ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

78/2018 29 de junio de 2018

*Margarita Robles Carrillo**

El proceso de transposición de la Directiva sobre seguridad de redes y sistemas de información en el derecho español

El proceso de transposición de la Directiva sobre seguridad de redes y sistemas de información en el derecho español

Resumen

El proceso de transposición de la Directiva 2016/1148 sobre seguridad de redes y sistemas de información en el derecho español constituye una prioridad legislativa por la importancia de la materia, la complejidad del régimen jurídico previsto en la norma europea y por la cercanía de la fecha límite prevista a esos efectos. El Anteproyecto de Ley de Seguridad de Redes y Sistemas responde a una estructura normativa comprensible y coherente. El análisis de su régimen jurídico, normativo, orgánico y de supervisión y sanción permite determinar el grado de adecuación de esta propuesta normativa respecto de la Directiva y, desde esa perspectiva, muestra avances y carencias.

Palabras clave

Seguridad de redes y sistemas, Directiva, anteproyecto de Ley.

Margarita Robles Carrillo

The transposition process of the Directive on Network and Information Systems Security into Spanish law

Abstract

The process of integrating Directive 2016/1148 on Network Security and Information Systems into Spanish law is a legislative priority. There are three reasons: the importance of the subject, the complexity of the legal regime envisaged in the Directive and the proximity of the expected deadline for its transposition. The Draft Law on Security of Networks and Systems establishes a comprehensible and coherent normative structure. The analysis of its legal, regulatory, organic and supervisory and sanctioning regime allows to determine the degree of adequacy of this normative with respect to the Directive. There are some advances and deficiencies.

Keywords

Security of Networks and Systems, Directive, Draft Law.

Introducción

Desde su adopción, el 6 de julio de 2016, la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de redes y sistemas de información de la Unión (en adelante, Directiva NIS)[1] ha sido definida como la piedra angular de la seguridad o la norma fundamental de ciberseguridad[2]. La aplicación de esta norma ha generado un amplio debate y una intensa actividad normativa tanto a nivel comunitario[3], como en el ámbito nacional[4].

En el marco europeo, la Comisión ha seguido dos líneas de actuación. Por una parte, ha adoptado algunas de las medidas normativas de desarrollo previstas en la Directiva NIS, en particular, la decisión de ejecución por la que se crea el Grupo de Cooperación previsto en su artículo 11[5] y el Reglamento de Ejecución (UE) 2018/151 por el que se establecen normas de aplicación específicas para los proveedores de servicios digitales según lo dispuesto en su art. 16.8[6]. Por otra parte, ha desarrollado mediante actos no vinculantes los contenidos de la Directiva NIS con vistas a facilitar su transposición y aplicación por parte de los Estados miembros, en concreto, la Comunicación de la Comisión «Aprovechar al máximo la SRI - hacia la aplicación efectiva de la Directiva (UE) 2016/1148» que se acompaña de un anexo[7].

En el plano nacional, el proceso de transposición por parte de los Estados miembros, que habría de estar culminado a más tardar el 9 de mayo de 2018, no ha resultado ser una tarea fácil. En España se encuentra en tramitación el Anteproyecto de Ley sobre la Seguridad de las Redes y Sistemas de Información (en adelante, anteproyecto NIS)[8]. No es necesario subrayar la relevancia de esta norma, por sí misma y por sus efectos

---

[1] *DOUE*. L 194, de 19 de julio de 2016, p. 1.

[2] Comunicación de la Comisión «Aprovechar al máximo la SRI - hacia la aplicación efectiva de la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión». COM 0476, final, 13-9-2017; Comunicación de la Comisión «Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovador». COM 410 final, 5-7-2016.

[3] ROBLES CARRILLO, M. «Seguridad de redes y sistemas de información en la Unión Europea: ¿un enfoque integral?». *Revista de Derecho Comunitario Europeo*, n.º 60, mayo-agosto 2018.

[4] MORET MILLÁS, V. «Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico español». *Documento de Opinión 21/2017, IEEE*, 3 de marzo de 2017; WEGENER, H. «La ciberseguridad en la Unión Europea». *Documento de Opinión 77bis/2014,* IEEE, 14 de julio de 2014.

[5] *DOUE*. L 28, de 2 de febrero de 2017, p. 73.

[6] *DOUE*. L 26, de 31 de enero de 2018, p. 48.

[7] COM 476, final, 13-9-2017.

[8] http://www.minetad.gob.es/telecomunicaciones/es-ES/Participacion/Documents/anteproyecto-ley-seguridad-redes-sistemas-informacion/Anteproyecto-Ley-NIS-29nov-2017.pdf.

respecto del resto de los ámbitos jurídicos que han requerido una regulación en términos de seguridad, incluido el marco estratégico general diseñado por la *Estrategia de Ciberseguridad Nacional de 2013*. En efecto, el artículo 8 del Anteproyecto NIS afirma que dicha estrategia seguirá desarrollando las prioridades, los objetivos estratégicos y las medidas adecuadas para alcanzar y mantener un elevado nivel de seguridad de redes y sistemas de información. Los arts. 1.2 y 7 de la Directiva NIS disponen que cada Estado adoptará una estrategia nacional de seguridad de las redes y sistemas de información especificando dichos objetivos estratégicos, junto con las medidas políticas y normativas necesarias para garantizar aquel nivel de seguridad. En la reunión del Consejo Nacional de Ciberseguridad de 19 de marzo de 2018 se hace un punto de situación sobre el Anteproyecto NIS, planteándose la conveniencia de elaborar una nueva estrategia de ciberseguridad nacional que debería entrar en vigor tras la publicación de aquella ley[9]. La importancia de esta norma es indudable. No ha de extrañar, por ello, la problemática que plantea su desarrollo normativo interno.

