ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

21/2017 3 de marzo 2017

*Vicente Moret Millás**

Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico español

Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico español

Resumen:

La Directiva NIS (*Network and Information Systems*), aprobada el 9 de julio de 2016, es el primer intento serio de la Unión Europea para hacer frente al reto de la ciberseguridad en el contexto actual en el cual es constante la preocupación por la seguridad en el ciberespacio, especialmente tras los cada vez más frecuentes incidentes de seguridad que se producen protagonizados en muchos casos por agentes gubernamentales al servicio de Estados. Este desafío no incluye solo incrementar la ciberseguridad de las personas, empresas y operadores de la red, sino también de las infraestructuras críticas, las redes de las Administraciones públicas, la infraestructuras y sistemas militares, o bien la actividad económica. A todos estos ámbitos se une ahora la utilización del ciberespacio como vector de desestabilización política e institucional. Su aprobación supone una serie de nuevas obligaciones muy relevantes tanto para los Estados miembros, como para ciertos actores que, en realidad, incluyen a la mayoría de los principales agentes económicos, en sectores tan relevantes como la energía, la banca o la sanidad. Además, los Estados deberán adaptar sus estructuras administrativas a estas nuevas obligaciones. En definitiva, el ciberespacio se ha convertido ya en el lugar en el cual se va a decidir en gran medida la prosperidad y seguridad de los países en el futuro próximo. Desde la aprobación de la Directiva NIS dotar de mayor seguridad a los sistemas es una

obligación ya impuesta por el Derecho comunitario en cumplimiento de la cual España no debería quedarse en un cumplimiento normativo estricto; debería ir más allá, creando un sólido sistema institucional que asegure un razonable nivel de ciberseguridad.

Abstract:

The NIS (Network and Information Systems) Directive, adopted on 9 July 2016, is the first serious attempt by the EU to address the cybersecurity challenge in the current context. Concerns for Cyberspace, are important after the increasingly frequent security incidents that are often carried out by government agents at the service of States. This challenge does not only increase the cybersecurity of people, companies and network operators, but also public critical infrastructures and military systems. To all these areas, the use of cyberspace as a vehicle for political and institutional destabilization is now a reality. Its adoption implies a series of new obligations which are very relevant both for the Member States and for certain actors which, in fact, include main economic agents in sectors so relevant as energy, banking or health. In addition, States should adapt their administrative structures to these new obligations. In short, cyberspace has already become the place where the countries prosperity and security in the near future will be decided. The approval of the NIS Directive to provide greater security to the information systems is an obligation already imposed by Community law under which Spain should not remain in strict regulatory compliance; should go further, creating a strong institutional system that ensures a reasonable level of cybersecurity.

Palabras clave:

Ciberseguridad, Directiva NIS, Unión Europea.

Keywords:

Cybersecurity, NIS Directive, European Union.

Introducción

Lograr un adecuado nivel de ciberseguridad en la red es uno de los retos más importantes a los que se enfrentan los Estados a la hora de proteger a sus ciudadanos. A las amenazas ya conocidas relativas a las infraestructuras críticas, las redes de las Administraciones públicas, las infraestructuras y sistemas militares, o bien la actividad económica, se une ahora la utilización del ciberespacio como vector de desestabilización política e institucional. En definitiva, el ciberespacio emerge así como un ámbito prioritario de acción de los Estados para proporcionar seguridad a sus ciudadanos. Esta, no debe olvidarse, es la primera de las obligaciones de todo Estado[1]. A este respecto debe señalarse que las amenazas en este entorno han sido hasta hace poco infravaloradas como un peligro real con una dimensión lo suficientemente grande como para poner en riesgo toda una infraestructura vital como son las redes de comunicación[2]. No obstante, la dificultad en este ámbito radica precisamente en que la acción de los Estados hasta la aparición del ciberespacio como escenario, ha estado delimitada claramente por la existencia de unas fronteras nacionales y por ello, de una limitación física a la aplicación de los poderes del Estado. Soberanía es siempre un atributo ligado al de territorio, población, y sistema político[3]. Y el problema radica en que en el ciberespacio no hay fronteras, sino un conjunto infinito de interconexiones basadas, eso sí, en una infraestructura física compuesta por servidores y redes de comunicaciones. En definitiva nos encontramos ante un nuevo contexto, que en su gravedad máxima supondría la utilización de la red para lanzar acciones militares contra las Fuerzas Armadas de otros Estados, añadiéndose así un quinto escenario para la guerra junto a los otros cuatro tradicionales; tierra, mar, aire y espacio[4].

