este Libro Verde, el Consejo de Justicia e Interior de diciembre de 2005 solicita a la Comisión que elabore una propuesta concreta de PEPIC, por lo que el 12 de diciembre de 2006 se publica una nueva Comunicación de la Comisión[12] en la que se establecen los principios, procesos e instrumentos para llevar a la práctica este PEPIC. Finalmente, en base a todo lo trabajado desde 2004, el 8 de diciembre de 2008 se dicta el texto normativo sobre el que va a versar gran parte de este trabajo: 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[13] (en adelante, Directiva 2008/114/CE).

1.2.2. Antecedentes en materia de ciberseguridad

El punto de arranque en esta materia se produce en 2013, con ocasión de la publicación de la Estrategia de Ciberseguridad de la UE[14], que establece el

[9] Unión Europea, "Libro Verde presentado por la Comisión, de 17 de noviembre de 2005, sobre un Programa Europeo para la Protección de Infraestructuras Críticas" (disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52005DC0576; última consulta 2/03/17).
[10] *Ibídem.*
[11] *Ibídem.*
[12] Unión Europea, "Comunicación de la Comisión, de 12 de diciembre de 2006, sobre un Programa Europeo para la Protección de Infraestructuras Críticas" (disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Al33260; última consulta 3/03/17)
[13] 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 (DO L 345 de 23.12.2008).
[14] Unión Europea, "Comunicación conjunta de la Comisión y la Alta Representante al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 7 de febrero de 2013, sobre la Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro" (disponible en: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es; última consulta 2/03/17).

planteamiento de la Unión acerca de la mejor manera de dar respuesta a las perturbaciones y/o ataques cibernéticos. Igualmente, fija un proyecto de directiva sobre seguridad de las redes y sistemas de información, de cara a promover la igualdad de condiciones de seguridad de los Estados miembros a través de la provisión de normas armonizadas. Tras largas negociaciones con el Parlamento Europeo y el Consejo, el proyecto de directiva culmina con la adopción de la Directiva 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[15] (en adelante, Directiva NIS). Junto con la Directiva 2008/114/CE mencionada en materia de IC, la Directiva NIS será el otro eje en torno al que gravite este trabajo.

1.3. Objetivos

Tal y como venimos diciendo, la preocupación por la protección de las IC se ha implantado con fuerza en la Comunidad Internacional y, dentro de ella, en la UE. No obstante, la rapidez con que ha tenido lugar la toma de conciencia de la situación, unida a su complejidad subyacente, lleva inevitablemente a disparidades interpretativas respecto de lo que realmente constituye una IC para los Estados. Estas disparidades interpretativas trascienden el mero ámbito conceptual y generan verdaderos problemas prácticos a la hora de proporcionar una protección de las IC en el seno de una organización internacional.

En este sentido, el presente Trabajo de Fin de Grado fija dos objetivos principales que se relacionan entre sí. En primer lugar, se trata de analizar la eficacia del mecanismo de designación de IC, previsto en la UE. Ciertamente, si la UE busca promover un verdadero mercado común seguro, tiene que ser capaz de facilitar sistemas de protección uniformes dirigidos a las infraestructuras previamente identificadas como críticas. Dicho de otra forma, se pretende dilucidar si el procedimiento de identificación de IC, que precede a la aplicación de las medidas protectoras, es suficientemente integrador y unívoco o si, por el contrario, resulta excesivamente flexible y puede dar

[15] Directiva 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 (DO L 194 de 19.7.2016).

lugar a respuestas dispares, por parte de los Estados miembros, que impidan el desarrollo de este mercado común seguro.

En segundo lugar, el presente trabajo persigue valorar si la normativa de la UE en materia de Ciberseguridad refuerza la relativa a las IC en aquellas carencias que ésta última pueda presentar.

1.4. Estructura

Vistos el objeto de estudio y los objetivos a alcanzar, el presente trabajo se estructura en dos bloques principales. El primero de ellos gira en torno al análisis de la Directiva 2008/114/CE, relativa a la identificación y designación de infraestructuras críticas europeas y a la evaluación de la necesidad de mejorar su protección. Así, se trata de examinar en detalle las previsiones que concurren en la identificación de infraestructuras críticas, toda vez que esta etapa resulta fundamental e indispensable a la hora de aplicar las medidas protectoras previstas en la directiva. El segundo de ellos, por su parte, atiende al análisis de la Directiva NIS, con el propósito de dilucidar si las previsiones de la misma pueden resultar complementarias a las de la Directiva 2008/114/CE en la compleja labor de proteger las infraestructuras críticas.

2. ANÁLISIS DE LA DIRECTIVA 2008/114/CE DEL CONSEJO[16]

Como ya hemos adelantado en la introducción de este trabajo, la protección de las IC resulta crucial en la sociedad del siglo XXI y, como actor internacional, la UE ha participado en esta preocupación, manifestándose y regulando al respecto durante los últimos años. Por otra parte, es evidente que para que una infraestructura se beneficie de los mecanismos protectores reservados a las IC, antes debe ser designada como tal. En consecuencia, en la compleja labor de protección de IC, reviste especial importancia la etapa relativa a su identificación. Así pues, a lo largo del presente epígrafe y en línea con el primero de los objetivos del trabajo, nos detendremos en el examen del mecanismo establecido por los organismos de la UE para la designación de lo que ha de constituir una IC, en aras de valorar y concluir sobre la eficacia del mismo.

Para la consecución de este objetivo, es imprescindible la remisión a 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 (en adelante, Directiva 2008/114/CE), que culmina un largo recorrido de disposiciones de la UE en las que sus distintos organismos ponen de manifiesto la necesidad de proteger las IC y arrancan los primeros trabajos en esta línea. Todavía en vigor, la Directiva 2008/114/CE se erige como norma de referencia en materia de IC a lo largo del territorio de la Unión, pues tiene como destinatarios a todos los Estados miembros (artículo 14).

El artículo 1 de la Directiva 2008/114/CE comienza por fijar el doble objeto de la misma, a saber, *"establecer un procedimiento de identificación y designación de infraestructuras críticas europeas ("las ICE") y un planteamiento común para evaluar la necesidad de mejorar la protección de dichas infraestructuras con el fin de contribuir a la protección de la población"*. Puesto que venimos reiterando la intención de centrar esta parte del trabajo en el proceso identificativo de IC, únicamente se hará referencia a aquellas disposiciones de la Directiva relativas al primero de los objetivos que consagra.

[16] 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 (DO L 345 de 23.12.2008).

Finalmente, antes de adentrarnos en el examen de los preceptos clave de la Directiva 2008/114/CE, señalar brevemente que comenzaremos por abordar la posición que adopta el Consejo en la materia. En un segundo momento, se revisarán los pasos a seguir en el proceso de identificación de IC. A continuación, se analizarán las características de la directiva como instrumento jurídico y las implicaciones de su empleo. Para terminar, se valorarán de forma conjunta las consecuencias de todo lo apuntado.

2.1. El Consejo, ¿en un segundo plano?

Los cuatro primeros considerandos de la Directiva hacen un repaso de los antecedentes normativos en materia de IC, mientras que el quinto, al igual que el artículo 1, se limita a establecer el objeto de la disposición. Así pues, comenzaremos nuestro análisis a partir de los preceptos que siguen.

El sexto considerando, bajo el lema *"La responsabilidad principal y última de proteger las ICE corresponde a los Estados miembros y a los propietarios u operadores de tales infraestructuras",* pone de manifiesto la importancia del papel de los Estados miembros en materia de IC, pese a la regulación del Consejo al respecto.

En cuanto al considerando séptimo, se refiere a la interdependencia de las IC y, en consecuencia, a la necesidad de que se les dé un tratamiento con un mínimo común en el seno de la Comunidad. Como ha puesto de relieve la doctrina, la interdependencia de las infraestructuras conlleva la posibilidad de que los problemas se desencadenen en cascada y, en consecuencia, de que acarreen fallos "*inesperados, generalizados y cada vez más graves de los servicios básicos*"[17]. La interdependencia y los fallos en cascada llaman, por lo tanto, a una acción conjunta o, cuanto menos, armonizada.

Comprobamos, todavía de forma sutil, una suerte de contradicción –o si se quiere, de dificultad-, en la relación de los dos últimos considerandos analizados. En efecto, se expresa la voluntad de llevar a cabo la identificación y designación de IC *"por un proceso común"* y, sin embargo, *"la responsabilidad principal y última de proteger las ICE"* recae en los Estados miembros y en los propietarios u operadores de las mismas. Aunque el considerando sexto se refiere al ámbito de la protección y el séptimo a los de

[17] SÁNCHEZ GÓMEZ, F.J., "Protección de infraestructuras críticas en España: marco regulatorio y organizativo", *Seguridad y Ciudadanía: Revista del Ministerio del Interior*, n.11, 2014, pp. 21-22 (disponible en http://www.interior.gob.es; última consulta 6/02/2017).

la identificación y designación, realmente el primero (protección) depende de los segundos (identificación y designación) y, en consecuencia, no puede pasarse por alto esta paradoja que enfrenta *proceso común* y *responsabilidad individual*.

