SEGURIDAD DE REDES Y SISTEMAS DE INFORMACIÓN EN LA UNIÓN EUROPEA: ¿UN ENFOQUE INTEGRAL?

MARGARITA ROBLES CARRILLO[1]
Universidad de Granada
mrobles@ugr.es

Cómo citar/Citation
Robles Carrillo, M. (2018).
Seguridad de redes y sistemas de información
en la Unión Europea: ¿un enfoque integral?
Revista de Derecho Comunitario Europeo, 60, 563-600.
doi: https://doi.org/10.18042/cepc/rdce.60.03

Resumen

La seguridad de redes y sistemas de información constituye, desde hace tiempo, una preocupación generalizada en el marco internacional y nacional que, en el ámbito de la Unión Europea, ha desembocado en diversos actos de carácter sectorial y, finalmente, ha conducido a la adopción de la Directiva 2016/1148, denominada directiva NIS. El análisis de su ámbito de aplicación material, funcional y subjetivo, con la distinción entre operadores de servicios esenciales y proveedores de servicios digitales, muestra que no responde al propósito inicial de asumir un enfoque integral. El régimen normativo diseñado en materia de requisitos de seguridad, notificación y normalización y los mecanismos de garantía de la efectividad de sus disposiciones tampoco se ajustan a aquel objetivo. El problema estriba en que sacraliza un tratamiento sectorial de la seguridad de redes y sistemas que difícilmente puede servir para

[1] Profesora titular de Derecho Internacional Público y Relaciones Internacionales, Grupo NESG-TIC 233, Universidad de Granada. Este trabajo se realiza en el marco del proyecto TIN2017-83494-R financiado parcialmente por el Gobierno de España.

afrontar, con unas mínimas posibilidades de éxito, el reto que supone garantizar la seguridad de redes y sistemas de información.

Palabras clave

Seguridad de redes y sistemas; datos personales; operadores de servicios esenciales; proveedores de servicios digitales.

SECURITY OF NETWORKS AND INFORMATION SYSTEMS IN THE EUROPEAN UNION: A COMPREHENSIVE APPROACH?

Abstract

The security of networks and information systems is a serious and general concern in the international and national framework. Within the scope of the European Union, it has led to various acts of a sectoral nature and to the adoption of Directive 2016/1148, called the NIS directive. The analysis of its material, functional and subjective scope of application shows that it does not respond to the initial purpose of assuming an integral approach. The normative regime established in terms of security requirements, notification and standardization and the mechanisms for guaranteeing the effectiveness of its provisions are also not adjusted to that objective. The problem is that it sanctifies a sectoral treatment of the security of networks and information systems that can hardly serve to confront the challenge of guaranteeing the security of networks and information systems.

Keywords

Security of networks and systems; personal data; operators of essential services; digital service providers.

SÉCURITÉ DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION DANS L'UNION EUROPÉENNE: UNE APPROCHE INTÉGRALE?

Résumé

La sécurité des réseaux et des systèmes d'information a longtemps été une préoccupation répandue dans le cadre international et national. Dans le cadre de l'Union européenne, elle a conduit à divers actes de nature sectorielle et à l'adoption de la Directive 2016/1148, dite directive SRI. L'analyse de son champ d'application matériel, fonctionnel et subjectif, avec la distinction entre opérateurs de services essentiels et fournisseurs de services numériques, montre qu'elle ne répond pas à l'objectif initial d'une approche intégrale. Le régime normatif établi en termes d'exigences de sécurité,

de notification et de normalisation et les mécanismes garantissant l'efficacité de ses dispositions ne sont pas non plus adaptés à cet objectif. Le problème est qu'il sanctifie un traitement sectoriel de la sécurité des réseaux et des systèmes qui peut difficilement servir à confronter, avec un minimum de chance de succès, le défi de garantir la sécurité des réseaux et des systèmes d'information.

Mots clés

Sécurité des réseaux et systèmes; données personnelles; opérateurs de services essentiels, fournisseurs de service numérique.

SUMARIO

I. INTRODUCCIÓN

La seguridad de redes y sistemas de información constituye, desde hace años, una prioridad en el marco nacional, internacional y de la Unión Europea (UE). Las estrategias nacionales de ciberseguridad coinciden en la necesidad de garantizar un uso seguro de las redes y sistemas de información y comunicación fortaleciendo, en particular, las capacidades de prevención, defensa, detección y respuesta frente a incidentes de seguridad y ciberataques y garantizando un alto de grado de resiliencia[2]. La Unión Internacional de Telecomunicaciones (UIT) considera que se trata de un componente crítico no solo para los propios sistemas de información y comunicación, sino para el conjunto de una sociedad y de una economía del conocimiento sustentadas en el avance de las tecnologías de la información y la comunicación (TIC)[3]. En esa misma línea, la Organización de Cooperación y Desarrollo Económico (OCDE, 2002) hace públicas sus primeras directrices sobre seguridad de redes y sistemas en 1992 que son actualizadas, una década después, abundando en la doble necesidad de generar una mayor conciencia y entendimiento de los aspectos de seguridad y de desarrollar una cultura de seguridad.

La preocupación sobre la seguridad de redes y sistemas de información se manifiesta en el marco de la UE, también tempranamente, con iniciativas y

[2] Un análisis detallado de las mismas se encuentra en ENISA (2016a).

[3] Véase: https://bit.ly/2LyG1pf. La actividad de la UIT en materia de seguridad de redes y sistemas de información se desarrolla principalmente en los sectores de telecomunicaciones y de normalización.

medidas de distinto alcance y naturaleza (Bangemann, 1994), que responden a un planteamiento sectorial. La normativa adoptada en materia de comunicaciones electrónicas (BIS, 2010)[4], firma electrónica[5] y servicios de la sociedad de la información, en particular, comercio electrónico[6], entre 1999 y 2002, se traduce en modalidades distintas de organización y de ejecución técnica que, a su vez, conducen a una aplicación heterogénea de los requisitos de seguridad. Esa situación no solo dificulta la efectividad misma de la normativa, sino que, además, obstaculiza el funcionamiento del mercado interior. Ello justifica la creación de la Agencia de Seguridad de Redes y Sistemas (ENISA), en 2004, como centro de conocimiento especializado para prestar asistencia a la Comisión y a los Estados miembros y facilitar su cooperación[7]. Esta solución

[4] El marco regulador de las comunicaciones electrónicas se adopta en 2002 y se modifica en 2009 mediante tres actos: a) la Directiva 2009/140/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas; la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión; y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas (DO L 337, 18 de diciembre de 2009, p. 37); b) la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) 2006/2004 sobre la cooperación en materia de protección de los consumidores (DO L 337, 18 de diciembre de 2009, p. 11); c) el Reglamento (CE) 1211/2009 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por el que se establece el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) y la Oficina (DO L 337, 18 de diciembre de 2009, p. 1). Actualmente se está discutiendo la reforma de esta normativa.

[5] La Directiva 1999/93/CE del Parlamento Europeo y del Consejo (DO L 13, 19 de enero de 2000, p. 12) es derogada por el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (DO L 257, 28 de agosto de 2014, p. 73).

[6] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (DO L 178, 17 de julio de 2000, p. 1).

[7] Reglamento (CE) 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información (DO L 77, de 13 de marzo de 2004, p. 1).

orgánica adolece de algunas carencias significativas, muy particularmente la diversidad normativa de fondo sobre la que se ve obligada a operar ENISA y el alcance limitado de sus atribuciones y recursos[8].

En realidad, la complejidad técnica de redes y sistemas, la diversidad de productos y servicios y la pluralidad y variedad de agentes implicados en su utilización y gestión explican la necesidad insoslayable y creciente de garantizar una mayor homogeneidad en cuanto a los requisitos de seguridad que no cubre la misión asignada a ENISA. Paulatinamente, se va generando en sucesivos actos normativos un cierto grado de coincidencia sobre la posibilidad de adoptar un enfoque común, integral o global[9]. Entre ellos merece destacarse

[8] La normativa sobre ENISA se localiza en: https://www.enisa.europa.eu/. Actualmente se encuentra en proceso una nueva Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a ENISA, la Agencia de Ciberseguridad de la UE, y por el que se deroga el Reglamento (UE) 526/2013, y relativo a la certificación de ciberseguridad de las tecnologías de la información y la comunicación, COM (2017) 477, final.

[9] Con ese propósito destacan los siguientes: a) la Recomendación del Consejo 95/144/CE, de 7 de abril de 1995, relativa a los criterios comunes de evaluación de la seguridad en las tecnologías de la información (DO L 23, de 26 de abril de 1995, p. 27); b) la comunicación de la Comisión de 2001 «Seguridad de las redes y de la información: Propuesta para un enfoque político europeo» traduce ese planteamiento justificando la presencia de la intervención pública, la asociación público-privada y la cooperación internacional [COM (2001) 298, final, no publicada en el DO]; c) la Resolución 2002/C 43/02 del Consejo relativa a un enfoque común y a acciones específicas en materia de seguridad de las redes y de la información insiste en ese mismo objetivo, aunque coincida, temporal y paradójicamente, con la aprobación del complejo marco regulador específico y diferenciado para las comunicaciones electrónicas (DO C 43, de 16 de febrero de 2002, p. 2); d) la Resolución 2003/C 48/01 del Consejo, de 18 de febrero de 2003, sobre un enfoque europeo orientado hacia una cultura de seguridad de las redes y de la información refuerza este planteamiento especificando, en particular, el ámbito subjetivo de los implicados y el tipo de medidas a desarrollar desde esa perspectiva (DO C 48, de 28 de febrero de 2003, p. 1); e) la Decisión 2256/2003/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, por la que se adopta un programa plurianual (2003-2005) para el seguimiento del plan de acción eEuropa 2005, la difusión de las buenas prácticas y la mejora de la seguridad de las redes y la información (Modinis), contempla medidas de carácter intersectorial dentro de un marco común para la interacción complementaria en el marco europeo de los diversos niveles nacionales, regionales y locales (DO L 336, de 23 de diciembre de 2003, p. 1); f) la comunicación de la Comisión, de 31 de mayo de 2006, «Una estrategia para una sociedad de la información segura — Diálogo, asociación y potenciación», reactiva el proyecto de enfoque integral identificándolo como una estrategia global y dinámica basada en el diálogo, la cooperación y la concienciación [COM

la Resolución 2009/C 321/01 del Consejo, de 18 de diciembre de 2009, relativa a un planteamiento de colaboración en materia de seguridad de las redes y de la información diseñado con el propósito de apoyar: a) las libertades y los derechos de los ciudadanos, incluido el derecho a la vida privada; b) una sociedad eficiente en relación con la calidad en la gestión de la información; c) la rentabilidad y el crecimiento del comercio y de la industria; y d) la confianza de los ciudadanos y las organizaciones en los sistemas de gestión de la información y de las TIC[10].

La perspectiva integral no solo se expresa material y funcionalmente, sino también en el plano subjetivo. La seguridad de redes y sistemas de información se define como una responsabilidad conjunta de todos los interesados, incluidos los operadores, los proveedores de servicios (Agustinoy Guilayn, 2016: 30), los proveedores de soporte físico y de programas informáticos, los usuarios finales, y las autoridades, instituciones y organismos públicos[11]. La necesidad de reforzar la confianza y la seguridad del conjunto de esos agentes es parte integrante, además, de la Estrategia para el Mercado Único Digital (Barrio Andrés, 2017: 425), que también asume una visión omnicomprensiva de esa realidad[12]. En definitiva, de modo progresivo y respecto de su alcance subjetivo, material, teleológico y funcional, en todos los sectores de actividad, cobra fuerza la idea de un enfoque integral y global de la seguridad de redes y sistemas.

