La Directiva NIS2, la ciberseguridad y la posición del Tribunal Supremo

I. Introducción

La Unión Internacional de Telecomunicaciones define la ciberseguridad como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de una organización y los usuarios en el *ciber entorno*.

Dada la naturaleza transversal de las tecnologías de la información y las comunicaciones, la ciberseguridad se concibe como un conjunto de mecanismos orientados a proteger las infraestructuras informáticas y la información digital que contienen los sistemas interconectados.

Hoy en día, la ciberseguridad no es simplemente un complemento, sino que debe incluirse dentro del concepto de seguridad nacional, tal y como queda reflejado en la Ley 36/2015, que la califica de materia de especial interés. La ciberseguridad, por tanto, es una actividad que se integra dentro de la seguridad pública.

En relación con la normativa actualmente aplicable en esta materia, debe mencionarse el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad (el "**Anteproyecto de Ley**") encargado de transponer la Directiva (UE) 2022/2555, conocida como *Directiva NIS 2*. Si bien esta Directiva debió trasponerse al ordenamiento jurídico interno antes de octubre de 2024, el Reino de España todavía no ha dado los pasos necesarios para aprobar la normativa exigida. Sin embargo, el Anteproyecto de Ley proporciona una imagen nítida de la legislación que presumiblemente se aplicará en nuestro país en los próximos años.

II. Objeto y ámbito de aplicación

Según el Anteproyecto de Ley, la norma tiene por objeto establecer medidas para alcanzar un elevado nivel común de ciberseguridad en España y contribuir a la ciberseguridad de la Unión Europea, lo que incluye: (i) el establecimiento de obligaciones que requieren la adopción de una estrategia nacional de ciberseguridad; (ii) la adopción de medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para determinadas entidades; y (iii) la fijación de normas y obligaciones relativas al intercambio de información sobre ciberseguridad y de supervisión y ejecución.

El artículo 3 del Anteproyecto de Ley recoge un amplio elenco de entidades sujetas a las obligaciones expuestas:

1. Aquéllas de índole pública o privada que tengan su residencia fiscal en España y que se encuentren dentro de los sectores de alta criticidad, en caso de contar con 50 o más trabadores y con un balance general anual que supere los 10 millones de euros.

2. Aquéllas que, independientemente de su tamaño, estén recogidas en el artículo 3.2 del Anteproyecto. Entre ellas, pueden destacarse las entidades que sean consideradas como proveedores únicos de un servicio esencial, las entidades pertenecientes al sector público, y las universidades y centros de investigación relacionados con sectores críticos.

III. La ciberseguridad como piedra angular del *compliance*

Desde el punto de vista del *compliance*, la relevancia de la NIS2 es evidente, ya que exige la puesta en marcha de ciertas medidas por parte del departamento legal y por parte del órgano de dirección de la empresa.

Las nuevas tecnologías suponen un riesgo latente para todo tipo de entidades. Los correos electrónicos fraudulentos, el *hackeo* de servidores y (entre otras prácticas maliciosas) el filtrado de información confidencial pueden materializarse en incumplimientos de la normativa de ciberseguridad y de protección de datos.

En esta misma línea, la exigencia de recibir formación periódica y específica para lograr el correcto desempeño de sus obligaciones y funciones se extiende también a la formación de empleados ajenos al departamento legal y a los órganos de dirección.

Además, el factor reputacional juega aquí un papel crítico, ya que muchas empresas no logran recuperarse de un incumplimiento de tal magnitud, más si cabe cuando éste ha sido denunciado por organismos estatales como la AEPD, la prensa o terceros afectados.

IV. El órgano de dirección y su responsabilidad

Tal es la importancia de la ciberseguridad que el Anteproyecto de Ley indica, en su artículo 35, que los miembros del órgano de dirección de las entidades responderán solidariamente por las infracciones que éstas cometan. Las implicaciones de este precepto no pasan desapercibidas, ya que cabe la posibilidad de que terceros reclamantes se dirijan directamente contra los directivos de una sociedad.

Este anteproyecto pretende aumentar la carga sobre el órgano de dirección, que no sólo deberá preocuparse de aplicar las medidas necesarias para cumplir con la normativa vigente en materia de ciberseguridad, sino que deberá llevar a cabo una labor de supervisión de cara a asegurar el correcto funcionamiento de las medidas adoptadas.

Surge, sin embargo, la duda acerca de qué debemos entender por órgano de dirección. A pesar de la tendencia general a considerar que este concepto se acota al consejo de administración, se debe tener en cuenta que el concepto engloba a cualquiera que dirija efectivamente la entidad o desempeñe una función clave en ella, tal y como establece el Reglamento DORA (*Digital Operational Resilience Act*) en su artículo 3.