La transposición de la Directiva NIS al derecho interno es técnicamente compleja, *ad internum*, por sus propios contenidos normativos y, *ad externum*, porque requiere un delicado ejercicio de coordinación legislativa desde una doble y complementaria perspectiva. Por una parte, transversalmente, ha de conciliarse con el régimen jurídico previsto respecto de materias como la protección de infraestructuras críticas (PIC), la protección de datos personales (PDP) o la normativa especial de seguridad en el sector público, en especial, el Esquema Nacional de Seguridad. Por otra parte, sectorialmente, ha de regularse teniendo en cuenta la normativa específica existente en materia de comunicaciones electrónicas y servicios de confianza, que ya están sujetos a sus propios requisitos de seguridad y notificación de conformidad con el artículo 1.3 de la Directiva NIS.

Como primera providencia, en el proceso de transposición se han barajado varias opciones de política legislativa: la modificación de la legislación interna sobre protección de infraestructuras críticas, la reforma de las normativas sectoriales reguladoras de los distintos sectores objeto de la Directiva NIS o la adopción de una ley de nueva planta, como ha acontecido finalmente.

[9] Puede verse en http://www.dsn.gob.es/ca/actualidad/sala-prensa/reuni%C3%B3n-del-consejo-nacional-ciberseguridad-1.

El Anteproyecto NIS cuenta con 42 artículos, tres disposiciones adicionales, una transitoria y tres finales, organizadas en cinco títulos: I. Disposiciones generales; II. Servicios esenciales y servicios digitales; III. Marco estratégico e institucional; IV. Obligaciones de seguridad; V. Notificación de incidentes; VI. Supervisión; y VII. Régimen sancionador.

La estructura general del Anteproyecto resulta extremadamente clara y coherente, al igual que gran parte de sus disposiciones de desarrollo. Hay, no obstante, algunas otras que, por carencias de fondo o de técnica normativa de la propia Directiva NIS o por su desarrollo concreto en el anteproyecto, no van a estar exentas de problemas. El objeto de este trabajo es analizar este anteproyecto desde la perspectiva de la Directiva NIS con objeto de explicar su mayor o menor adaptación a la norma europea. Para ello se aborda, en primer lugar, el modelo diseñado para los operadores de servicios esenciales (OSE) y los proveedores de servicios digitales (PSD).

Régimen jurídico de OSE y PSD

La Directiva NIS marca jurídicamente la diferencia entre OSE y PSD no solo estableciendo un régimen normativo distinto para cada categoría sino, además, separando estructuralmente, incluso cuando son similares o idénticas, las disposiciones respecto de cada uno de ellos en normas y capítulos diferentes. El anteproyecto NIS sigue una fórmula más sencilla y coherente al optar por un tratamiento conjunto de OSE y PSD y agrupar materialmente los distintos aspectos normativos —seguridad, notificación, control o sanción— realizando, en caso de ser necesarias, las correspondientes diferencias en cuanto a su régimen jurídico. Este planteamiento es, desde esa perspectiva global, más adecuada en términos de transparencia y comprensión del modelo de seguridad de redes y sistemas de información aunque, como se verá, no ocurre igual en la regulación de algunos de sus aspectos concretos.

El artículo 2 del Anteproyecto NIS establece que se aplicará a los OSE establecidos en España y a los PSD que tengan su sede social en España o la hayan designado para tener en ella su representante en la UE.

El concepto de PSD se define en sentido amplio, en el art. 4.6 de la Directiva NIS, como «toda persona jurídica que preste un servicio digital», entendiendo por tal un servicio en el sentido del art. 1.1.b) de la Directiva (UE) 2015/1535, esto es, «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»[10]. El anexo III de la Directiva NIS recoge los tipos de servicios digitales incluidos dentro de esta normativa. El anteproyecto NIS asume la misma definición remitiendo a la legislación interna y delimitando su ámbito de aplicación, respecto de las mismas categorías de servicios incluidos en la Directiva, en el artículo 2.1.b) que precisa que se trata de mercados en línea, motor de búsqueda en línea y servicios de computación en nube.

Mientras que el régimen de los PSD no se aparta de lo previsto en la Directiva NIS[11], en el caso de los OSE, la fórmula utilizada es más amplia pero, también, innecesariamente más complicada. Esa regulación puede ser valorada positivamente en la medida en que asume un concepto amplio de OSE que extiende el ámbito de aplicación de la normativa NIS y, también, negativamente por cuanto utiliza unos criterios de identificación del OSE algo más complejos que los previstos en la Directiva NIS.

La ampliación del concepto de OSE

El concepto de OSE es importante porque determina el ámbito de aplicación material y funcional de las disposiciones de la Directiva y, con ello, del modelo de seguridad de redes y sistemas de información. En este punto son dos las aportaciones principales del Anteproyecto NIS: 1) la previsión del artículo 2.1 respecto del artículo 4.1 de la Directiva; y 2) la disposición contenida en el art. 2.3 respecto del artículo 1.3 de la Directiva.