La adopción de un enfoque integral en la normativa sobre seguridad de las redes y sistemas se justifica, además, por motivos técnicos, fácticos y de orden general[13]. Sin entrar en un análisis o una relación pormenorizada de los mismos, que excede el propósito de este trabajo (Díaz Orueta *et al.*, 2014), hay dos órdenes generales de cuestiones que explican esa situación: por una parte, como factores propios naturales, el mayor número, diversidad y

(2006) 251 final, no publicada en el DO]; g) la Resolución 2007/C 68/01 del Consejo, de 22 de marzo de 2007, sobre una estrategia para una sociedad de la información segura en Europa subraya nuevamente el enfoque global y dinámico (DO C 68, de 24 de marzo de 2007, p. 1); h) la Resolución 2007/C 68/01 del Consejo, de 22 de marzo de 2007, sobre una estrategia para una sociedad de la información segura en Europa (DO C 68, de 24 de marzo de 2007, p. 1) subraya los aspectos no meramente técnicos requeridos de un enfoque integral.

10 DO C 321, de 29 de diciembre de 2009, p. 1.

11 *Ibid*.

12 Comunicación de la Comisión «Mejorar el mercado único: más oportunidades para los ciudadanos y las empresas», COM (2015) 0550 final, 28-10-2015.

13 Una panorámica sobre esta problemática puede verse en World Economic Forum (2018) y CISCO (2018).

complejidad de los dispositivos, redes y sistemas y la mayor dependencia respecto de los mismos del conjunto de los agentes y usuarios; y, por otra parte, como factores sobrevenidos, la mayor vulnerabilidad de dispositivos, redes y sistemas, la multiplicación, diversificación y deslocalización de los riesgos y amenazas a la seguridad y, como consecuencia de todo ello, el crecimiento exponencial de los incidentes fortuitos y los ciberataques[14]. Junto a esto, la interconexión de redes y sistemas permite con dificultad su aislamiento como método de segurización, al tiempo que exige, abundando en ello, la adopción de un enfoque integral y global.

Desde esa perspectiva, la Estrategia de Ciberseguridad de la UE adoptada en 2013 reconoce dos prioridades que se definen como medidas estratégicas: por una parte, determinar requisitos mínimos comunes en materia de seguridad de las redes y sistemas de información a escala nacional; y, por otra, establecer mecanismos coordinados de prevención, detección, respuesta y atenuación que hagan posible el intercambio de información y la asistencia mutua entre las autoridades nacionales competentes en esta materia[15]. En este contexto se plantea el objetivo de elaborar una normativa a esos efectos que desemboca en la adopción de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de redes y sistemas de información de la Unión (en adelante, directiva NIS)[16].

La directiva NIS ha sido definida como la piedra angular de la seguridad[17] o la norma fundamental de ciberseguridad[18]. El proceso de transposición

---

14 Un fenómeno que crece y se diversifica, como advierte ENISA (2018b).

15 Comunicación de la Comisión «Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro», JOIN (2013) 1 final, 7-2-2013, pp. 6 y 8.

16 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 de julio de 2016, p. 1).

17 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 (2017) 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 (2016) 410 final, 5-7-2016.

18 La directiva NIS ha sido comúnmente denominada «directiva de ciberseguridad». Sobre la problemática que plantea el uso de ese término resulta de interés consultar ENISA (2015c).

interna por parte de los Estados miembros, que había de estar culminado a más tardar el 9 de mayo de 2018, no ha resultado ser una tarea fácil. En el caso de España, al cierre de este trabajo, aún no está aprobada la ley de seguridad de redes y sistemas. Pero más allá de esa problemática, que sigue abierta, la directiva NIS plantea un dilema de fondo (Robles Carrillo, 2018b).

A lo largo de este proceso se ha defendido no solo el compromiso de garantizar la seguridad de redes y sistemas de información, sino también, y de modo creciente —por haber advertido el incremento de las amenazas, así como las vulnerabilidades de la aproximación sectorial—, la importancia de adoptar una metodología y un enfoque integral en la articulación de esa política de seguridad. El análisis de las disposiciones de la directiva NIS no permite afirmar que ese haya sido el procedimiento y el resultado. La ausencia de un enfoque integral en materia de seguridad de redes y sistemas de información se aprecia en los dos aspectos esenciales de esta normativa: el ámbito de aplicación de la Directiva (epígrafe I de este artículo) y el régimen jurídico establecido en materia de obligaciones y requisitos de seguridad, notificación y normalización y garantía de la efectividad de sus disposiciones (epígrafe II de este artículo). La escasez de aportaciones científicas, más allá de los aspectos técnicos, justifica especialmente la necesidad de abordar el estudio de esta materia. Esta circunstancia, unida a la inexistencia de jurisprudencia, explica la opción por un análisis basado en los principios rectores de la interpretación de la normativa de la UE[19]. Asumiendo esa metodología, el propósito de este trabajo es analizar aquellos aspectos de la directiva NIS con objeto de demostrar la ausencia de una perspectiva integradora, la problemática que encierra en cada caso y la necesidad de plantear la posibilidad de reforma prevista en el art. 23 asumiendo, real y efectivamente, un enfoque integral de la seguridad de redes y sistemas.

II. ÁMBITO DE APLICACIÓN

El objeto y ámbito de aplicación de la directiva NIS vienen determinados en su art. 1. Esa disposición establece obligaciones para los Estados, dispone requisitos de seguridad y notificación para operadores de servicios esenciales

[19] La formulación, el contexto y los objetivos de la directiva son los criterios recomendados a esos efectos, ante la escasez de jurisprudencia y doctrina, en el anexo a la comunicación de la Comisión al Parlamento Europeo y al Consejo «Sacar el máximo partido a la SRI: hacia la aplicación efectiva de la Directiva (UE) 2016/1148», COM (2017) 476 final, anexo I, 4-10-2017.

(OSE) y proveedores de servicios digitales (PSD) y contempla la creación del Grupo de Cooperación y de la red de equipos de respuesta a incidentes de seguridad informática (Red CSIRT).

El propósito de un enfoque integral en materia de seguridad de redes y sistemas quiebra, en los planos material y funcional, por la fragmentación normativa que implica la exclusión de la aplicación de la directiva NIS respecto de ámbitos que mantienen un régimen jurídico diferenciado y, en el plano subjetivo, por la determinación de su ámbito de aplicación en función de la naturaleza de los servicios prestados y su consideración como servicios esenciales o servicios digitales en lugar de atender a la titularidad de los mismos.

1. ÁMBITO DE APLICACIÓN MATERIAL Y FUNCIONAL

El objetivo de la directiva NIS es establecer medidas para lograr un elevado nivel común de seguridad de redes y sistemas de información de la UE a fin de mejorar el funcionamiento del mercado interior. Esa seguridad es definida en el art. 4 de la directiva NIS como «la capacidad de las redes y los sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos».

El propósito de lograr un elevado nivel común de seguridad debe entenderse desde una perspectiva material respecto de los datos almacenados, transmitidos o tratados y desde una perspectiva funcional respecto de los servicios que se prestan o a los que se accede a través de esas redes y sistemas. Ello implica, en primer lugar, que hay que distinguir entre dos posibles categorías de incidentes, los que comprometen datos y/o servicios y los que no, porque solo los primeros encajan en el marco de la directiva. Una afectación de la capacidad de redes y sistemas que no se traduzca en una incidencia sobre los datos y/o sobre los servicios no supondría un déficit de seguridad a esos efectos. Una vulnerabilidad fáctica o técnica dentro de una red y/o un sistema no sería calificada como tal, en los términos de esta directiva, si no tiene una incidencia en los datos o los servicios. En segundo lugar, hay que diferenciar entre tres posibles situaciones resultantes del hecho de que se vean afectados datos, servicios o ambos. Una incidencia sobre el acceso o la provisión del servicio es una incidencia de seguridad, pero si afecta a la disponibilidad, autenticidad, integridad o confidencialidad de los datos constituye un incidente no solo de seguridad, sino también en materia de protección de datos por el hecho de vulnerar, además, la normativa específica existente en esta materia, que es

distinta según se trate de comunicaciones electrónicas[20] o no y, en este segundo supuesto, difiere si es de aplicación la normativa general —la Directiva 95/46 derogada a partir del 25 de mayo de 2018 por el Reglamento General de Protección de Datos (RGPD)[21]—, la específica aplicada en el caso de las instituciones y órganos de la UE conforme al Reglamento (CE) 45/2001[22] o la relativa a la administración electrónica (Troncoso Reigada, 2008). El régimen jurídico es, en consecuencia, diferente atendiendo a si se han afectado o no datos o servicios, si ha ocurrido respecto de unos u otros o ambos y dependiendo, en caso de ser datos, de la naturaleza electrónica o no de la comunicación, de si el tratamiento de los datos se realiza o no por las instituciones y órganos de la UE o de si se trata del ámbito de la administración electrónica.

La situación se complica, adicionalmente, por la definición de redes y sistemas de información realizada en el art. 4.1 de la directiva, por dos motivos. El primero es que se define ese concepto por remisión a la Directiva 2002/21/CE, entendiendo por tal una red de comunicaciones electrónicas en el sentido de su art. 2.a)[23]. Ello implica que, tratándose del mismo concepto, el elemento determinante no es materialmente la red o el sistema, sino el servicio o el uso que se da a los mismos, lo que marca su diferente régimen jurídico, que será el

---

20 Véase la nota 4. La Comisión ha presentado una propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE [(Reglamento sobre la privacidad y las comunicaciones electrónicas), COM/2017/010 final, 10-1-2017].

21 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (DO L 119, de 4 de mayo de 2016, p. 1). Véase Piñar Mañas (2016).

22 Reglamento (CE) No. 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8, de 12 de enero de 2001, p. 1).

23 Una red de comunicaciones electrónicas se define como «los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes, incluido Internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada».

del marco regulador de las comunicaciones electrónicas o el de la directiva NIS, según se use o no con esa otra finalidad. En segundo lugar, dentro de la definición de redes y sistemas, se incluyen los datos digitales almacenados, tratados, recuperados o transmitidos mediante una red electrónica o a través de cualquier dispositivo o grupo de dispositivos interconectados o relacionados entre sí[24]. Como consecuencia de ello, mientras el régimen de comunicaciones electrónicas separa la regulación del medio de la regulación del contenido, la directiva NIS incluye el contenido mismo en la definición del medio, pero no todo el contenido, sino solo los datos, prescindiendo del componente de los servicios.

Situada en ese contexto normativo, la directiva NIS delimita su marco de aplicación mediante la exclusión de determinados ámbitos de alcance más general (art. 1.4 y 6 y considerando 45) y de algunos aspectos concretos de distinta naturaleza (art. 1.3, 5 y 7).

A) Con carácter general, la directiva NIS establece en el art. 1.6 una cláusula de salvaguardia relativa al cumplimiento de funciones estatales esenciales, en particular, la seguridad nacional y el orden público. Dispone, asimismo, en su art. 1.4, que se entenderá sin perjuicio de lo previsto en la Directiva 2011/93/UE, relativa a la lucha contra los abusos y la explotación sexual infantil[25], la Directiva 2013/40/UE del Parlamento Europeo y del Consejo relativa a los ataques a los sistemas de información[26] y la Directiva 2008/114/CE del Consejo sobre identificación y designación de infraestructuras críticas y la evaluación de la necesidad de mejorar su protección[27]. Las dos primeras no ofrecen realmente posibilidades de colisión con el contenido de la directiva NIS.

