InDret
1.2024

La ciberseguridad en el Derecho digital europeo: novedades de la Directiva NIS2

Moisés Barrio Andrés
Universidad Complutense de Madrid

Sumario

Hoy la ciberseguridad es una de las piezas estructurales de la infraestructura digital. Su misión central es limitar las vulnerabilidades de Internet conservando sus ventajas tecnológicas y de soporte de la sociedad digital. Para actualizar el marco normativo en el Derecho digital europeo ha sido aprobada la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI2 o NIS2). La primera Directiva NIS1, adoptada en 2016, pretendía ofrecer un elevado nivel común de ciberseguridad en todos los Estados miembros, pero resultó difícil de aplicar. La nueva Directiva NIS2 responde a las nuevas amenazas planteadas por la transformación digital y el aumento general de los ciberataques, y lo lleva a cabo intensificando los requisitos de seguridad, incluyendo la seguridad de la cadena de suministro, y establece medidas de supervisión pública más estrictas. En este artículo analizaremos las principales innovaciones de este instrumento normativo.

Abstract

Today, cybersecurity is one of the building blocks of the digital infrastructure. Its central mission is to limit the vulnerabilities of the Internet while preserving its technological and support advantages for the digital society. To update the regulatory framework in European digital law, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity throughout the Union (SRI2 or NIS2 Directive) has been adopted. The first NIS1 Directive, adopted in 2016, aimed to provide a high common level of cybersecurity across all Member States, but proved difficult to implement. The new NIS2 Directive responds to the new threats posed by the digital transformation and the general increase in cyber-attacks, and does so by intensifying security requirements, including supply chain security, and establishes stricter public oversight measures. In this paper we will analyze the main innovations of this regulatory instrument.

Title: *Cybersecurity in European digital law: new provisions of the NIS2 Directive*

Palabras clave: ciberseguridad, ciberresiliencia, ciberataque, Directiva NIS, Directiva SRI, ENISA
Keywords**:** *cybersecurity, cyber-resilience, cyber-attack, NIS Directive, SRI Directive, ENISA*

InDret

1.2024

Recepción
18/09/2023
-
Aceptación
13/11/2023
-

Índice
-

-

1. Introducción*

La seguridad no fue una de las principales preocupaciones de los creadores de lo que finalmente[1] se ha convertido en Internet. Esta fue postergada para priorizar otros aspectos del desarrollo del ciberespacio. Pero, y de forma gradual, los Estados y la Unión Europea han promulgado normas jurídicas al respecto.[2] A mi juicio, hoy la ciberseguridad es uno de los grupos normativos más relevantes del Derecho digital.[3]

La misión central de la ciberseguridad es limitar las vulnerabilidades de Internet conservando sus ventajas tecnológicas y de soporte de la sociedad digital.[4] Sin embargo, las características técnicas[5] de Internet suponen un reto permanente para salvaguardar la ciberseguridad. Los ciberataques[6] pueden perpetrarse desde la comodidad del hogar o la oficina y no suelen requerir más equipamiento especial que un ordenador y los conocimientos técnicos pertinentes. La naturaleza clandestina de los ciberataques hace extremadamente difícil localizar[7] a sus autores. Además, los ciberdelincuentes suelen aventajar a las autoridades policiales y judiciales y desarrollan constantemente nuevos *modus operandi* motivados por el dinero, los impulsos emocionales adolescentes, la política o la religión.[8]

Estas razones han abonado la conversión[9] de la ciberseguridad en una pieza esencial del Derecho digital europeo. A la postre, la ciberseguridad es el conjunto de técnicas y procesos dirigidos a garantizar la «preservación de la confidencialidad, integridad y disponibilidad de la información

---

* Moisés Barrio Andrés (contacto@moisesbarrio.es).

Este artículo ha sido elaborado en el marco del proyecto PID2022-136964NB-I00 "El Derecho ante la salud digital, personalizada y robótica" (SALUDPYR) financiado por MCIN/ AEI /10.13039/501100011033/ y por FEDER Una manera de hacer Europa.

[1] Sobre este proceso, *vid*. BARRIO ANDRÉS, Moisés, *Fundamentos del Derecho de Internet*, Centro de Estudios Políticos y Constitucionales, Madrid, 2020, 2.ª edición, p. 67 y ss.

[2] FUERTES LÓPEZ, Mercedes, *Metamorfosis del Estado. Maremoto digital y ciberseguridad*, Marcial Pons, Madrid, 2022, p. 21 y ss.

[3] BARRIO ANDRÉS, Moisés, *Manual de Derecho digital*, Tirant lo Blanch, Valencia, 2022, 2.ª edición, p. 311 y ss.

[4] ÁLVAREZ ROBLES, Tamara, «El derecho de acceso universal a internet en el marco normativo español: presente y futuro», en *Revista LA LEY Derecho Digital e Innovación*, número 7, 2021, p. 2 y ss.

[5] BARRIO ANDRÉS, Moisés, *Fundamentos del Derecho de Internet, op. cit.,* pp. 45-50.

[6] BARRIO ANDRÉS, Moisés, *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, Wolters Kluwer, Madrid, 2018.

[7] VELASCO SAN MARTÍN, Cristos, *Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos*, Tirant lo Blanch, Valencia, 2016.

[8] LORIA GARCÍA, Paz, «Delitos y redes sociales: los nuevos atentados a la intimidad, el honor y la integridad moral (especial referencia al «sexting»)», en *Revista LA LEY penal: revista de derecho penal, procesal y penitenciario*, número 105, 2013, p. 3.

[9] DE LA IGLESIA MONJE, María Isabel, «Relevancia del análisis de riesgos en la protección de datos en la ciudad inteligente», en PLAZA PENADÉS, Javier y MARTÍNEZ VELENCOSO, Luz (dirs.), *Retos normativos del mercado único digital europeo*, Tirant lo Blanch, Valencia, 2023, pp. 91-114; ESTÉBANEZ GARCÍA, Margarita, «El impacto del COVID-19 en la ciberseguridad y las infraestructuras críticas», en *Revista LA LEY Derecho Digital e Innovación*, número 6, 2020.

en el ciberespacio» (norma ISO/IEC CD 27032.3). Pero, dada su esencialidad para el adecuado funcionamiento de la sociedad digital, es también un derecho digital[10] (art. 82 LOPDGDD[11] y numeral VI[12] de la Carta de Derechos digitales de España).

Así las cosas, la ciberseguridad se ve comprometida por los ciberincidentes. Un ciberincidente es cualquier suceso que pueda suponer un riesgo para la seguridad de las infraestructuras digitales de un usuario u organización, bien sea provocado por un agente de forma intencionada o debido a una mala práctica. El número, la magnitud, la sofisticación, la frecuencia y los efectos de los ciberincidentes van en aumento y representan una grave amenaza para el funcionamiento de tales infraestructuras digitales.[13]

En efecto, los incidentes de ciberseguridad han ido en aumento desde hace bastante tiempo. Según Eurostat, el 22 % de las empresas de la Unión Europea sufrieron diversas afecciones debido a incidentes de seguridad relacionados con las infraestructuras digitales en 2021.[14] En 2018, esta cifra era solo del 12 %.[15] Entre estas consecuencias, cabe subrayar la indisponibilidad de los servicios, la destrucción o deterioro de los datos o la divulgación de datos personales o estratégicos de la entidad.

Del mismo modo, cabe destacar el auge de los ciberataques. Así, por ejemplo, los ataques de *ransomware* han crecido casi un 40 % en 2023.[16] También los ataques por correo electrónico, especialmente el *phishing*, han aumentado un 47,2 % en 2023.[17] Los ciberataques también han empezado a centrarse en la interrupción de las cadenas de suministro, que ya se vieron alteradas tras la pandemia de COVID-19 y más aún desde el inicio de la guerra en Ucrania.[18]

El coste de estos incidentes también se está disparando. Un estudio realizado en 2020 por el Centro Común de Investigación de la Comisión Europea (JRC) estimó que el coste mundial de la ciberdelincuencia alcanzaría los 5,5 billones de euros a finales de 2020, frente a los 2,7 billones

---

[10] Barrio Andrés, Moisés, *Los derechos digitales y su regulación en España, la Unión Europea e Iberoamérica*, Colex, A Coruña, 2023, p. 40 y ss.

[11] Domínguez Álvarez, José Luis, «Derecho a la seguridad digital: génesis, evolución y perspectivas de futuro», en Rodríguez Ayuso, Juan Francisco (coord.), *Nuevos retos en materia de derechos digitales en un contexto de pandemia: perspectiva multidisciplinar*, Aranzadi, Pamplona, 2022, pp. 91-118.

[12] Recio Gallo, Miguel, «Seguridad digital: ¿derecho o expectativa de derecho? A propósito del Proyecto de Carta de Derechos Digitales», en *Revista LA LEY Derecho Digital e Innovación*, número 7, 2020.

[13] Tejerina Rodríguez, Ofelia (coord.), *Aspectos jurídicos de la ciberseguridad*, RA-MA, Madrid, 2020.

[14] Eurostat, «El 22 % de las empresas de la UE tuvieron incidentes de seguridad de las TIC», 14 de febrero de 2023. Disponible en https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20230214-1?language=es&etrans=es.

[15] Eurostat, «Medidas de seguridad de las TIC adoptadas por la gran mayoría de empresas de la UE», 13 de enero de 2020. Disponible en https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f.

[16] Zscaler, «Informe ransomware 2023». Disponible en https://www.zscaler.es/press/zscalers-ransomware-report-2023-shows-global-ransomware-attack-growth-of-nearly-40-percent.

[17] Zscaler, «Informe phising 2023». Disponible en https://www.zscaler.es/blogs/security-research/2023-phishing-report-reveals-472-surge-phishing-attacks-last-year.

[18] Real Instituto Elcano, «Ucrania en busca de refugio digital», de 4 de marzo de 2022. Disponible en https://www.realinstitutoelcano.org/comentarios/ucrania-en-busca-de-refugio-digital.

de 2015.[19] Las estimaciones para 2025 son de hasta 10,5 billones de dólares.[20] El coste medio mundial de una brecha de seguridad de datos en 2022 se estimó en 4,35 millones de dólares.[21] Ciertamente, esta cifra depende del sector -así, las brechas de datos en el sector sanitario alcanzan una media de 10,10 millones de dólares-, del tipo de ataque -los ataques destructivos alcanzan una media de 5,12 millones de dólares- y de la región afectada -las brechas de datos en Estados Unidos alcanzan una media de 9,44 millones de dólares-.