El décimo considerando establece la complementariedad de la presente Directiva en relación con las medidas sectoriales de la UE y de los propios Estados miembros, lo que significa que ésta no deroga la normativa anterior, imponiéndose como marco de referencia único y exclusivo en la materia, sino que, al contrario, se configura como un compendio de mecanismos complementarios. De nuevo, a pesar del propósito armonizador, que queda patente tanto en el séptimo considerando como en la elección del instrumento jurídico (la directiva), parece que, en cierto modo, el Consejo da marcha atrás y se posiciona en un segundo plano *complementario*.

Los considerandos que siguen abordan temas de protección, cooperación y comunicación en materia de IC que –aunque importantes-, van más allá de nuestro objeto de estudio.

Será en el vigésimo considerando cuando, al fin, se constate que los objetivos de la Directiva *"no pueden ser alcanzados de manera suficiente por los Estados miembros"* y que por ello la Comunidad está en todo su derecho de adoptar medidas de acuerdo con el principio de subsidiariedad que impera en la UE. Este principio viene recogido en el artículo 5.3 del Tratado de la Unión Europea (en adelante, TUE), que dispone:

> En virtud del principio de subsidiariedad, en los ámbitos que no sean de su competencia exclusiva, la Unión intervendrá sólo en caso de que, y en la medida en que, los objetivos de la acción pretendida no puedan ser alcanzados de manera suficiente por los Estados miembros, ni a nivel central ni a nivel regional y local, sino que puedan alcanzarse mejor, debido a la dimensión o a los efectos de la acción pretendida, a escala de la Unión.

Tal y como apunta MANGAS MARTÍN[18], "*la subsidiariedad es, pues, un principio regulador del modo de ejercicio de las competencias compartidas entre los Estados miembros y la Unión Europea"*. Así, señala también que no es título de atribución ni de reparto de competencias, sino que delimita y racionaliza el ámbito de las competencias compartidas[19]. En base a este principio, cuando la Unión no ostente la competencia exclusiva de una materia, deberá valorar la potencial labor normativa de los Estados y sus entes locales. Sólo cuando se estime que la actuación de la Unión será más eficaz

[18] MANGAS MARTÍN, A., "El sistema institucional", en *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, 2005, pp. 118-119.
[19] *Ibídem.*

que la de los Estados miembros y sus entes locales, lo cual no siempre resulta evidente, podrá ésta intervenir al respecto, debiendo abstenerse en caso contrario. Vista la trascendencia de las IC y su carácter transnacional, cabe preguntarse si la protección de las mismas no debería pasar a ser una competencia exclusiva de la UE, aunque posicionarse al respecto parece extralimitar los objetivos de este trabajo. Volviendo a nuestro primer objetivo, la Directiva admite que aborda unos objetivos complejos cuya consecución por parte de los Estados miembros necesita la intervención de la UE. Ahora bien, a pesar de la dificultad que entraña la identificación y protección de IC, la Comunidad no se erige como legislador único en la materia, sino que, por el carácter compartido de la misma, ostenta el derecho a adoptar medidas siempre y cuando respete el referido principio de subsidiariedad.

En definitiva, hasta ahora hemos comprobado que la protección en materia de IC entraña una primera dificultad derivada de la configuración de su regulación. Pese a ser una materia de trascendencia vital y marcado carácter transnacional, el hecho de que sea compartida conlleva una obligación de respeto al principio de subsidiariedad y, en consecuencia, la potencial intervención normativa estatal o local. Por si fuera poco, la Directiva se presenta como *complementaria*, y no como única o principal, a la par que consagra la responsabilidad última de los Estados en materia de protección de IC. ¿Realmente el propósito armonizador es tan fuerte como, supuestamente, atestigua el uso de una directiva? ¿Resultan estas previsiones suficientes para una materia como la que se está tratando? En el apartado siguiente, se tratará de arrojar algo de luz a estos interrogantes mediante el estudio detallado del mecanismo de identificación de IC que articula la Directiva 2008/114/CE.

2.2. El proceso de identificación de infraestructuras críticas previsto en la Directiva 2008/114/CE

Tras esta primera toma de contacto con lo que parece una dificultad en la protección de IC europeas, el presente apartado se propone examinar minuciosamente aquellas previsiones de la Directiva 2008/114/CE relacionadas con el proceso de identificación y calificación.

Con el artículo 2, dedicado a "Definiciones" nos adentramos ya en el corazón del problema a dilucidar: ¿Qué es una infraestructura crítica? El artículo en cuestión, literalmente, reza:

> A efectos de la presenta Directiva, se entenderá por:
> a) "Infraestructura crítica", el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones;
>
> b) "Infraestructura crítica europea" o "ICE", la infraestructura crítica situada en los Estados miembros cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros. La magnitud de la incidencia se valorará en función de criterios horizontales, como los efectos de las dependencias intersectoriales en otros tipos de infraestructuras; […]

La definición provista, por lo tanto, puede calificarse de amplia en tanto que suscita interrogantes como los siguientes: ¿qué son las funciones sociales vitales? ¿qué debe entenderse por perturbación o destrucción? ¿cómo de grave ha de ser la afectación del Estado miembro provocada por la perturbación?

Es cierto que difícilmente puede configurarse una definición inequívoca de la IC sin proceder a una lista *numerus clausus* de lo que ha de entenderse como tal. No obstante, una definición que agotase lo que debe considerarse en todo caso IC resultaría excesivamente larga, compleja, probablemente incompleta, y rápidamente desactualizada. Por ello, en este estadio de la Directiva, debemos admitir que, aunque la previsión ofrezca dudas, éstas son fruto de una definición *razonable*.

El problema se plantea en el artículo 3 que, tras esta definición abierta de lo que constituye una IC o ICE, procede a fijar el mecanismo para su identificación concreta. Procedamos al análisis por partes.

En su apartado primero, establece el artículo 3 que:

> 1. Cada Estado miembro identificará, conforme al procedimiento establecido en el anexo III, ICE potenciales que se ajusten a la vez a los criterios horizontales y sectoriales y a las definiciones recogidas en el artículo 2, letras a) y b).
>
> La Comisión, a petición de los Estados miembros, podrá asistirles en la identificación de ICE potenciales.
>
> La Comisión podrá señalar a la atención de los Estados miembros interesados la existencia de infraestructuras críticas potenciales que pueda considerarse que cumplen los requisitos para su designación como ICE.

Lo primero que llama la atención de esta previsión es que corresponde a cada Estado miembro la identificación de potenciales ICE. Cierto es que en este proceso deberán seguirse determinadas pautas y que la Comisión podrá asistir a los Estados en su cometido, pero la realidad es que, en última instancia, la última palabra la tienen los Estados miembros. En cuanto a la nota de potencialidad, se relaciona con el hecho de que la IC sea europea, esto es, con que afecte a más de un Estado miembro, lo que supone que para la identificación definitiva como ICE deberán llevarse a cabo conversaciones entre los Estados implicados (nos referiremos a este asunto más adelante). En relación con las pautas que habrán de seguirse en esta identificación cabe preguntarse, además, si realmente acotan la labor de los Estados o si, por el contrario, les dejan un amplio margen de actuación. Para dilucidar esta cuestión, conviene detenerse en el estudio individualizado de cada una de ellas, a saber: el seguimiento del procedimiento establecido en el anexo III; el respeto de los criterios horizontales y sectoriales; y el respeto de las definiciones recogidas en el artículo 2, letras a) y b), que hemos abordado unas líneas más arriba.

Alterando el orden en que aparecen en el artículo 3.1, comencemos por referirnos a los criterios horizontales y sectoriales, para lo que debemos acudir al apartado segundo de este artículo 3.

> Los criterios horizontales a que se refiere el apartado 1 incluirán:
> a) El número de víctimas (valorado en función del número potencial de víctimas mortales o de heridos);
> b) El impacto económico (valorado en función de la magnitud de las pérdidas económicas o el deterioro de productos o servicios, incluido el posible impacto medioambiental);
> c) El impacto público (valorado en función de la incidencia en la confianza de la población, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida de servicios esenciales).
> Los umbrales de los criterios horizontales atenderán a la gravedad de las repercusiones de la perturbación o destrucción de una infraestructura concreta. Los umbrales concretos que se aplicarán a los criterios horizontales los determinarán los Estados miembros de que se trate en función de la infraestructura crítica considerada. Cada Estado miembro informará anualmente a la comisión del número de infraestructuras por sector sobre la que se hayan discutido los umbrales de los criterios horizontales.
> Los criterios sectoriales tendrán en cuenta las características de los diferentes sectores de las ICE.
> La Comisión, junto con los Estado miembros, elaborará directrices para la aplicación de los criterios horizontales y sectoriales y definirá umbrales aproximados que se utilizarán para identificar las ICE. Los criterios constituirán información clasificada. La utilización de tales directrices será facultativa para los Estados miembros.