La Directiva 2008/114/CE relativa a las infraestructuras críticas no contempla la infraestructura digital o las redes y sistemas de información entre los sectores y subsectores del anexo I. En 2009, en paralelo a la introducción de los requisitos de seguridad en el marco regulador de las comunicaciones electrónicas con la aprobación de la Directiva 2009/140/CE, la Comisión adopta la Comunicación sobre protección de infraestructuras críticas de información identificando amenazas y riesgos que requieren garantizar un elevado nivel de seguridad y resistencia[28]. Pero la Directiva 2008/114/CE no establece requisitos de seguridad y notificación como los previstos en materia de comunicaciones

[24] Además de la red de comunicaciones electrónicas y de los datos digitales se incluye en esta categoría, siguiendo la definición del art. 4.1, «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».

[25] DO L 335, de 17.12.2011, p. 1.

[26] DO L 218, de 14.8.2013, p. 8.

[27] DO L 345, de 23.12.2008, p. 75.

[28] COM (2009) 149 final, 30-3-2009.

electrónicas, prestadores de servicios de confianza o en la propia directiva NIS. El objeto de esta norma es, de conformidad con su art. 1, establecer un procedimiento de identificación y designación de infraestructuras críticas europeas (ICE) y un planteamiento común para evaluar la necesidad de mejorar su protección. El primero difiere del establecido en la directiva NIS para la identificación de operadores de servicios[29], mientras que el segundo se concreta, básicamente, en la previsión de los planes de seguridad del operador (PSO), los responsables de enlace para la seguridad y los mecanismos de información y evaluación. El anexo II, al disponer el procedimiento PSO ICE, identifica como componente del mismo dos órdenes de medidas, permanentes y graduales, incluyendo dentro de las primeras una referencia a medidas técnicas, organizativas, de control y verificación y seguridad de los sistemas de información que no admite comparación con lo dispuesto en la directiva NIS. La Ley 8/2011, de 28 de abril[30], por la que se transpone la directiva al derecho español incluye, sin embargo, dos disposiciones específicas relativas a la seguridad de los sistemas de información y comunicaciones en el art. 15 y a la seguridad de los datos clasificados en el art. 18. Curiosamente, también ofrece un concepto de «servicio esencial» que tampoco se identifica con su definición en la directiva NIS. El resultado de todo ello es que los requisitos de seguridad y notificación son diferentes en cada caso.

Finalmente, hay una exclusión también de orden general explicada en el considerando 45 al advertir que la directiva se aplica únicamente a las administraciones públicas que hayan sido identificadas como OSE. Es, por ello, responsabilidad de los Estados garantizar la seguridad de redes y sistemas de información de las administraciones públicas en la medida en que no presten esos servicios incluidos en el ámbito de aplicación de la directiva. En el anexo a la comunicación de la Comisión «Sacar el máximo partido a la SRI», esta institución estima que sería conveniente que los Estados consideraran la posibilidad de inclusión de la Administración Pública dentro del ámbito de aplicación de la directiva, al realizar la transposición a su derecho interno, incluso cuando se trate de servicios no incluidos dentro del anexo II ni encajables dentro de los requisitos del art 5.2[31]. El problema estriba en que depende

[29] Comparar el art. 3 de la Directiva PIC con el anexo V de la directiva NIS.

[30] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (BOE 102, de 29 de abril de 2011, p. 43.370).

[31] La Administración está incluida entre los sectores recogidos en el anexo de la Ley 8/2011 a los que en España se aplica la normativa NIS por tratarse de OSE, de conformidad con el art. 2.1 del Anteproyecto de Ley de Seguridad de Redes y Sistemas.

de los Estados esa calificación cuando, en realidad, la Administración habría de ser considerada en su totalidad como un servicio esencial por su propia naturaleza y porque cumple los criterios establecidos en el art. 5.2 en la medida en que presta un servicio esencial para el mantenimiento de actividades económicas o sociales, lo hace a través de redes y sistemas de información y un incidente puede tener efectos perturbadores significativos en la prestación de dicho servicio[32].

B) Sobre aspectos concretos, la directiva NIS delimita su ámbito de aplicación en el art. 1.3 respecto de los requisitos de seguridad y de notificación, en el art. 1.5 respecto de la confidencialidad de la información y en el art. 1.7 cuando exista una *lex specialis* con un efecto equivalente al de las obligaciones establecidas en esta directiva para OSE y PSD.

a) Las obligaciones impuestas a los OSE y a los PSD en cuanto a los requisitos de seguridad y notificación no serán de aplicación, de conformidad con el art. 1.3, a las empresas sujetas a los requisitos de los arts. 13 bis y 13 ter de la Directiva 2002/21/CE, donde se establece el marco regulador de las comunicaciones electrónicas, ni a los proveedores de servicios de confianza sometidos a los requisitos del art. 19 del Reglamento (UE) 910/2014[33], que contiene la normativa sobre identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior.

En realidad, el Reglamento (UE) 910/2014 establece en el art. 8 los niveles de seguridad de los sistemas de identificación electrónica y en el art. 19, los requisitos de seguridad aplicables a los proveedores de servicios de confianza. Al tratarse de un reglamento, el alcance y la naturaleza de las obligaciones son distintos. Pero es que, además, hay un régimen diferente en identificación electrónica que se refiere a datos y en requisitos de seguridad que abarcan datos y servicios, así como un sistema de supervisión más estricto en el caso de los proveedores cualificados de servicios de confianza respecto de los no cualificados. En materia de identificación electrónica, el art. 8 establece tres

[32] En España se adopta el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica. La finalidad del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. Siguiendo los términos de esa disposición, el ENS tiene presentes las recomendaciones de la Unión Europea. Pueden verse sus guías de seguridad en: https://bit.ly/2JdSosd.

[33] DO L 257, de 28 de agosto de 2014, p. 73.

niveles de seguridad —bajo, medio y alto[34]— basados en los correspondientes criterios de determinación fijados en función de las especificaciones técnicas, las normas y los procedimientos adoptados mediante actos de ejecución de la Comisión, de conformidad con lo previsto en su apdo. 3, que reenvía al procedimiento del art. 48.2[35]. Por su parte, en cuanto a los requisitos de seguridad aplicables a los proveedores de servicios de confianza, el art. 19 establece que adoptarán las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios y para evitar y reducir el impacto de los incidentes e informar a los interesados. La notificación, sin demoras indebidas y en un plazo máximo de 24 horas, se realizará al organismo de supervisión; a los organismos relevantes; a la persona física o jurídica víctima del incidente, en su caso; a los organismos de supervisión de los Estados afectados y a ENISA, si supera el marco del Estado, y al público si reviste un interés de esa naturaleza (art. 19.2)[36]. El organismo de supervisión, cuyas atribuciones no son equiparables a las de las autoridades competentes en la directiva NIS o en la normativa de comunicaciones electrónicas[37], ha de informar a ENISA anualmente sobre estas notificaciones (art. 19.3).

Por su parte, atendiendo a la otra norma a la que se refiere el art. 1.3 de la directiva NIS para excluir su aplicación, la Directiva 2002/21/CE establece el marco regulador común para las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles

---

34 Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (DO L 235, de 9 de septiembre de 2015).

35 Los criterios utilizados en el Reglamento de Ejecución son bajo, sustancial y alto. Aunque, como se explica en el texto, se ha tenido en cuenta la norma internacional ISO/CEI 29115 en relación con las especificaciones y procedimientos, en la medida en que el Reglamento 910/2014 se aparta de ella, en el anexo no se hace referencia a los contenidos específicos de esa norma internacional (*ibid.*).

36 Decisión de Ejecución (UE) 2015/1984 de la Comisión, de 3 de noviembre de 2015, por la que se definen las circunstancias, formatos y procedimientos de notificación con arreglo al artículo 9, apartado 5, del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (DO L 289, de 5 de noviembre de 2015, p. 18).

37 Véase el art. 17 del Reglamento 910/2014.

para el público, abarcando la regulación de la transmisión, pero no la regulación de los contenidos de los servicios prestados. La Directiva 2009/140/CE del Parlamento Europeo y del Consejo, de 25 de noviembre, por la que se modifica, entre otras, esa llamada directiva marco, incorpora un art. 13 bis relativo a la seguridad e integridad de las redes y de los servicios y un art. 13 ter sobre aplicación y cumplimiento de esa normativa. El art. 13 bis establece que los Estados miembros velarán por que las empresas en cuestión adopten las medidas técnicas y organizativas adecuadas para gestionar los riesgos, para evitar y reducir el impacto de los incidentes[38] y para garantizar la integridad de las redes a efectos de garantizar la continuidad del servicio (art.13 bis 1 y 2)[39]. Esta última exigencia no se incluye en el caso de los proveedores de servicios de confianza. Las previsiones en materia de notificación son similares en ambos casos[40], pero la información anual por parte de los organismos de supervisión se ha de dirigir a la Comisión y a ENISA en el caso de las redes y servicios de comunicaciones electrónicas (art. 13 bis 3) y solo a ENISA en el caso de los proveedores de servicios de confianza (art. 19.3)[41]. El art. 13 ter dispone que los Estados miembros velarán para que las autoridades nacionales de reglamentación estén facultadas para dar instrucciones vinculantes a las empresas, para exigirles el suministro de información para la evaluación de seguridad y la realización de auditorías de seguridad y para investigar los casos de incumplimiento. Esta última previsión no se contempla expresamente en el caso de los OSE y PSD, mientras que solo respecto de los OSE —y no respecto de los PSD, ni tampoco para los servicios y redes de comunicaciones electrónicas— está previsto que las autoridades competentes especifiquen la información exigida e indiquen la finalidad de su petición (art. 15.2 de la directiva NIS).

En consecuencia, los requisitos de seguridad y notificación cuentan con un régimen normativo en el ámbito de las comunicaciones electrónicas, otro para la identificación electrónica y otros tres para los proveedores de servicios de confianza —cerrado, normal y cualificado—, a los que se suman, ahora, los dos aportados por la propia directiva para OSE y PSD[42].

La situación se complica, además, porque cabe la posibilidad de que la prestación de servicios por parte de una empresa no se limite exclusivamente

[38] Los criterios no coinciden precisamente con los previstos en la directiva NIS y en el Reglamento de Ejecución de la Comisión (UE) 2018/151. Véase ENISA (2015b).

[39] Estas medidas son detalladas en ENISA (2014c).

[40] Puede verse ENISA (2014b).

[41] Sobre sus particularidades véase ENISA (2015a).

[42] En el caso de la UIT se realiza un tratamiento conjunto de la seguridad de las telecomunicaciones y de la seguridad de la información. Véase UIT (2006).

a los incluidos en el ámbito de aplicación de uno de aquellos conjuntos normativos. Un proveedor de servicios puede abarcar más de uno de esos ámbitos funcionales de actuación. En el caso de que un proveedor ofrezca servicios incluidos dentro del ámbito de aplicación de la directiva NIS, por tratarse de alguno de los comprendidos en los anexos II y III, respecto de ellos la empresa queda sujeta a la normativa NIS. El resto de los servicios se ajustarán a los requisitos previstos en cada ámbito normativo. Un mismo sujeto habrá de adaptarse respecto de la misma materia —los requisitos de seguridad y notificación— a regímenes normativos diferentes determinados por el tipo de servicio prestado en cada caso. El enfoque sectorializado conduce a que la normativa aplicable depende del tipo de servicio, no de la materia, ni de la titularidad del mismo, de manera que un sujeto puede estar sometido a requisitos y procedimientos de seguridad diferentes en cada caso. Además de una notable falta de transparencia y coherencia del modelo de seguridad, implica un escaso respeto al principio de economía de medios, cargas y procedimientos[43].

