Ana Marzo Portera
Marzo & Abogados

La ciberseguridad es "cosa de todos"

En los últimos años oímos hablar cada vez más de la ciberseguridad como una cuestión de gran importancia para nuestra economía y nuestra sociedad. A primera vista no es fácil determinar el momento exacto en que surge la inquietud por la ciberseguridad y lo más importante, el momento en que pasa de ser una prioridad para las grandes empresas tecnológicas, para ser una obligación de cualquier empresa o ciudadano.

La ciberseguridad se ha "colado" en nuestro Derecho interno poco a poco y sin hacer mucho ruido, empezando como una cuestión de seguridad pública o de la "Ciberdefensa" para ser una cuestión general que afecta a los intereses de las administraciones públicas, a los de las empresas privadas y a los derechos y libertades de los ciudadanos.

En el año 2013 la Comisión Europea puso de manifiesto que los sistemas de información pueden verse afectados por incidentes relacionados con la seguridad causados por errores humanos, fenómenos naturales, fallos técnicos o ataques malintencionados siendo la envergadura, frecuencia y complejidad de estos incidentes cada vez mayor. El grado de afectación llega hasta el punto que la falta de seguridad en las redes e información puede llegar a comprometer servicios vitales (que dependen de la integridad de las redes y los sistemas de información), interrumpiendo las actividades de las empresas, generando cuantiosas pérdidas financieras para la economía de la UE e incidiendo negativamente en el bienestar de la sociedad y los ciudadanos.

En el año 2016 se aprobó la llamada Directiva NIS (Network Information Security) con el objetivo de garantizar un elevado nivel común de seguridad de las redes y de la información (SRI) a efectos de lo cual la Directiva considera necesario, por una parte, instar a los Estados miembros a estar más preparados e incrementar la cooperación entre ellos, y, por otra, exigir a los operadores de infraestructuras críticas (como energía, transporte, agua, banca, infraestructuras de los mercados financieros, asistencia sanitaria e infraestructura digital), a los proveedores clave de servicios de la sociedad de la información o servicios digitales (como motores de búsqueda, servicios de cloud computing y mercados en línea) y a las administraciones públicas que adopten las medidas oportunas para, por un lado, gestionar los riesgos de seguridad y, por otro lado, notificar los incidentes graves a las autoridades nacionales competentes.

En realidad, esta Directiva supone una estrategia europea de ciberseguridad cuyo fin es garantizar un entorno digital seguro y fiable. No obstante, la Directiva no es la única medida, sino que se complementa con otras destinadas a intensificar la lucha contra la ciberdelincuencia y elaborar una política internacional de ciberseguridad para la Unión Europea. Entre ellas, la asociación público-privada lanzada por la Comisión Europea en el marco de su programa de investigación e innovación Horizonte 2020.

La Directiva parte de la base de que las capacidades y mecanismos de SRI actuales son, sencillamente, insuficientes para seguir el ritmo de unas amenazas, en rápida mutación, y para garantizar un nivel elevado de protección igual en todos los Estados miembros, máxime si tenemos en cuenta que, cuando estamos tratando de instrumentos de comunicación sin fronteras, un problema grave de estos sistemas en un Estado miembro puede afectar a otros Estados miembros y a la UE en su conjunto.

Los Estados miembros tienen que aprobar y publicar, como tarde el 9 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la citada Directiva a partir del 10 de mayo de 2018.

La Directiva NIS parte de la necesidad de establecer en los Estados miembros las siguientes medidas para lograr su objetivo de seguridad:

a) la adopción de una estrategia nacional de seguridad de las redes y sistemas de información;
b) la creación de un Grupo de Cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros;
c) la creación de una Red de Equipos de Respuesta a Incidentes de Seguridad Informática (red de CSIRT, por sus siglas en inglés de "Computer Security Incident Response Teams") con el fin de contribuir una cooperación operativa rápida y eficaz;

d) la exigencia a los operadores de servicios esenciales (como energía y transporte) y proveedores de servicios digitales (como plataformas de comercio electrónico, redes sociales, motores de búsqueda, cloud, webmail u otros) de requisitos en materia de seguridad y notificación;
e) la designación de autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información.

Dos cuestiones queremos resaltar sobre esta nueva rama del Derecho que está siendo objeto de regulación por la Unión Europea.

Por una parte, la característica común con otras ramas del derecho, como son la protección de datos o las telecomunicaciones, de llevar a cabo la notificación a los órganos reguladores de brechas de seguridad. Véase que el Reglamento General de Protección de Datos de la Unión Europea (que también será aplicable a partir de mayo de 2018) exige tanto a los responsables como a los encargados del tratamiento la adopción de medidas en esta línea.

Por otra parte, el establecimiento de un régimen sancionador aplicable en caso de incumplimiento de las disposiciones nacionales aprobadas al amparo de la normativa europea (en este caso, de la Directiva NIS) con la imposición de sanciones "efectivas, proporcionadas y disuasorias". Parece por tanto que, también la ciberseguridad será cumplida a "golpe de sanción".

Tendremos que esperar en todo caso a ver los términos de transposición de esta Directiva que hace cada uno de los Estados miembros, y en concreto España, para poder valorar efectivamente el alcance de los sujetos obligados, las obligaciones impuestas y el régimen sancionador propuesto, así como en su caso, el órgano con potestad para sancionar.

La Directiva NIS es la primera pieza de la legislación comunitaria sobre seguridad cibernética pero, a buen seguro, no será la última.

De hecho, en mayo de 2017, la Comisión presentará un "informe europeo sobre el progreso digital en el mercado único" para revisar dónde nos encontramos y proponer ideas para el futuro.

Lo que es un hecho es que la Unión Europea ha incorporado en su catálogo de competencias el de la regulación de la ciberseguridad y el fortalecimiento de la capacidad cibernética de Europa, que ahora ha pasado a ser, "cosa de todos".

Lo que es un hecho es que la Unión Europea ha incorporado en su catálogo de competencias el de la regulación de la ciberseguridad y el fortalecimiento de la capacidad cibernética de Europa, que ahora ha pasado a ser, "cosa de todos".