Además, los daños de la ciberdelincuencia no se limitan a las entidades afectadas. Dado que más del 45 % de los ciberdelitos afectan a datos personales, los ciudadanos de todo el mundo quedan expuestos a diversos riesgos, como el robo de identidad y el fraude financiero. Los daños pueden ser incluso no económicos. Los hospitales y las infraestructuras críticas, como las centrales nucleares, están cada vez más en el punto de mira de los ciberdelincuentes, por lo que también existe un riesgo evidente para la vida humana. Por ejemplo, en Alemania un paciente murió después de que el hospital más cercano no pudiera proporcionarle atención urgente debido a un ataque de *ransomware* en ejecución que paralizó su funcionamiento.[22]

A pesar de la regulación y políticas públicas promulgadas[23] para armar a las entidades contra las ciberamenazas, el 54 % de las entidades siguen afirmando que no están adecuadamente equipadas para hacer frente a los ciberataques más sofisticados. En esta dirección, la UE adoptó la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva SRI o NIS, por sus siglas inglesas de *Network and Information Security Directive*. Nos referiremos a ella como Directiva NIS1).

El objetivo de la Directiva NIS1 fue imponer un nivel común de ciberseguridad en la UE a los operadores de determinados servicios esenciales y proveedores de servicios digitales al amparo del artículo 114 del TFUE[24]. Sin embargo, como se verá más adelante, la transposición de la

[19] Comisión Europea, «Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 – part 1», SWD (2020) 345 final, p. 16.

[20] Universitat Oberta de Catalunya, «El coste anual mundial de los ciberataques se triplicará en 2025 respecto a 2015», 9 de febrero de 2023. Disponible en https://www.uoc.edu/portal/es/news/actualitat/2023/027-ciberseguridad-securing.html.

[21] IBM, «Cost of a Data Breach Report 2023», 1 de marzo de 2023. Disponible en https://www.ibm.com/reports/data-breach.

[22] Comisión Europea, «Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 – part 1», SWD (2020) 345 final, p. 16.

[23] A nivel comparado, puede verse ISHIKAWA, Tomoko y KRYVOI, Yarik (eds.), *Public and Private Governance of Cybersecurity: Challenges and Potential*, Cambridge University Press, Cambridge, 2023; o WONG, Helen, *Cyber Security: Law and Guidance,* Bloomsbury Professional, Londres, 2018. En España, *vid*. ELTJON, Mirashi, *Tratamiento procesal del cibercrimen y diligencias de investigación tecnológica,* Aranzadi, Pamplona, 2023; CONAL FUERTES, Iker, *Ciberseguridad y Derecho penal,* Aranzadi, Pamplona, 2022; o RUEDA MARTÍN, María Ángeles, «Los ataques de denegación de servicios como ciberdelito en el Código Penal español», en *Revista Penal*, número 49, 2022, pp. 183-216.

[24] Tratado de Funcionamiento de la Unión Europea (TFUE). En efecto, la lógica del mercado interior permea toda la Directiva. Así, su considerando 3 pone de manifiesto que la seguridad de las redes y los sistemas de información es esencial para el buen funcionamiento del mercado interior, ya que «las redes y los sistemas de información, y

Directiva resultó ser bastante divergente entre los Estados miembros. Esto ha dado lugar a unas condiciones de competencia desiguales y a una preparación insuficiente de esas entidades frente a los nuevos y cambiantes retos de la ciberseguridad. Como resultado, la Directiva NIS1 ha sido sustituida por la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI2 o NIS2, a la que nos referiremos en lo sucesivo como Directiva NIS2). Deberá ser traspuesta en los Estados miembros antes del próximo 17 de octubre de 2024.

En este estudio nos ocuparemos, en primer lugar, de apuntar las deficiencias de la Directiva NIS1, puestas de manifiesto durante su proceso de revisión, y los principales objetivos políticos de la Directiva NIS2. A continuación, analizaremos las novedades de la Directiva NIS2 y compararemos su marco con el de la NIS1. También enmarcaremos esta norma en los grupos normativos generales de ciberseguridad de la UE, y tras ello formularemos nuestras conclusiones.

2. La revisión de la Directiva NIS1

La Directiva NIS1 se adoptó el 6 de julio de 2016. Debía ser transpuesta por los Estados miembros antes del 9 de mayo de 2018, siendo aplicable al día siguiente. Como es habitual, no todos los Estados miembros lograron cumplir este plazo y, por ejemplo, España no transpuso la norma hasta septiembre de 2018.[25]

Como analizaremos en el próximo epígrafe, la Directiva NIS1 dejó un grado sustancial de discrecionalidad a los Estados miembros en su transposición. Esto ha dado lugar a divergencias significativas. Por ejemplo, en algunos Estados miembros, los hospitales se consideran servicios esenciales, mientras que en otros Estados miembros no lo son. Del mismo modo, un operador ferroviario importante en un Estado miembro grande está cubierto, pero un operador de tamaño similar en otro no lo está.[26] Estas divergencias tienen un efecto negativo en el mercado único digital, ya que las entidades en un Estado miembro deben asumir los costes operativos para el cumplimiento de este grupo normativo, mientras que entidades similares en otro Estado miembro pueden no resultar obligadas.[27]

Como hemos indicado en la introducción, el nivel de amenaza y la variedad de los ciberataques han aumentado significativamente en los últimos años. A ello hay que añadir la creciente dependencia de los sistemas de información, debido esencialmente al aumento del teletrabajo durante la pandemia de COVID-19 y la subsiguiente intensificación de los procesos de

principalmente Internet, desempeñan un papel esencial a la hora de facilitar la circulación transfronteriza de bienes, servicios y personas».

[25] Se llevó a cabo a través del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

[26] Comisión Europea, «Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 – part 1», SWD (2020) 345 final, p. 11.

[27] Comisión Europea, «Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 – part 1», SWD (2020) 345 final, p. 14.

transformación digital. Así las cosas, es imprescindible un nivel aún mayor de resistencia cibernética para proteger a las entidades críticas y esenciales. Se constató que la NIS1 no cubría suficientemente este aumento de la interconexión y las interdependencias entre sectores.[28]

El resultado de la evaluación del marco de la Directiva NIS1 puso de manifiesto que los problemas antes mencionados, combinados con los nuevos retos en materia de ciberseguridad, hacen que el impacto efectivo de la Directiva siga siendo limitado debido a su falta de armonización real.[29] Además, también el intercambio de información entre los Estados miembros y los principales actores sigue siendo insuficiente. Asimismo, la supervisión y los recursos correspondientes son limitados en algunos Estados miembros. En fin, se constató que algunos Estados miembros apenas notificaban incidentes, lo que claramente no se corresponde con la realidad.[30]

La Comisión Europea sopesó varias opciones de reforma.[31] No se consideró eficaz no hacer nada o limitarse a proporcionar orientaciones adicionales sobre las infraestructuras digitales. Además, una mera ampliación del ámbito de aplicación de la Directiva NIS1 únicamente resolvería algunos de los problemas detectados. En consecuencia, se decidió que era necesario derogarla por completo y sustituirla por una nueva directiva.

La nueva Directiva NIS2 se basaría así en tres principios estructurales. Primero, la necesaria ampliación de su ámbito de aplicación a otras entidades públicas y privadas del mercado interior que desempeñen funciones importantes para la sociedad. Segundo, la consecución de una mayor armonización en el ámbito de aplicación, en los requisitos de seguridad y notificación de incidentes, en la supervisión y ejecución por parte de los Estados miembros del cumplimiento de la normativa y en las capacidades de las autoridades competentes nacionales. Tercero, el fomento de la coordinación y cooperación entre los Estados miembros en materia de ciberseguridad y establecer un marco de gobernanza sólido y efectivo ante incidentes o crisis a gran escala.

La propuesta de Directiva NIS2 se publicó con fecha 16 de diciembre de 2020.[32] La Directiva NIS2 se adoptó formalmente el 14 de diciembre de 2022. Entró en vigor a los 20 días de su publicación en el Diario Oficial de la Unión Europea.[33] Los Estados miembros tendrán que transponer la Directiva antes del 17 de octubre de 2024, y empezar a aplicar sus medidas a partir del 18 de octubre de 2024.[34] Ese último día, el marco NIS1 también quedará derogado.[35] La Comisión

[28] Comisión Europea, «Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 – part 1», SWD (2020) 345 final, p. 13.

[29] ARTEAGA MARTÍN, Félix, «La evaluación y la revisión de la Directiva NIS», en *Análisis del Real Instituto Elcano*, número 19, 2021, p. 2 y ss.

[30] Comisión Europea, «Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 – part 1», SWD (2020) 345 final, p. 36.

[31] *Ibid*., p. 68-69 y 89-93.

[32] COM (2020) 823 final.

[33] Artículo 45 de la Directiva NIS2.

[34] Artículo 41 de la Directiva NIS2.

[35] Artículo 44 de la Directiva NIS2.

Europea llevará a cabo una revisión de su funcionamiento antes del 17 de octubre de 2027 y cada 36 meses a partir de entonces, debiendo dar cuenta de ello al Parlamento Europeo y al Consejo.[36]

3. Principales novedades de la Directiva NIS2

3.1. Objeto y ámbito de aplicación

La nueva Directiva NIS2 se compone de 46 artículos estructurados en 9 capítulos y precedidos de 144 considerandos.

Ambas directivas establecen medidas «que tienen por objeto alcanzar un elevado nivel común de ciberseguridad en toda la Unión con el objetivo de mejorar el funcionamiento del mercado interior».[37]

No obstante, la principal diferencia es que la Directiva NIS1 se focalizaba en la «seguridad de las redes y sistemas de información», mientras que la Directiva NIS2 se centra en la noción más amplia de «ciberseguridad», tal y como se define en el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad -la *European Union Agency for Network and Information Security*-) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 (el Reglamento sobre la Ciberseguridad de la Unión). Este relevante cambio significa que el objetivo no es sólo proteger los sistemas de red y de información, sino también a los usuarios de dichos sistemas y a otras personas afectadas por las ciberamenazas. Dados los riesgos que los ciberataques plantean a los usuarios de los sistemas de TIC, y a los ciudadanos en general, se trata de una ampliación del ámbito de aplicación bien acogida por la doctrina.