La problemática derivada de la ausencia de un enfoque integral en materia de requisitos de seguridad de redes y sistemas de información se complica, asimismo, por la previsión de mecanismos distintos y específicos en materia de protección de datos personales y/o de la privacidad[44]. Hay un régimen especial en el ámbito de las comunicaciones electrónicas (Comisión, 2015), además del general recogido en el RGPD a partir de mayo de 2018 (Martínez: 2018), del previsto en el art. 2 de la directiva NIS respecto del tratamiento de datos por parte de las instituciones y órganos de la UE y del establecido en el marco de la administración electrónica. La falta de un enfoque común en materia de seguridad, protección de datos y privacidad ha sido considerada un obstáculo principal en el camino del mercado único digital[45], incluso por las divergencias existentes en materia de notificación de incidentes[46].

b) El art. 1.5 establece, sin perjuicio del art. 346 del TFUE, el régimen en materia de información confidencial. La información que merezca esta calificación según la normativa europea o nacional se intercambiará con la

43 Sobre la importancia de un lenguaje común, véase ENISA (2018a).

44 Sobre la necesidad y la dificultad de conciliar ambas normativas, en materia de redes y servicios de comunicaciones electrónicas, véase ENISA (2013a).

45 Esta situación «can lead to a lack of understanding of the crosscutting nature of digital services and the pervasiveness of cybersecurity, resulting in insufficient cooperation and coordination between the national data protection and information security authorities» (EPRS, 2017: 27).

46 La doctrina también se ha ocupado de comparar la normativa en materia de notificación en el marco de la directiva NIS y en el RGPD (Jasmontaite, 2008; Menges y Pernul, 2008).

Comisión y otras autoridades competentes solo en la medida necesaria, pertinente y proporcionada para la aplicación de la normativa NIS y preservando la confidencialidad y los intereses de seguridad y comerciales de los OSE y PSD.

c) Las obligaciones de la directiva NIS tampoco serán de aplicación, según el art. 1.7, en los supuestos en los que exista o se adopte una *lex specialis*, siempre y cuando los requisitos de seguridad y de notificación establecidos en ella sean, al menos, equivalentes a las disposiciones correspondientes de la directiva. En esos supuestos se aplicará el acto jurídico sectorial específico, incluidas las disposiciones relativas a la competencia judicial[47].

Tampoco en este caso va a ser una operación fácil aplicar esta exclusión porque, una vez identificados los servicios, exigirá comprobar los requisitos específicos de seguridad de la norma sectorial para mantenerlos en caso de que sean equivalentes o superiores a los contemplados en la directiva NIS o para excluir la aplicación de esa *lex specialis* si no lo son. En los considerandos 10 a 13 de la directiva NIS se contemplan tres supuestos: el transporte marítimo y fluvial, la regulación y la supervisión del sector bancario y las infraestructuras de los mercados financieros[48]. Siguiendo el anexo de la comunicación de la Comisión «Sacar el máximo partido a la SRI», no hay legislación sectorial relativa a los PSD que establezca requisitos similares a los de la directiva NIS. En el caso de los OSE, los ámbitos sectoriales dotadas de requisitos de seguridad o notificación potencialmente equiparables se limitan al sector financiero y, en particular, la banca y las infraestructuras de los mercados financieros[49].

El resultado es que, desde una perspectiva material y funcional, la directiva NIS no supone una homogeneización de la seguridad de redes y sistemas para el conjunto de los servicios realizados a través de redes y sistemas de información, para todos los prestadores y para todos los ámbitos materiales de actuación en los que pueden verse afectados datos y/o servicios. No existe

---

47 Siguiendo el considerando 9 de la directiva, «los Estados miembros deben aplicar lo dispuesto en los mencionados actos jurídicos sectoriales de la Unión, incluidos los relativos a cuestiones de competencia judicial, y no deben llevar a cabo el proceso de identificación de los operadores de servicios esenciales, tal como se definen en la presente Directiva».

48 Sobre la problemática que plantea la gestión de las diferentes normativas presentes en este ámbito, véase ENISA (2014a).

49 Se trataría de la Directiva (UE) 2015/2366 sobre servicios de pago 2 (DO L 337, de 23 de diciembre de 2015, p. 35), el Reglamento (UE) 648/2012 de 4 de julio de 2012 (DO L 201, de 27 de julio de 2018, p. 1) y la Directiva 2014/65/UE del PE y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (DO L 173, de 12 de junio de 2014, p. 349).

un modelo común uniforme en materia de obligaciones, requisitos o procedimientos en materia de seguridad de redes y sistemas de información, ni tampoco de notificación, sino que la propia directiva sacraliza la diversidad de regímenes normativos y procedimentales. A ello se suma la circunstancia de que el núcleo de esta construcción normativa es el «servicio», no el titular del mismo, ni los sujetos públicos o privados, ni tampoco exactamente los ámbitos materiales de actuación, sino la naturaleza de los servicios prestados y, en su caso, de los datos vinculados a esos servicios.

2. ÁMBITO DE APLICACIÓN SUBJETIVA

La directiva NIS establece un régimen jurídico diferenciado para dos categorías de sujetos: los OSE y los PSD. Los primeros son definidos en el art. 4.1 como la entidad pública o privada incluida en el anexo II que cumple los requisitos establecidos en el art. 5.2, donde se establecen los criterios y el procedimiento para su identificación por parte de los Estados miembros. Los PSD se conciben en sentido amplio, según 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»[50].

2.1. Operadores de servicios esenciales (OSE)

El concepto de OSE sujeto a la normativa de la directiva NIS viene determinado por tres parámetros de distinto alcance y naturaleza: a) La inclusión en alguno de los sectores o subsectores del anexo II; b) El cumplimiento de los criterios establecidos en el art. 5.2 y, entre ellos, el concepto de efecto perturbador recogido en el art. 6, donde se establecen factores intersectoriales y factores específicos; y c) La identificación por parte de los Estados miembros siguiendo el procedimiento previsto en el art. 5.

A) El anexo II incluye los siguientes sectores y, en su caso, subsectores: energía (electricidad, crudo y gas); transporte (aéreo, terrestre, marítimo y fluvial y por ferrocarril); banca; infraestructuras de mercados financieros; sanitario; suministro y distribución de agua potable; e infraestructura digital.

La mayoría de estos sectores son definidos en la normativa comunitaria previamente adoptada a la que remite el propio anexo II. No es el caso de la

[50] DO L 241, de 17 de septiembre de 2015, p. 1.

infraestructura digital, razón por la cual la Comisión procede a su definición en el anexo a la comunicación «Sacar el máximo partido a la SRI», donde se designa y explica el punto de intercambio de internet (IXP), el sistema de nombres de dominio (DNS) y el registro de nombres de dominio de primer nivel (TLD)[51]. Más allá del hecho de que esas definiciones no cuentan con el respaldo de su formulación normativa en un acto jurídicamente vinculante, se aprecian algunos errores y carencias significativas en su definición. La confusión de la IANA con la ICANN y la asignación a la primera de las funciones que realiza la segunda a través de una nueva entidad, llamada Public Technical Identifiers (PTI) —no de la IANA—, desde la reforma de la ICANN que se hace efectiva el 1 de octubre de 2016, es sintomática de un deficiente conocimiento de esta, por lo demás, compleja materia[52]. También la gestión de la zona raíz del DNS es competencia de la ICANN, a la que no se hace referencia en el documento de la Comisión[53], a pesar de constituir el componente principal y básico de la misma (Robles Carrillo, 2016). No es posible determinar si la ausencia de referencia a los registros de dominio con código de país (ccTLD) se debe a su consideración como no esenciales —absolutamente discutible—, a la ausencia de acuerdo institucional entre los legisladores comunitarios para su inclusión en el anexo II o a un impreciso conocimiento sobre el alcance y la importancia de los ccTLD como infraestructura digital. Cualquier incidencia sobre los mismos puede causar efectos igualmente perturbadores a los previsibles en el caso de los TLD. En el caso de los demás subsectores, extraña la ausencia de referencia a ámbitos de valor significativo por los servicios que prestan como otras modalidades distintas de suministro de energía, el sector alimentario o medioambiental o protección civil.

En este punto, si el OSE presta un servicio cubierto por alguna *lex specialis* en los términos del art. 1.7 de la directiva, no se continuará el proceso de identificación, al estar excluido del ámbito de aplicación de la directiva NIS[54]. En caso contrario, se ha de continuar dicho proceso siguiendo los criterios del art. 5.2.

---

51 Anexo a la comunicación de la Comisión «Sacar el máximo partido a la SRI», COM (2017) 476 final, 4-10-2017, pp. 21-23.

52 *Ibid.*, pp. 22-23.

53 *Ibid*. La importancia del DNS en la infraestructura digital es un hecho poco conocido que ha sido analizado doctrinalmente poniendo de relieve su función en términos de gobernanza del ciberespacio (Musiani, 2016).

54 Anexo a la comunicación de la Comisión «Sacar el máximo partido a la SRI», COM (2017) 476 final, 4-10-2017, p. 26.

B) El OSE viene definido en el art. 4 de la directiva como la entidad pública o privada del Anexo II que reúne los criterios del art. 5.2 que son: a) la prestación de un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales; b) esa prestación depende de redes y sistemas de información; y c) un incidente tendría efectos perturbadores significativos sobre la prestación de dicho servicio. Para ello se recurre a dos tipos de criterios: los factores genéricos intersectoriales[55] y los factores específicos para cada sector[56]. En caso de cumplirse, se inicia en sentido estricto el proceso de calificación.

C) El procedimiento de calificación comienza con la identificación por parte de cada Estado de los OSE existentes en su territorio para cada sector y subsector del anexo II, antes del 9 de noviembre de 2018, mediante la elaboración de una lista de servicios (art. 5.3). Si la entidad presta servicios en más de uno, los Estados se consultarán con carácter previo[57]. A partir de ahí, tienen la obligación de revisar y actualizar regularmente esa lista (art. 5.5) y de remitir a la Comisión la información necesaria para evaluar la aplicación de la directiva, en particular las medidas nacionales de identificación de los OSE, la lista de servicios, el número y los umbrales existentes, en su caso, para determinar el nivel de suministro adecuado o la importancia del OSE en concreto (art. 23.1).

Atendiendo al principio de armonización mínima del art. 3, los Estados pueden ampliar los sectores o subsectores sometidos a los requisitos de seguridad y notificación extendiendo el ámbito subjetivo de los OSE. Entre los supuestos objeto de consideración a esos efectos se encuentran, principalmente, las administraciones públicas que no se incluyen en el anexo II, ni cumplen los criterios del art. 5.2 la industria química y nuclear o los sectores alimentario, postal, medioambiental o protección civil[58].

---

55 Entre ellos se encuentran el número de usuarios, la dependencia de otros sectores, la repercusión en términos de grado y duración, la cuota de mercado, la extensión geográfica y la importancia de la entidad para mantener un nivel suficiente de servicio.

56 Estos, que se relacionan en los considerandos de la directiva, son: el volumen generado en el caso de la energía, el volumen de tráfico en el transporte, la importancia sistémica de la entidad de crédito o el número de pacientes en el marco sanitario, entre otros.

57 La finalidad de esta consulta es facilitar la evaluación sobre el carácter crítico del OSE en términos de impacto transfronterizo. Si no se llegase a un acuerdo, se puede solicitar la asistencia del Grupo de Cooperación.