En relación con los criterios horizontales, lo primero que llama la atención es que se reduzcan solamente a tres. El primero de ellos está relacionado con el número de víctimas, cuyo número no sólo no se concreta, sino que tampoco se proporcionan métodos de determinación al efecto. Así, por ejemplo, podría haberse establecido un ratio (*e.g.* un porcentaje sobre la población total), un punto de referencia (*e.g.* el número de víctimas de un suceso concreto), o cualquier otra herramienta que permitiese a los Estados miembros determinar de forma cuasi mecánica si el número de víctimas supera determinados umbrales y, en consecuencia, la infraestructura debiese calificarse como crítica. En su lugar, sin embargo, el artículo únicamente deja constancia de que el número de víctimas es un factor determinante de la existencia de IC, pero no establece en qué medida condiciona la calificación.

El segundo de los criterios horizontales se refiere al impacto económico, "*valorado en función de la magnitud de las pérdidas económicas o el deterioro de productos o servicios, incluido el posible impacto medioambiental*". De nuevo, no consta ningún criterio o regla que permita valorar de forma objetiva si la magnitud del impacto económico es efectivamente suficiente para que la infraestructura devenga crítica. En relación con este criterio horizontal, habría sido más sencillo que en el anterior fijar determinados valores de referencia (*e.g.* el umbral de la cuantía económica que debe sobrepasarse, el número de metros cuadrados de zonas verdes perjudicadas, el volumen de gases tóxicos liberados en la atmósfera, etc.) y sin embargo, tal y como sucedía antes, queda constancia de su importancia pero no del grado de la misma.

Finalmente, la Directiva se refiere al impacto público, "*valorado en función de la incidencia en la confianza de la población, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida de servicios esenciales*", que sin duda constituye el criterio con mayor dificultad de concreción de los tres. Se trata aquí de conceptos abstractos, en los que resulta complicado determinar cómo de afectada tiene que resultar la confianza, si el término "población" debe entenderse referido a la localidad afectada o al conjunto de la nación, qué nivel de sufrimiento físico se requiere o cómo de alterada debe quedar la vida cotidiana.

Los tres criterios horizontales provistos, por lo tanto, están dotados de una marcada flexibilidad y amplitud que dejan la puerta abierta a interpretaciones y valoraciones muy dispares por parte de los Estados miembros. Por si fuera poco, el propio artículo destaca que "*los umbrales concretos que se aplicarán a los criterios horizontales los*

determinarán los Estados miembros de que se trate en función de la infraestructura crítica considerada", por lo que los criterios de la Directiva no sólo resultan poco concretos, sino que también son susceptibles de adaptación.

En relación ahora con los criterios sectoriales, la Directiva se limita a establecer que "*tendrán en cuenta las características de los diferentes sectores de las ICE*", lo cual más que añadir información concreta al precepto parece una simple alusión a su existencia.

Para terminar este apartado segundo del artículo 3, la Directiva señala *in fine* que la Comisión "*elaborará directrices para la aplicación de los criterios horizontales y sectoriales y definirá umbrales aproximados*". Parece que, en primera instancia, la Comisión viene a suplir las carencias puestas de relieve en los párrafos anteriores mediante la elaboración de directrices, pero lo cierto es que la utilización de estas directrices y estos umbrales –que son sólo *aproximados*- será "*facultativa para los Estados miembros*". Los Estados miembros que decidan no seguirlas tendrán, por lo tanto, total libertad a la hora de fijar el número de víctimas, el impacto económico o el impacto público determinantes de la consideración de IC.

A continuación, pasamos al análisis de las definiciones de IC e ICE del artículo 2, letras a) y b), a las que ya hemos aludido brevemente al principio de este capítulo. Las definiciones en cuestión ponen el acento de lo que debe considerarse IC en la concurrencia de dos elementos:

1. La esencialidad de las funciones que prestan: "*funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población*".
2. La grave afectación para la población de un Estado miembro (o de varios, en el caso de la ICE) en caso de verse interrumpida la prestación de alguna de estas funciones.

Pues bien, aunque antes admitíamos la razonabilidad de esta definición abierta, en tanto que una lista cerrada de elementos suscita problemas de seguridad jurídica, lo cierto es que como pauta para la identificación de IC se queda corta, toda vez que realmente no constituye un requisito que pueda comprobarse de forma objetiva.

Abordemos ya, para terminar el análisis del artículo 3, el procedimiento a seguir por los Estados miembros en la identificación de ICE., recogido el Anexo III de la

Directiva. En el anexo, el legislador establece cuatro pasos consecutivos e ineludibles, que podemos resumir como sigue:

1. Aplicación de los criterios sectoriales de cara a una primera selección de potenciales ICE;
2. Aplicación, a estas potenciales ICE, de la definición de infraestructura crítica del artículo 2;
3. Aplicación del elemento transfronterizo de la definición de ICE del artículo 2; y
4. Aplicación de los criterios horizontales a las ICE potenciales que hayan superado los pasos anteriores.

En la medida en que estos pasos retoman los criterios analizados más arriba, con sus respectivas inconcreciones, este procedimiento no aporta mayor claridad que el orden de aplicación de los mismos.

Como adelantábamos al principio del apartado, realmente lo que hemos abordado hasta ahora es la identificación de ICE *potenciales*, en tanto que para ser europeas han de afectar *"al menos a dos Estados miembros"* (art. 2 b)) y por ello es preciso que antes de su designación *definitiva* como ICE los Estados miembros implicados se pongan de acuerdo.

Así pues, el artículo 4 se refiere a esta designación de ICE y al papel que ha de desempeñar la UE en la misma.

En su apartado primero, el artículo 4 comienza por señalar que los Estados miembros habrán de informar sobre las ICE potenciales que hayan identificado a aquellos otros Estados miembros a los que puedan afectar de forma significativa. En el apartado segundo, se establece que se entablarán entonces conversaciones entre los Estados para determinar si efectivamente las infraestructuras en cuestión han de considerarse ICE y llevar a cabo su designación como tal. En este proceso, la Comisión podrá participar en las conversiones, pero no tendrá derecho a conocer información pormenorizada que le permita identificar inequívocamente la infraestructura de que se trate. Esto enlaza directamente con una frase del artículo 3.2 (relativo a la identificación de ICE) que dice "*Los criterios* [horizontales y sectoriales] *constituirán información clasificada".* Ambos datos ponen de relieve cierta falta de transparencia en materia de ICE: la Comisión participa de las conversaciones, pero realmente no conoce la ICE a la

que se hace alusión; y, en el mismo sentido, aunque la Comisión elabore directrices en relación con los criterios de identificación, éstos constituirán información clasificada.

Así pues, comprobamos que la labor de identificación de ICE potenciales corresponde a los Estados miembros de forma individual, para lo que cuentan con pautas de actuación relativamente amplias. Su designación efectiva como ICE corresponde, en cuanto a ella, al conjunto de Estados miembros afectados, que deberán entablar conversaciones y aprobar la decisión del Estado que haya tomado la iniciativa. En todo este proceso, la Comisión puede estar presente e incluso prestar su ayuda pero, tal y como hemos visto, el papel que desempeña está limitado, toda vez que se le restringe el acceso a cierta información y sus aportaciones son, en muchos casos, de utilización facultativa. En consecuencia, podemos concluir que la labor de identificación y designación de ICE recae fundamentalmente y en última instancia en los Estados miembros.

Los artículos subsiguientes (del 6 al 14) están dedicados al segundo de los objetivos de la Directiva, a saber, el establecimiento de "*un planteamiento común para la evaluación de la necesidad de mejorar la protección de dichas infraestructuras"*. No nos detendremos en su análisis, en tanto que no constituyen el objeto de nuestro estudio.

2.3. La elección del instrumento normativo: la directiva

En el apartado que sigue, se abordan los rasgos relativos a la directiva, en aras de valorar la pertinencia de este instrumento normativo en relación con las IC.

La definición legal de la directiva se recoge en el Tratado Fundacional de la Unión Europea (en adelante, TFUE) que, en su artículo 288, dispone:

> La directiva obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios.

Se trata, como apunta LIÑÁN NOGUERAS[20], de un instrumento regulador cuyo objetivo es armonizar las legislaciones nacionales (en la búsqueda de *"la seguridad del edificio jurídico europeo"*), pero sin recurrir a la sustitución del poder legislativo

[20] LIÑÁN NOGUERAS, D. J., "El sistema de normas y actos en la Unión Europea (II)", en *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, 2016, pp. 397-399.

nacional, como sí hace el reglamento. En este sentido, este autor lleva a cabo un análisis de la definición provista en el tratado, destacando sus rasgos fundamentales[21].

