ARI 28/2021
2 de marzo de 2021

Dos años de vigencia de la trasposición de la directiva NIS en España: balance de una aplicación heterogénea

Vicente Moret Millás | Letrado de las Cortes Generales y Of Counsel de Andersen Tax & Legal.

Tema

Se cumplen dos años desde la trasposición en España de la Directiva NIS para armonizar la respuesta europea ante los retos de la seguridad de redes y sistemas de información. Una iniciativa con resultados positivos que, sin embargo, precisa ahora una revisión.

Resumen

En septiembre de 2018 se aprobó el Real Decreto-ley 12/2018 que trasponía en España la Directiva sobre la seguridad de las redes y los sistemas de información de la UE (Directiva NIS). La aplicación de la Directiva NIS y sus trasposiciones nacionales han contribuido a crear una cultura de protección común frente al riesgo tecnológico, impulsando actuaciones técnicas, jurídicas y de capacitación de recursos humanos. No obstante, se hace necesario actualizar el acervo normativo para que la nueva Directiva NIS 2 y sus futuras trasposiciones aprovechen la experiencia acumulada durante los años de vigencia, y se adapten a los profundos cambios tecnológicos y también geopolíticos, económicos y sociales. Este ARI desarrolla el balance de lo logrado e identifica los retos a los que se enfrenta su revisión.

Análisis

Desde la aprobación el pasado mes de septiembre de 2018 del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, las circunstancias han cambiado sustancialmente, tanto desde el punto de vista regulatorio, como desde el punto de vista de la acelerada, profunda e improvisada transformación digital que estanos viviendo impulsada por la pandemia de COVID-19.

A nivel general se puede decir que los asuntos relativos a la ciberseguridad han pasado de ser cuestiones que más bien preocupaban a los iniciados en la materia, procedentes del sector IT, a convertirse en un asunto global, geopolítico, que ocupa un lugar preferente en las agendas de los gobiernos de todo el mundo. El dominio digital ya es entendido como prioritario por los estados. La UE también lo ha entendido así. La Directiva NIS, aprobada en 216, no fue la primera iniciativa en este sentido. Fue precedida por la aprobación del bloque regulador europeo de la protección de infraestructuras críticas. Si bien no fue la primera regulación, sí constituyó el primer intento decidido y de calado por regular de forma homogénea una respuesta común de los países miembros de la UE ante los crecientes retos que implica la seguridad de redes y sistemas.

La actual Comisión Europea ha apostado por un nuevo marco regulador en materia digital que tenga como eje asegurar una cierta soberanía digital y el impulso a una visión europea de las fuertes transformaciones económicas, sociales y jurídicas que está originando el proceso de cambio digital a todos los niveles. Lo que está en juego, una vez perdida la hegemonía tecnológica, es conseguir que Europa lidere el sometimiento de la revolución tecnológica a una serie de principios que están en el ADN de la UE; derechos fundamentales, Estado de Derecho y Democracia. La herramienta que la UE ha decidido utilizar para imponer ese esquema de valores es la aprobación de normas jurídicas que sirvan de base regulatoria segura para la protección de los ciudadanos europeos, pero que al mismo tiempo sirvan de inspiración para otros países, tal y como ha ocurrido con el RGPD. De esta forma, esa suerte de *soft power* quiere contribuir a embridar un fenómeno de cambio civilizatorio, que hasta hace unos años parecía estar al margen de las fronteras, los gobiernos y sus leyes.

La Directiva NIS puede entenderse, sin lugar a dudas, como una norma que ha marcado un antes y un después en la forma en la cual la cuestión esencial de la seguridad de las redes y sistemas es abordada desde el poder de la autoridad pública. Constituyó un iniciativa valiente, novedosa y pionera por asentar las bases de una aproximación común hasta lo que en ese momento había sido una competencia netamente nacional. Ese es quizá el gran acierto de NIS, mostrar a las claras que la ciberseguridad es una cuestión que trasciende fronteras y que sólo se podrá gestionar con garantías de éxito mediante estrategias e instrumentos de cooperación entre Estados. Por todo lo anterior, se considera que este es un buen momento para hacer balance.

Las limitaciones del balance

La Comisión Europea ya ha puesto en marcha del proceso de configuración y elaboración de lo que será la Directiva NIS 2, y es necesario atender a cuáles han sido los impactos reales de la normativa NIS en España, traspuesta mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Vaya por delante que el balance es netamente positivo. Por primera vez se ha dispuesto de una norma de cabecera a nivel europeo capaz de poner de relieve la crucial relevancia del tema, así como de sentar unas bases comunes para abordar una regulación legal de la materia, por otra parte, tan compleja de normar, como todas las materias que tienen que ver con la tecnología digital y los cambios que ha producido.