58 Anexo a la comunicación de la Comisión «Sacar el máximo partido a la SRI», COM (2017) 476 final, pp. 23-24.

2.2. Proveedores de servicios digitales (PVD)

El anexo III de la directiva NIS recoge los tipos de servicios digitales incluidos dentro del ámbito de aplicación del art. 4.5: mercado en línea, motor de búsqueda en línea y servicios de computación en la nube. El capítulo V de la directiva, donde se desarrolla la normativa sobre requisitos en materia de seguridad y notificación y su régimen normativo específico, no se aplica a los PSD cuando sean microempresas o pequeñas empresas en los términos definidos en la Recomendación 2003/361/CE de la Comisión[59].

El mercado en línea es un servicio digital que permite a los consumidores o a los comerciantes, en los términos definidos en la Directiva 2013/11/UE, celebrar contratos de compraventa o de servicios en línea con comerciantes, ya sea en el sitio web del mercado en línea o en un sitio web de un comerciante que utilice servicios informáticos proporcionados por el mercado en línea (art. 4.17)[60].

El motor de búsqueda en línea es un servicio digital que permite a los usuarios hacer búsquedas de todos los sitios web o de sitios web en una lengua en concreto mediante una consulta sobre un tema cualquiera en forma de palabra clave, frase u otro tipo de entrada, y que, en respuesta, muestra enlaces en los que puede encontrarse información relacionada con el contenido solicitado (art. 4.18)[61].

El servicio de computación en la nube hace posible el acceso a un conjunto modulable y elástico de recursos informáticos que se pueden compartir (art. 4.19)[62]. Ello incluye recursos como redes, servidores u otras infraestructuras, sistemas de almacenamiento, aplicaciones y servicios que se proporcionan a múltiples usuarios que, actuando por separado al mismo, comparten un acceso común al servicio. El considerando 17 de la directiva precisa que el término «modulable» se refiere a los recursos de computación que el PSD puede asignar de manera flexible con independencia de la localización geográfica de los recursos para hacer frente a fluctuaciones de la demanda. El término

[59] DO L 124, de 20 de mayo de 2003, p. 36.

[60] Siguiendo el considerando 15, no pueden tener por objeto servicios que constituyan solo un paso intermedio para acceder a servicios prestados por terceros con los que finalmente se celebra el contrato, ni limitarse a la comparación de sus precios.

[61] No incluye las funciones de búsqueda que se limiten al contenido de un sitio web en concreto, ni tampoco a servicios en línea que se solo se dediquen a comparar precios o servicios.

[62] Hay diferentes tipos de nube. Técnicamente son similares pero, jurídicamente, se distingue entre públicas, privadas, híbridas y comunitarias. Véanse: ENISA (2017: 14; 2015d y 2013b).

«elástico» describe los recursos de los que se abastece y que se ponen a la venta según la demanda (Herbst *et al.*, 2013). Por su parte, el anexo de la comunicación de la Comisión «Sacar el máximo partido a la SRI» recoge tres tipos principales de servicios de computación en nube: infraestructura como servicio (IaaS); plataforma como servicio (PaaS); y *software* como servicio (SaaS)[63].

Sobre la base de esa diferenciación, la directiva NIS establece un régimen jurídico distinto para OSE y para PSD.

III. RÉGIMEN NORMATIVO

El sistema normativo diseñado en la directiva NIS no responde a un enfoque integral. El análisis de las disposiciones relativas a las obligaciones asignadas a los Estados permite identificar tres categorías diferentes porque se establecen determinadas obligaciones de resultado[64], junto con otras de

[63] La IaaS es una categoría de servicio en la que el tipo de capacidad que se proporciona al cliente es una infraestructura que incluye la entrega virtual de recursos informáticos en forma de *hardware*, servicios de redes y de almacenamiento. En la PaaS, el tipo de capacidad que se proporcionan al cliente es una plataforma informática en línea que permite a las empresas hacer funcionar aplicaciones existentes o desarrollar y probar aplicaciones nuevas. En el SaaS, se proporciona una aplicación o *software* desplegado en internet, por lo que eliminan la necesidad de que el usuario final compre, instale y gestione *software*, y presenta la ventaja de que se puede acceder a este desde cualquier lugar que disponga de una conexión a internet [anexo a la comunicación de la Comisión «Sacar el máximo partido a la SRI», COM (2017) 476 final, 4-10-2017, pp. 33-34]. Véase ENISA (2017: 13 y ss.).

[64] Entre las obligaciones de resultado se encuentran las siguientes: a) La adopción de una estrategia nacional de seguridad de redes y sistemas de información (art. 7); b) la designación de las autoridades nacionales competentes, el punto de contacto único (art. 8) y los CSIRT (art. 9). Considerando las diferencias existentes en términos de estructuras y modelos de gobierno, los Estados tienen la opción de optar por un planteamiento centralizado —basado en los principios de subsidiariedad, cooperación y legislación sectorial—, descentralizado —con una autoridad central para todos los sectores y una legislación general— o híbrido, combinando ambos, a la hora de definir las autoridades nacionales competentes siguiendo, con ello, la experiencia existente en relación con la transposición de la normativa en materia de protección de las infraestructuras críticas [anexo a la comunicación de la Comisión «Sacar el máximo partido a la SRI», COM (2017) 476 final, 4-10-2017, pp. 11 y ss]; c) La representación en el Grupo de Cooperación y en la Red de CSIRT (arts. 11, 12 y 24.3); d) la identificación de los OSE (art. 5); e) la no imposición de nuevos requisitos de seguridad o notificación a los PSD (art. 16.10); y f) el establecimiento del régimen de sanciones (art. 21).

comportamiento[65], además de meramente informativas o de control[66]. No son realmente equivalentes a las que tienen atribuidas en el marco regulador de las comunicaciones electrónicas, en protección de infraestructuras críticas, en identificación electrónica o en relación con los proveedores de servicios de confianza[67]. También es diferente el organigrama funcional. En el caso de la directiva NIS, está compuesto por las autoridades nacionales competentes en

[65] Entre las obligaciones de comportamiento se incluye velar: a) por la adopción de las medidas técnicas y de organización adecuadas y proporcionadas por los OSE y PSD para gestionar los incidentes (arts. 14.1 y 16.1), para prevenir y reducir sus efectos (arts. 14.2 y 16.2) y para notificarlos sin dilación (arts. 14.3 y 16.3) (Bannelier y Christakis, 2017: 22); b) para que, en relación con los OSE, las autoridades competentes dispongan de las competencias y los medios necesarios para evaluar el cumplimiento de las obligaciones y los efectos (art.15.1) y para exigirles que les proporcionen la información y las pruebas de aplicación efectiva de las políticas de seguridad (art. 15.2); c) para que, en el caso de los PSD, las autoridades competentes adopten medidas de supervisión *a posteriori* (art. 17.1); d) para que las autoridades competentes y los CSIRT reciban las notificaciones de incidentes y, si no han de ser notificados los CSIRT, que tengan acceso a los datos necesarios para la gestión de los incidentes (art. 10.2); e) para que las autoridades y CSIRT informen a los puntos de contacto únicos sobre las notificaciones de incidentes; y f) para que los CSIRT tengan acceso a una infraestructura de comunicación e información apropiada, segura y resiliente a nivel nacional.
Dentro de esta categoría se incluyen, asimismo, las siguientes obligaciones: asignar los recursos necesarios a las autoridades y a los puntos de contacto (art. 8.5) y a los CSIRT (art. 9.2); garantizar una cooperación efectiva, eficiente y segura de los representantes delegados en el Grupo de Cooperación (art. 8.5); consultar a otros Estados miembros en el marco del proceso de identificación de los OSE (art. 5.4); revisar la lista de OSE (art. 5.5); tener en cuenta los factores intersectoriales y sectoriales en la determinación del efecto perturbador significativo (art. 6); y fomentar, sin imponer ni favorecer el uso de un tipo específico de tecnología, la utilización de normas y especificaciones aceptadas a nivel europeo o internacional (art.19.1).

[66] Las obligaciones de información a la Comisión se refieren a la aplicación misma de la directiva (art. 4.7); la comunicación de las estrategias nacionales (art. 7.3); la notificación sin dilación de las autoridades competentes y el punto de contacto único que ha de hacerse pública (art. 8.7); las medidas nacionales de identificación de los OSE, la lista de servicios, el número de OSE y los umbrales existentes, en su caso, para determinar el nivel de suministro adecuado o la importancia del OSE en concreto (art. 23.1); y el mandato y los elementos principales del proceso de gestión de incidentes de sus CSIRT (art. 9. 4).

[67] No hay referencia expresa tampoco a la compleja cuestión de la responsabilidad del Estado directamente afectado por ciberincidentes (Gross, 2015: 14).

materia de seguridad de redes y sistemas[68], los puntos únicos de contacto[69], los equipos de respuesta a incidentes de seguridad informática (CSIRT)[70], la Red de CSIRT[71] y el Grupo de Cooperación[72]. ENISA tiene asignadas funciones específicas en varias disposiciones, al igual que la Comisión, en particular para la adopción de las normas de ejecución de las disposiciones de la directiva. Responde a una dinámica por niveles que distingue estructuras nacionales y europeas.

En el plano normativo, una obligación principal de los Estados establecida en el art. 1.2 y desarrollada en el art. 7 consiste en la adopción de una estrategia nacional de seguridad de redes y sistemas de información que plantea el dilema entre una aproximación generalista o específica y entre la creación de nuevas o la readaptación de las estrategias preexistentes (1). Los requisitos

---

68 Su función consiste en supervisar la aplicación nacional de la directiva NIS (art. 8.2). Ello implica, en particular, la atribución de competencias para controlar la aplicación y observancia de los requisitos de seguridad y notificación de incidentes por parte de los OSE y los PSD (arts. 15 y 17).

69 La identificación de un punto de contacto único se requiere cuando existe más de una autoridad competente porque, de ser solo una, ejercería directamente las funciones de enlace y de información (art. 8.3). Tiene atribuidas dos funciones: enlace en el marco de la cooperación transfronteriza entre las autoridades de los Estados miembros, la Red CSIRT y el Grupo de Cooperación (art. 8.4); e información anual al Grupo de Cooperación sobre notificaciones, incidentes y acciones desarrolladas en el marco de los arts. 14.3 y 5 y 16.3 y 6 (art. 10.3).

70 Los CSIRT tienen asignada la responsabilidad en la gestión de incidentes y riesgos, siguiendo los procedimientos establecidos de conformidad con el art. 9 y en el anexo I de la directiva. Sus funciones consisten en supervisar y responder a incidentes a escala nacional, difundir alertas, realizar un análisis dinámico de riesgos e incidentes y participar en la Red CSIRT.

71 La Red CSIRT cuenta con una composición heterogénea porque está formada por los representantes de los CSIRT nacionales, la Comisión tiene el estatuto de observador y ENISA asume la Secretaría (art. 12.2). Las misiones asignadas consisten en el intercambio de información, la respuesta coordinada frente a incidentes, el apoyo transfronterizo, la búsqueda de una cooperación operativa en aspectos concretos, el análisis de capacidades y experiencias compartidas y la difusión de directrices en aras de una convergencia operativa general (art. 12.3).