Una medida que resulta ahora potenciada es la obligación de los Estados miembros de adoptar estrategias nacionales de ciberseguridad y designar o establecer autoridades competentes, autoridades de gestión de crisis de ciberseguridad, puntos de contacto únicos sobre ciberseguridad (puntos de contacto únicos) y equipos de respuesta a incidentes de seguridad informática (CSIRT).[38] Entre las nuevas obligaciones, se han incorporado medidas de gestión de riesgos de ciberseguridad y presentación de informes, normas y obligaciones sobre intercambio de información en materia de ciberseguridad, y obligaciones de supervisión y ejecución para los Estados miembros. Estas últimas adiciones encarnan el mayor énfasis de la Directiva NIS2 en la aplicación efectiva de sus medidas, paliando así una de las grandes debilidades de su predecesora.

En cuanto a su ámbito de aplicación, la Directiva NIS2 se aplica a entidades públicas o privadas de tamaño mediano o mayor en sectores de alta criticidad (Anexo I de la Directiva) y en otros sectores críticos (Anexo II de la Directiva)[39], y que reciben ahora la denominación de entidades

[36] Artículo 40 de la Directiva NIS2.

[37] Artículo 1.1 de ambas directivas.

[38] Artículo 1.2 de ambas directivas.

[39] Artículo 2.1 de la Directiva NIS2.

esenciales e importantes. Con esta configuración, la Directiva pretende eximir a las pequeñas empresas y microempresas de su ámbito de aplicación.

No obstante, la nueva directiva puede aplicarse a entidades de cualquier tamaño en los sectores enumerados en los anexos I y II cuando:[40]

> a) sean proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles para el público, prestadores de servicios de confianza o proveedores de servicios de registros de nombres de dominio de primer nivel y de sistemas de nombres de dominio (DNS);
>
> b) la entidad es el único proveedor en un Estado miembro de un servicio esencial para actividades sociales o económicas críticas;
>
> c) la interrupción del servicio prestado podría tener un impacto significativo en la seguridad pública, el orden público o la salud pública, o inducir un riesgo sistémico significativo, en particular con impacto transfronterizo;
>
> d) la entidad sea crítica debido a su importancia para un determinado sector o tipo de servicio, o para otros sectores interdependientes; o
>
> e) la entidad es una entidad de la Administración pública central o regional.

Novedad de calado es la inclusión de los prestadores de servicios de confianza, que estaban parcialmente exentos en virtud de la NIS1.[41] Al igual que la Administración General del Estado y de las Comunidades Autónomas. Asimismo, los Estados miembros también pueden aplicar la nueva directiva a las administraciones públicas locales y a las instituciones educativas, «en particular cuando lleven a cabo actividades críticas de investigación».

Además, la Directiva NIS2 se aplica a las entidades de cualquier tamaño consideradas entidades críticas[42] según la Directiva (UE) 2022/2557 (la Directiva CER) y a las entidades que prestan servicios de registro de nombres de dominio.[43]

La Directiva NIS2 se aplica sin perjuicio de la responsabilidad de los Estados miembros de salvaguardar la seguridad nacional y otras funciones esenciales del Estado, incluida la garantía de la integridad territorial y el mantenimiento del orden público.[44] La Directiva tampoco exige el suministro de información que sea contrario a la seguridad nacional o pública o a la defensa de un Estado miembro.[45] La Directiva no se aplica a las entidades de la Administración pública que

[40] Artículo 2.2 de la Directiva NIS2.

[41] Artículo 2.9 de la Directiva NIS2.

[42] Bajo la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo.

[43] Artículos 2.3 y 2.4 de la Directiva NIS2.

[44] Artículo 2.6 de la Directiva NIS2.

[45] Artículo 2.11 de la Directiva NIS2.

lleven a cabo actividades en los ámbitos de la seguridad nacional, la seguridad pública, la defensa o la aplicación del Derecho, incluida la prevención, investigación, detección y enjuiciamiento de infracciones panales.[46] Además, los Estados miembros pueden eximir en cierta medida a las entidades que presten tales servicios a las administraciones públicas.[47]

Al igual que la NIS1, la Directiva NIS2 se entiende sin perjuicio de otros grupos normativos y sólo exige el intercambio de información confidencial cuando sea necesario.[48] Del mismo modo, los datos personales deben tratarse de conformidad con las normas de protección de datos de la UE.[49]

En fin, el alcance de la NIS2 sigue siendo de armonización mínima.[50]

Con respecto a otra normativa de la UE que imponga requisitos de ciberseguridad sectoriales al menos equivalentes, la Directiva NIS2 no se aplicará a las entidades cubiertas efectivamente por esa legislación.[51] Por lo tanto, la Directiva NIS2 debe considerarse como la *lex generalis* en términos de ciberseguridad, actuando sin perjuicio de la *lex specialis* sectorial en los ámbitos no cubiertos.

De este modo, a mi juicio la nueva directiva busca una cobertura mayor de los sectores y servicios de vital importancia para todas aquellas actividades consideradas fundamentales dentro del mercado interior, dado que amplía su ámbito de aplicación no solo a todas las entidades medianas y grandes –sean públicas o privadas– que operen en los sectores o presten servicios cubiertos por la Directiva NIS2, sino también a aquellas que las autoridades nacionales determinen por su relevancia para la sociedad, la economía o para determinados sectores o tipos de servicios. Sin embargo, la armonización sigue siendo mínima, y se mantienen exenciones muy relevantes, como son las administraciones locales, que son aquellas responsables de prestar los servicios públicos en el escalón más próximo al ciudadano (ya sea mediante gestión directa o indirecta del servicio público).[52]

3.2. Entidades esenciales e importantes

Una de principales novedades de esta nueva directiva es la supresión de la anterior dicotomía entre operadores de servicios esenciales (OSE) y proveedores de servicios digitales (DSP) y la introducción de dos nuevas categorías: entidades esenciales y entidades importantes.

De una parte, las entidades esenciales son las siguientes:[53]

[46] Artículo 2.7 de la Directiva NIS2.

[47] Artículo 2.8 de la Directiva NIS2.

[48] Artículos 2.12 y 2.13 de la Directiva NIS2.

[49] Artículo 2.14 de la Directiva NIS2.

[50] Artículo 5 de la Directiva NIS2.

[51] Artículo 4 de la Directiva NIS2.

[52] Artículo 85 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

[53] Artículo 3.1 de la Directiva NIS2.

a) Entidades de tamaño medio o superior contempladas en el Anexo I;
b) Prestadores cualificados de servicios de confianza, registros de nombres de dominio de primer nivel y proveedores de servicios DNS, independientemente de su tamaño;
c) Proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones servicios de comunicaciones electrónicas disponibles al público;
d) Entidades de la Administración General del Estado o de las Comunidades Autónomas;
e) Cualquier otra entidad de las mencionadas en los anexos I o II que un Estado miembro identifique como esencial;
f) Entidades críticas con arreglo a la Directiva (UE) 2022/2557; y
g) Entidades identificadas antes del 16 de enero de 2023 como operadores de servicios esenciales con arreglo a la Directiva NIS1.

De otra, las entidades importantes son todas aquellas entidades de los anexos I y II que no se consideren esenciales.[54]

Los Estados miembros deben establecer sus listas de entidades esenciales e importantes, así como de servicios de registro de nombres de dominio, antes del 17 de abril de 2025.[55] La Comisión Europea y la Agencia de la Unión Europea para la Ciberseguridad (ENISA) proporcionarán directrices y plantillas para los informes de los Estados miembros.[56] Ambas listas serán revisadas y actualizadas cada dos años.

A mi juicio, esta novedad supone un cambio significativo con respecto a la Directiva NIS1, en la que los Estados miembros gozaban de una discrecionalidad casi absoluta a la hora de identificar a sus operadores de servicios esenciales.[57] La NIS1 sólo proporcionaba unos pocos criterios para orientar a los Estados miembros en esta habilitación, que a menudo dependía de conceptos jurídicos indeterminados, tales como «efecto perturbador significativo».[58] Este defecto ha dado lugar a una aplicación muy dispar de la Directiva NIS1. Por ejemplo, en lo que respecta a la asistencia sanitaria, algunos Estados miembros identificaron sólo unos pocos hospitales, o incluso ninguno, como operadores de servicios esenciales. Otros Estados miembros, en cambio, incluyeron en la categoría a todos los hospitales y, en algunos casos, incluso a los profesionales sanitarios privados. Debido a estas discrepancias, la Directiva NIS2 incluye una redacción más clara y directa, dejando mucho menos margen de maniobra a los Estados miembros a la hora de identificar las entidades esenciales e importantes.

En cuanto a las entidades cubiertas, la Directiva NIS2 ha ampliado sustancialmente su ámbito de aplicación. En aras de la exhaustividad incluimos el listado, con las nuevas incorporaciones en cursiva.

[54] Artículo 3.2 de la Directiva NIS2.

[55] Artículo 3.3 de la Directiva NIS2.

[56] Artículo 3.4 de la Directiva NIS2.

[57] Artículo 5.1 de la Directiva NIS1.