1. La Directiva NIS define el OSE en su artículo 4.1 como la entidad pública o privada incluida en el anexo II que cumple los requisitos establecidos en el artículo 5.2, donde se establecen los criterios y el procedimiento para su identificación por parte de los Estados miembros. El artículo 2.1 del Anteproyecto NIS dispone que esta normativa se aplicará a los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la ley PIC. Ello supone la ampliación del concepto de OSE más allá de lo previsto en el anexo II de la Directiva porque el anexo de la Ley PIC incluye, además de los contemplados en el anexo II de la Directiva, los siguientes ámbitos: administración, espacio, industrias

[10] *DOUE.* L 241, de 17 de septiembre de 2015, p. 1.
[11] Puede verse ENISA. *Technical Guidelines for the implementation of minimum security measures for Digital Service Providers*. Heraklion: ENISA Publications 2016.

química y nuclear, alimentación, sectores financiero y tributario y tecnologías de la información y las comunicaciones en su conjunto.

La extensión del ámbito material y funcional de aplicación de la normativa constituye una aportación muy positiva. Había sido, incluso, recomendada en la propia Directiva NIS y en la comunicación de la Comisión[12]. En la medida en que este anexo legislativo engloba un mayor número de sectores que el anexo II de la Directiva NIS, se amplía el concepto y el número de OSE desde la perspectiva del derecho interno, poniendo de manifiesto que se trata de una categoría funcional y relativa, no necesariamente idéntica o uniforme en todo el territorio de la UE, porque se hace depender de la calificación otorgada por los Estados.

El reconocimiento de ese margen de apreciación a los Estados es importante porque permite materializar los enfoques singulares que puedan tener o requerir individualmente en esta materia. Pero no hay que obviar que contribuye a incrementar la heterogeneidad del modelo general y sus eventuales disfunciones, en particular, cuando un operador presta servicios en más de un Estado miembro. Es cierto que el artículo 5.4 de la Directiva contempla esa eventualidad, aunque se limita a establecer una obligación de consulta previa a la decisión sobre la identificación. El Grupo de Cooperación tiene asignada la misión de apoyar a los Estados miembros para que adopten un planteamiento coherente en el proceso de identificación de los OSE (artículo 5.6 de la Directiva), pero esa función se concreta, en su artículo 11, en intercambiar buenas prácticas con la asistencia de ENISA.

Sobre este particular, el anteproyecto NIS se limita a reconocer que «se tendrán en cuenta, en la mayor medida posible, las recomendaciones» del Grupo de Cooperación y que, cuando un operador preste servicios en más de un Estado, se informará al punto de contacto único de dicho Estado sobre la intención de identificarlo como OSE. No es una formulación precisa atendiendo a los términos de la Directiva, pero la primacía de esta norma —que hace inaplicable la norma nacional opuesta— y la jurisprudencia Marleasing del TJUE —que obliga a una interpretación de la normativa nacional conforme al derecho comunitario— excluyen que ello pueda ser un problema, más allá del hecho de haber perdido la oportunidad de desarrollar adecuadamente aquella previsión de la Directiva.

[12] COM 476 final, 2017, pp. 23-24.

En definitiva, siendo positiva la ampliación del concepto de OSE a nuevos ámbitos de actuación más allá de los recogidos en el anexo II de la Directiva, habría sido conveniente articular en la propia Directiva y en su desarrollo interno un mecanismo de cooperación más efectivo para evitar posibles incoherencias derivadas de la diferente calificación de los OSE por parte de los Estados.

2. El artículo 1.3 de la Directiva NIS excluye la aplicación de los requisitos de seguridad y notificación respecto de los operadores sometidos al marco regulador de las comunicaciones electrónicas y los proveedores de servicios de confianza. Siguiendo ese enunciado, el art. 2.3 del anteproyecto establece que no se aplicará a los operadores de redes y servicios de comunicaciones electrónicas y a los prestadores de servicios de confianza «que no sean designados como operadores críticos en virtud de la Ley 8/2011».

El concepto de «operador crítico» es definido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (en adelante Ley PIC) como «las entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica con arreglo a la presente Ley». Este concepto sirve para someter al régimen de OSE a operadores que, en principio, por estar cubiertos por la normativa de comunicaciones electrónicas o servicios de confianza no estarían sujetos a dicha normativa, pero el hecho de ser calificados como operadores críticos permite esa operación.

Como consecuencia de ello, el concepto de OSE se amplía también al ámbito de las comunicaciones electrónicas y los servicios de confianza respecto de los sujetos considerados como operador crítico siguiendo la Ley PIC. Aunque esta opción podría suscitar alguna posibilidad de conflicto con lo dispuesto en el artículo 1.3 de la Directiva, merece ser calificada positivamente en la medida en que extiende y uniformiza los requisitos de seguridad y notificación de redes y sistemas de información.

En definitiva, la extensión del concepto de OSE —ampliando los ámbitos de actuación hasta hacerlos coincidir con los de la Ley PIC y abarcando a los operadores críticos de los sectores de comunicaciones electrónicas y servicios de confianza— se encuentra entre las principales aportaciones del Anteproyecto, aunque pueda plantear algunos problemas de orden operativo. No merece la misma opinión la reformulación de los criterios de identificación de los OSE realizada en el anteproyecto.

Los criterios de calificación del OSE

La Directiva NIS define el OSE como la entidad pública o privada que cumple los requisitos del artículo 5.2, además de estar recogida en su anexo II, y precisa en su artículo 6 el concepto de «efecto perturbador significativo», que es uno de aquellos requisitos, distinguiendo entre factores intersectoriales en su apartado 1 y factores específicos en su apartado 2. El Anteproyecto NIS remite, para la definición del OSE, a su artículo 6.2.