72 El Grupo de Cooperación está compuesto por los representantes de los Estados, ENISA y la Comisión, que asume la Secretaría (art. 11.2). Tiene asignada la misión general de apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados, así como de desarrollar confianza y seguridad para la consecución del objetivo común de alcanzar un elevado nivel de seguridad de las redes y sistemas de información.

de seguridad (2) y de notificación y normalización (3) implican el establecimiento de obligaciones a cargo de los Estados en relación con los OSE y los PSD, así como el marco normativo básico que ha de presidir la realización y la supervisión y control de su actividad. Mientras que respecto de los primeros se produce una duplicidad normativa no suficientemente justificada, en relación con los segundos se aprecia una falta innecesaria de homogeneidad. Finalmente, la garantía de efectividad de esta normativa se articula también siguiendo un modelo en el que la duplicidad de regímenes no acaba de encontrar su explicación (4).

1. LA ESTRATEGIA NACIONAL DE SEGURIDAD DE REDES Y SISTEMAS

La directiva NIS establece, en su art. 1.2, la obligación de los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información, definida en el art. 4.3, como «un marco que proporciona prioridades y objetivos estratégicos de seguridad de las redes y sistemas de información a escala nacional». Esa obligación se precisa definiendo su objeto y alcance en el art. 7, donde se establece el enfoque integral, la naturaleza estratégica, el ámbito de aplicación —que ha de extenderse, como mínimo, a los sectores de actividad incluidos en los anexos II y III— y un contenido normativo pormenorizado[73]. En su comunicación «Aprovechar al máximo la SRI», la Comisión subraya el objetivo de exhaustividad de las estrategias nacionales, la necesidad de revisar las estrategias previas[74], identificando tanto las lagunas como las buenas prácticas, y la importancia de afrontar los nuevos desafíos mediante un tratamiento holístico y coherente que puede extenderse más allá de lo previsto en la directiva NIS, pero no debe mantenerse estático[75].

---

[73] Debe contener los siguientes aspectos: los objetivos y prioridades; el marco de gobernanza, incluyendo funciones y responsabilidades públicas y de otros agentes; la identificación de las medidas de preparación, respuesta y recuperación y la cooperación público-privada; la indicación de los programas de educación, concienciación, formación, investigación y desarrollo; un plan de evaluación de riesgos; y un listado de los diversos agentes participantes en la ejecución de la estrategia. Con los datos de septiembre de 2017, fecha de publicación del «Commission Staff Working Document Assessment of the EU 2013 Cybersecurity Strategy», veinticinco Estados habían desarrollado o actualizado sus estrategias en cumplimiento de esta obligación (SWD (2017) 295 final, de 13.9.2017, p. 11).

[74] Esa misma opinión mantiene ENISA (2016a).

[75] Comunicación de la Comisión «Aprovechar al máximo la SRI. Hacia la aplicación efectiva de la Directiva (UE) 2016/1148», COM (2017) 0476, final, 4-10-2017, p. 4.

En el anexo de esa comunicación de la Comisión, como prueba adicional de la voluntad de impulsar nuevas estrategias específicas sobre seguridad de redes y sistemas o reformas substanciales de las estrategias generales en vigor, se explican dos de sus aspectos esenciales: el alcance[76] y el contenido, y procedimiento[77]. En este punto se justifica una metodología *multistakeholder* y un proceso de adopción en cinco etapas concretas consistentes en lo siguiente: a) fijación de los principios rectores y los objetivos estratégicos, que han de ser específicos, medibles, alcanzables, realistas y acotados en el tiempo (objetivos SMART); b) elaboración del contenido incluyendo medidas facilitadoras, actuaciones acotadas en el tiempo e indicadores clave del resultado con objeto de poder evaluar, perfeccionar y mejorar la estrategia, que podría ser encargado a un grupo de dirección presidido por un ministerio principal y realizado por varios grupos de redacción; c) desarrollo de un marco de gobernanza en el contexto de las estructuras administrativas y políticas nacionales y contando con partes interesadas clave; d) compilación y revisión del borrador de estrategia mediante el análisis de debilidades, amenazas, fortalezas y oportunidades (análisis DAFO) y una consulta pública; y e) adopción formal a nivel político con la necesaria dotación presupuestaria.

El alcance y el contenido asignados a las estrategias nacionales y el procedimiento previsto, en particular, identificando partes interesadas y mecanismos de asociación de la sociedad civil al proceso de elaboración de las estrategias, son indicadores sólidos y evidentes de la necesidad de adoptar nuevas estrategias, incluso si están limitadas a la seguridad de redes y sistemas, o de reformar sustancialmente las existentes que, habiendo sido adoptadas en su mayoría antes de la directiva NIS[78], difícilmente pueden dar respuesta a sus previsiones materiales, organizativas y finalistas[79].

---

76 El alcance de la estrategia viene determinado por la obligación recogida en el art. 7 de abarcar los sectores de los anexos II y III y por el principio de armonización mínima del art. 3, que permite a los Estados ampliar su ámbito de aplicación, razón por la cual la Comisión defiende la elaboración de una estrategia comprehensiva de todos los sectores de la sociedad y de la economía y no solo de los contemplados en la directiva (anexo a la comunicación de la Comisión al Parlamento Europeo y al Consejo «Sacar el máximo partido a la SRI», COM (2017) 476 final, 4-10-2017, p. 5).

77 El contenido y el procedimiento se identifican atendiendo a las indicaciones del propio art. 7, a las herramientas de formación de ENISA, la UIT, la OCDE y foros académicos sobre este aspecto y al análisis de la experiencia de Estados miembros y terceros (*ibid.*, p. 6).

78 En el caso de España, puede verse el borrador de Anteproyecto de Ley sobre la seguridad de las redes y sistemas de información en: https://bit.ly/2GZvobi.

79 La comunicación de las estrategias a la Comisión ha de realizarse en el plazo de tres meses desde su adopción (art. 7.3). No queda claro, si se compara con otras disposi-

2. REQUISITOS EN MATERIA DE SEGURIDAD DE REDES Y SISTEMAS DE INFORMACIÓN

Los requisitos en materia de seguridad se encuentran recogidos en el art. 14 para los OSE y en el art. 16 para los PSD, en términos similares pero no idénticos[80]. En ambos casos se establece que los Estados miembros velarán para que los OSE y los PSD procedan a: 1) la adopción de medidas técnicas y organizativas de gestión adecuadas y proporcionadas en función de los riesgos (arts. 14.1 y 16.1); y 2) la adopción de medidas de prevención y de reducción del impacto de los incidentes (arts. 14.2 y 16.2). En ambos se establecen las mismas funciones a cargo de la autoridad competente o el CSIRT en cuanto a la información que han de transmitir al resto de los afectados y en relación con la obligación de preservar en el desarrollo de esas tareas la confidencialidad, la seguridad y los intereses comerciales de OSE y PSD (arts. 14.5 y 16.6).

A partir de ese núcleo común, se aprecian las diferencias en su régimen jurídico. En primer lugar, en el marco de la gestión de riesgos, solo respecto de los PSD se especifican los diferentes aspectos que han de ser objeto de consideración, esto es, la seguridad de los sistemas e instalaciones, la gestión de incidentes, la gestión de la continuidad de las actividades, la supervisión, auditoría y pruebas y el cumplimiento de las normas internacionales[81]. En segundo término, los parámetros de evaluación de impacto de un incidente son comunes en el caso del número de usuarios afectados, la duración y la extensión geográfica, pero para los PSD se añaden además el grado de perturbación del funcionamiento del servicio y el alcance del impacto sobre las actividades económicas y sociales. En tercer lugar, las categorías y calificaciones a las que

ciones relativas a los plazos, en qué medida la fecha de transposición de la directiva opera, como debería ser, para fijar el plazo máximo en el que las estrategias deberían haber sido adoptadas y comunicadas a la Comisión.

80 Sobre los requisitos de seguridad de PSD, véase ENISA (2016b). Para los OSE, el Grupo de Cooperación ha adoptado el «Documento de referencia sobre medidas de seguridad de los operadores de servicios esenciales» (comunicación de la Comisión «Duodécimo informe de situación relativo a una Unión de la Seguridad genuina y efectiva», COM (2017) 779 final, 12.12.2012, p. 12).

81 Estos aspectos son objeto de desarrollo en el Reglamento de Ejecución (UE) 2018/151 de la Comisión, de 30 de enero de 2018, por el que se establecen normas de aplicación de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo en lo que respecta a la especificación de los elementos que han de tener en cuenta los proveedores de servicios digitales para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información, así como de los parámetros para determinar si un incidente tiene un impacto significativo (DO L 26, de 31 de enero de 2018, p. 48).

se hace referencia son diferentes en unos supuestos e intercambiables en otros, arrojando una inexplicable confusión sobre el conjunto y los elementos del sistema. Los factores enunciados como intersectoriales en relación con la determinación de la «importancia de un efecto perturbador» en la prestación de un servicio en el caso de los OSE coinciden con los identificados como parámetros de «importancia de los efectos» de un incidente en relación con los mismos OSE y como parámetros de importancia «significativa» en los PSD en tres aspectos: el número de usuarios, la duración y la extensión geográfica de la zona afectada por el incidente (arts. 14.4 y 16.4). Mientras, la dependencia de otros sectores, la cuota de mercado y la importancia de la entidad para mantener un nivel suficiente de servicio son factores intersectoriales para determinar la «importancia de un efecto perturbador» en el contexto del art. 6, no constituyen parámetros de la importancia de un incidente en el caso de los OSE en el art. 14.4, ni para los PSD en el art. 16.4, que, a su vez, utiliza nociones equivalentes cuando se refiere al grado de perturbación en el funcionamiento del servicio o al alcance del impacto sobre las actividades económicas y sociales. Finalmente, cuando se trata de los factores intersectoriales y específicos, son los Estados quienes han de tenerlos en cuenta, pero no se precisa quiénes han de considerar los parámetros. Parece evidente la necesidad de una formulación más clara y coherente de cada uno de esos supuestos, incluso sin que se pretenda una homologación exacta en el estatuto a esos efectos de los OSE y los PSD.

Para terminar, una diferencia insoslayable entre ambos regímenes normativos deriva del hecho de que en el marco de los OSE está previsto un posible desarrollo normativo sobre los parámetros recogidos en el art. 16.4 de la directiva NIS por parte de las autoridades competentes en el marco del Grupo de Cooperación y en el contexto de la notificación de incidentes. En cambio, respecto de los PSD, el art. 16.8 dispone que la Comisión adoptará los actos de ejecución necesarios para especificar los requisitos relativos a los elementos de seguridad y a los parámetros para la determinación del alcance significativo de un incidente. Ello ha conducido a la adopción, el 30 de enero de 2018, del 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. No ha debido ser un trámite sencillo teniendo en cuenta que se ha adoptado varios meses después del plazo fijado para ello por la propia Directiva, el 9 de agosto de 2017. En cualquier caso, el grado de desarrollo y de precisión de este reglamento de la Comisión aumenta las posibilidades de una mayor diversificación de los condiciones de seguridad[82], si se

[82] *Ibid*. El reglamento desarrolla los elementos de seguridad recogidos en la directiva, determina los parámetros para determinar el alcance significativo de un incidente y

tiene en cuenta que la normativa correspondiente para los OSE ha de provenir de un sujeto distinto y no abundan las posibilidades de lograr un cierto grado de coincidencia en cuanto a su contenido (Robles Carrillo, 2018a).