[58] Artículos 5.2 y 6 de la Directiva NIS1.

a. Sectores de alta criticidad (Anexo I)

- **Electricidad**: empresas eléctricas, gestores de redes de distribución, gestores de redes de transporte de transporte, *productores, operadores de mercado designados, participantes en el mercado de la electricidad, operadores de puntos de recarga*.
- **Operadores de sistemas urbanos de calefacción o de refrigeración**.
- **Petróleo (crudo)**: operadores de oleoductos, operadores de producción de crudo, instalaciones de refinado y tratamiento, almacenamiento y transporte, *entidades centrales de almacenamiento*.
- **Gas**: empresas de suministro, gestores de la red de distribución, gestores de la red de transporte, gestores de almacenamiento, gestores de la red de GNL, compañías de gas natural, operadores de instalaciones de refinado y tratamiento.
- ***Hidrógeno**: operadores de producción, almacenamiento y transporte.*
- **Transporte**: compañías aéreas, entidades gestoras de aeropuertos y operadores de control de la gestión del tráfico; administradores de infraestructuras ferroviarias y empresas ferroviarias; empresas de transporte marítimo y fluvial y de cabotaje, organismos gestores de los puertos y operadores de servicios de tráfico de buques (STB); autoridades viarias y operadores de sistemas de transporte inteligentes.
- **Banca**: entidades de crédito.
- **Infraestructuras de los mercados financieros**: gestores de centros de negociación y entidades de contrapartida central (ECC).
- **Sector sanitario**: prestadores de asistencia sanitaria, *laboratorios de referencia, entidades que realizan actividades de investigación y desarrollo de medicamentos, fabricantes de productos farmacéuticos de base y especialidades farmacéuticas y fabricantes de productos sanitarios que se consideran esenciales en situaciones de emergencia de salud pública*.
- **Agua potable**: suministradores y distribuidores de aguas destinadas al consumo humano.
- ***Aguas residuales**: empresas dedicadas a la recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas o industriales*.
- **Infraestructura digital**: proveedores de puntos de intercambio de internet (IXP), proveedores de servicios de DNS, excluidos los operadores de servidores raíz, registros de nombres de dominio de primer nivel (TLD), *proveedores de servicios de computación en nube, proveedores de servicios de centro de datos, proveedores de redes de distribución de contenidos, prestadores de servicios de confianza, proveedores de redes públicas de comunicaciones electrónicas y proveedores de servicios de comunicaciones electrónicas disponibles para el público*.
- ***Gestión de servicios de TIC (B2B)**: proveedores de servicios gestionados y proveedores de servicios de seguridad gestionados*.
- ***Administración pública**: entidades de la Administración General del Estado y de las Administraciones de las Comunidades Autónomas*.
- ***Espacio**: operadores de infraestructuras terrestres, cuya propiedad, gestión y explotación descansa en los Estados miembros o en entidades privadas, que apoyan la prestación de servicios espaciales, excepto los proveedores de redes públicas de comunicaciones electrónicas*.

b. Otros sectores críticos (Anexo II)

- ***Servicios postales y de mensajería****: proveedores de servicios postales y proveedores de servicios de mensajería.*
- ***Gestión de residuos****.*
- ***Fabricación, producción y distribución de sustancias y mezclas químicas****.*
- ***Producción, transformación y distribución de alimentos****: empresas alimentarias que se dediquen a la distribución al por mayor y a la producción y transformación industriales.*
- ***Fabricación****: fabricantes de productos sanitarios y de productos sanitarios para diagnóstico in vitro; fabricantes de productos informáticos, electrónicos y ópticos; fabricantes de material eléctrico; fabricantes de maquinaria y equipo n.c.o.p.; fabricantes de vehículos de motor, remolques y semirremolques; y fabricantes de otro material de transporte.*
- **Proveedores de servicios digitales**: proveedores de mercados en línea, proveedores de motores de búsqueda en línea y *proveedores de plataformas de servicios de redes sociales*.
- ***Investigación****: organismos de investigación*.

Esta panorámica recién expuesta muestra cómo varios nuevos sectores han pasado a estar ahora sujetos *ex lege* a este régimen jurídico y cómo también hay ampliaciones sustanciales del ámbito de aplicación en sectores que ya estaban cubiertos por la Directiva NIS1. Además, se ha suprimido la categoría de «proveedores de servicios digitales» de NIS1, considerándose ahora los servicios en la nube como altamente críticos y los mercados en línea y los mercados en línea y motores de búsqueda como críticos normales.

3.3. Marcos coordinados de ciberseguridad

En consonancia con lo anterior, la Directiva NIS2 amplía su ámbito de aplicación de las estrategias nacionales de seguridad de las redes y los sistemas de información a las estrategias nacionales de ciberseguridad.[59]

Cada Estado miembro adoptará una estrategia nacional de ciberseguridad en la que se establecerán los objetivos estratégicos, los recursos necesarios para alcanzar esos objetivos y las medidas políticas y normativas adecuadas con objeto de alcanzar y mantener un elevado nivel de ciberseguridad. La Directiva NIS2 hace más hincapié en la necesidad de un marco de gobernanza que aclare las funciones y responsabilidades de las partes interesadas pertinentes a nivel de país, enumerando las distintas autoridades y partes interesadas que participan en la aplicación de la estrategia, y un marco político para mejorar coordinación entre las autoridades competentes.[60] Para garantizar un nivel de calidad europeo más común, la Directiva NIS2 también incluye más densidad regulatoria sobre el contenido de la estrategia, exigiendo que incluya diversas políticas -por ejemplo, en relación con la ciberseguridad de la cadena de suministro, la divulgación de vulnerabilidades, las herramientas de intercambio de información, la promoción y desarrollo de la educación y la formación en materia de ciberseguridad, etc.-[61] Las estrategias deben notificarse a la Comisión Europea y evaluarse, al menos, cada cinco años.[62]

[59] Artículo 7 de la Directiva NIS2.

[60] Artículo 7.1 de la Directiva NIS2.

[61] Artículo 7.2 de la Directiva NIS2.

[62] Artículos 7.3 y 7.4 de la Directiva NIS2.

Al igual que en la directiva anterior, los Estados miembros deben designar autoridades competentes para supervisar la aplicación del régimen jurídico, así como un punto de contacto único.[63]

Otra novedad relevante de la nueva Directiva NIS2 es que obliga a los Estados miembros a que designen o establezcan una o varias autoridades competentes responsables de la gestión de incidentes y crisis de ciberseguridad a gran escala (las «autoridades de gestión de crisis de ciberseguridad»).[64] El objetivo de esta novedad es que los Estados miembros adopten un plan nacional de respuesta a incidentes y crisis de ciberseguridad a gran escala en el que se establezcan los objetivos y las disposiciones para la gestión de incidentes y crisis de ciberseguridad a gran escala, incluyendo:[65]

a) los objetivos de las medidas y actividades nacionales en materia de preparación;
b) las funciones y responsabilidades de las autoridades de gestión de crisis de ciberseguridad;
c) los procedimientos de gestión de crisis de ciberseguridad;
d) las medidas nacionales de preparación, incluidos los ejercicios y las actividades de formación;
e) las partes interesadas públicas y privadas pertinentes y la infraestructura implicada;
f) los procedimientos y mecanismos nacionales entre las autoridades y los organismos nacionales pertinentes para garantizar la participación efectiva del Estado miembro en la gestión coordinada de incidentes y crisis de ciberseguridad a gran escala a nivel de la UE, así como su apoyo a dicha gestión.

Al igual que bajo la directiva anterior, los Estados miembros deben designar equipos de respuesta a incidentes de seguridad informática (CSIRT).[66] Este requisito es en gran medida el original, con algunos elementos añadidos como que los CSIRT deben tener a su disposición una infraestructura de comunicación e información adecuada, segura y resistente a través de la cual intercambien información con entidades esenciales e importantes y otras partes interesadas pertinentes en términos de cooperación.

Sin embargo, hay una serie de nuevos requisitos en términos de capacidades técnicas y tareas para los CSIRT.[67]

Deben, por ejemplo, garantizar un alto nivel de disponibilidad de sus canales de comunicación evitando los puntos únicos de fallo, operar desde emplazamientos seguros y estar equipados con sistemas redundantes y un espacio de trabajo de reserva para garantizar la continuidad de sus servicios. En cuanto a sus tareas, deben vigilar y analizar las ciberamenazas, vulnerabilidades e incidentes a nivel nacional, alertar rápidamente, responder a los incidentes y prestar asistencia,

[63] Artículo 8 de la Directiva NIS2.

[64] Artículo 9 de la Directiva NIS2.

[65] Artículo 9.4 de la Directiva NIS2.

[66] Artículo 9 de la Directiva NIS1 y artículo 10 de la Directiva NIS2.

[67] Artículo 11 de la Directiva NIS2.

recoger y analizar datos forenses, realizar un escaneo proactivo de las redes, participar en la red de CSIRT y contribuir al despliegue de herramientas seguras de intercambio de información. También deben establecer relaciones de cooperación con los actores relevantes del sector privado y promover la adopción y el uso de prácticas, sistemas de clasificación y taxonomías comunes o normalizados. Estos requisitos adicionales incorporados en la nueva directiva tienen por objeto garantizar un estándar común de operaciones entre los CSIRT nacionales.

Un nuevo requisito se refiere a la divulgación coordinada de vulnerabilidades y a una base de datos europea de vulnerabilidades.[68] Esta flamante previsión permite a los CSIRT actuar como intermediarios de confianza para informar y divulgar vulnerabilidades. Si la vulnerabilidad notificada puede tener un impacto significativo en otros Estados miembros, el CSIRT puede notificarla a la red de CSIRT. Y ENISA mantendrá una base de datos de vulnerabilidades de la UE en la que podrán divulgarse voluntariamente las vulnerabilidades conocidas públicamente.

Al igual que en su predecesora, las autoridades competentes de los Estados miembros y los CSIRT deben cooperar a nivel nacional e intercambiar información periódicamente.[69] Debe garantizarse que reciban notificaciones de incidentes significativos, incidentes periódicos, ciberamenazas y cuasiincidentes. En cuanto a los incidentes, el alcance de esta noción se ha ampliado a «todo hecho que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos».[70] Un cuasiincidente se configura como «un hecho que habría podido comprometer la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos, pero cuya materialización completa se previno de manera satisfactoria o que no llegó a materializarse».[71] Por su parte, la ciberamenaza sigue la definición del del Reglamento (UE) 2019/881.[72]

3.4. Cooperación a nivel de la Unión Europea e Internacional

Las grandes crisis de ciberseguridad han puesto de manifiesto que la seguridad en el ciberespacio, debido a las crecientes interdependencias de una red cada vez más interconectada y transfronteriza, es una tarea que incumbe tanto al sector público como al sector privado. La utilización de infraestructuras claves de toda la UE, cuya propiedad, gestión y explotación corresponde tanto al sector público como al sector privado[73], ha demostrado que compartir sus experiencias y estrategias puede ser de máxima utilidad para poder hacer frente a un mayor espectro de riesgos, y que los diferentes actores pueden reforzarse mutuamente mediante el intercambio de información. De este modo, ha arraigado una corresponsabilidad y la

[68] Artículo 12 de la Directiva NIS2.

[69] Artículo 10 de la Directiva NIS1 y artículo 13 de la Directiva NIS2.

[70] Artículo 6(6) de la Directiva NIS2.

[71] Artículo 6(5) de la Directiva NIS2.

[72] Se trata de «cualquier situación potencial, hecho o acción que pueda dañar, perturbar o afectar desfavorablemente de otra manera las redes y los sistemas de información, a los usuarios de tales sistemas y a otras personas».