En primer lugar, la directiva impone a los Estados miembros a los que se dirige (pues no necesariamente tiene alcance general) un obligación de resultado que debe cumplirse dentro de un plazo concreto. Esta obligación de resultado ha sido objeto de diversas interpretaciones. Así, los hay que la configuran como una obligación de "recepción", en atención al hecho de que los destinatarios sean los Estados y al margen de discrecionalidad de éstos en cuanto a la aplicación de la directiva. Por otra parte, la lectura "autónoma" concibe la obligación de resultado como una verdadera obligación de "ejecución". En este sentido, esta segunda lectura entiende que la directiva es un instrumento normativo integrado y equiparable al resto de normas de la Unión, de las que únicamente se diferencia por el carácter mediato de sus efectos, al exigir la intermediación de los Estados miembros. Según LIÑÁN NOGUERAS, esta lectura se respalda en la posibilidad de sancionar a los Estados que incumplan la obligación contenida en la directiva[22].

En segundo lugar, la directiva no sólo supone una obligación de resultado, sino que también requiere de los Estados la adopción de las medidas nacionales necesarias para la consecución de dicho resultado, dejando, sin embargo, a las autoridades "*la elección de la forma y de los medios"*. A este proceso consistente en la adopción de medidas nacionales con discrecionalidad en cuanto a la forma y los medios se le conoce como *transposición de la directiva* al Derecho interno. Ahora bien, desde el punto de vista de la segunda lectura (obligación de ejecución), lo cierto es que la transposición está más condicionada de lo que, en una primera instancia, pueda parecer. Así pues, no sólo deberá respetar el resultado exigido y el plazo provisto, sino que además habrá de emplear la forma y los medios adecuados a este resultado, así como garantizar la seguridad jurídica de las normas internas dictadas al efecto.

Tal y como continúa el autor, esta exigencia de seguridad jurídica de las normas internas está directamente relacionada con la tercera y última característica de la directiva: "*la vinculación de los efectos jurídicos a la norma nacional de transposición"*. En efecto, en tanto que requiere la intermediación de los Estados miembros, la directiva carece de aplicabilidad o eficacia directa y, por ello, los efectos

[21] *Ibídem.*
[22] *Ibídem.*

jurídicos han de quedar vinculados a la norma interna de transposición. Esta característica, que deriva de la ausencia de eficacia directa, introduce *"un alto grado de complejidad en este instrumento jurídico"*. Así, cuando la transposición se hace fuera de plazo o de forma incompleta o incorrecta, los derechos de los particulares pueden verse lesionados, en tanto que la posibilidad de sancionar al Estado infractor no soluciona la ausencia de aplicabilidad directa de la directiva[23]. En vista de este problema, el Tribunal de Justicia[24] ha tratado de asegurar el *"efecto útil"* de la directiva[25] y, en este sentido, ha señalado que:

> En todos los casos en que las disposiciones de una directiva parecen ser, desde el punto de vista de su contenido, incondicionales y suficientemente precisas, dichas disposiciones, si no se han adoptado dentro del plazo prescrito medidas de aplicación, pueden ser invocadas contra cualquier disposición nacional no conforme a la directiva o, en la medida en que definen derechos que los particulares pueden alegrar, frente al Estado[26].

En definitiva, para garantizar los derechos de los particulares frente al Estado infractor, el Tribunal de Justicia reconoce el efecto directo de la directiva, pudiendo ésta invocarse frente a la normativa interna contraria. Ahora bien, esta aplicabilidad directa *vertical*[27] requiere que las disposiciones de la directiva sean "*incondicionales y suficientemente precisas*" pues, de lo contrario, no es posible sustentar pretensión alguna.

Pues bien, el epígrafe 2.2. ha versado justamente sobre la falta de precisión del proceso identificativo de IC establecido en la Directiva 2008/114/CE. Así, en caso de que un Estado miembro no transponga la directiva o lo haga de forma errónea o incompleta, los particulares no podrán invocar su aplicabilidad directa, en tanto que no existen contenidos concretos que revindicar. En consecuencia, el incumplimiento de un Estado miembro dará lugar a la frustración del proyecto armonizador, comprometiendo así la seguridad de las IC en el territorio de la UE.

---

[23] *Ibídem.*
[24] El Tribunal de Justicia (en adelante, TJ) es la instancia superior del Tribunal de Justicia de la Unión Europea (en adelante, TJUE), esto es, de la institución que encarna el poder judicial en la Unión Europea (LIÑÁN NOGUERAS, D. J., "El Tribunal de Justicia de la Unión Europea", en *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, 2016, pp. 285 y 288).
[25] Sentencia de 5 de abril de 1979, *Ratti*, 148/78, p.1642.
[26] Sentencia de 19 de enero de 1982, *Ursula Becker c. Finanzamt Münster-Innenstadt*, 8/81, p.71.
[27] La eficacia directa vertical significa que aplica a la relación del particular frente al Estado y, además, únicamente en ese sentido (Sentencia *Becker*, 8/81, ya citada, fund.24).

Por otra parte, MANGAS MARTÍN ha puesto de relieve[28] que la obligación contenida en la directiva no se ciñe a la acción legislativa o reglamentaria, "*sino que el resultado de la directiva, a falta de la transposición general o erga omnes, puede y debe ser asegurado por el juez, en el marco de sus competencias, aunque con un efecto limitado a las partes en litigio"*[29]. Así, ante la falta de transposición o en caso de transposición incorrecta, el juez deberá interpretar el Derecho nacional "*anterior o posterior a la directiva, introducido o no para transponer la directiva, a la luz de la letra y de la finalidad de la directiva*"[30]. Sin embargo, esta segunda solución a la posible ausencia o incorrección de la transposición por parte de los Estados miembros todavía plantea dos problemas. En primer lugar, como es lógico, es necesario que exista ley nacional que interpretar. Así, siendo como es la protección de las infraestructuras críticas una materia relativamente nueva, es posible que el juez no cuente con disposiciones internas que interpretar. Por otra parte, los efectos de la interpretación del juez nacional se limitan al caso concreto, por lo que puede suceder que la concurrencia de distintos casos y jueces de lugar a interpretaciones dispares.

En síntesis, la directiva se constituye como un instrumento normativo europeo que busca armonizar las legislaciones nacionales. Ahora bien, en tanto que únicamente obliga en plazo y resultado, confiriendo a los Estados miembros cierta discrecionalidad en la elección de las medidas internas, el uso de la directiva conlleva el riesgo de que los Estados miembros no transpongan o de que lo hagan incorrectamente. Existen ciertos mecanismos dirigidos a paliar este riesgo y garantizar los derechos de los particulares. En primer lugar, destaca el reconocimiento de la eficacia directa de la directiva y, en segundo, la obligación de los jueces internos de interpretar la legislación nacional de acuerdo con la directiva. Sin embargo, estas soluciones no siempre resultan eficaces: la aplicabilidad directa necesita que los preceptos de la directiva sean precisos, mientras que la interpretación del juez nacional requiere de la existencia de una norma que interpretar. En tanto que la Directiva 2008/114/CE no es precisa con respecto a la identificación de IC y que la problemática de la protección de IC es relativamente reciente y puede no haber sido legislado a nivel nacional, cabe plantearse que tal vez el empleo de este instrumento normativo europeo no haya sido el más acertado. En esta

[28] En base a la jurisprudencia del TJUE de los últimos años.
[29] MANGAS MARTÍN, A., "Los principios de Derecho de la Unión Europea en sus relaciones con los ordenamientos internos (I)", en *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, 2005, pp. 415-420.
[30] *Ibídem.*

línea, es posible que la regulación de la materia mediante reglamento hubiese planteado menos dificultades[31].

2.4. Las implicaciones de la Directiva 2008/114/CE

Lo visto en relación con la definición legal del concepto de IC (europeas) y su proceso de identificación nos conduce a una conclusión muy clara: a día de hoy, la línea seguida por la UE en la materia no permite determinar de forma cuasi automática lo que ha de constituir o no una IC. Ciertamente, corresponde a los Estados miembros la identificación y designación de IC y, en el desempeño de esa labor, tienen un margen de actuación muy elevado. En efecto, los Estados tienen la facultad de concretar ellos mismos los criterios y umbrales conforme a los que habrán de decidir y, en el mismo sentido, podrán optar por seguir, o no, las directrices de la Comisión. Por su parte, la labor de la UE se llega a calificar de complementaria y se hace énfasis en el principio de subsidiariedad. En este contexto, es perfectamente plausible que los Estados miembros lleguen a conclusiones muy distintas en la materia y, en consecuencia, que algunos consideren IC lo que otros no creen merecedor de tal calificación. Esto resulta especialmente importante en la medida en que la calificación como IC conlleva que la infraestructura en cuestión se beneficie de las medidas de protección previstas al efecto y, en sentido contrario, que su no calificación como IC la excluya de su ámbito de aplicación. Dada la esencialidad de determinadas infraestructuras para la población de uno o varios Estados miembros (recordemos aquí la noción de interdependencia), consideramos que no debería quedar al arbitrio de los mismos la concesión a una infraestructura de su calificación como crítica y, en última instancia, de su sometimiento a medidas de prevención y respuesta a los riesgos.