Es por ello que en el ámbito europeo, se comprendió la necesidad de reforzar la cooperación entre Estados en esta materia, cumpliendo por otra parte con uno de los parámetros básicos fundacionales de la Unión que es precisamente servir de estructura que permita la cooperación entre Estados. Por ello se consideró imprescindible

[1] Kelsen, Hans. Teoría General del Estado. Editorial Nacional. 1979. México. P. 55.

[2] Necesidad de una conciencia nacional de ciberseguridad. Monografías de la Escuela de Altos Estudios de la Defensa. Núm. 137. Ministerio de Defensa. 2013. P. 11.

[3] Pérez-Serrano, Nicolás. Tratado de Derecho Político. Civitas. Madrid. 1984. P. 95.

[4] Ballesteros Martín, Miguel Ángel. En: Panorama geopolítico de los conflictos 2013. Instituto Español de Estudios Estratégicos. Ministerio de Defensa. 2013. P. 12.

establecer unos parámetros y estándares comunes de ciberseguridad mediante un incremento de la cooperación y colaboración entre los Estados miembros de la UE. Por las propias características del ciberespacio es evidente que solo una acción concertada será una acción eficaz en esta materia. Este es el único modo de lograr una actuación eficaz y eficiente, que otorgue a los países de la Unión una cierta garantía frente a los múltiples y graves retos a los que ahora se enfrenta y que incluyen de forma evidente riesgos geopolíticos, como los acontecimientos más recientes revelan. Es necesario un nivel de protección real y aceptable de las personas, las instituciones económicas y los órganos de naturaleza política y que son manifestación por excelencia de la soberanía de los Estados. Muchos de los incidentes de seguridad más graves que afectan a estas instituciones de gobernanza estatal a menudo tienen un carácter transfronterizo y, por tanto, afectan a más de un Estado miembro. En muchos casos estas ciberamenazas constituyen auténticos supuestos de enfrentamientos entre Estados para los cuales el Derecho ya está empezando a proponer soluciones para intentar establecer regulación de carácter internacional de los aspectos relacionados con la ciberseguridad[5].

La inexistencia de una estrategia de protección común o bien la existencia de una estrategia fragmentada hace vulnerables a todos los países miembros, con independencia de las medidas adoptadas a nivel nacional, siendo así que la ciberseguridad colectiva se asemeja a una cadena, en la cual cada Estado es un eslabón. Por ello, la fortaleza de esa cadena frente a ciberataques depende de la fortaleza que tenga el más débil de los eslabones que forman esa cadena.

Por estas razones y otras muchas que son bien conocidas, el pasado día 6 de julio de 2016, se aprobó la Directiva NIS (*Network and Information Systems*) 2016/1148, del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Como afirma esta Directiva «La magnitud, la frecuencia y los efectos de los incidentes de seguridad se están incrementando y representan una grave amenaza para el funcionamiento de las redes y sistemas de información. Esos sistemas pueden convertirse además en objetivo de acciones nocivas deliberadas destinadas a perjudicar o interrumpir su funcionamiento. Este tipo de incidentes puede interrumpir las actividades

[5] Schmitt, Michael. «Classification of Cyber Conflict». J Conflict Security Law (Summer 2012) 17 (2): 245-260. Oxford Journals. 2012.

económicas, generar considerables pérdidas financieras, menoscabar la confianza del usuario y causar grandes daños a la economía de la Unión»[6].

Con esta nueva norma comunitaria se pretende fijar niveles comunes de seguridad en todos los Estados miembros impulsando la cooperación entre ellos. La Directiva establece que los Estados miembros dispondrán de 21 meses para llevar a cabo la trasposición a la legislación nacional, y seis meses más para proceder a identificar a los operadores de servicios esenciales. Efectivamente, uno de los aspectos más destacados de esta Directiva, que deberá ser traspuesta a los distintos ordenamientos nacionales, es decir incorporada a ellos, contempla la obligación de los Estados de identificar a las empresas susceptibles de ser declaradas como *«operadores de servicios esenciales»* en sectores tan esenciales como el energético, el del transporte, servicios sanitarios o banca. En este sentido los Estados tienen la obligación de designar a las compañías clave en cada uno de los sectores anteriores, usando criterios específicos, tales como, el que un servicio sea o no esencial para que la sociedad y la economía se desenvuelvan con normalidad, o que un incidente que afecte a esa empresa pueda generar graves perturbaciones en la prestación de ese servicio[7]. En este sentido, los proveedores de algunos servicios digitales tales como el comercio en línea, los motores de búsqueda, o los servicios prestados desde la nube también estarán obligados a tomar medidas para garantizar la seguridad de su infraestructura. Además en estos casos también se deberá informar a la autoridad competente en caso de incidentes graves.