[73] BOIX PALOP, Andrés, «Digital Platform Competition Regulatory Challenges», en *Revista General de Derecho de los Sectores Regulados: RSR*, número 8, 2021.

colaboración público-privada[74] en el marco de «cultura de ciberseguridad» que comparten el sector público y el privado.

Sobre esta base, la normativa anterior introdujo tímidamente la necesidad de cooperación entre los sectores público y privado, que se tradujo en la colaboración obligatoria entre los CSIRT y el sector privado, así como la participación de éste último en la elaboración de las diferentes estrategias nacionales de seguridad de las redes y sistemas de información. Ahora, la Directiva NIS2 impulsa el intercambio de información entre los Estados miembros con el objetivo de reforzar el nivel de ciberseguridad mediante la prevención, detección o respuesta a incidentes y la confianza mutua. Del mismo modo, fortalece la colaboración entre ambos sectores en el ámbito de la ciberseguridad mediante políticas públicas que apoyen la creación de asociaciones público-privadas específicas (las PPP por sus siglas inglesas de *Public-Private-Partnerships*) en materia de ciberseguridad. Se trata de asociaciones enfocadas al intercambio de información con la finalidad de prevenir, detectar, responder o mitigar incidentes, o incluso de intensificar la señalada cultura de ciberseguridad.

Por tanto, y a nivel de la UE, la Directiva NIS2 mantiene el Grupo de Cooperación, compuesto por representantes de los Estados miembros, la Comisión y ENISA.[75] Aunque la positivización precisa de sus tareas se ha actualizado algo para reflejar los nuevos retos y el nuevo escenario de ciberseguridad, el funcionamiento del Grupo sigue siendo en gran medida el mismo.

Los CSIRT nacionales son miembros de la red de CSIRT de la UE.[76] También en este caso hay algunas actualizaciones en la descripción de las tareas para adaptarlas al nuevo escenario, pero la regulación continúa siendo en esencia la misma.

Novedad de la Directiva NIS2 es la creación de la denominada Red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe).[77] Esta red apoya la gestión coordinada de los incidentes y las crisis de ciberseguridad a gran escala de la UE en el ámbito operativo. También garantiza el intercambio regular de información relevante entre los Estados miembros y las instituciones, los órganos y los organismos de la propia UE. Está formada por representantes de las autoridades de gestión de crisis de ciberseguridad de los Estados miembros y de la Comisión Europea. ENISA proporciona su Secretaría, las infraestructuras y las herramientas que permiten una cooperación eficaz para responder a incidentes, ataques y crisis de ciberseguridad a gran escala y transfronterizos.[78]

Entre los cometidos de EU-CyCLONe, cabe destacar aumentar el nivel de preparación ante incidentes y crisis de ciberseguridad a gran escala, desarrollar un conocimiento compartido de la

[74] DOMÉNECH PASCUAL, Gabriel, «Las regulaciones experimentales», en *Anuario del buen gobierno y de la calidad de la regulación: ABGCR*, número 1, 2022, pp. 103-146.

[75] Artículo 11 de la Directiva NIS1 y artículo 14 de la Directiva NIS2.

[76] Artículo 12 de la Directiva NIS1 y artículo 15 de la Directiva NIS2.

[77] Artículo 16 de la Directiva NIS2.

[78] ENISA también apoya la organización de ejercicios para los miembros de CyCLONe, como CySOPex (para el personal público) y BlueOLEx (para ejecutivos del sector privado). El objetivo de estos ejercicios es identificar mejoras y posibles lagunas en la forma normalizada de responder a incidentes y crisis (es decir, los Procedimientos Operativos Estándar), formar sobre el conocimiento de la situación y los procesos de intercambio de información.

situación en caso de incidentes y crisis de ciberseguridad a gran escala, evaluar las consecuencias y el impacto de los incidentes y crisis de ciberseguridad a gran escala pertinentes, coordinar la gestión de los incidentes y crisis de ciberseguridad a gran escala y debatir, a petición de un Estado miembro, los planes nacionales de respuesta a incidentes y crisis de ciberseguridad a gran escala. Se prevé que la red apruebe un reglamento interno de funcionamiento.

Tal y como estableció la directiva anterior, la UE podrá celebrar acuerdos de cooperación internacional con terceros países u organizaciones internacionales.[79]

Como cierre de este apartado, hay que subrayar cómo la nueva directiva obliga a que ENISA, en cooperación con la Comisión Europea y el Grupo de Cooperación, un elabore informe bianual sobre el estado de la ciberseguridad en la Unión.[80] Este informe llevará a cabo una evaluación de los riesgos de ciberseguridad a escala de la Unión, teniendo en cuenta el panorama de ciberamenazas, evaluará el desarrollo de las capacidades de ciberseguridad -tanto en el sector público como en el privado-, evaluará el nivel general de concienciación sobre la ciberseguridad y la ciberhigiene entre los ciudadanos y las empresas, así como una evaluación agregada de las evaluaciones interpares y del nivel de madurez de las capacidades y recursos de ciberseguridad en toda la Unión. El informe también incluirá recomendaciones políticas concretas para subsanar las deficiencias detectadas.

Mención especial debe hacerse de la obligación de llevar a cabo revisiones interpares.[81] Bajo la Directiva NIS1, los Estados miembros eran libres de formular sus propias estrategias nacionales sin apenas aportaciones de terceros. Con la NIS2, en cambio, las estrategias nacionales pueden someterse voluntariamente a la revisión por pares de expertos en ciberseguridad designados por, al menos, dos Estados miembros. La revisión por pares puede abarcar aspectos como el nivel de aplicación de las medidas de gestión de riesgos de ciberseguridad y las obligaciones de información, el nivel de capacidades, las capacidades operativas de los CSIRT, el nivel de aplicación de la asistencia mutua, el nivel de aplicación de los acuerdos de intercambio de información sobre ciberseguridad o cuestiones específicas de carácter transfronterizo o intersectorial. El Grupo de Cooperación desarrollará una metodología con criterios objetivos, no discriminatorios, justos y transparentes. Los Estados miembros que participen en una revisión interpares deberán prestar su plena cooperación.

3.5. Gestión de riesgos y obligaciones de notificación

La Directiva NIS2 impone una mayor responsabilidad a los órganos de dirección de las entidades obligadas.[82] Éstos deben aprobar las medidas de gestión de riesgos de ciberseguridad de su entidad y supervisar su aplicación. También se establece explícitamente que pueden ser considerados responsables de sus incumplimientos. Además, se les exige que sus integrantes sigan una formación en este ámbito, con el fin de dotarles de conocimientos y competencias suficientes. Esta atribución directa de responsabilidad y obligación a los órganos de dirección tiene por objeto garantizar su participación e implicación en la ciberseguridad de su entidad. Un

[79] Artículo 13 de la Directiva NIS1 y artículo 17 de la Directiva NIS2.

[80] Artículo 18 de la Directiva NIS2.

[81] Artículo 19 de la Directiva NIS2.

[82] Artículo 20 de la Directiva NIS2.

punto de fracaso a menudo crítico en este ámbito es que los departamentos de informática de las entidades no reciben el apoyo y la financiación adecuados de la alta dirección. Al implicar a la alta dirección en este régimen jurídico, ahora se convierten en partes interesadas directas en este proceso. Ahora bien, en la práctica esta obligación de formación expresa no es tan relevante en 2023, puesto que las entidades obligadas ya contarán con personal o incluso departamentos propios dedicados a la ciberseguridad.

Al igual que sucedía con la directiva anterior, las entidades deben adoptar medidas adecuadas y proporcionadas para gestionar los riesgos de ciberseguridad.[83] Sin embargo, la Directiva NIS2 desarrolla más claramente este enfoque basado en el riesgo, e incluso impone una serie de elementos que deben estar presentes en cualquier caso. Entre ellos figuran el análisis de riesgos y la seguridad de los sistemas de información, la gestión de incidentes, la continuidad de la actividad, incluidas las copias de seguridad, la gestión de crisis y la recuperación en caso de catástrofe, la seguridad de la cadena de suministro, la seguridad en la adquisición, el desarrollo y el mantenimiento, incluidas la gestión y la divulgación de vulnerabilidades, la evaluación de la eficacia de las medidas de gestión de riesgos de ciberseguridad, las prácticas básicas de ciberhigiene y la formación, el uso de criptografía y, en su caso, de cifrado, la seguridad de los recursos humanos, el control de acceso y la gestión de activos, y el uso de soluciones de autenticación multifactor o de autenticación continua.

Al establecer estas normas mínimas, la Directiva NIS2 pretende claramente dar a las entidades menos margen para adoptar un enfoque minimalista de la ciberseguridad. Se sigue así una tendencia, que hemos estudiado en otro lugar[84], de trasladar quien determina las obligaciones de *compliance*: «si en el marco del RGPD, el regulado es el responsable de lograr ese equilibrio, la decisión adoptada en estas últimas normas del Derecho de la Unión es trasladar progresivamente esa competencia del regulado al regulador». Además, la Comisión Europea adoptará actos de ejecución por los que se establezcan requisitos técnicos y requisitos técnicos y metodológicos para las entidades de la infraestructura digital y los proveedores digitales.[85]

El Grupo de Cooperación, en colaboración con la Comisión y la ENISA, podrá realizar evaluaciones coordinadas de los riesgos para la seguridad de determinados servicios, sistemas o cadenas de suministro de productos digitales críticos.[86]

Al igual que en el régimen anterior, los incidentes significativos deben notificarse a los CSIRT sin demora indebida.[87] La novedad es que los destinatarios de los servicios también tendrán que ser notificados cuando sea probable que se vean afectados negativamente. También debe

[83] Artículo 14 de la Directiva NIS1 y artículo 21 de la Directiva NIS2.

[84] BARRIO ANDRÉS, Moisés, «El cumplimiento basado en el riesgo o risk-based compliance, pieza cardinal del nuevo Derecho digital europeo», en *Análisis del Real Instituto Elcano*, número 34, 2023, p. 6.

[85] Es decir, respecto de los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centros de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, así como los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales, y los prestadores de servicios de confianza.

[86] Artículo 22 de la Directiva NIS2.

[87] Artículo 14.3 de la Directiva NIS1 y artículo 23 de la Directiva NIS2.

notificarse a los posibles afectados las medidas o soluciones adoptadas en respuesta a la amenaza.