Retomando nuestro primer objetivo, a saber, la valoración de la eficacia del proceso de identificación de IC en el seno de la UE, creemos poder afirmar que se trata de un mecanismo laxo que da pie a interpretaciones de diversa índole por parte de los Estados miembros. En tanto que la no calificación como IC impide la aplicación de ciertas

[31] El artículo 288 del TFUE establece que "*El reglamento tendrá un alcance general. Será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro*". Se trata, como apunta LIÑÁN NOGUERAS, "*del instrumento de regulación jurídica más acabado dentro del sistema comunitario"* (LIÑÁN NOGUERAS, D. J., "El sistema de normas y actos en la Unión Europea (II)", en *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, 2005, p. 362).

medidas de seguridad, esto puede desembocar en niveles de protección desiguales (y en ocasiones insuficientes) de infraestructuras esenciales a lo largo del territorio de la Unión. Esto viene sin duda favorecido por la elección del instrumento normativo: la directiva. Tal y como hemos apuntado, la directiva puede derivar en disparidades legislativas de un Estado miembro a otro, y más si se trata de una directiva poco precisa o de si la normativa nacional en la materia es escasa. Por eso, cabe plantearse si no tendría más sentido regular la protección de IC mediante reglamento o, cuanto menos, mediante una directiva más rigurosa.

Como resumen de este primer epígrafe dedicado a la Directiva 2008/114/CE, parece acertada la frase del poeta y dramaturgo inglés, William Shakespeare:

> Las medidas templadas, que equivalen a remedios prudentes, son hartamente nocivas cuando el mal es violento.

3. LA DIRECTIVA NIS, ¿AL RESCATE?

Una vez analizada la Directiva 2008/114/CE, debemos remitirnos al segundo objetivo de este Trabajo de Fin de Grado. Constatadas ciertas carencias en la normativa de la UE en materia de IC, se trata de valorar si la reciente normativa en otra materia, la ciberseguridad, puede verter algo de luz sobre nuestro problema. Para dilucidar esta cuestión, nos detendremos en el examen de la Directiva (UE) 216/1148 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[32], conocida por sus siglas en inglés como Directiva NIS[33]. La Directiva NIS es la culminación de un largo proceso normativo iniciado por la UE en febrero de 2013 con la publicación de la Estrategia de Ciberseguridad de la Unión Europea[34]que, durante años, ha sido objeto de debate. Así, el pasado verano se publicó la Directiva NIS, que

[32] Directiva 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 (DO L 194 de 19.7.2016).
[33] *Network and Information Systems*
[34] Comunicación conjunta de la Comisión y la Alta Representante al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 7 de febrero de 2013, sobre la Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro (disponible en: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es; última consulta 2/03/17).

constituye la primera directiva europea en materia de ciberseguridad y que nos va a servir de base para nuestro análisis.

En un primer momento, se dedicará un apartado a dilucidar la relación que puede instaurarse entre la Directiva NIS (dedicada a la ciberseguridad) y las IC. Más adelante, se atenderá a los procedimientos de identificación de operadores de servicios esenciales y de proveedores de servicios digitales, dos nociones introducidas por la referida directiva. Finalmente, se pondrá de relieve el espíritu armonizador que impera a lo largo del texto, tanto por las obligaciones que impone en materia de cooperación como por el deseo del legislador de universalizar los sistemas de protección.

3.1. El nexo entre la Directiva NIS y las infraestructuras críticas

La Directiva NIS se dicta con el propósito de *"lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior"* (artículo 1). Para que no haya lugar a dudas respecto de lo que constituye una RSI, remitámonos al artículo 4.1, que consagra:

> 1) "Redes y sistemas de información":
> a) Una red de comunicaciones electrónicas en el sentido del artículo 2, letra a), de la Directiva 2002/21/CE;
> b) Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí en el que uno o varios de ellos realizan, mediante un programa, el tratamiento automático de datos digitales, o
> c) Los datos digitales almacenados, tratados, recuperados o transmitidos mediante elementos contemplados en las letras a) y b) para su funcionamiento, utilización, protección y mantenimiento;

Pues bien, las redes y sistemas de seguridad (en adelante RSI) juegan un papel crucial para las actividades económicas y sociales, particularmente para el correcto desenvolvimiento del mercado interior (Considerando (1)). En efecto, contribuyen de forma decisiva a facilitar la circulación transfronteriza de productos, servicios y personas en la UE, revelando un claro componente transnacional. Un incidente en una RSI puede, por ello, afectar a más de un Estado miembro e incluso al conjunto de la Unión (Considerando (3)). Este carácter transnacional, unido al incremento de *"la magnitud, la frecuencia y los efectos de los incidentes de seguridad"* (Considerando (2)), determinan la necesidad tanto de proteger las RSI como de hacerlo de forma *común*. En este sentido, la Directiva impone obligaciones para todos los Estados

miembros (artículo 1.2), entre las que destaca que los operadores de servicios esenciales y los proveedores de servicios digitales de los Estados respeten determinados requisitos en materia de seguridad y notificación (artículo 2.d)). Como veremos más adelante, se trata de aquellas entidades que, prestando un servicio esencial para la sociedad, tienen un componente RSI que las hace merecedoras de una protección especial.

Cabe preguntarse ahora cuál es la relación que mantienen estas RSI con las IC tratadas en la primera parte del trabajo. Hemos visto que constituye una IC *"el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población"*. En este sentido, en la medida en que no se atribuya la calificación de IC, el elemento, sistema o parte de éste de que se trate no tendrá acceso a las medidas de seguridad de la Directiva 2008/114/CE. Ahora bien, es difícil concebir hoy en día una prestación de servicios que no incorpore RSI, como las que hemos definido más arriba, menos aún si se trata de un servicio *esencial*. Por lo tanto, podemos pensar que en el caso de que una infraestructura no llegue a calificarse como crítica, sí que podrá constatarse la presencia de RSI y admitirse su carácter esencial, de forma que los operadores de la misma, aun no sujetos a la Directiva 2008/114/CE, puedan beneficiarse de las previsiones de la Directiva NIS. Esto es precisamente lo que apunta BORREDÁ en su análisis de la Directiva NIS para el caso español[35], en el que destaca que:

> […] todos los operadores críticos designados por la Ley PIC[36] son operadores de servicios esenciales, pero al margen de ellos existen otros operadores de servicios esenciales para los que no es de aplicación la Ley PIC y sí la Directiva NIS en tanto en cuanto actúe en los sectores a que ésta se refiere.

Además, con frecuencia, las IC subcontratan a otras empresas, no IC, la prestación de servicios relacionados con RSI, por lo que la sujeción de estas empresas a la Directiva NIS fortalece indirectamente las medidas de seguridad que recibe la IC. En consecuencia, parece razonable admitir que la Directiva NIS y sus previsiones en materia de RSI pueden acoger bajo su paraguas protector a aquellas infraestructuras

[35] BORREDÁ, A., "Directiva NIS: la oportunidad", *Seguritecnia*, n. 434, 2016, p.21 (disponible en: http://www.seguritecnia.es/revistas/seg/434/index.html#22; última consulta 25/03/17) .

[36] Se trata de la Ley 8/2011 de Protección de Infraestructuras Críticas, transposición de la Directiva 114/2008 del Consejo, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

esenciales no calificadas como IC, así como incrementar la seguridad de las que sí han recibido tal calificación.

3.2. Los procedimientos de identificación de operadores de servicios esenciales y proveedores de servicios digitales

Como ya hemos adelantado, de las obligaciones que impone la Directiva NIS nos interesan las que atañen a los operadores de servicios esenciales y a los proveedores de servicios digitales, toda vez que son las que podemos relacionar con la materia de IC.

Para que los requisitos en materia de seguridad y de notificación de las RSI resulten aplicables a una entidad, es preciso, tal y como sucedía con las IC, que ésta reciba una calificación especial: la de "operador de servicios esenciales" o la de "proveedor de servicios digitales". En relación con esta calificación, la Directiva NIS establece en el considerando décimo noveno que "*Los Estados miembros deben ser responsables de determinar qué entidades cumplen los criterios de la definición"*. Cabría pensar en una primera instancia que vuelve a repetirse la misma dificultad que encontrábamos en materia de IC: una protección que depende de una calificación, que a su vez queda al arbitrio de los Estados miembros. Sin embargo, la presente Directiva tiene una clara vocación unificadora, a la que hace alusión en repetidas ocasiones, y por ello establece procedimientos de determinación mucho más rigurosos que los de la Directiva 2008/114/CE, encaminados a la consecución de niveles equivalentes de protección en toda la Unión (Considerandos (5) y (6)). Se trata ahora de examinar estos mecanismos de identificación a los que nos acabamos de referir y de valorar su eficacia en relación con el *"necesario planteamiento global en la Unión"* (Considerando (6)) .