No obstante, flaco favor le estaríamos haciendo al avance en la regulación de estas materias si sólo nos fijásemos en los aspectos positivos y no intentásemos encontrar los puntos de mejora que deberían formar parte de la iniciativa NIS 2. Ese es el objetivo de este trabajo cuya meta es encontrar los aspectos que son susceptibles de mejorar la regulación en vigor tras analizar lo que ha ido ocurriendo en estos dos años y 5 meses de vigencia.

Por otra parte, debe señalarse que forzosamente ese análisis será incompleto. La trasposición de la Directiva NIS ha sido complementada en su desarrollo legal recientemente por el esperado Real Decreto 43/2021, de 26 de enero, por el que se

desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Esta norma es el complemento necesario para que el RD-ley 12/2018 despliegue en toda su plenitud sus efectos, con lo cual esta recapitulación sobre los dos años de vigencia de la trasposición de la Directiva NIS en España será por fuerza incompleta dado que su desarrollo a nivel reglamentario ha tardado en llegar más de lo previsto. Ello supone que la operatividad, sobre todo en el ejercicio por parte de las autoridades administrativas de todas las competencias que el RD-ley les atribuía, se ha visto bastante limitado por la ausencia de una disposición que lo desarrollase en todos sus aspectos. Así mismo, la nueva norma ha venido a aclarar muchos aspectos hasta ahora poco desarrollados.

Una dificultad añadida al análisis que ahora se propone es que, salvo error u omisión, hasta ahora no se ha publicado ningún estudio o informe completo por parte de las autoridades públicas sobre el balance de los dos años de vigencia de esta norma jurídica. No obstante, sí se han publicado diversos informes sobre la situación de la ciberseguridad en España con carácter anual, sus tendencias, fortalezas y amenazas. Estos informes, sumados a las encuestas y estudios realizados por empresas privadas y consultoras, son la base para intentar formar una idea clara del impacto y consecuencias de la aplicación de la Directiva NIS y su trasposición en España[1].

Por otra parte, la Comisión Europea sí realizo un esfuerzo de evaluación para poder encarar con garantías de éxito la aprobación de la directiva NIS 2. En concreto, es forzoso referirse al estudio de ENISA sobre la cuestión, publicado con el título *NIS Investments Report* en diciembre de 2020 y que constituye hasta ahora la más completa evaluación del impacto de la Directiva NIS en todos los países de la UE[2].

Conclusiones sobre el balance

Por todo ello, a continuación, se exponen algunas de las principales conclusiones que se extraen de las informaciones tanto públicas como privadas que durante estos años han ido apareciendo de forma esporádica, así como de las informaciones obtenidas de empresas, autoridades y medios de comunicación. También de informaciones oficiales y de opiniones vertidas por responsables al frente de cometidos de ciberseguridad, tanto del sector público como privado.

De todo el caudal de información disponible procedente de las fuentes antes citadas podemos extraer unas **conclusiones** que tiene un carácter cualitativo más que cuantitativo, dada la escasa información disponible al respecto.

1. La **redacción de las categorías de sujetos obligados incluida en el Real Decreto 12/2018 resultan confusas y poco trasparentes** a la hora de que una empresa pueda identificarse como obligada al cumplimiento de las obligaciones contenidas en esta norma. Es evidente que el sistema de designación como Operador de

[1] Deloitte, “El estado de la ciberseguridad en España”, 2020.

[2] ENISA, “NIS Investments Report”, 11 de diciembre de 2020.

Servicios Esenciales (OSE) por parte de la Administración competente, constituía un sistema de designación claro y evidente. Sólo las empresas designadas tienen la obligación de cumplir la normativa NIS, y por ello están sometidas al posible régimen sancionador. Esta aparente claridad se torna confusión cuando los sujetos eran incluidos en otro grupo, el de los OSE no críticos y por ello no designados. Se trata de una confusión que es consecuencia de la unificación de dos categorías distintas, la de operador de infraestructuras críticas en la categoría de OSE. Este concepto de operador crítico procede de la normativa reguladora de las infraestructuras críticas de 2011 y que en nuestro país entró en vigor por la Ley 8/2011. Ello ha generado cierta confusión y muchas consultas constantes sobre si una empresa concreta está o no sometida a este ámbito de aplicación que, se insiste, no queda reducido a las entidades designadas como críticas, sino que va más allá. Mayor confusión si cabe se derivaba de la identificación de los Prestadores de Servicios Digitales, sobre todo en lo que hace referencia a la categoría de mercados online.