Los criterios recogidos en el artículo 6.2 del Anteproyecto no concuerdan exactamente con los previstos en el artículo 5.2 de la Directiva NIS. La norma interna se aparta de los criterios, especialmente claros y por ello mismo útiles, de calificación del OSE de la Directiva, asocia la definición de OSE fundamentalmente con el efecto perturbador significativo que puede tener una incidencia en la prestación del servicio y, finalmente, parece centrarse más en la importancia del servicio que en los efectos perturbadores del incidente sobre dicho servicio.

Siguiendo el artículo 6.2 del Anteproyecto, se identificará a un operador como OSE «si un incidente pudiera tener efectos perturbadores significativos en la prestación del servicio, para lo que se tendrán en cuenta, al menos, los siguientes criterios». Esos criterios atienden a la importancia del servicio prestado o se definen en relación con los clientes de la entidad en cuestión. El desarrollo de cada uno de esos contenidos guarda alguna coincidencia, que no identidad, con los factores intersectoriales de determinación de la importancia de un efecto perturbador recogidos en el artículo 6.1 de la Directiva. Al final, además de utilizar una clasificación innecesaria, porque todos los criterios organizados por separado en el artículo 6.2 del Anteproyecto se encuentran relacionados conjuntamente en el artículo 6.1 de la Directiva, no se explica tampoco la necesidad de alterar el orden y la redacción cuando el mayor grado de coincidencia entre la Directiva y la norma interna, cuando no es necesario un mayor o mejor desarrollo normativo, es una garantía de transparencia y coherencia normativas.

En mi opinión, la regulación de los criterios del artículo 5.2 y de los factores del artículo 6.1 de la Directiva NIS es suficientemente clara y precisa para hacer innecesaria una formulación normativa interna como la prevista en el artículo 6.2 del Anteproyecto. Es cierto que puede darse por supuesto que son un desarrollo de lo dispuesto en el artículo 5.2 de la Directiva NIS, pero también es verdad: 1. El contenido de la Directiva es extremadamente claro y coherente por lo que no precisaba realmente una reformulación

como la realizada en el Anteproyecto; 2. El Anteproyecto no aporta nada nuevo respecto de la Directiva, salvo la innecesaria clasificación de los criterios en dos categorías y alguna diferencia en su organización y redacción que dificulta su comprensión; y 3. A diferencia del reglamento, las directivas obligan a los Estados y es la norma de transposición interna la que se dirige al ciudadano, por lo que el mayor grado de coincidencia entre ambas demuestra en mayor medida no solo el cumplimiento de la obligación de transposición por parte del Estado sino, también, su transparencia y racionalidad normativas. Por todo ello, habría sido aconsejable limitarse a reproducir en el anteproyecto el art. 5.2 de la Directiva encajando, en su caso, los factores intersectoriales enunciados en su artículo 6.1.

Régimen normativo y orgánico

Los principios informadores del Anteproyecto NIS pueden clasificarse en dos categorías: los derivados de la Directiva NIS y los incorporados en su desarrollo interno. Entre los primeros destaca la adopción de una perspectiva integral y de un enfoque normativo global. Entre los segundos adquieren especial relevancia la equiparación del ámbito de aplicación de las leyes NIS y PIC, el tratamiento conjunto de los requisitos de seguridad y de notificación de OSE y PSD y la clarificación de las atribuciones de los distintos órganos de gestión realizada con ocasión de la transposición de la Directiva NIS.

Aproximación de la normativa NIS y PIC

La operación de acercamiento entre las normativas NIS y PIC se concreta en tres aspectos principales. En primer lugar, como ya se ha indicado anteriormente, el anteproyecto NIS amplía el ámbito de definición del OSE más allá de lo previsto en la Directiva porque añade a los sectores previstos en la misma —energía, transporte, banca, infraestructuras de mercados financieros, sanitario, suministro y distribución de agua potable, e infraestructura digital— los contemplados adicionalmente en la Ley PIC que son administración, espacio, industrias química y nuclear, alimentación, sectores financiero y tributario y tecnologías de la información y las comunicaciones en su conjunto. Con ello hace coincidir el ámbito de aplicación de ambas normativas y resuelve, desde esa perspectiva, el tema de su compatibilidad con la Directiva 2008/114/CE sobre protección de infraestructuras críticas a la que hace referencia expresamente el artículo 1.4 de la Directiva NIS.

En segundo lugar, el anteproyecto NIS asume el concepto de «servicio esencial» del art. 2 de la Ley PIC entendiendo por tal el «servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones públicas, que dependa para su provisión de las redes y sistemas de información».

En tercer lugar, el Anteproyecto NIS atribuye a los órganos de la Ley PIC la determinación de los servicios esenciales y de los OSE sujetos a la normativa NIS y equipara, asimismo, el modelo orgánico en la identificación de autoridades competentes y de los CSIRT de referencia.

Obligaciones de seguridad

El Anteproyecto dedica el título IV a los requisitos de seguridad de OSE y PSD asumiendo un tratamiento de conjunto más accesible y coherente que el realizado en la Directiva donde se situaban en capítulos distintos, extensos y con una redacción no siempre afortunada. No se obvia, a pesar de ello, la especificidad de cada uno de aquellos sujetos como ocurre, en particular, al referirse a las medidas de seguridad de los PSD en el artículo 15.4.