Aspectos más destacados de la Directiva NIS

Uno de los principales aspectos de esta Directiva es la creación de nuevos mecanismos de cooperación europea. Para abordar de una vez y con garantías de éxito esta necesidad imperiosa de colaboración, se establece en la Directiva el establecimiento de un «grupo de cooperación» para intercambiar información y prestar colaboración a los países miembros en el desarrollo de sus herramientas y sistemas de ciberseguridad. Por

[6] 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. https://www.boe.es/doue/2016/194/L00001-00030.pdf.

[7] «The cost of immaturity». The Economist. 5 nov. 2015. «The cyber-security industry is booming. A report by Bank of America Merrill Lynch reckons the market is $75 billion a year now and will be $170 billion by 2020. Not only is demand soaring, but barriers to entry are low. Anyone able to spout a bit of computer jargon can set up shop (it also helps if you can say you have a background in an intelligence service or the military)».

ello se obliga a cada Estado miembro a adoptar una estrategia nacional que fije una hoja de ruta y que asuma unos compromisos. La parte práctica operativa de estas estrategias viene dada por la obligación de los países de crear una red de equipos de respuesta ante incidentes de seguridad informática para gestionar amenazas, riesgos e incidentes, así como cooperar en materia de seguridad transfronteriza.

En esta labor de coordinación que es vital va a tener un protagonismo central la Agencia Europea de Seguridad en las Redes (ENISA), la cual desempeñará un papel esencial, particularmente en las materias relativas a la cooperación entre autoridades. No obstante, a este respecto debe tenerse en cuenta un límite insoslayable que enmarcará estos esfuerzos; la nueva regulación de la protección de datos establecida en el nuevo Reglamento 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Por otra parte se debe señalar que los esfuerzos de la Unión Europea en esta materia no son nuevos. El aumento que han experimentado en los últimos años las amenazas tecnológicas y sus potenciales peligros le llevaron hace unos años a diseñar la Estrategia Europea de Ciberseguridad, en 2013, que sentaba las bases de los objetivos de los 28 en materia de protección de las tecnologías de la información y las comunicaciones. Fue aquel mismo año cuando se comenzó a gestar la propuesta para la elaboración de una Directiva sobre ciberseguridad, la cual debía fijar unas reglas uniformes para todos los Estados miembros. Tres años después, esa iniciativa ha desembocado en la Directiva UE 2016/1148, también conocida como Directiva NIS.

A nivel operativo la Directiva establece como mecanismo de respuesta rápida ante incidentes graves una red de equipos de respuesta a incidentes de seguridad informática (CSIRT), compuesta por el resultante del total de los CSIRT nacionales de referencia, designados por los 28 países de la Unión Europea. En definitiva esta red es el instrumento real y operativo de que encarna los principios antes citados de cooperación rápida y eficaz. A este respecto, se debe insistir en la necesidad de cooperación, necesidad que ya se ha ido poniendo de manifiesto en otros foros como el Consejo de Europa[8].

[8] Resolution 2070 (2015) «Increasing co-operation against cyberterrorism and other large scale attacks on the Internet». Asamblea Parlamentaria del Consejo de Europa.

A este respecto, por lo que se refiere a nuestro país, España cuenta en la actualidad con varios de estos equipos que podrían cumplir los requisitos que marca la Directiva, como son el CERT de Seguridad e Industria, el del Centro Criptológico Nacional (CCN-CERT), y el del Mando Conjunto de Ciberdefensa (MCCD), entre otros.

Resumiendo, los principales ejes de la nueva normativa se centrarán en el cumplimiento de una serie de obligaciones por parte de los Estados nacionales. Los Estados miembros deberán identificar antes del 9 de noviembre de 2018 a las compañías que tendrán la consideración de operadores de servicios esenciales en los siete sectores señalados por la Directiva. Para llevar a cabo esta compleja tarea esta norma establece unos criterios como el grado de dependencia de dichos servicios para su funcionamiento de las redes y sistemas de la información, o los efectos que podría causar un incidente de ciberseguridad si este se llega a materializar. No obstante, el hecho de que se establezca en el inicio esa lista no significa que el esfuerzo acabe ahí, ya que los Estados miembros deberán revisar esa lista de operadores, al menos, una vez cada dos años.

Por otro lado, como ya se dijo antes, los Estados miembros tienen la obligación de contar con estrategias nacionales de ciberseguridad para poder establecer sus objetivos estratégicos en esta materia. En ese sentido, España cuenta ya con una Estrategia de Ciberseguridad Nacional desde el año 2013, con lo cual parte del camino ya se ha andado. No obstante, uno de los puntos clave que tendrá que resolver nuestro país, al igual que sus socios europeos, es el nombramiento de una o varias autoridades nacionales competentes, que serán las responsables de la implementación de la Directiva y además de liderar las acciones recogidas en dicha norma. A este respecto el asunto central será la designación de un «punto de contacto único nacional» que ejercerá de nexo de comunicación entre las autoridades de los Estados miembros, así como entre estas y el Grupo de Cooperación. Teniendo en cuenta la transversalidad de la materia, así como la existencia de varias Administraciones y órganos estatales con competencias cruzadas o concurrentes en muchos casos, fijar responsabilidades, así como fijar superioridades o subordinaciones no será fácil.