La Directiva NIS2 también modifica los criterios para determinar la importancia de un incidente. Mientras que la NIS1 se centraba en el número de usuarios afectados, la duración y la extensión geográfica, los criterios de la NIS2 para calificar a un incidente como «significativo» son la perturbación grave de las operaciones o las pérdidas financieras para la entidad, y la capacidad del incidente para causar daños materiales o inmateriales considerables a personas físicas o jurídicas. Aunque estos nuevos criterios siguen dejando margen para la interpretación, son ciertamente menos ambiguos que los de la NIS1.

Otra novedad es que la Directiva NIS2 impone unos plazos breves para la notificación de incidentes: 24 horas después de tener conocimiento del incidente para una alerta temprana, 72 horas para una notificación de incidente y un mes para un informe final. El CSIRT también puede solicitar un informe provisional. El CSIRT o la autoridad competente responderá y proporcionará orientación y apoyo adicionales, si así se solicita. Se puede informar al público si es necesaria la concienciación ciudadana para prevenir o gestionar un incidente significativo. Y las estadísticas sobre incidentes significativos deben comunicarse a ENISA.

Por tanto, la nueva directiva ha creado un sistema de notificación en varias fases donde las entidades afectadas deben presentar ante el CSIRT o autoridad competente, según corresponda, las siguientes comunicaciones:[88]

a) Una alerta temprana, sin demora y en el plazo máximo de 24 horas, desde que se haya tenido constancia del incidente significativo;
b) Una notificación del incidente (que se actualizará cuando proceda) y una evaluación inicial incluyendo su gravedad en el plazo máximo de 72 horas desde que se haya tenido constancia del incidente significativo;
c) Un informe intermedio actualizado, si así lo requiere el CSIRT o la autoridad competente;
d) Un informe final, a más tardar un mes después de presentar la notificación del incidente, en el que se recojan los siguientes elementos: i) una descripción detallada del incidente, incluyendo su gravedad e impacto; ii) el tipo de amenaza o causa principal que probablemente haya desencadenado el incidente; iii) las medidas paliativas aplicadas y en curso; y iv) cuando proceda, las repercusiones transfronterizas del incidente.

Mención especial debe hacerse a los sistemas de certificación de la ciberseguridad, que se introdujeron en el Derecho digital europeo en virtud del meritado Reglamento sobre ciberseguridad de la Unión Europea de 2019. Los Estados miembros pueden exigir a las entidades esenciales e importantes que utilicen productos, servicios y procesos certificados.[89] También puede fomentarse[90] el uso de normas y especificaciones técnicas europeas e internacionales.[91]

[88] Artículo 23.4 de la Directiva NIS2.

[89] Artículo 24 de la Directiva NIS2.

[90] Artículo 25 de la Directiva NIS2.

[91] *Vid*. ÁLVAREZ GARCÍA, Vicente, *Las normas técnicas armonizadas. (Una peculiar fuente del Derecho europeo)*, Iustel, Madrid, 2020.

3.6. Jurisdicción y registro

En términos de jurisdicción, las entidades en principio caen bajo la jurisdicción del Estado miembro en el que están establecidas.[92] Las excepciones son que las redes y servicios de comunicaciones electrónicas están sometidas a la jurisdicción del Estado miembro en el que prestan sus servicios, que la infraestructura digital y sus proveedores caen bajo la jurisdicción del Estado miembro en el que tienen su establecimiento principal, y que las administraciones públicas están sometidas a la jurisdicción del Estado miembro que las estableció. Si no cuenta con establecimiento en la UE, la entidad debe designar un representante de la UE. Esta previsión es similar al régimen anterior[93], ahora con más orientaciones sobre lo que debe considerarse un establecimiento principal.[94]

ENISA mantendrá un registro de entidades de infraestructura digital y proveedores digitales.[95] Otra base de datos recogerá datos sobre el registro de nombres de dominio.[96]

3.7. Intercambio de información

La Directiva NIS2 hace mayor hincapié en el intercambio de información.[97] Los Estados miembros deben garantizar que las entidades puedan compartir voluntariamente información relativa a amenazas, cuasiincidentes, vulnerabilidades, etc. para prevenir incidentes y elevar el nivel general de ciberseguridad. Este intercambio de información requiere concertar los acuerdos necesarios dada la naturaleza sensible de la información, que deben ser facilitados por los Estados miembros. Las entidades deben notificar los acuerdos en los que participan. Como ya se ha señalado, aunque esta disposición se ha formulado de forma un poco más contundente que en el marco de la Directiva NIS1, sigue siendo voluntaria y, por lo tanto, su impacto en la práctica está por ver.

Como antes, las entidades también pueden notificar voluntariamente a los CSIRT asuntos no cubiertos por la obligación de notificación.[98] Esta previsión va destinada a las entidades obligadas para incidentes regulares, amenazas y cuasi incidentes, y a las entidades no obligadas por la directiva para incidentes significativos.

3.8. Supervisión y ejecución

La supervisión del cumplimiento del grupo normativo está redactada de forma más precisa en la Directiva NIS2[99], estableciendo ahora una lista mínima de potestades públicas de supervisión y

[92] Artículo 26 de la Directiva NIS2.

[93] Artículo 18 de la Directiva NIS1.

[94] Artículo 26, apartados 2 y 3, de la Directiva NIS2.

[95] Artículo 27 de la Directiva NIS2.

[96] Artículo 28 de la Directiva NIS2.

[97] Artículo 29 de la Directiva NIS2.

[98] Artículo 20 de la Directiva NIS1 y artículo 30 de la Directiva NIS2.

[99] Artículo 15 de la Directiva NIS1 y artículo 31 de la Directiva NIS2.

ejecución. Y, al igual que sucedía en el régimen anterior, las autoridades competentes deben colaborar con las autoridades de protección de datos cuando se trate de datos personales.

Una relevante novedad es que las autoridades pueden priorizar sus tareas en función de los riesgos.

Las potestades de las autoridades competentes en relación con las entidades esenciales se han ampliado e incluyen -junto a las solicitudes de información, el acceso a los datos y las solicitudes de pruebas de aplicación- inspecciones *in situ* y supervisión a distancia, incluidos controles aleatorios realizados por profesionales cualificados, auditorías de seguridad periódicas y específicas o *ad hoc*, y análisis de seguridad basados en criterios de evaluación de riesgos objetivos, no discriminatorios, justos y transparentes.[100] Las auditorías específicas deben ser realizadas por un organismo independiente o una autoridad competente, y la entidad auditada debe correr con los gastos de las mismas. En particular, esta última salvedad puede ser preocupante, dado el ritmo general de este tipo de auditorías, y debe evitarse que las entidades se enfrenten a facturas importantes que les imponen unas autoridades excesivamente rigurosas.

Además, las autoridades competentes tienen que estar dotadas de potestades coercitivas específicas, incluidas las potestades de emitir advertencias, adoptar instrucciones vinculantes, ordenar el cese de una determinada conducta, ordenar el cumplimiento, ordenar la información a las personas físicas y jurídicas potencialmente afectadas, ordenar la aplicación de las recomendaciones de una auditoría de seguridad, designar a un responsable de supervisión, ordenar la divulgación de sus infracciones e imponer multas administrativas. Si estas medidas no conducen a resultados satisfactorios, las autoridades pueden suspender temporalmente una certificación o autorización relativa a una parte o a la totalidad de los servicios pertinentes prestados o de las actividades realizadas por la entidad esencial, o prohibir temporalmente al director general o al representante legal en la entidad esencial que ejerza funciones de dirección en dicha entidad. Estas últimas medidas están previstas como *ultima ratio* en casos extremos, con criterios claros sobre cuándo pueden aplicarse. En todo caso, estimo que la responsabilidad personal de los altos directivos servirá de incentivo para la cooperación.

Las potestades relativas a las entidades importantes son un poco más limitadas, pero siguen siendo más sustanciales que las relativas a los proveedores de servicios digitales en virtud de la Directiva NIS1.[101] Como en el caso de las entidades esenciales, las inspecciones, auditorías y análisis de seguridad también están habilitadas aquí, al igual que las solicitudes de información y acceso a datos y las solicitudes de acreditación de su *compliance*. Asimismo, las medidas que pueden imponerse son en gran medida similares a las de las entidades esenciales, con la excepción de que las medidas de último recurso no se incluyen para las entidades importantes.

En suma, la supervisión pública respecto de las entidades esenciales tiene un carácter más proactivo e intenso, mientras que la concerniente a las entidades importantes es fundamentalmente *ex post*.

[100] Artículo 32 de la Directiva NIS2.

[101] Artículo 17 de la Directiva NIS1 y artículo 33 de la Directiva NIS2.

En cuanto a las multas administrativas, las entidades esenciales pueden ser objeto de multas administrativas de un máximo de, al menos, 10 millones de euros o de un máximo de, al menos, el 2 % del volumen de negocios total anual a nivel mundial en el ejercicio financiero anterior, optándose por la cifra de mayor cuantía.[102] Para las entidades importantes, las multas pueden ascender a un máximo de, al menos, 7 millones de euros o de un máximo de, al menos, el 1,4 % del volumen de negocios total anual a nivel mundial en el ejercicio financiero anterior, optándose también por la cifra de mayor cuantía. Además, pueden imponerse multas coercitivas para obligar a una entidad obligada –sea esencial o importante– a poner fin a su infracción.

Si una infracción también constituye una violación de la seguridad de los datos personales, se notificará a las autoridades competentes en materia de protección de datos.[103]

Al igual que bajo la directiva anterior, los Estados miembros deben establecer las sanciones.[104] Tales sanciones serán efectivas, proporcionadas y disuasorias.

Cuando esté implicado más de un Estado miembro dado el ámbito de la entidad o sus servicios, las autoridades competentes deberán prestarse asistencia mutua en su aplicación.[105]

Por lo demás, la Comisión Europea está facultada para adoptar actos delegados y de ejecución, asistida por un comité.[106]

4. El resto del marco jurídico europeo de la ciberseguridad

Desde la aprobación de la Directiva NIS1 en 2016, la UE ha adoptado algunas normas más en el ámbito de la ciberseguridad.