El art. 15 del anteproyecto reproduce las obligaciones de seguridad de OSE y PSD, en los términos fijados en los artículos 14.1 y 16.1 de la Directiva, dispone el desarrollo reglamentario de las medidas necesarias a esos efectos y refuerza la coordinación entre las autoridades competentes y los diversos órganos sectoriales con objeto, razonablemente, de evitar duplicidades y facilitar su cumplimiento por parte de los prestadores de servicios. El régimen jurídico propio de los sectores de actividad con normativas específicas sectoriales, al que se hace referencia en el art. 1 de la Directiva, se incluye en el art. 17 del Anteproyecto, recordando que esa situación no ha de afectar al modelo de coordinación y de cooperación entre autoridades y órganos competentes.

Para terminar, a diferencia de la Directiva NIS que dedica un capítulo específico, el VI, a la normalización y la notificación voluntaria, el anteproyecto NIS incluye dentro del capítulo dedicado a los requisitos de seguridad la promoción del uso de las normas técnicas como función asignada a las autoridades competentes. El artículo 16 remite al Reglamento (UE) 1025/2012 sobre normalización europea y, en ausencia de disposición

específica sobre algún extremo, encomienda la promoción de la aplicación de la normativa internacional pertinente en la materia.

Notificación de incidentes

El título V del Anteproyecto se ocupa de la notificación de incidentes destacando en su regulación dos aspectos: la homogeneización del régimen de OSE y PSD y el extenso y pormenorizado desarrollo legislativo de dicha obligación que, salvo en algunos aspectos concretos, redunda en su coherencia normativa superando, a esos efectos, las previsiones de la Directiva[13]. En algunas de sus disposiciones está prevista, además, la elaboración de disposiciones reglamentarias, instrucciones y guías.

El régimen unitario para OSE y PSD incluye una obligación de notificar que no se limita a los incidentes que puedan tener incidencia sobre los servicios esenciales o digitales, sino que también contempla los sucesos o incidencias que pueden afectar a las redes y sistemas de información, aunque aún no hayan tenido un efecto adverso real sobre los mismos (artículo 18). Contempla, asimismo, los siguientes aspectos: la protección del notificante (artículo 19), los factores y criterios de determinación de la importancia de los efectos del incidente (artículo 20), la flexibilidad (artículo 22), las incidencias en servicios digitales (artículo 23), la tramitación (artículo 24), las modalidades de información (artículos 25 a 27), la obligación de resolver los incidentes, informar y colaborar (artículo 28), la protección de datos (artículos 29 y 30) y las notificaciones voluntarias (artículo 31). Dentro de ese conjunto de disposiciones, el apartado 1 del artículo 28 no tiene un fácil encaje porque establece la obligación a cargo de los OSE y los PSD de resolver los incidentes de seguridad que les afecten y de solicitar ayuda cuando no puedan hacerlo por sí mismos, incluyendo esa previsión dentro del título V del Anteproyecto dedicado a la notificación. Atendiendo a la naturaleza y el contenido de esa obligación, su regulación habría encontrado mejor acomodo en el título IV relativo a las obligaciones de seguridad.

El modelo común establecido en este punto para OSE y PSD se manifiesta particularmente valioso en el artículo 20 del Anteproyecto que consigue homogeneizar los factores y criterios para determinar la importancia de los efectos de un incidente mejorando la deficiente reglamentación de ese extremo en la Directiva NIS. Plantea, no obstante, dos órdenes de problemas: por una parte, conceptualmente, los interrogantes

[13] Puede verse ENISA. *Incident Notification for DSPs in the context of the NIS Directive*. Heraklion: ENISA Publications 2017.

acerca de su compatibilidad con el artículo 16.10 de la Directiva, que no autoriza a los Estados a ampliar los requisitos de seguridad o notificación a los PSD; por otra parte, en los planos operativo y funcional, la dificultad de conciliar en su desarrollo y ejecución una normativa europea diferenciadora con una normativa nacional como la prevista tendente a aproximar el régimen de OSE y PSD.

El artículo 20 del anteproyecto NIS establece un modelo homogéneo para todas las entidades obligadas a la notificación de incidentes consistente en sumar, a los tres parámetros establecidos en la Directiva para valorar la importancia de los efectos de los incidentes de los OSE —el número de usuarios, la duración del incidente y la extensión geográfica (artículo 14.4 de la Directiva NIS)—, los parámetros adicionales establecidos para los PSD —el grado de perturbación del funcionamiento del servicio y el alcance del impacto sobre las actividades económicas y sociales (artículo 16.4 de la Directiva NIS)— y, adicionalmente, la importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial y el daño reputacional.

Esta normativa supone una mejora muy significativa respecto de la Directiva NIS[14], en términos sistemáticos y operativos, por cuanto contribuye a la transparencia, coherencia y funcionalidad del sistema y, además, amplia razonablemente el ámbito de aplicación de la obligación de notificación. A pesar de ello, no es una opción regulatoria exenta de problemas como consecuencia del diferente modelo de desarrollo normativo previsto en la Directiva NIS para OSE y para PSD respecto de esta obligación. El artículo 14.7 de la Directiva encomienda a las autoridades competentes actuando dentro del Grupo de Cooperación la facultad de adoptar directrices en materia de notificación para los OSE. El artículo 16.9 atribuye esa misión a la Comisión respecto de los PSD. La posibilidad de que esas normativas de desarrollo sean idénticas o, simplemente, homogéneas no está garantizada material, funcional o temporalmente. De hecho, el 30 de enero de 2018, la Comisión adopta el Reglamento de Ejecución (UE) 2018/151 donde se especifican los elementos de seguridad y los parámetros de importancia y de impacto significativo de un incidente en el caso de los PSD[15].