En definitiva, es una constante la afirmación de que el ámbito de aplicación del Real Decreto no es claro, y no da seguridades a los potenciales obligados. Sólo los OSE designados como críticos saben a qué atenerse, dejando en un entorno jurídico difuso a los OSE no críticos. Esa confusión se genera desde el mismo momento en el cual una empresa debe averiguar si está o no incluida en el ámbito de aplicación de la norma como OSE no críticos.

2. **Percepción extendida de escasa o nula actividad de control por parte de la Administración en cuanto al cumplimiento de las obligaciones** contenidas en el Real Decreto 12/2018. Existe una percepción clara entre las empresas potencialmente obligadas, de que en materia de incumplimientos la administración no ha desplegado una actividad sancionadora activa, como si lo hace de forma eficazmente en otras materias, como por ejemplo la de Protección de datos. Ello ha generado un relajamiento por parte de estos sujetos obligados a la hora de aplicar medidas e implantar políticas. Esa inacción se puede deber a la ausencia de un reglamento de desarrollo que ahora si existe tras la aprobación del RD 43/2021. Esta norma ha tardado dos años en llegar y ello ha dificultado que la transposición de la Directiva NIS haya desplegado todos sus efectos en España. El citado RD es el complemento indispensable para una eficaz y plena aplicación de muchos aspectos, ente otros, del régimen sancionador con todas las garantías administrativas que nuestro Ordenamiento Jurídico prescribe a la hora de aplicar el régimen sancionador.

3. **Complejidad del esquema de autoridades competentes** a la hora de aplicar la norma en toda su extensión. El complejo reparto de competencias supone una cierta confusión de roles y por ello, la imposibilidad en ocasiones de que las empresas obligadas puedan tener clara cuál es su autoridad de referencia en los distintos sectores. Ello ha supuesto una falta de cultura de cumplimiento y de colaboración público-privada con el objeto de fortalecer mecanismos de cooperación entre Administraciones Públicas y empresas obligadas. Ello es especialmente visible en sectores con una escasa cultura de cumplimiento normativo. No ocurre lo mismo en

otros como en el financiero o energía en los cuales hay una bien asentada cultura de cumplimiento[3].

4. **Falta de parámetros y umbrales de notificación de incidentes** claramente especificados. Ese problema ha sido resuelto recientemente por la inclusión de la Instrucción Nacional de Notificación y Gestión de incidentes en el RD 43/2021. No obstante, dado que las notificaciones de incidentes son una parte muy importante de las obligaciones de cumplimento normativo, habría sido de mucha utilidad su desarrollo y aprobación poco después de la aprobación y posterior convalidación del Real Decreto-ley en 2018 y no dos años y medio después. Es por tanto difícil hacer una evaluación de la efectividad de las obligaciones de notificación incluidas en la norma debido al retraso en la aprobación de la norma de desarrollo.

5. **La distinción tajante entre los regímenes jurídicos aplicables a los OSE y a los PSD**. Se trata sin duda de una diferenciación de rieguen jurídico contenida en la propia Directiva NIS pero que debería de alguna manera haberse mitigado en lo posible al regular a nivel nacional en la trasposición. Algunos PSD son tan relevantes para el funcionamiento de la economía y la sociedad digital, que no tiene ningún sentido no someterles a las mismas obligaciones que a los OSE. Esta disparidad de regímenes proyecta una imagen falsa del nivel de relevancia y, por tanto, de exigencia con respecto a los PSD. Algunos de ellos son tan críticos para el mantenimiento de las estructuras y sistemas como cualquier OSE designado como tal. De hecho, el borrador de directiva NIS 2 que ya ha sido publicado, elimina esa diferenciación.