La más sobresaliente es el precitado Reglamento sobre la ciberseguridad de la Unión. El objetivo del Reglamento (UE) 2019/881 es doble. Por un lado, el Reglamento confiere un nuevo mandato a la ENISA, otorgándole un mandato permanente como agencia de la UE para la ciberseguridad. Por otro lado, el Reglamento establece un sistema de certificación para los productos, procesos y servicios de las TIC, creado y mantenido por ENISA. Esta certificación permite que tales productos, procesos y servicios se certifiquen una sola vez para toda la UE, y proporciona a sus usuarios confianza en su ciberresiliencia. La Directiva NIS2 se inscribe claramente en este Reglamento, al asignar funciones específicas a la ENISA en la realización de sus objetivos. Además, el sistema de certificación también está integrado en NIS2, permitiendo incluso a los Estados miembros exigir el uso de productos, procesos y servicios certificados en algunos casos.

Tras el Reglamento (UE) 2019/881, la Comisión Europea anunció una nueva Estrategia de Ciberseguridad de la UE el 16 de diciembre de 2020.[107] La estrategia configura la ciberseguridad

[102] Artículo 34 de la Directiva NIS2.

[103] Artículo 35 de la Directiva NIS2.

[104] Artículo 36 de la Directiva NIS2.

[105] Artículo 37 de la Directiva NIS2.

[106] Artículos 38 y 39 de la Directiva NIS2.

[107] JOIN(2020) 18 final.

como esencial para construir una Europa resistente, verde y digital. Reconoce la creciente dependencia de la sociedad de sistemas de información y redes cada vez más interconectados. Esto queda ejemplificado por el creciente número de dispositivos conectados, así como por el aumento del teletrabajo durante la pandemia de COVID-19. Al mismo tiempo, el número y la variedad de las ciberamenazas sigue creciendo. Para contrarrestar esta amenaza, la UE se propone aumentar su resistencia general frente a las ciberamenazas. Para ello, la estrategia establece tres pilares: (1) resistencia, soberanía tecnológica y liderazgo; (2) capacidad operativa para prevenir, disuadir y responder; y (3) cooperación para avanzar en un ciberespacio global y abierto.

La Estrategia de Ciberseguridad de la UE 2020 sienta las bases para una serie de ulteriores instrumentos jurídicos, uno de los cuales es la Directiva NIS2. Otro es la nueva Directiva (UE) 2022/2557 sobre la resistencia de las entidades críticas de 2022 (Directiva CER, por sus siglas inglesas de *Critical Entities Resilience Directive*).[108] Este instrumento sustituye a la Directiva sobre infraestructuras críticas de 2008.[109] La nueva Directiva designa entidades críticas en 11 sectores. Estas se solapan en gran medida con la designación de entidades esenciales de la NIS2. Se trata de una decisión de técnica normativa consciente, pero a mi juicio desacertada. La Directiva CER se refiere principalmente a la seguridad física de dichas entidades, mientras que la Directiva NIS2 se refiere a su ciberseguridad. Dado que ambos aspectos están interrelacionados, era importante para NIS2 establecer un enfoque coherente con la Directiva CER.[110] Como resultado, las entidades pueden tener que cumplir con ambos grupos normativos, y las autoridades competentes de ambos marcos deben colaborar estrechamente en algunos asuntos. No parece que la transposición de ambas directivas vaya a ser conjunta, sino que los Estados miembros están optando por sendas leyes, lo cual incrementa la complejidad e inseguridad jurídica en este sector.

Otra norma a la cual debemos referirnos es el Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero de 2022[111] (Reglamento DORA por sus siglas inglesas de *Digital Operational Resilience Act*). DORA se centra específicamente en las entidades financieras, con una lista de 21 tipos de entidades reguladas, entre las que se incluyen entidades de crédito, entidades de pago y de dinero electrónico, empresas de inversión, empresas de seguros y reaseguros, proveedores de servicios de *crowdfunding*, etc. Aparte de las entidades financieras propiamente dichas, el Reglamento DORA también se aplica en cierta medida a terceros que les prestan servicios relacionados con las TIC. El objetivo de este grupo normativo es establecer requisitos comunes para su resistencia operativa digital, que por supuesto también incluye la ciberseguridad. Hace especial hincapié en la gestión de riesgos, las pruebas, la gestión de riesgos de terceros y la supervisión de los proveedores de terceros críticos. Y la Directiva NIS2 no se aplica a las entidades exentas del DORA.[112] Esta excepción está en consonancia con la condición

[108] Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo.

[109] Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

[110] Considerando 30 de la Directiva NIS2.

[111] Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011.

[112] Artículo 2.10 de la Directiva NIS2.

de *lex generalis* de la Directiva NIS2, mientras que el Reglamento DORA actúa como *lex specialis*. Y también en este caso, las autoridades competentes de ambos marcos deben trabajar juntas en algunos asuntos.

Recientemente, el 15 de septiembre de 2022 la Comisión Europea ha presentado una propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020 (comúnmente conocida como Reglamento de Ciberresiliencia o *Cyber Resilience Act*). Este instrumento reforzará las normas de ciberseguridad sobre los productos que se venden con elementos digitales y garantizará, de esta forma, un hardware y software más seguros tanto para las empresas como para los consumidores finales.

En fin, otros sectores con regímenes jurídicos sectoriales específicos son la energía, la aviación y las comunicaciones electrónicas.[113]

Para racionalizar los requisitos de ciberseguridad, el texto final de la Directiva NIS2 suprimió algunas referencias a la ciberseguridad de otros grupos normativos.[114] Esto garantiza que la Directiva NIS2 se erija en la referencia principal en términos de obligaciones de ciberseguridad, confirmando una vez más su condición de *lex generalis* en este campo.

5. Conclusión

En sus orígenes, las previsiones del Derecho digital europeo en cuanto a la ciberseguridad se encontraban tímidamente recogidas en la legislación sectorial, y eran las autoridades nacionales las encargadas de su concreción. Sin embargo, la evolución de Internet y las infraestructuras digitales han convertido a la ciberseguridad en un elemento cardinal del Derecho digital.

Hoy todos somos cada vez más vulnerables a los riesgos de ciberseguridad, desde los ciudadanos hasta las grandes empresas y los Estados. Los ciberdelincuentes aprovechan la mayor conectividad que trae el Internet de las Cosas para llevar a cabo ataques motivados por el ánimo de lucro, la ideología u otras razones. Los ciberataques comprenden desde el intrusismo informático e interceptación de las comunicaciones (*hacking*), la utilización no autorizada de imágenes previamente obtenidas con el consentimiento de la víctima en un lugar privado (*sexting* y *revenge porn*), daños y sabotajes (*cracking*), delitos contra el patrimonio hasta ciberterrorismo perpetrado contra infraestructuras críticas, como redes eléctricas, hospitales y centrales nucleares. Los daños así causados pueden suponer no sólo graves pérdidas económicas, sino también una vulneración de derechos humanos fundamentales como el derecho a la vida y a la salud. Entre los autores de ciberataques se encuentran actores privados, públicos e híbridos (no estatales y estatales), que tienen diferentes motivaciones. Además de los autores privados, que

[113] Así, Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, sobre la preparación frente a los riesgos en el sector de la electricidad y por el que se deroga la Directiva 2005/89/CE; Reglamento de Ejecución (UE) 2019/1583 de la Comisión, de 25 de septiembre de 2019, por el que se modifica el Reglamento de Ejecución (UE) 2015/1998 por el que se establecen medidas detalladas para la aplicación de las normas básicas comunes de seguridad aérea, en lo que se refiere a las medidas de ciberseguridad; o Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.

[114] Artículos 42 y 43 de la Directiva NIS2.

suelen tener motivaciones financieras o ideológicas, los terroristas pueden utilizar las tecnologías en línea para establecer comunicaciones seguras, difundir contenidos que inciten al odio y recaudar fondos para sus actividades. En fin, algunos Estados pueden aplicar tecnologías de espionaje y filtrado contra sus ciudadanos por motivos políticos, como localizar y reprimir a sus disidentes.

Por eso, hoy la ciberseguridad plantea retos jurídicos que van mucho más allá de los obstáculos al mercado único. La ciberseguridad en la UE es cada vez más una responsabilidad compartida entre el sector público, que debe proporcionar los marcos jurídicos pertinentes, el sector privado, que tiene que diseñar y comercializar productos con una ciberseguridad eficaz, y los usuarios finales, que también deben observar en su utilización las denominadas prácticas de ciberhigiene (así como un uso seguro y responsable de los dispositivos digitales).

En este artículo, hemos puesto de relieve el creciente factor de amenaza de los incidentes de ciberseguridad, así como la vertiginosa evolución de los tipos de ciberataques. Esto, unido a la creciente dependencia de la sociedad de los servicios y productos de las TIC -ejemplificada por el gran crecimiento del teletrabajo tras la pandemia COVID-19 y la intensificación ulterior de los procesos de transformación digital- hace que la ciberseguridad sea cada vez más esencial en el funcionamiento de toda organización, incluso de la propia sociedad. Aunque la UE ya había adoptado un marco jurídico inicial destinado a mejorar el nivel general de ciberresiliencia en la UE con la Directiva NIS1, su puesta en práctica ha puesto de relieve que dejaba demasiada discrecionalidad a los Estados miembros. Esto dio lugar a divergencias significativas en la transposición de la norma, lo que condujo a un campo de juego desigual y a una supervisión y aplicación dispares.

Estos problemas fueron, por tanto, los factores que impulsaron la derogación del grupo normativo anterior y la adopción de una nueva Directiva NIS2 a finales de 2022. Aunque la nueva directiva sigue eximiendo en gran medida a las pequeñas empresas y microempresas, la Directiva NIS2 tiene un ámbito de aplicación sustancialmente mayor que la NIS1, incluyendo muchos nuevos tipos de entidades -como las Administraciones públicas-, y se ha centrado más en las infraestructuras digitales y los servicios de TIC. Además, la nueva directiva ha eliminado gran parte de las facultades discrecionales de los Estados miembros, lo que debería traducirse en un ámbito de aplicación mucho más coherente en toda la UE.

En cuanto a las obligaciones, la Directiva NIS2 desarrolla más explícitamente los requisitos de las estrategias nacionales de ciberseguridad de los Estados miembros, con lo que se pretende alcanzar un nivel de calidad más común en toda la UE. Asimismo, añade la obligación de garantizar la gestión y respuesta a los incidentes a gran escala a nivel nacional. También otras entidades, como los CSIRT, tienen ahora sus competencias y tareas más claramente perfiladas.

Por lo que se refiere a la coordinación internacional y de la UE, la Directiva NIS2 prioriza hacer efectiva la coordinación entre los Estados miembros, algo que apenas era desarrollado en el marco de la directiva anterior. Un nuevo organismo, EU-CyCLONe, coordinará la gestión de incidentes y crisis a gran escala en la UE. Del mismo modo, se asignan a la ENISA tareas mejor definidas, al ser ahora la agencia oficial de la UE para la ciberseguridad.