3.2.1. Operadores de servicios esenciales

El procedimiento de identificación de operadores de servicios esenciales viene detallado en los decimonoveno y vigésimo considerandos, así como en los artículos 4.4 y 5.2 de la Directiva. Tras haber analizado en detalle estos preceptos, estamos en condiciones de explicar de forma ordenada los pasos que deben seguirse en este proceso identificativo.

En primer lugar, los Estados miembros deben, como mínimo, referirse a todos los sectores y subsectores del anexo II y valorar, dentro de los mismos, qué servicios resultan esenciales. El anexo en cuestión establece una lista con siete sectores (y sus respectivos subsectores) que el legislador ha considerado susceptibles de albergar servicios esenciales. Se trata, por orden de aparición, de los sectores de energía (electricidad, crudo y gas), transporte (aéreo, por ferrocarril, marítimo y fluvial y por carretera), banca, infraestructuras de los mercados financieros, sector sanitario, suministro y distribución de agua potable e infraestructura digital. Así, dentro de los mismos, cada Estado miembro deberá valorar qué servicios resultan esenciales y cuáles no, pues, tal y como indica el considerando vigésimo segundo, *"Por ejemplo, en el sector del transporte aéreo, los aeropuertos prestan servicios que un Estado miembro puede considerar esenciales, como la gestión de las pistas, pero también una serie de servicios que pueden considerarse no esenciales, como la oferta de zonas comerciales"*. Por lo tanto, si bien es cierto que corresponde a los Estados miembros determinar qué servicios se consideran esenciales, también lo es que deberán llevar a cabo esta labor, obligatoriamente y como mínimo, en un total de doce sectores o subsectores. De esta forma, la Unión constriñe el cometido de los Estados miembros, imponiendo unos ámbitos mínimos en los que deberán identificar lo que constituyen servicios esenciales. Ya no será posible, por ejemplo, que un Estado miembro regule en materia de infraestructuras de los mercados digitales, y que otro, por el contrario, decida omitir este sector.

Una vez identificados los servicios esenciales, los Estados miembros deberán entonces atender a la lista de entidades provista en el mismo anexo. Citemos, por poner dos ejemplos, los gestores de las instalaciones de refinado y tratamiento de gas natural y los operadores de oleoductos de transporte de crudo. Para cada una de las entidades que figuran en el anexo, los Estados miembros deberán entonces valorar si cumplen los criterios de identificación de los operadores de servicios esenciales que constan en el artículo 5.2, a saber:

1. Una entidad presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales;
2. La prestación de dicho servicio depende de las redes y sistemas de información, y
3. Un incidente tendría efectos perturbadores significativos en la prestación de dicho servicio.

Respecto al primer criterio, se trata, sencillamente, de comprobar si la entidad presta uno de los servicios identificados en el paso anterior. En cuanto al segundo, simplemente impone que la entidad dependa de las RSI, lo que puede comprobarse de forma fácil y objetiva. Finalmente, el tercer criterio (que recuerda a la definición de IC) requiere una labor de comprobación más compleja, relativa a la existencia de un efecto perturbador, que enseguida se tratará. Hasta ahora, los pasos que han tenido que seguir los Estados miembros pueden recopilarse como sigue: el estudio de doce sectores o subsectores, la elaboración de una lista de servicios esenciales, y la valoración de si los treinta tipos de entidades provistas en el anexo prestan los servicios esenciales fijados a la par que presentan una dependencia de alguna RSI. El último paso consiste en determinar si las entidades que han pasado los filtros anteriores verían el servicio que prestan significativamente perturbado por un incidente, para lo cual nos remitimos al artículo 6 de la Directiva. En su apartado primero, el artículo establece:

> A la hora de determinar la importancia de un efecto perturbador tal como se indica en el artículo 5, apartado 2, letra c), los Estados miembros tendrán en cuenta al menos lo siguientes factores intersectoriales:
> a) El número de usuarios que confían en los servicios prestados por la entidad de que se trate;
> b) La dependencia de otros sectores que figuran en el anexo II sobre el servicio prestado por la entidad;
> c) La repercusión que podrían tener los incidentes, en términos de grado y duración, en las actividades económicas y sociales o en la seguridad pública;
> d) La cuota de mercado de la entidad;
> e) La extensión geográfica con respecto a la zona que podría verse afectada por un incidente;
> f) La importancia de la entidad para mantener un nivel suficiente del servicio, teniendo en cuenta la disponibilidad de alternativas para la prestación de ese servicio.

Lo primero que llama la atención es que esta lista de factores intersectoriales recuerda a la de criterios horizontales vistos en materia de IC; ahora bien, en lugar de reducirse a tres elementos, ahora contamos con seis. Además de por su superioridad numérica, los criterios intersectoriales a los que ahora nos referimos también se distinguen de los relativos a las IC por su mayor concreción. En efecto, desaparecen los conceptos abstractos como "*la confianza de la población*" o "*el posible impacto medioambiental*" y, en su lugar, encontramos otros de carácter cuantificable como "*cuota de mercado*" o "*extensión geográfica*". De hecho, si atendemos al considerando vigesimoquinto, "*para determinar qué entidades están sujetas* […] *podría alcanzarse mediante la elaboración de una lista en la que se enumere a todos los operadores de servicios esenciales, o bien mediante la adopción de medidas nacionales que incluyan*

criterios objetivos y cuantificables, como la producción del operador o el número de usuarios". En la misma línea, también se observa que estos criterios no sólo resultan más fáciles de cuantificar, sino que también pueden comprobarse de forma objetiva. Así, por ejemplo, basta con acudir al anexo II y revisar las características de la entidad para comprobar si se cumple o no *"la dependencia de otros sectores que figuran en el anexo II"*(art. 6.1.b)). Finalmente, la remisión a los considerandos iniciales permite delimitar todavía más estos seis criterios, pudiendo encontrar preceptos como el que sigue:

> (27) A fin de determinar si un incidente podría tener un efecto perturbador significativo, los Estados miembros deben tener en cuenta distintos factores, como el número de usuarios que confían en dicho servicios para fines tanto privados como profesionales. La utilización de ese servicio puede ser directa, indirecta o mediante intermediario. Al evaluar el impacto, en términos de magnitud y duración, que podría tener un incidente en las actividades económicas y sociales o en la seguridad pública, los Estados miembros deben considerar también el tiempo que probablemente tendría que transcurrir antes de que la discontinuidad empiece a tener repercusiones negativas.

La lectura de este precepto aporta información adicional muy valiosa. En concreto, instruye a los Estados miembros acerca de la posibilidad de que el servicio se utilice tanto de forma directa, como indirecta o mediante intermediario. Igualmente, señala nuevas consideraciones a la hora de evaluar el impacto del incidente en términos de magnitud y duración (el tiempo que probablemente tendría que transcurrir antes de que la discontinuidad empiece a tener repercusiones negativas), aportando claridad en la valoración del criterio consagrado en el apartado c).

Por otra parte, el artículo 6 *in fine* continúa con la definición de lo que ha de constituir un incidente con efecto perturbador significativo y, si en el apartado primero nos referíamos a los factores intersectoriales, en el apartado segundo se hace alusión a los factores sectoriales.

> 2. A fin de determinar si un incidente podría tener efectos perturbadores significativos, los Estados miembros también tendrán en cuenta factores específicos del sector, cuando proceda.

Aunque, en una primera instancia, pueda parecer que el precepto no aporta demasiada claridad, conviene referirse al considerando vigesimoctavo, que provee una larga lista ejemplificativa de lo que pueden conformar estos factores sectoriales. Éste reza:

En el caso de los proveedores de energía, esos factores podrían ser el volumen o la proporción de la energía nacional generada; en el caso de los proveedores de petróleo, el volumen diario; en el caso del transporte aéreo, incluidos aeropuertos y compañías aéreas, del transporte ferroviario y de los puertos marítimos, la proporción del volumen de tráfico nacional y el número de viajeros u operaciones de transporte de mercancías anuales; en el caso de la banca o las infraestructuras del mercado financiero, su importancia sistémica, valorada según los activos totales o la razón entre estos y el producto interior bruto; en el caso del sector sanitario, el número de pacientes atendidos al año por el prestador de servicios sanitario; en el caso de la producción, tratamiento y abastecimiento de agua, el volumen y el número y los tipos de usuarios abastecidos incluidos, por ejemplo, hospitales, organismos que presten servicios públicos o particulares, y la existencia de fuentes alternativas de suministro de agua para abastecer la misma zona geográfica.

Podemos alabar la exhaustividad del precepto, en tanto que hace un barrido de todos los sectores que figuran en el anexo II, proporcionando una forma de concretar cada uno de ellos.

Con esto finaliza el proceso de identificación de operadores de servicios esenciales, cuya lista deberá ser revisada y, en su caso, actualizada, por los Estados miembros *"con regularidad, y al menos cada dos años a partir del 9 de mayo de 2018"* (art. 5.5).