3. REQUISITOS EN MATERIA DE NOTIFICACIÓN Y NORMALIZACIÓN

El régimen jurídico de la notificación se encuentra recogido en los arts. 14 y 16 de la directiva NIS, junto con los requisitos de seguridad, y en el art. 20, dentro de un apartado propio, el capítulo VI de dicha directiva. Haber separado los requisitos de seguridad y de notificación y tratado conjuntamente todos los aspectos de la notificación habría conducido a un resultado más coherente, transparente y homogéneo de ambos extremos. En este punto, hay que plantearse, además, si el tratamiento conjunto de los requisitos de seguridad —que son procedimentales en su condición de medios, pero finalistas desde el punto de vista de la seguridad material que se pretende alcanzar— y los de notificación —en esencia, procedimentales— podría incidir negativamente en el significado y el valor intrínseco de los primeros, que son el componente básico de esta normativa. Quizás habría sido conveniente distinguir, subrayando su mayor relevancia jurídica, la necesidad de homogeneizar los requisitos materiales de seguridad de redes y sistemas, por un lado, respecto de los procedimientos de notificación de los incidentes de seguridad, por otro.

Los arts. 14.3 y 16.3 establecen para los OSE y para los PSD, respectivamente, el requisito de notificación sin dilación indebida de los incidentes de seguridad a la autoridad competente o al CSIRT. Los elementos comunes en su régimen jurídico son los siguientes: a) ha de incluir la información necesaria para valorar su posible alcance transfronterizo; b) una vez realizada, no sujetará al notificante a una mayor responsabilidad; y c) cabe la posibilidad de informar al público, previa consulta al OSE y al PSD (arts. 14.6 y 16.7). En cuanto a las diferencias entre ambos, con carácter general, la obligación de notificación se circunscribe, en el caso de los OSE, a los incidentes que tengan efectos significativos en la continuidad de los servicios, en tanto que, para los PSD, se precisa en un doble sentido porque la notificación ha de incluir toda la información necesaria para valorar el impacto del incidente y porque

precisa los criterios de impacto significativo. El análisis de esa disposición permite identificar tres modalidades de valoración: 1) la cuantificación numérica del grado de afectación del servicio; 2) la combinación de una cuantificación numérica y un resultado; y 3) la existencia de un riesgo de resultado por afectación de la seguridad pública o pérdida de vidas humanas.

se aplica solo en la medida en que disponga de acceso a esa información en función de los parámetros indicados en el apdo. 4 del art. 16[83].

Hay otras diferencias adicionales en el régimen de notificación por parte de OSE y de PSD y entre ellas: a) cabe la opción de exigir el suministro de esa información al propio PSD (art. 16.7); b) solo respecto de los OSE y solo cuando las circunstancias lo permitan, está prevista la posibilidad de que la autoridad competente o el CSIRT proporcionen información sobre el seguimiento de la notificación de un incidente (art. 14.5); c) la información al público después de consultar a OSE y a PSD, en el primer caso, es competencia de la autoridad competente o el CSIRT, mientras que, en el segundo, puede ser realizada por dichas instituciones o exigir al PSD directamente que lo haga (art. 14.6); d) la publicidad de la información se justifica para los OSE cuando es necesaria la concienciación pública para evitar o gestionar un incidente en tanto que para los PSD se requiere, además, que esa divulgación redunde en interés público (art. 16.7); y e) las autoridades competentes dentro del Grupo de Cooperación podrán adoptar directrices sobre las circunstancias y parámetros en los que resulta exigible la notificación de incidentes a los OSE (art. 14.7), mientras que es la Comisión la encargada de adoptar los actos de ejecución a esos efectos en relación con los PSD (art. 16.8 y 9). A esas diferencias, que responden a distintos formatos (Menges y Pernul, 2008: 87), hay que sumar las que pueden producirse si la notificación contempla un incidente de seguridad que haya afectado a los datos (Jasmontaite, 2017: 131), marcando una diferencia adicional respecto de aquellos que solo afectan a servicios.

En el capítulo V de la directiva, el art. 20 recoge la posibilidad de notificación voluntaria de incidentes que tengan efectos significativos en sus actividades por parte de entidades que no son PSD y tampoco han sido calificadas como OSE. En este caso, el régimen normativo es el siguiente: a) el procedimiento aplicable es el recogido para los OSE en el art. 14; b) los Estados tienen la opción de dar prioridad a las notificaciones obligatorias sobre las voluntarias; c) las notificaciones voluntarias se tramitarán siempre que no supongan una carga desproporcionada o indebida para los Estados; d) no supondrá la imposición a la notificante de obligaciones que no le corresponderían de no haberse producido la notificación.

La notificación voluntaria es un expediente valioso en la medida en que permite extender el ámbito de aplicación de este mecanismo más allá de lo previsto para OSE y PSD y, con ello, los niveles de conocimiento sobre los

[83] El OSE dependiente de un PSD para la prestación de un servicio esencial será el responsable de notificar el incidente del PSD que tenga un efecto significativo sobre la continuidad del servicio.

incidentes, los sujetos y el estado de la seguridad de redes y sistemas, que ha de contribuir necesariamente a una mejora global de la misma. Precisamente por ello, el hecho de que los Estados tengan la opción de no proceder a su tramitación puede desalentar su uso, del mismo modo que privilegiar, con carácter general, las obligatorias sobre las voluntarias puede ser un problema si se produce un incidente de una gravedad considerablemente superior en un supuesto voluntario —que, específicamente, ha de tener efectos significativos, según el art. 20— que puede terminar relegado frente a un incidente menor respecto del cual existe una obligación de notificación.

En el capítulo V de la directiva, el art. 19 establece medidas en materia de normalización[84]. El objetivo es promover una aplicación convergente del art. 14.1 y 2 relativo a los OSE y el art. 16.1 y 2 referido a los PSD. Hay, sin embargo, dos disposiciones que pueden dificultar ese proceso o encauzarlo en una dirección distinta de la prevista en el art. 19. La primera de ellas es el art. 16.1, que incluye el cumplimiento de normas internacionales entre las medidas técnicas y organizativas que han de adoptar los PSD y al que no se hace referencia en el art. 14.1. La segunda es el art. 16.8, que encomienda a la Comisión la adopción de los actos de ejecución para el desarrollo de esos elementos de seguridad. Como consecuencia de ese mandato, en el art. 2.5 del Reglamento de Ejecución (UE) 2018/151[85], la Comisión identifica las dos categorías de normas internacionales a cuyo cumplimiento remite el art. 16.1: por una parte, las adoptadas por un organismo internacional de normalización en los términos definidos en el art. 2.1.a) del Reglamento (UE) 1025/2012[86]; y, por otra, las normas y especificaciones aprobadas a nivel europeo, internacional o nacional, de acuerdo con lo previsto en el art. 19 de la directiva NIS.

Esta situación implica que el objetivo de convergencia en la normalización para OSE y PSD se ve dificultado por la circunstancia de que hay un procedimiento previsto a esos efectos en el art. 19, con la intervención de los Estados y de ENISA, mientras que se ha desarrollado otro, por aplicación del art. 16.8, por parte de la Comisión en el que se especifica la normativa de certificación respecto de los PSD. Hay una cierta falta de congruencia entre esas disposiciones que, posiblemente, podría verse resuelta si se procede a la

[84] Por una parte, los Estados fomentarán la utilización de normas y especificaciones aceptadas a nivel europeo o internacional sin imponer ni favorecer el uso de un tipo específico de tecnología. Por otra parte, en colaboración con ellos, ENISA elaborará directrices y orientaciones sobre las áreas técnicas que habrán de examinarse a esos efectos y sobre las normas ya existentes, en particular en el marco nacional.

[85] DO L 26, de 31 de enero de 2018, p. 48.

[86] DO L 316, de 14 de noviembre de 2012, p. 12.

adopción del reglamento por el que se pretende reformar ENISA y establecer una certificación de ciberseguridad a nivel europeo[87].

4. MECANISMOS DE GARANTÍA DE EFECTIVIDAD

El art. 15 de la directiva NIS regula la aplicación y observancia de la normativa en el caso de los OSE, mientras que el art. 17 hace lo propio respecto de los PSD. En este supuesto, dada su naturaleza, se completa con el art. 18 relativo al ejercicio de la jurisdicción. El art. 21 se ocupa de las sanciones[88].

4.1. Control de la aplicación y observancia

El modelo de control de la aplicación de la normativa es diferente para OSE y para PSD, de conformidad con lo previsto en los arts. 15 y 17 de la directiva. En ambos supuestos, los Estados miembros tienen asignada la función de dotar a las autoridades competentes de los atributos para el cumplimiento de esa misión, aunque el alcance de los mismos es diferente en cada caso.

El modelo de control previsto para OSE supone la atribución a dichas autoridades de cuatro competencias concretas de evaluación, información, decisión y cooperación. El carácter vinculante que se otorga a las fundamentales —información y decisión—, y se proyecta sobre las demás, muestra el alcance, naturaleza y potencial efectividad de este mecanismo de control y marca una diferencia cualitativa, no meramente cuantitativa, respecto del previsto para los PSD.

En este contexto, las autoridades competentes tienen asignada una función general de evaluación en una doble y complementaria dimensión porque, por una parte, intrínseca y materialmente verifica el grado de cumplimiento de la normativa por parte de los OSE; y, por otra, externa y teleológicamente comprueba sus efectos sobre la seguridad de las redes y sistemas de información. Para el ejercicio de esa competencia disponen de dos atributos principales.

---

87 Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a ENISA, la Agencia de Ciberseguridad de la UE, y por el que se deroga el Reglamento (UE) 526/2013, y relativo a la certificación de ciberseguridad de las tecnologías de la información y la comunicación, COM (2017) 477 final, 4-10-2017.

88 El art. 21 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 han de ser efectivas, proporcionadas y disuasorias. Los Estados habían de comunicar el régimen previsto a la Comisión, a más tardar el 9 de mayo de 2018, así como notificar las modificaciones posteriores.

En primer lugar, cuentan con el poder de exigir a los OSE la información necesaria para realizar su evaluación y las pruebas de la aplicación efectiva de las políticas de seguridad respetando, en ambos casos, los principios de legitimidad y proporcionalidad del objetivo perseguido, ya que habrán de indicar la finalidad y especificar la necesidad concreta. En segundo término, una vez realizada la auditoría o evaluación, tienen el poder de impartir instrucciones vinculantes a los PSD para subsanar las eventuales carencias. Esta facultad constituye una garantía esencial en cuanto a la efectividad de la evaluación de las autoridades en cuestión como mecanismo obligatorio de fiscalización. Para terminar, se establece una obligación subjetiva y materialmente específica de cooperación con las autoridades responsables en materia de protección de datos cuando el incidente de seguridad haya conducido a su violación.

El modelo de control previsto para los PSD difiere del previsto para los OSE. Como primera providencia, se establece la condición «si fuera necesario», que no solo excluye la obligatoriedad del control, sino que apunta a la posible necesidad de justificar, en su caso, su realización. En efecto, en segundo término, se define como una supervisión *a posteriori* condicionada a la existencia de pruebas de que un PSD no cumple los requisitos establecidos en el art. 16. En tercer lugar, el art. 17.2 reconoce a las autoridades el poder de exigir a los PSD que suministren la información necesaria para su evaluación y que subsanen cualquier incumplimiento de aquellos requisitos. Además de la ausencia de referencia al carácter vinculante de sus instrucciones, el problema estriba en que la supervisión se circunscribe *a posteriori* pero está condicionada a la demostración de su necesidad y a la obtención de pruebas a esos efectos. Para terminar, el sistema se completa con el establecimiento de una obligación de asistencia mutua y cooperación entre las autoridades competentes en los supuestos en los que está implicado más de un Estado por la no coincidencia entre el lugar de establecimiento del proveedor o su representante y el lugar de localización de las redes y sistemas de información.

4.2. Ejercicio de la jurisdicción

La determinación de la jurisdicción aplicable constituye, junto con la trazabilidad y la atribución de responsabilidad, un obstáculo principal para garantizar el respeto del derecho en el ciberespacio.