También se ha reforzado el régimen de las obligaciones de notificación, dado que bajo el régimen anterior apenas eran notificados los incidentes de ciberseguridad de una manera efectiva. La

Directiva NIS2 trata de encontrar un equilibrio entre la imposición de una obligación de notificación estricta y la necesidad de no generar demasiados trámites burocráticos adicionales. La práctica tendrá que demostrar si el planteamiento de la nueva directiva tendrá éxito, sobre todo a la luz de otras obligaciones de notificación concurrentes en otros grupos normativos como el Reglamento General de Protección de Datos (RGPD) y la Segunda Directiva de Servicios de Pago (PSD2).

Del mismo modo, se fomenta en mayor medida el intercambio de información, pero sin imponer demasiada transparencia. También, en este caso, la práctica tendrá que demostrar si este enfoque será exitoso.

En fin, se han reforzado la supervisión pública y el control de su cumplimiento. Las autoridades competentes tienen ahora potestades más intensas y delimitadas de un modo más certero. Asimismo, la nueva directiva impone ahora los umbrales para las multas administrativas.

Del mismo modo, hemos examinado cómo encaja la Directiva NIS2 en la regulación más amplia de la UE en este ámbito, que se ha ampliado considerablemente desde la adopción de la Directiva NIS1. Con sus tareas para ENISA y sus referencias a la certificación, la Directiva NIS2 enlaza con el Reglamento europeo de Ciberseguridad de 2019. También guarda estrecha relación con la nueva Directiva sobre entidades críticas, que se centra en la seguridad física. Además, la NIS2 sirve ahora de *lex generalis* en el ámbito de la ciberseguridad, mientras que las leyes sectoriales se configuran como *lex specialis*. Así, el Reglamento sobre resiliencia operativa digital en el sector financiero es un ejemplo de este tipo de legislación sectorial específica, que enlaza con NIS2.

En general, el marco NIS2 puede considerarse a mi juicio como una actualización positiva del régimen jurídico existente. Mantiene el enfoque general de la Directiva NIS1 y se centra específicamente en endurecer los puntos en los que la NIS1 no funcionaba adecuadamente. Al suprimir el amplio margen de discrecionalidad que dejaba a los Estados miembros la NIS1, la Directiva NIS2 debería lograr una mayor igualdad de condiciones en toda la UE en esta materia. Al mismo tiempo, la NIS2 mantiene el planteamiento de no ser demasiado enérgica en algunos aspectos, y habrá que ver si su enfoque renovado conduce a mejores resultados que su predecesora. Por último, aunque es ciertamente positivo que la NIS2 deje margen para una legislación sectorial más centrada en los problemas específicos de cada sector, también hay que asegurarse de que esta opción de política legislativa no dé lugar a una fragmentación por la que los problemas similares que se plantean en varios sectores se traten de forma diferente.

Por lo demás, estoy profundamente convencido que la ciberseguridad deberá convertirse en un próximo derecho fundamental reconocido al más alto nivel en el Derecho de la Unión Europea y el Derecho constitucional de los Estados. Avanzando en esta dirección, podemos poner en valor los pasos dados por nuestra LOPDGDD de 2018 y la Carta de Derechos Digitales de España de 2021[115], que han tenido su reflejo en el Derecho europeo por medio de la Declaración Europea

[115] En el numeral VI de la Carta de Derechos Digitales de España se establece lo siguiente: «1. Conforme al ordenamiento jurídico, toda persona tiene derecho a que los sistemas digitales de información que utilice para su actividad personal, profesional o social, o que traten sus datos o le presten servicios, posean las medidas de seguridad adecuadas que permitan garantizar la integridad, confidencialidad, disponibilidad, resiliencia y autenticidad de la información tratada y la disponibilidad de los servicios prestados.
2. Los poderes públicos, de conformidad con la regulación europea y nacional, velarán para que las garantías expresadas en el número anterior sean satisfechas por todos los sistemas de información, ya sean de titularidad

sobre los Derechos y Principios Digitales de 2022. Esta última recoge el compromiso de colocar a la persona en el núcleo de la transformación digital de la Unión Europea, añadiendo después que la «tecnología debe servir y beneficiar a todas las personas que viven en la UE y empoderarlas para que cumplan sus aspiraciones, en total seguridad y respetando plenamente sus derechos fundamentales». A mi juicio, este nuevo derecho fundamental a la ciberseguridad busca garantizar el acceso a tecnologías digitales seguras y que protejan la privacidad (es decir, cubre productos y servicios digitales). Y tiene como complemento, por una parte, medidas para aumentar la resistencia de las tecnologías y los productos digitales y, por otra, normas para exigir responsabilidades a quienes traten de socavar la seguridad en línea y la integridad del entorno digital.

6. Bibliografía

ALONSO LECUIT, Javier y GALÁN, Carlos, «Un libro blanco para la cooperación público-privada en ciberseguridad», en *Análisis del Real Instituto Elcano*, número 67, 2019.

ÁLVAREZ GARCÍA, Vicente, *Las normas técnicas armonizadas. (Una peculiar fuente del Derecho europeo)*, Iustel, Madrid, 2020.

ÁLVAREZ ROBLES, Tamara, «El derecho de acceso universal a internet en el marco normativo español: presente y futuro», en Revista LA LEY Derecho Digital e Innovación, número 7, 2021.

ARTEAGA MARTÍN, Félix, «La evaluación y la revisión de la Directiva NIS», en *Análisis del Real Instituto Elcano*, número 19, 2021.

BARRIO ANDRÉS, Moisés, «El cumplimiento basado en el riesgo o risk-based compliance, pieza cardinal del nuevo Derecho digital europeo», en *Análisis del Real Instituto Elcano*, número 34, 2023.

BARRIO ANDRÉS, Moisés, «Las nuevas coordenadas del Derecho digital europeo», en *Anuario Diálogos Jurídicos*, número 8, 2023.

BARRIO ANDRÉS, Moisés, *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, Wolters Kluwer, Madrid, 2018.

BARRIO ANDRÉS, Moisés, *Fundamentos del Derecho de Internet*, Centro de Estudios Políticos y Constitucionales, Madrid, 2020, 2ª edición.

BARRIO ANDRÉS, Moisés, *Internet de las Cosas,* Reus, Madrid, 2022, 2ª edición.

BARRIO ANDRÉS, Moisés, *Los derechos digitales y su regulación en España, la Unión Europea e Iberoamérica*, Colex, A Coruña, 2023.

BARRIO ANDRÉS, Moisés, *Manual de Derecho digital*, Tirant lo Blanch, Valencia, 2022, 2ª edición.

pública o privada, proporcionalmente a los riesgos a los que estén expuestos. A tal efecto podrán contar con la colaboración de la sociedad civil.
3. Los poderes públicos promoverán la sensibilización y formación en materia de ciberseguridad de toda la sociedad e impulsarán mecanismos de certificación».

BOIX PALOP, Andrés, «Digital Platform Competition Regulatory Challenges», en *Revista General de Derecho de los Sectores Regulados: RSR*, número 8, 2021.

CONAL FUERTES, Iker, *Ciberseguridad y Derecho penal*, Aranzadi, Pamplona, 2022.

DE LA IGLESIA MONJE, María Isabel, «Relevancia del análisis de riesgos en la protección de datos en la ciudad inteligente», en PLAZA PENADÉS, Javier y MARTÍNEZ VELENCOSO, Luz (dirs.), *Retos normativos del mercado único digital europeo*, Tirant lo Blanch, Valencia, 2023.

DELGADO MARTÍN, Joaquín, «La regulación de la ciberseguridad», en MONTERO PASCUAL, Juan José (coord.), *Digitalización y Derecho*, Tirant lo Blanch, Valencia, 2023.

DOMÉNECH PASCUAL, Gabriel, «Las regulaciones experimentales», en *Anuario del buen gobierno y de la calidad de la regulación: ABGCR*, número 1, 2022.

DOMÍNGUEZ ÁLVAREZ, José Luis, «Derecho a la seguridad digital: génesis, evolución y perspectivas de futuro», en RODRÍGUEZ AYUSO, Juan Francisco (coord.), *Nuevos retos en materia de derechos digitales en un contexto de pandemia: perspectiva multidisciplinar, Aranzadi*, Pamplona, 2022.

ELTJON, Mirashi, *Tratamiento procesal del cibercrimen y diligencias de investigación tecnológica*, Aranzadi, Pamplona, 2023.

ESTÉBANEZ GARCÍA, Margarita, «El impacto del COVID-19 en la ciberseguridad y las infraestructuras críticas», en *Revista LA LEY Derecho Digital e Innovación*, número 6, 2020.

FUERTES LÓPEZ, Mercedes, *Metamorfosis del Estado. Maremoto digital y ciberseguridad*, Marcial Pons, Madrid, 2022.

ISHIKAWA, Tomoko y KRYVOI, Yarik (eds.), *Public and Private Governance of Cybersecurity: Challenges and Potential*, Cambridge University Press, Cambridge, 2023.

LORIA GARCÍA, Paz, «Delitos y redes sociales: los nuevos atentados a la intimidad, el honor y la integridad moral (especial referencia al «sexting»)», en *Revista LA LEY penal: revista de derecho penal, procesal y penitenciario*, número 105, 2013.

RECIO GALLO, Miguel, «Seguridad digital: ¿derecho o expectativa de derecho? A propósito del Proyecto de Carta de Derechos Digitales», en *Revista LA LEY Derecho Digital e Innovación*, número 7, 2020.

ROSINO CALLE, Roberto, « La construcción del Mercado Único Digital. Primeros pasos», en *REDE. Revista española de derecho europeo*, número 86, 2023.

RUEDA MARTÍN, María Ángeles, «Los ataques de denegación de servicios como ciberdelito en el Código Penal español», en *Revista Penal*, número 49, 2022.

TEJERINA RODRÍGUEZ, Ofelia (coord.), *Aspectos jurídicos de la ciberseguridad*, RA-MA, Madrid, 2020.

VELASCO SAN MARTÍN, *Cristos, Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos*, Tirant lo Blanch, Valencia, 2016.

WONG, Helen, *Cyber Security: Law and Guidance, Bloomsbury Professional*, Londres, 2018.