6. **Ausencia de un catálogo bien definido de obligaciones** a cumplimentar por los operadores incluidos en el ámbito de aplicación de la norma. En este caso, es evidente que la norma nació con carencias de contenido en este aspecto, que introducían confusión en cuanto a qué estaban obligados los sujetos. En este sentido la reciente aprobación del RD 43/2021 ha contribuido a definir de forma mucho más precisa el alcance de esas obligaciones, aunque como ya se dijo antes se ha hecho de forma muy tardía, con dos años de retraso. Esa ausencia de un catálogo bien definido de acciones y políticas obligatorias a cumplimentar por las empresas ha supuesto una gran heterogeneidad en cuanto al cumplimiento normativo de la norma, e incluso a la propia obligatoriedad de la norma que, en algunos sectores, se percibe como una mera declaración de principios y no como una norma realmente vinculante que obligaba a iniciar acciones para darle cumplimiento.

7. Sigue existiendo **una baja cultura de cumplimiento**, en general debido a la percepción de que la ciberseguridad y su cumplimiento normativo es una carga y no es vista como una forma de proteger activos y preservar la empresa. Se trata de una oportunidad para proteger a las organizaciones e incluso convertirse en una ventaja competitiva. Esta percepción de cumplimiento no voluntario ha llevado a que se entienda este nuevo cumplimiento normativo como un *compliance* incompleto, fragmentario y de difícil cumplimiento, que no tiene la madurez ni la obligatoriedad

[3] PWC, "Informe del Estado de cultura de ciberseguridad en el entorno empresarial", 2020.

de otros. Es el caso, por ejemplo, del relativo a la Protección de datos de carácter personal que sí es percibido como plenamente aplicable y relevante. Ello se debe también a que este cumplimiento tiene una autoridad administrativa que lo respalda con fuertes sanciones. Los estudios realizados demuestran una tendencia a catalogar la norma como ineficaz o irrelevante.

8. **Necesidad de incrementar la cultura de ciberseguridad dentro de las organizaciones obligadas**. Se extrae de las encuestas un bajo conocimiento todavía de los fundamentos básicos de la seguridad de las redes y sistemas a nivel usuario. Aunque la situación ha mejorado mucho gracias a los esfuerzos de empresas y Administraciones competentes hay que seguir avanzando en esa línea. A este respecto, el RD-ley podría haber sido un instrumento muy poderoso para cambiar la cultura interna de muchas organizaciones, y en general de todos los sujetos obligados hayan sido designados o no como críticos, en aras a aumentar la resiliencia total de las organizaciones. Es importante señalar junto al componente tecnológico, el componente humano; las personas y la organización, son tan relevantes ya como la propia tecnología. Se trata de un esfuerzo en el cual todos los empeños públicos y privados serán todavía pocos, dada la magnitud del desafío y, en general, del desconocimiento que todavía existe en muchas capas de población con respeto al desarrollo de habilidades digitales, incluidas las relativas a la ciberseguridad.

9. **Cierta confusión entre el ámbito NIS y el de la protección de datos RGPD**. Existe una opinión muy extendida que erróneamente entiende que el cumplimiento en esta materia se reduce a lo regulado en el RGPD. Se identifica ciberseguridad con protección de datos, lo cual es una reducción enorme de los riesgos a los cuales están expuestas las organizaciones. Además, esta visión limitada reduce la protección de las propias empresas al reducir el panorama de amenazas sólo a las que se centran en la integridad y disponibilidad de la información y obvian otras que atacan la propia continuidad del negocio. Falta todavía el grado de madurez necesario para entender en toda su extensión que la ciberseguridad se enmarca en el contexto más amplio de la gestión del riesgo. La aplicación del RD-ley no ha conseguido individualizar y visualizar esos otros parámetros de ciberseguridad completamente, del mismo modo que sí han conseguido otras normas alcanzar esa notoriedad y concienciación en cuanto a la necesidad de invertir y consolidar una función de control de riesgos de ciberseguridad.

Conclusiones

En definitiva, la aplicación de la Directiva NIS y sus trasposiciones nacionales, han supuesto un importante avance en el establecimiento de un marco normativo que consolide una cultura de protección frente al riesgo tecnológico, impulsando actuaciones técnicas, jurídicas y de capacitación de recursos humanos. No obstante, este camino inicial debe ser continuado con la nueva Directiva NIS 2 y por ello, es necesario que el nuevo texto legal incorpore la experiencia acumulada de 4 años de vigencia y de profundos cambios tecnológicos y también geopolíticos, económicos y sociales.

Convertir a Europa en referente de una buena gobernanza de la ciberseguridad, que logre un adecuado nivel de protección para sus ciudadanos, es un reto que bien merece la pena el esfuerzo de hacer un balance. Sólo así se podrá acometer los cambios regulatorios necesarios aprendiendo de los aspectos que necesitan un proceso de mejora.