El art. 18 de la directiva NIS establece el principio de jurisdicción sobre un título territorial basado en el doble criterio del establecimiento y de la prestación de servicios en un Estado miembro. La primera opción supone que un PSD estará sometido a la jurisdicción del Estado en el que tiene su establecimiento principal entendido como el domicilio social. La segunda, que opera en caso de no estar establecido en algún Estado, implica que el

PSD, en la medida en que es prestador de los servicios del anexo III en la UE, estará sujeto a la jurisdicción del Estado en el que se encuentre establecido el representante que obligatoriamente habrá de designar en alguno de los Estados donde se realice la prestación. La figura del representante opera como mecanismo de conexión del PSD con un Estado miembro a efectos de ejercicio de su jurisdicción porque no excluye, según el apdo. 3 del art. 18, el ejercicio de acciones legales contra el propio PSD. Hay que entender que, con esta fórmula, se habilita la opción de actuar frente al representante en el marco de la jurisdicción del Estado donde se encuentra establecido y frente al PSD en cualquier jurisdicción respecto de la que exista un título competencial válido.

IV. CONCLUSIONES

La necesidad de un enfoque integral en materia de seguridad de redes y sistemas se justifica, desde muy diversas perspectivas y con distintos argumentos, en sucesivos actos de las instituciones europeas[89]. A pesar de ello, la normativa adoptada en materia de comunicaciones electrónicas, identificación electrónica, proveedores de servicios de confianza y protección de infraestructuras críticas organiza los requisitos de seguridad, notificación y normalización, en su caso, asumiendo una aproximación sectorial que parece desconocer dos datos. El primero es que la definición singularizada del régimen jurídico de un sector de actividad no necesariamente ha de trasladarse a todos y cada uno de sus aspectos, sino que es perfectamente compatible con el establecimiento de regímenes homogéneos o, incluso, idénticos a los de otros sectores en relación con aspectos concretos que pueden ser comunes, como ocurre con la seguridad de redes y sistemas. El segundo es que los requisitos de seguridad de redes y sistemas no han de ser diferentes porque lo sean los distintos sectores en los que se aplican, sino que, por el contrario, habrían de guardar una amplio grado de homogeneidad o, incluso, de identidad por dos motivos principales: la característica e ineludible interconectividad de las redes y sistemas y, junto a ello, la natural y frecuente coincidencia entre los prestadores de servicios de esta naturaleza, que se ven particularmente perjudicados por esta profusión de regímenes jurídicos.

La directiva NIS no responde a un planteamiento integral de la seguridad de redes y sistemas de información, sino que sacraliza el tratamiento sectorial por varios motivos que han sido desarrollados a lo largo de este trabajo.

89 Véanse las notas 9 y 10 de este trabajo.

Los requisitos de seguridad, notificación y, en su caso, normalización son diferentes en materia de protección de infraestructuras críticas, en el ámbito de las comunicaciones electrónicas, en el sector de la identificación electrónica, en el caso de los proveedores de servicios de confianza —con tres regímenes internos—, en relación con los OSE y respecto de los PSD. La normativa en materia de protección de datos y, en su caso, privacidad tiene un régimen jurídico también diferente en el ámbito de las comunicaciones electrónicas, en el marco del RGPD y en el Reglamento (CE) 45/2001. La combinación de las diferentes normas sobre seguridad de redes y sistemas y protección de datos es ineludible en la medida que una afectación de estos últimos constituye un incidente de seguridad, aunque no toda incidencia de seguridad conlleva, a su vez, necesariamente una afectación de datos. El resultado es que hay diferentes requisitos de seguridad y en materia de protección de datos/privacidad respecto de cada uno de aquellos ámbitos materiales de actuación.

Además de la falta de transparencia, la complejidad y la escasa razonabilidad de este modelo de acción, hay un problema adicional. El enfoque sectorializado conduce a que la normativa aplicable depende del tipo de servicio, no de la titularidad del mismo, de manera que un mismo sujeto, incluidas las administraciones, habrá de adaptarse respecto de la misma materia —los requisitos de seguridad, notificación, normalización, protección de datos y privacidad— a regímenes normativos diferentes determinados en función del tipo de servicio prestado en cada caso. Para ello, además, en los casos en los que exista un acto jurídico sectorial se habrán de comprobar los requisitos específicos de ese sector para mantenerlos si son equivalentes o superiores a los dispuestos en la directiva NIS, o para excluirlos si son inferiores.

El modelo normativo establecido para OSE y PSD muestra aspectos coincidentes y divergentes sin que se encuentre siempre una justificación lógica para ese proceder. Si resulta justificado el diferente tratamiento realizado para cada una de esas categorías en relación con su identificación y designación, no merecen la misma valoración las diferencias establecidas entre ambos en cuanto a los requisitos de seguridad, notificación y normalización. No solo hay disposiciones materiales innecesariamente distintas o poco congruentes, sino que, además, las previsiones de desarrollo normativo realizadas para OSE y PSD han de conducir necesariamente a un agravamiento de esas diferencias al haberse atribuido la competencia a instituciones y órganos diferentes en cada caso. Los mecanismos de garantía de la efectividad de las disposiciones de la directiva son distintos, con una cierta justificación, para OSE y PSD si bien fuese mejorable su formulación en este último caso.

El problema de la ausencia de un enfoque integral en materia de seguridad de redes y sistemas de información puede agravarse si, en cumplimiento de la obligación de adoptar una estrategia nacional de seguridad de redes y

sistemas prevista en la directiva NIS, los Estados se limitan a desarrollar los aspectos reflejados en esta directiva, reforzando con ello esa aproximación sectorial que conduce a una parcelación de la realidad, en lugar de asumir una metodología eficaz de garantía de esa seguridad mediante un tratamiento integral. Pero no es solo un problema de eficacia.

El enfoque integral en materia de seguridad de redes y sistemas es, realmente, fundamental para los titulares de esos diferentes tipos de prestaciones —porque han de cumplir los diferentes requisitos establecidos en cada caso—, para los usuarios —porque han de conocer las obligaciones exigidas en cada supuesto y sus correspondientes derechos—, para las administraciones —que han de gestionar los procedimientos y velar por su cumplimiento— y, en definitiva, para el conjunto de una sociedad y una economía basadas en el conocimiento.

Bibliografía

Agustinoy Guilayn, A. (2016). *Aspectos legales de las redes sociales*. Barcelona: Bosch.

Bannelier, K. y Christakis, T. (2017). *Cyber-Attacks. Prevention-Reactions: The Role of States and Private Actors*. Paris: Les Cahiers de la Revue Défense Nationale.

Barrio Andrés, M. (2017). *Fundamentos de Derecho de Internet*. Madrid: Centro de Estudios Políticos y Constitucionales.

CISCO (2018). *Annual Cybersecurity Report*. Disponible en: https://bit.ly/2KISsNS.

Comisión Europea (2015). *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*. Brussels: European Union.

Department for Business, Innovation and Skills (BIS) (2010). *Implementing the Revised EU Electronic Communications Framework. Impact Assessment*. London: BIS.

Díaz Orueta, G., Alzórriz Armendáriz, I., Sancristóbal Ruíz, E. y Castro Gil, M. A. (2014). *Procesos y herramientas para la seguridad de las redes.* Madrid: UNED.

ENISA (2013a). *Security framework for Article 4 and 13a*. Heraklion: ENISA Publications.

—— (2013b). *Cloud security incident reporting. Framework for reporting about major cloud security incidents*. Heraklion: ENISA Publications.

—— (2014a). *Network and Information Security in the Finance Sector*. Heraklion: ENISA Publications.

—— (2014b). *Technical Guideline on Incident Reporting*. Heraklion: ENISA Publications.

—— (2014c). *Technical Guideline on Security Matters*. Heraklion: ENISA Publications.

—— (2015a). *Proposal for Article 19 Incident Reporting*. Heraklion: ENISA Publications.

—— (2015b). *Security incidents indicators. Measuring the impact of incidents affecting electronic communications*. Heraklion: ENISA Publications.

—— (2015c). *Definition of cybersecurity. Gaps and overlops in standarisation*. Heraklion: ENISA Publications.

—— (2015d). *Security framework for Goverment clouds*. Heraklion: ENISA Publications.

—— (2016a). *NCCS Good Practice Guide. Designing and Implementing National Cyber Security Strategies*. Heraklion: ENISA Publications.
—— (2016b). *Technical Guidelines for the implementation of minimum security measures for Digital Service Providers*. Heraklion: ENISA Publications
—— (2017). *Incident Notification for DSPs in the context of the NIS Directive*. Heraklion: ENISA Publications.
—— (2018a). *Building a common language to face future incidents*. Heraklion: ENISA Publications.
—— (2018b). *Looking into the crystal ball. A report of emerging technologies and security challenges*. Heraklion: ENISA Publications.
EPRS (2017). *Cybersecurity in the EU Common Security and Defence Policy. Challenges and Risks*. Brussels: European Union.
Gross, O. (2015). *Legal Obligations of States Directly Affected by Cyber-Incidents*. Legal Studies Research Paper Series, 15-03, 48, 1-38.
Herbst, N. R., Kounev, S. y Reussner, R. (2013). *Elasticity in Cloud Computing: What It Is, and What It Is Not*. Disponible en: https://bit.ly/2IDa7tV.
Bangemann. (1994). *Europa y la sociedad global de la información: Informe Bangemann*. Disponible en: https://bit.ly/2HZGRcy.
Jasmontaite, L. (2008). Building a Cybersecurity Culture in the EU Through Mandatory Notification of Data Breaches and Incidents: Differences and Similarities of Data Vulnerability Reporting Tools. En *Managing Risk in the Digital Society* (pp. 129-142). Barcelona: Universitá Oberta de Catalunya.
Martínez López-Sáez, M. (2018). *Una revisión del derecho fundamental a la protección de datos de carácter personal. Un reto en clave de diálogo judicial y constitucionalismo multinivel en la Unión Europea*. Valencia: Tirant Lo Blanch.
Menges, F. y Pernul, G. (2008). A comparative analysis of incident reporting formats. *Computer and Security*, 73, 1-24.
Musiani, F. (2016). Alternative Technologies as Alternative Institutions: The Case of the Domain Name System. En F. Musiani, D. L. Cogburn, L. DeNardis, N. S. Levinson (eds.). *The Turn to Infrastructure in Internet Governance* (pp. 72-86). London: Palgrave Macmillan.
OCDE (2002). *Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad*. Paris: OECD.
Piñar Mañas, J. L. (2016). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Reus.
Robles Carrillo, M. (2016). El proceso de reforma de la ICANN. Objetivos, régimen jurídico y estructura orgánica. *Revista de Privacidad y Derecho Digital,* 7, 25-65.
—— (2018a). Medidas de aplicación de la Directiva NIS: alcance y limitaciones. En *Actas de las IV Jornadas Nacionales de Investigación en Ciberseguridad*. San Sebastián: Mondragon Unibertsitatea.
—— (2018b). El proceso de transposición de la directiva sobre seguridad de redes y sistemas en el derecho español. IEEE, 78/201, 1-21.
Troncoso Reigada, A. (2008). La administración electrónica y la protección de datos personales. *Revista Jurídica de Castilla y León*, 16, 31-111.
UIT (2006). *La seguridad de las telecomunicaciones y las tecnologías de la información*. Ginebra: Oficina de Normalización de las Telecomunicaciones.
World Economic Forum (2018). *The Global Risks Report*. Geneva: WEF.