[14] La Directiva NIS utiliza categorías y expresiones diferentes en unos casos e intercambiables en otros para designar los supuestos en los que se precisa la notificación o respecto de los cuales hay un impacto significativo en términos de seguridad, en particular, en sus arts. 14.4 y 16.4.

[15] *DOUE*. L 26, de 31 de enero de 2018, p. 48. Puede verse ROBLES CARRILLO, M. y GARCÍA TEODORO, P. «Medidas de aplicación de la Directiva NIS: alcance y limitaciones». *Actas de las IV Jornadas Nacionales de Investigación en Ciberseguridad*. Donostia-San Sebastián, 2018.

En consecuencia, la voluntad del legislador español de convertir el régimen diferenciado a esos efectos de notificación de la Directiva NIS en un estatuto homogéneo se enfrenta al problema que plantea la previsión de un desarrollo normativo en materia de ejecución también diferenciado y su atribución a instituciones y órganos diferentes.

Hay tres disposiciones del Anteproyecto NIS que de algún modo expresan o materializan esa cierta incoherencia dispositiva de la Directiva. Por una parte, el artículo 18.4 del anteproyecto hace expresamente referencia, como criterio para desarrollar reglamentariamente esa disposición, a las directrices adoptadas por el Grupo de Cooperación, pero no menciona los actos reglamentarios procedentes de la Comisión. Por otra parte, el apartado 4 del artículo 21 establece que esta disposición relativa a las modalidades de notificación se aplicará a las notificaciones de incidentes que padezcan los PSD «en defecto de lo que establezcan los actos de ejecución previstos en los apartados 8 y 9 del artículo 16» de la Directiva NIS. Con esta previsión se introduce una quiebra apreciable y realmente innecesaria al modelo único, pero como consecuencia de lo previsto en la Directiva. Finalmente no en orden de importancia, el artículo 4 del anteproyecto dispone la obligación de tener en cuenta los actos de ejecución de la Directiva, así como todas las recomendaciones y directrices emanadas del Grupo de Cooperación y la información sobre buenas prácticas de dicho grupo y de la Red CSIRT.

En definitiva, la cuestión estriba en que un modelo único y homogéneo de notificación de incidentes resulta necesario, importante y valioso. Si no ha sido posible su adopción a nivel europeo en el marco de la propia Directiva NIS, podía haber sido factible su diseño en el marco nacional con ocasión de su transposición. Pero la posibilidad de hacerlo efectivo y operativo, sin disfunciones, disminuye como consecuencia de la dualidad establecida en la Directiva al diferenciar no solo entre OSE y PSD sino, incluso, el modelo de desarrollo normativo respecto de cada uno de ellos en materia de notificación. Si la primera diferenciación podría estar justificada, no lo está la segunda. La distinción entre OSE y PSD no necesariamente debía llevarse al extremo de atribuir a instituciones y órganos diferentes el desarrollo normativo de las disposiciones de ejecución, porque ello perjudica y limita la opción de homogeneización de su estatuto a nivel interno que autoriza y alienta el principio de armonización mínima recogido en el artículo 3 de la propia Directiva, dentro de los límites establecidos por el artículo 16.10. Un modelo único, simplificado, abundaría sin lugar a dudas en una mayor transparencia y coherencia del sistema en su conjunto.

Por último, la notificación voluntaria que el artículo 20 de la Directiva NIS limita a determinados incidentes y servicios es concebida con alcance general en el artículo 31 del Anteproyecto, porque se extiende a todos los OSE, los PSD y las entidades que no reciban esa calificación respecto de los incidentes para los que no existe aquella obligación. El régimen jurídico, por lo demás, será el mismo de las notificaciones obligatorias, salvo por el hecho de que estas últimas gozan de prioridad a efectos de su gestión en aplicación de lo que dispone, asimismo, el artículo 20.2 de la Directiva NIS.

Modelo orgánico

La clarificación de las funciones desarrolladas por los distintos órganos y entidades competentes en materia de ciberseguridad en España constituye uno de los objetivos del Anteproyecto NIS, aunque el resultado no es convincente en todos sus extremos.

La Directiva NIS dispone la creación, en el plano europeo, del Grupo de Cooperación y de la Red CSIRT y, en el marco nacional, la designación de las autoridades competentes y de los CSIRT, así como de un punto de contacto único cuando hay más de una autoridad competente.

El artículo 9 del Anteproyecto determina las autoridades competentes, siguiendo un modelo posiblemente complejo en exceso porque opera en función de tres opciones que, a su vez, se hacen depender de distintas categorías de sujetos. El resultado es el siguiente: 1) La Secretaría de Estado de Seguridad, del Ministerio de Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), será la autoridad competente en el caso de OSE que sean operadores críticos conforme a la Ley PIC; 2) La autoridad sectorial correspondiente por razón de la materia tendrá la competencia para los OSE que no sean operadores críticos; 3) La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, del Ministerio de Energía, Turismo y Agenda Digital se ocupará de los PSD; 4) El Ministerio de la Presidencia y para las Administraciones públicas, a través del Centro Criptológico Nacional, tendrá la competencia para PSD y OSE que sean operadores críticos y se encuentren comprendidos en el marco de aplicación de la Ley 40/2015, de 1 de octubre, de régimen jurídico de la administración del Estado. La coordinación entre ellos se atribuye al Consejo de Seguridad Nacional. El modelo diseñado responde a una visión sectorial o segmentada en sectores de actividad que parece obviar el hecho de que un mismo operador o proveedor puede prestar servicios esenciales, críticos, digitales o de

naturaleza pública y privada de manera que, respecto de cada uno de ellos, podría estar sujeto a una autoridad competente diferente. Es, además, complejo en su organización. Incluso, si técnica y funcionalmente resultase idóneo y comprensible para OSE y PSD, no lo es menos que resulta poco transparente y accesible para el resto de agentes y usuarios.