V. Algunas aportaciones del Anteproyecto de Ley

Conviene realizar una breve referencia a los sectores comúnmente considerados críticos, entre los que se encuentran, entre otros, la energía, la tecnología, las infraestructuras digitales, el sector financiero, el transporte, la salud, el agua, la Administración pública y la industria nuclear. A éstos se añaden nuevos sectores incorporados por el Anteproyecto de Ley, como los servicios postales y de mensajería, la gestión de residuos, la seguridad privada, determinados servicios digitales y la industria química.

Más allá de las categorías y definiciones previstas en la propia Directiva NIS 2, el legislador español ha optado por introducir obligaciones adicionales. Entre ellas destaca la exigencia de que las entidades realicen una autoevaluación, con el fin de determinar su sujeción a las obligaciones establecidas en la Directiva. Asimismo, las empresas que queden incluidas en su ámbito de aplicación deberán comunicarlo de forma proactiva a la autoridad competente en el plazo de tres meses desde la aprobación del Anteproyecto de Ley, ya que, en caso de no hacerlo, se enfrentan a la imposición de una sanción económica.

VI. La sentencia del Tribunal Supremo de 19 de febrero de 2025

Las exigencias y medidas anteriormente mencionadas tendrán una importancia mayúscula en los próximos años. Prueba de ello es que, sin haberse traspuesto la Directiva al ordenamiento jurídico español, la Sala de lo Penal del Tribunal Supremo, en su sentencia nº 136/2025, de 19 de febrero [ECLI:ES:TS:2025:699], ya sentó (en parte) las bases interpretativas de los preceptos recogidos en la Directiva NIS2.

En este sentido, el Tribunal Supremo afirma que, si una empresa es víctima de un ciberataque y no ha tomado las medidas razonablemente exigibles para evitarlo, con la producción de un daño a un tercero, dicha entidad podrá ser responsable civil subsidiaria frente a este tercero.

Las implicaciones de esta sentencia son muy relevantes, ya que confirma que la propia empresa, víctima de un ciberataque, puede ser a su vez responsable civil subsidiaria.

El Tribunal Supremo rechaza que pueda sostenerse, de forma razonable, que el sistema informático y los medios tecnológicos utilizados por el empresario queden al margen del concepto de establecimiento, en la medida en que constituyen activos esenciales para el desarrollo de la actividad empresarial.

Sobre esta base, la Sala considera que el hecho de que la sociedad hubiera sido objeto de un ciberataque reciente –materializado a través del envío de un correo electrónico fraudulento que inducía a un cliente a efectuar un pago pendiente en una cuenta bancaria distinta de la habitual– era circunstancia suficiente para activar un deber reforzado de diligencia.

En particular, se afirma que la entidad debió reaccionar ante dicha brecha de ciberseguridad, alertar al conjunto de sus clientes e implantar las medidas oportunas para prevenir la reiteración del ataque.

En este sentido, el Alto Tribunal aprecia que la falta de comunicación por parte de la sociedad facilitó la consumación del fraude, al no advertirse de manera fehaciente a terceros de la necesidad de abstenerse de realizar pagos sin una verificación previa de que la cuenta indicada correspondía efectivamente a la entidad. Esta omisión permitió que una empresa efectuara un pago a un tercero como consecuencia del engaño articulado mediante un correo electrónico y una cuenta bancaria falsos.

La Sala concluye, así, que la sociedad infringió las reglas de actuación profesional exigibles conforme a los estándares de diligencia propios de su sector, incurriendo en una vulneración del deber de cuidado que ocasionó un daño a un tercero, criterio que encuentra sólido respaldo en la doctrina jurisprudencial consolidada (entre otras, sentencia nº 768/2009, de 16 de julio, y sentencia nº 212/2015, de 11 de junio).

VII. Conclusiones

Pese a que la Directiva NIS 2 aún no ha sido incorporada al ordenamiento jurídico interno, no deben ignorarse las principales obligaciones que impone, entre las que destacan la adopción de nuevas medidas de ciberseguridad por parte de las entidades afectadas; así como las responsabilidades específicas que recaen sobre sus órganos de administración y dirección.

En este contexto, el Anteproyecto de Ley constituye, en la actualidad, la referencia más precisa y representativa del conjunto de obligaciones que deberán observar las entidades sujetas a este régimen normativo.

En todo caso, aun cuando una entidad concreta no quede formalmente comprendida dentro del ámbito de aplicación conforme a los criterios legales, la adopción voluntaria de los mecanismos necesarios para alinearse con las exigencias de la Directiva NIS 2 resulta claramente beneficiosa, en la medida en que contribuye a reforzar su nivel de protección y resiliencia a medio y largo plazo.

En definitiva, como expresa la conocida máxima *prevenir es mejor que curar*, por lo que la anticipación sigue siendo la estrategia más eficaz. Si bien el riesgo cero resulta inalcanzable, invertir en un sistema de ciberseguridad sólido y alineado con el marco normativo europeo constituye un pilar esencial de una adecuada política de mitigación de riesgos, basada en el reconocimiento del valor estratégico que tiene la adaptación de este tipo de normas en el seno de la organización.