3.2.2. Proveedores de servicios digitales

El procedimiento de identificación de proveedores de servicios digitales es mucho más sencillo que el de operadores de servicios esenciales, no necesitando siquiera un artículo dedicado al efecto. Sencillamente, el legislador se limita a incluir en el artículo 4 de la Directiva (dedicado a las definiciones), las líneas que siguen:

A los efectos de la presente Directiva, se entenderá por:

6) "proveedor de servicios digitales": toda persona jurídica que preste un servicio digital

5) "servicio digital": un servicio en el sentido del artículo 1, apartado 1, letra b) de la Directiva (UE) 2915/1535 del Parlamento Europeo y del Consejo[37] que sea de uno de los tipos que figuran en el anexo III.

Remitiéndonos a los preceptos que indica este artículo, la Directiva 2915/1535 aludida señala que se entenderá por "servicio":

"servicio": todo servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios.

A efectos de la presente definición, se entenderá por:

i) "a distancia", un servicio prestado sin que las partes estén presentes simultáneamente,

[37] Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p.1).

ii) “por vía electrónica”, un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético,

iii) “a petición individual de un destinatario de servicios”, un servicio prestado mediante transmisión de datos a petición individual.

En cuanto al anexo III, éste concreta tres tipos de servicios digitales a efectos del artículo 4.5: los mercados en línea, los motores de búsqueda en línea y los servicios de computación en nube.

En base a lo expuesto, constatamos que la identificación de los proveedores de servicios digitales no ofrece mayor dificultad: se trata simplemente de hallar las personas jurídicas que presten uno de los tres servicios señalados y que lo hagan a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios. La constatación de si concurren o no estos requisitos no requiere labor interpretativa alguna, y por ello el proceso identificativo no da lugar a equívocos.

En síntesis, puede afirmarse que los mecanismos previstos por la Directiva de cara a la identificación de las entidades que habrán de sujetarse a los requisitos de seguridad, son exhaustivos y concretos. Exhaustivos porque se establecen de forma ordenada y completa todos los pasos a seguir por los Estados miembros; concretos por cuanto los requisitos están minuciosamente definidos, son cuantificables e incluso vienen ilustrados por ejemplos. Así pues, aunque la labor identificativa corresponde a los Estados miembros, éstos han de sujetarse a una pautas que difícilmente dan pie a interpretaciones dispares.

3.3. Una pronunciada vocación unificadora

Hasta ahora, hemos podido destacar el rigor con que la Directiva NIS fija los procesos identificativos de los entes que deberán cumplir los requisitos de seguridad y notificación fijados por la misma. En efecto, tal y como indica el vigesimotercer considerando, se trata de “*garantizar la coherencia global del proceso de identificación en todos los Estados miembros*”. En esta misma línea, por si el detalle de este proceso no bastase, sobresalen en la Directiva otros mecanismos orientados a la consecución de su objetivo armonizador.

3.3.1. La cooperación como gran protagonista

Con la mirada puesta en una Unión Europea integrada en materia de ciberseguridad, la Directiva NIS hace especial hincapié en la cooperación que debe imperar entre los Estados miembros. Sin ir más lejos, el sexto considerando ya alude a la "*creación de un mecanismo global y eficaz de cooperación en la Unión"*. Igualmente, señala MORET que "*uno de los principales aspectos de la Directiva es la creación de nuevos mecanismos de cooperación europea*"[38]. De acuerdo con lo dicho, cabe ahora detenerse en aquellos preceptos de la Directiva que trabajan en la idea de cooperación e imponen obligaciones a los Estados miembros en este sentido. Para ello, debemos comenzar por remitirnos al Capítulo III de la Directiva, titulado "Cooperación".

La primera previsión al respecto consiste en la creación de un Grupo de cooperación "*formado por representantes de los Estaos miembros, la Comisión y la ENISA[39]"* (art. 11.2), cuyo cometido consiste *"apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros* […]" (art. 11.1). Verdaderamente, el legislador considera vital la cooperación interestatal en la búsqueda de niveles comunes de seguridad y, por ello, asigna al Grupo de cooperación una larga lista de hasta trece cometidos (art. 11.3). Entre ellos, y en relación con los objetivos de este trabajo, destaca el velar por que la identificación de los operadores de servicios esenciales por parte de los Estados miembros se lleve a cabo de forma coherente (arts. 5.6 y 11.3.l)).

Por otra parte, la Directiva también prevé la creación de una red de CSIRT[40] nacionales. Junto con los representantes de las CSIRT de cada Estado miembro, en la red de CSIRT también participarán la Comisión, en calidad de observador, y la ENISA, que desempeñará un papel activo. Esta red tendrá cometidos relacionados principalmente con el intercambio de información entre Estados miembros y el asesoramiento a los mismos en materia de ciberseguridad.

---

[38] MORET, V., "Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico español", *Instituto Español de Estudios Estratégicos: Documentos de opinión*, 3 de marzo 2017 (disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO21-2017_DirectivaNIS_VicenteMoret.pdf; última consulta 28/03/17)

[39] ENISA: Del inglés *European Network and Information Security Agency*, se trata de la Agencia Europea de Seguridad de las Redes y de la Información.

[40] CSIRT: Del inglés *computer security incident response teams*, se trata de los equipos de respuesta a incidentes.

Finalmente, el artículo 8 de la Directiva prevé la designación por cada Estado miembro de un punto de contacto único, cuyo cometido es ejercer "*una función de enlace para garantizar la cooperación transfronteriza entre las autoridades de los Estados miembros y con las autoridades competentes en otros Estados miembros y con el Grupo de Cooperación* […] *y la red de CSIRT* […]*".*

En definitiva, con el fin de alcanzar un elevado nivel común de seguridad de las RSI en el seno de la Unión, la Directiva establece una serie de mecanismos destinados a promover la cooperación entre Estados miembros.

3.3.2. La preocupación por la seguridad de las entidades excluidas del ámbito de aplicación de la Directiva

Todavía en línea con la consecución de una verdadera integración europea en materia de seguridad de las RSI, la Directiva NIS se preocupa por la protección de aquellas entidades no incluidas en su ámbito de aplicación. Así, llaman la atención dos considerandos, que se reproducen a continuación:

> (45) La presente Directiva 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 presente Directiva.
>
> (67) Puede ocurrir que entidades no incluidas en el ámbito de aplicación de la presente Directiva sufran incidentes que tengan efectos significativos en los servicios que prestan. Cuando tales entidades consideren de interés público notificar que se han producido esos incidentes, deben poder hacerlo a título voluntario. […].

Esto mismo pone de relieve MORET, cuando afirma que:

> En el marco de esa voluntad de extender la ciberseguridad lo máximo posible en el ámbito de la Unión, la Directiva acude no sólo a la obligación *ex norma* sino que también prevé que aquellas empresas que no se encuentren obligadas por la propia Directiva, pero quieran notificar los incidentes que afectan a la continuidad de sus servicios, puedan hacerlo de forma voluntaria[41].

En vista de esto, es de admirar la preocupación del legislador por prever, aun de forma sucinta, mecanismos orientados a la seguridad y notificación de incidentes de aquellas entidades que, por no considerarse operadores de servicios esenciales, no puedan acogerse a las previsiones de la disposición.

[41] MORET, V., *op. cit.*, nota 38.

3.4. Reflexión final sobre la Directiva NIS

Lo visto a lo largo del análisis de la Directiva NIS ha permitido dilucidar una serie de cuestiones en relación con nuestro objeto de estudio. En primer lugar, se ha puesto de relieve que es posible aplicar la Directiva NIS a aquellos operadores que no lleguen a calificarse como críticos, en la medida en que presten servicios esenciales y se relacionen con las RSI. Igualmente, la Directiva NIS también refuerza la protección de los operadores identificados como IC, al aplicarse a los servicios tecnológicos que éstas generalmente subcontratan. En segundo lugar, se ha observado el rigor y precisión del proceso de identificación de operadores de servicios esenciales y de proveedores de servicios digitales. Parece que, a la luz de los mecanismos identificativos provistos, los Estados miembros llegarán a conclusiones muy similares. Finalmente, se ha apreciado la preocupación del legislador por extender la ciberseguridad lo máximo posible en el ámbito de la UE, incluso cuando *ex norma* no deban cumplirse los requisitos de seguridad y notificación.

4. CONCLUSIONES

A lo largo de este Trabajo de Fin de Grado, se ha llevado a cabo una labor investigadora dirigida a la consecución de dos objetivos. En primer lugar, se ha buscado enjuiciar la protección de las infraestructuras críticas prevista en la UE desde el enfoque de su mecanismo identificativo. En segundo lugar, se ha perseguido dilucidar si la reciente normativa en materia de ciberseguridad complementa la relativa a las IC en aquellas carencias que ésta última pueda presentar. Fruto de los análisis realizados, pueden extraerse las siguientes conclusiones finales.

Primera-. La normativa relativa a la protección de las infraestructuras críticas en la UE presenta ciertas carencias en su proceso identificativo.