Los equipos de respuesta a incidentes de seguridad (CSIRT) regulados en el artículo 9 de la Directiva deben cumplir los requisitos y funciones consignados en su anexo I que se reproducen íntegramente en el artículo 12 del Anteproyecto NIS[16]. Los CSIRT son identificados en el artículo 11 del anteproyecto donde se distingue entre aquellos que operan en relación con los OSE y los que lo hacen respecto de los PSD. En el primer supuesto se incluyen el CCN-CERT, al que corresponde la comunidad de referencia constituida por las entidades sujetas a la Ley 40/2015 de régimen jurídico del sector público, el INCIBE-CERT que opera respecto de las entidades que no están sometidas a esa legislación, y el ESPDEF-CERT que cooperará con los anteriores en aquellas situaciones en las que requieran su apoyo respecto de servicios esenciales y en los que tengan incidencia en la defensa nacional. En el caso de los PSD, se ocupa INCIBE-CERT respecto de los no comprendidos en la comunidad de referencia del CCN-CERT, así como para los ciudadanos, entidades de derecho privado y otras entidades no cubiertas por el apartado 1. Hay, también, una obligación de coordinación entre ellos y respecto de otros nacionales o internacionales que será asumida por el CCN-CERT en los supuestos de especial gravedad que se determinen reglamentariamente[17]. El Ministerio de Interior, a través de la Oficina de Coordinación Cibernética del CNPIC será el centro de coordinación cuando se pueda afectar de alguna manera a operadores críticos.

El punto de contacto único tiene asignadas funciones de información, enlace y consulta en los artículos 8 y 10 de la Directiva. Solo respecto de la primera se encuentra una mención expresa en el artículo 13 del Anteproyecto que asigna esa condición al Consejo de Seguridad Nacional. A la consulta se hace referencia general en el artículo 14 relativo a la cooperación con otras autoridades con competencias en materia de seguridad o específicas sectoriales.

[16] La única diferencia entre el anexo I de la Directiva y el art. 12 del Anteproyecto es la inclusión en un mismo apartado, el 3, del contenido normativo de los apartados b) y c) del punto 2 del anexo.

[17] La reactivación del Grupo CSIRT.es muestra la importancia de esta coordinación (https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/5779-las-principales-entidades-expertas-en-ciberseguridad-se-unen-para-proteger-el-ciberespacio-espanol-2.html).

Régimen de control y de sanción

El Anteproyecto NIS implica un desarrollo amplio y pormenorizado del contenido de la Directiva en materia de sanciones, mientras que resulta excesivamente reducido en cuanto al régimen de supervisión.

Supervisión

El título VI del Anteproyecto NIS establece el régimen de supervisión del cumplimiento de la normativa en materia de seguridad de redes y sistemas de información distinguiendo, en sus artículos 32 y 33, la situación de OSE y PSD siguiendo la filosofía diferenciadora de la Directiva NIS. No hay, en este punto, un desarrollo normativo interno al nivel requerido por las previsiones de esta norma europea.

El artículo 15 de la Directiva NIS contiene una regulación muy precisa sobre la aplicación y observancia de las obligaciones por parte de los OSE en la que se definen detalladamente las atribuciones y funciones asignadas a las autoridades competentes. Con una parquedad probablemente innecesaria y que no parece justificada, en dos apartados, el artículo 32 del anteproyecto se limita a atribuir a las autoridades competentes tres facultades de control sobre los OSE: 1) requerir información para evaluar la seguridad de sus redes y sistemas de información y la aplicación efectiva de esas políticas; 2) exigirles que se sometan a auditorías externas; y 3) ordenarles la subsanación de los incumplimientos. Comparando esta norma con el artículo 15 de la Directiva se aprecian las siguientes diferencias.

En primer lugar, el apartado 1 del artículo 15 de la Directiva se refiere a la facultad de las autoridades competentes para evaluar el cumplimiento de las obligaciones por parte de los OSE y los efectos que tengan sobre la seguridad de redes y sistemas de información. Esta doble, necesaria y complementaria dimensión de su actividad de supervisión está ausente en el artículo 32 del Anteproyecto. En segundo lugar, el apartado 2 del artículo 15 de la Directiva permite a las autoridades exigir la información y las pruebas de la aplicación de las políticas que pueden ser efectivamente auditorías pero no necesariamente solo auditorías y, respecto de las cuales, las autoridades competentes habrán de indicar la finalidad de la petición y especificar la información exigida. Tampoco se encuentra mención a esos extremos en el artículo 32 del anteproyecto. En tercer lugar, no hay mención alguna en el artículo 32 del Anteproyecto a la previsión realizada en el

apartado 4 del artículo 15, al disponer que la autoridad competente cooperará estrechamente con las autoridades responsables en materia de protección de datos respecto de este tipo de incidencias. En cualquier caso, más allá de estos aspectos, la redacción y organización del artículo 15 de la Directiva es comprensible, sencilla y coherente de manera que su mera reproducción, adaptada al derecho interno, habría conducido a un resultado mejor en términos de transparencia y seguridad jurídica que el contenido en el artículo 32 del Anteproyecto.

El modelo de control previsto para los PSD en el artículo 33 del anteproyecto NIS no difiere sensiblemente del establecido en el artículo 17 de la Directiva aunque, también en este caso, resulta más clara y precisa la formulación de la norma europea. Extraña que, en su segundo apartado, el artículo 33 haga referencia a incidencias que afecten de modo significativo a servicios digitales ofrecidos por proveedores establecidos en España en otros Estados miembros, cuando se trata de un tema transfronterizo que encontraría mejor acomodo en el artículo 34 que se dedica precisamente a esa cuestión estableciendo las correspondientes obligaciones de colaboración y cooperación.

Modelo sancionador

El art. 21 de la Directiva NIS prevé que los Estados miembros establecerán el régimen de sanciones en caso de incumplimiento de las disposiciones internas de desarrollo de la Directiva NIS y adoptarán las medidas necesarias para garantizar su aplicación. Las sanciones habrán de ser efectivas, proporcionadas y disuasorias. El título VII, artículos 35 a 42, del anteproyecto se ocupa de este aspecto estableciendo el mismo régimen para OSE y PSD, mientras que el artículo 40 se dedica a las Administraciones públicas.

El artículo 36 distingue y relaciona tres categorías de infracciones —leves, graves y muy graves— respecto de las cuales el artículo 37 establece una sanción de multa, diferente en cada caso, en su apartado 1, y una de publicidad, a través del BOE y del sitio de Internet de la autoridad competente, en el apartado 2. La competencia sancionadora regulada en el artículo 41 viene determinada por la calificación de las infracciones.

La cuantía de la sanción se hace depender de tres factores: 1) La calificación de la infracción como leve, grave o muy grave, de conformidad con el artículo 36, aplicando los baremos del artículo 37; 2) Los criterios recogidos en el artículo 38; y 3) el principio de moderación de sanciones del artículo 39 que reviste dos modalidades. Por una parte, en los supuestos recogidos en el artículo 39.1, el órgano sancionador determinará la

cuantía aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en cuestión. Por otra parte, en caso de que concurran los presupuestos definidos en el artículo 39.2, atendiendo a la naturaleza de los hechos y a la concurrencia de los criterios del apartado 1, el órgano sancionador podrá acordar la no apertura del procedimiento o el apercibimiento del responsable. Finalmente, se establecen las reglas en caso de concurrencia de infracciones en el art. 42 del anteproyecto.

Conclusiones

El Anteproyecto NIS cuenta con una estructura general comprensible y coherente porque, a diferencia de la Directiva, opta por un tratamiento conjunto del régimen de OSE y PSD, sin obviar sus diferencias, y ordena materialmente los diferentes aspectos de su régimen jurídico: marco estratégico general, obligaciones de seguridad, notificación, supervisión y sanción.

Desde el punto de vista de los destinatarios, el anteproyecto NIS ha de ser valorado positivamente porque aporta un concepto más amplio de OSE, que extiende el ámbito de aplicación de la normativa NIS. No merece la misma calificación la reformulación de sus criterios de identificación, innecesariamente complicados en su definición y ordenación, que podría haberse redactado siguiendo el modelo de la Directiva, más claro y comprensible, del mismo modo que se ha hecho, acertadamente, respecto de los PSD. La idea de realizar un tratamiento conjunto de ambas categorías plantea, sin embargo, en determinadas situaciones, el problema de conciliar las normativas de desarrollo comunitarias con la norma homogeneizadora nacional.

En el plano normativo destacan, asimismo, positivamente la aproximación de la normativa NIS y PIC realizada, mediante la remisión a la Ley 8/2011, y la regulación conjunta de los requisitos de seguridad, notificación de incidentes, supervisión y régimen sancionador para OSE y PSD marcando, en cada caso, sus especificidades. No obstante, hay un importante desequilibrio entre las disposiciones dedicadas a los requisitos de seguridad y las correspondientes a la notificación de incidentes. El desarrollo extenso y pormenorizado de estas últimas contrasta con la parquedad de aquellas, a pesar de ser el núcleo esencial de esta normativa. La referencia a su desarrollo reglamentario no cubre ese déficit precisamente porque, por el carácter básico

de la materia, los requisitos de seguridad habrían merecido su regulación a nivel legislativo como mínimo al nivel dispensado a las obligaciones de notificación.

Una situación similar se reproduce en materia de supervisión y sanción. Las disposiciones del título VI del Anteproyecto constituyen una versión reducida y poco ordenada de las contenidas en la Directiva en materia de aplicación y observancia cuya mera reproducción en el derecho interno habría dado lugar a un resultado normativo más sólido en su definición, además de más claro y comprensible. El régimen sancionador es, en cambio, objeto de un desarrollo normativo extenso y detallado en el que se identifican con claridad las infracciones, las sanciones y los procedimientos y mecanismos para su aplicación, incluidos, expedientes de moderación y flexibilidad.

La importancia de la normativa sobre seguridad de redes y sistemas de información justifica un debate amplio, jurídico, técnico y político, con vistas a garantizar una transposición conforme con los contenidos de la Directiva NIS pero, también, clara, coherente y comprensible para el conjunto de los agentes y usuarios afectados por sus disposiciones. El propósito de este trabajo ha sido contribuir a ese debate.

*Margarita Robles Carrillo**
Profesora titular Derecho Internacional Público y RR. II.
Grupo NESG-TIC 233. Univ. Granada

* Este trabajo se realiza en el marco del proyecto TIN2017-83494-R financiado parcialmente por el Gobierno de España.