Lo primero que llama la atención es la paradoja entre la trascendencia de las infraestructuras críticas y el segundo plano en que se posiciona la UE. Pese a destacar el carácter transnacional de las infraestructuras críticas y la necesidad de darles un tratamiento mínimo común, el Consejo consagra la responsabilidad principal de los Estados miembros y alude a las disposiciones de la Directiva 2008/114/CE como complementarias. Para mayor abundamiento, la naturaleza compartida de la materia implica un respeto ineludible del principio de subsidiariedad.

Asimismo, la Directiva 2008/114/CE prevé un proceso de identificación de infraestructuras críticas relativamente abstracto, que deja un margen de interpretación muy amplio a los Estados miembros. En la medida en que la calificación de una infraestructura como crítica condiciona la aplicación de las medidas protectoras, la concurrencia de procedimientos identificativos dispares se torna en niveles de protección desiguales.

Finalmente, la utilización de la directiva como instrumento jurídico puede derivar en indefensión de los particulares si el Estado miembro incumple la obligación de transponer o lo hace de forma incorrecta. Aunque existen mecanismos dirigidos a contrarrestar la falta o deficiencia de transposición por parte de un Estado miembro, ninguno de ellos resulta útil en el caso que nos ocupa. En efecto, no es posible acudir a la eficacia directa de la Directiva 2008/114/CE, pues sus preceptos carecen de la precisión necesaria para que puedan invocarse. Tampoco arroja mayor luz la obligación

de los jueces nacionales de interpretar la norma interna de acuerdo con la Directiva 2008/114/CE, en la medida en que la actualidad de la materia supone que las regulaciones estatales todavía pueden ser escasas.

Segunda-. La reciente Directiva NIS adquiere una función complementaria *de facto* en relación con la protección de las infraestructuras críticas.

Toda vez que la calificación como crítica condiciona la aplicabilidad de la Directiva 2008/114/CE a una infraestructura, se desprende que aquellas que no tengan la fortuna de alcanzar este rango quedarán desprotegidas. Las infraestructuras que presten servicios esenciales pero no críticos no encontrarán, por tanto, cobijo bajo el paraguas protector de la normativa de IC. No obstante, la reciente Directiva NIS en materia de ciberseguridad se dirige a aquellas entidades que presten servicios esenciales y, al mismo tiempo, dependan de redes y sistemas de información. En consecuencia, la Directiva NIS podrá aplicarse a aquellos prestadores de servicios esenciales que, habiéndose quedado al margen de las infraestructuras críticas, presenten esta faceta tecnológica. Más aún, la Directiva NIS podrá aplicarse también a las empresas que gestionen las redes y servicios de información de las IC, reforzando su protección. En definitiva, aunque no es una norma dirigida a la protección de las infraestructuras críticas, ocurre que, *de facto,* la Directiva NIS complementa los mecanismos de seguridad de estas entidades vitales. En cierto modo, se puede decir que el ciberespacio se constituye en fuente de amenazas para las infraestructuras críticas, pero también, y por medio de la Directiva NIS, en su salvación.

Partiendo de esta premisa, no sólo destaca la aplicabilidad de la Directiva NIS sino también la calidad de sus previsiones. Ciertamente, los mecanismos de identificación de operadores de servicios esenciales y de proveedores de servicios digitales se configuran de forma completa y rigurosa, en aras de garantizar procedimientos identificativos homogéneos entre los Estados miembros y, por ende, una ciberseguridad verdaderamente armonizada.

Por último, esta voluntad de garantizar una armonización efectiva se ve reforzada mediante los mecanismos de cooperación y la preocupación del legislador por extender la ciberseguridad incluso en aquellos casos en los que, *ex norma*, la Directiva NIS no resulte de aplicación.

Tercera-. Pese a la publicación de la Directiva NIS, todavía deben tomarse pasos encaminados a la protección de las infraestructuras críticas.

A pesar de este complemento jurídico que, indirectamente, supone la Directiva NIS en la protección de las infraestructuras críticas, lo cierto es que las carencias de la Directiva 2008/114/CE siguen presentes, toda vez que no se ha promulgado, desde 2008, disposición europea alguna en la materia. Así, aunque muy socorrida a efectos prácticos, la Directiva NIS constituye más un "parche" en materia de protección de IC que una regulación dictada al efecto.

Por otra parte, no puede obviarse que la Directiva NIS todavía está pendiente de transposición, finalizando el plazo el 9 de mayo de 2018. Es evidente que, aunque se espera que las transposiciones de los Estados miembros sean homogéneas, hasta que no finalice el plazo concedido no podrá concluirse con certeza al respecto.

En vista de la complejidad de la materia y de su importancia para la subsistencia de las sociedades, cabe preguntarse si tal vez no sería más acertado que la protección de las infraestructuras críticas pasase a ser una materia exclusiva de la Unión Europea, procediéndose a su regulación mediante reglamento.

5. BIBLIOGRAFÍA Y DOCUMENTACIÓN

Libros

- MANGAS MARTÍN, A., LIÑÁN NOGUERAS, D. J., Instituciones y Derecho de la Unión Europea, Tecnos, Madrid, 2016.

- MANGAS MARTÍN, A., LIÑÁN NOGUERAS, D. J., Instituciones y Derecho de la Unión Europea, Tecnos, Madrid, 2005.

Capítulos de libro

- LIÑÁN NOGUERAS, D. J., "El Tribunal de Justicia de la Unión Europea", en *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, 2016, pp. 285-307.
    - "El sistema de normas y actos en la Unión Europea (II)", en *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, 2016, pp. 387-408.
    - "El sistema de normas y actos en la Unión Europea (II)", en *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, 2005, pp. 358-388.

- MANGAS MARTÍN, A., "Los principios de Derecho de la Unión Europea en sus relaciones con los ordenamientos internos (I)", en *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, 2005, pp. 389-449.

    - "El sistema institucional", en *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, 2005, pp. 105-128.

Artículos en revistas

- GILES, M., "Defending the digital frontier", *The Economist (Special Report on Cyber-Security)*, pp.1-2 (disponible en el enlace siguiente: http://www.economist.com/sites/default/files/20140712_cyber-security.pdf; última consulta 8/03/2017).

Normativa y otros documentos

A. De la Unión Europea

a. Tratados

- Tratado Fundacional de la Unión Europea (TFUE).

- Tratado de la Unión Europea (TUE).

b. Directivas

- 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 (DO L 345 de 23.12.2008).

- Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p.1).

- 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 (DO L 194 de 19.7.2016).

c. Comunicaciones

- Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 20 de octubre de 2004, sobre la protección de las infraestructuras críticas en la lucha contra el terrorismo.

- Comunicación de la Comisión, de 12 de diciembre de 2006, sobre un Programa Europeo para la Protección de Infraestructuras Críticas (disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Al33260; última consulta 3/03/17).

- Comunicación conjunta de la Comisión y la Alta Representante al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las

Regiones, de 7 de febrero de 2013, sobre la Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro (disponible en: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es; última consulta 2/03/17).

d. Otros documentos

- Libro Verde presentado por la Comisión, de 17 de noviembre de 2005, sobre un Programa Europeo para la Protección de Infraestructuras Críticas (disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52005DC0576; última consulta 2/03/17).

B. Del Estado español

- Presidencia del Gobierno, "Estrategia de Seguridad Nacional", 2013, (disponible en http://www.lamoncloa.gob.es; última consulta 2/04/2017).

Jurisprudencia

- Sentencia de 5 de abril de 1979, *Ratti*, 148/78, p.1642.

- Sentencia de 19 de enero de 1982, *Ursula Becker c. Finanzamt Münster-Innenstadt*, 8/81, p.71.

Recursos web

- BORREDÁ, A., "Directiva NIS: la oportunidad", *Seguritecnia*, n. 434, 2016, pp.16-22 (disponible en el enlace siguiente: http://www.seguritecnia.es/revistas/seg/434/index.html#22; última consulta 25/03/17).

- MIRANZO, M. y DEL RÍO, C., "La protección de infraestructuras críticas", *UNISCI Discussion Papers,* n.35, 2014, pp. 339-340 (disponible en https://www.ucm.es/data/cont/media/www/pag-72481/UNISCIDP35-17DELRIO-MIRANZO.pdf; última consulta 2/02/2017).

- MORET, V., "Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico español", *Instituto Español de Estudios Estratégicos:*

Documentos de opinión, 3 de marzo 2017 (disponible en el siguiente sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO21-2017_DirectivaNIS_VicenteMoret.pdf; última consulta 28/03/17).

- SÁNCHEZ GÓMEZ, F.J., "Protección de Infraestructuras Críticas en España: Marco Regulatorio y Organizativo", Seguridad y Ciudadanía: Revista del Ministerio del Interior, n.11, 2014, p.19 (disponible en http://www.interior.gob.es; última consulta 6/02/2017).
- SÁNCHEZ GÓMEZ, F.J., "Las políticas de protección de infraestructuras críticas en España", *Seguridad y Ciudadanía: Revista del Ministerio del Interior*, n.11, 2014, p.15 (disponible en http://www.interior.gob.es; última consulta 6/02/2017).