No obstante, lo más novedoso quizá de la directiva no haga referencia a la organización administrativa o pública de las actuaciones previstas. Teniendo en cuenta el papel protagonista de las empresas privadas prestadoras de servicios esenciales o y de los proveedores de servicios digitales, también de naturaleza jurídica privada, nada se conseguiría si las obligaciones que fija la Directiva solo se refiriesen a los actores

públicos, Estados y Administraciones Públicas. Por ello, la Directiva extiende sus obligaciones a actores privados. Los operadores de servicios esenciales y proveedores de servicios digitales tendrán que establecer una serie de medidas de seguridad para proteger sus redes y sistemas de la información.

El aspecto más novedoso y que más implicaciones jurídicas y económicas tiene, está relacionado con el deber de esas empresas de notificar los incidentes graves que afecten a sus redes y sistemas. Se establece la obligación de que estas empresas trasladen «sin dilación indebida» a la autoridad competente o al CSIRT nacional aquellos incidentes de seguridad que sufran y puedan afectar a la continuidad de sus actividades. No obstante, se establece una salvedad en el caso de los proveedores de servicios digitales ya que dicha obligación únicamente se entenderá exigible cuando las empresas tengan acceso a la información necesaria para valorar el impacto de un incidente. En definitiva esta cláusula supone dejar en manos de la empresa que ha sufrido el incidente la capacidad de valorar cuando se considera que se está en posesión de esa información, y en consecuencia, proceder a la comunicación.

Además, se establece que cuando los efectos de ese incidente grave puedan extenderse a los servicios esenciales de otro Estado de la Unión, las autoridades nacionales designadas habrán de informar a sus homólogas en los Estados miembros que pudiesen resultar afectados. Su relevancia, y por tanto la obligatoriedad o no de proceder a la notificación de ese incidente, viene fijada en la Directiva por la existencia de unos parámetros, tales como el número de usuarios afectados, la duración del incidente, la extensión geográfica, el grado de perturbación del funcionamiento del servicio o el alcance del impacto.

En el marco de esa voluntad de extender la ciberseguridad lo máximo posible en el ámbito de la Unión, la Directiva acude también no solo a la obligación *exnorma* sino que también prevé que aquellas empresas que no se encuentren obligadas por la propia Directiva, pero quieran notificar los incidentes que afecten a la continuidad de sus servicios, puedan hacerlo de forma voluntaria.

A este respecto, uno de los aspectos esenciales para la vigencia de la norma y su aplicación será sin duda, el régimen sancionador que se establezca por el incumplimiento de la Directiva. Se trata sin duda de la cuestión más compleja y delicada de cuantas operaciones jurídicas requiere la trasposición de esta Directiva, ya que como es notorio la fijación de un régimen sancionador supone una limitación del ámbito de libertad de

individuos y empresas y por ello debe ser construido respetando y siguiendo la doctrina constitucional que configura la potestad sancionadora de las Administraciones Públicas. Los Estados miembros deberán establecer un régimen de sanciones efectivas, proporcionadas y disuasorias para las empresas que no cumplan las disposiciones fijadas en la normativa, sin renunciar además a recoger también todas las garantías y limitaciones de esa potestad sancionadora, dadas las negativas consecuencias reputacionales que dichas notificaciones pueden suponer.

La incorporación de la Directiva NIS a los ordenamientos nacionales

Los Estados miembros de la Unión ya están comenzando los procedimientos para la trasposición a sus ordenamientos jurídicos de la Directiva, teniendo como plazo para ello hasta el 9 de mayo de 2018. Una labor que no será sencilla ni siquiera para países como España, que en los últimos años ha llevado a cabo avances notables en varios aspectos que también son abordados por la nueva regulación europea. En esta Directiva existen aspectos que previsiblemente darán lugar a un importante esfuerzo de análisis normativo para poder llevar a cabo una transposición adecuada.

La Unión Europea ya ha puesto de relieve la importancia de esa fase de trasposición y por ello ha elaborado diversos documentos al respecto siendo entre todos ellos el más destacable por su concisión y precisión el publicado por *Digital Europe* con el objeto de lograr una trasposición armoniosa en toda la Unión[9]. Como afirma este documento, «Ninguna de las leyes de ejecución nacionales debe obviar los dos objetivos principales de la Directiva: (1) garantizar un elevado nivel de ciberseguridad de las infraestructuras críticas del país; (2) el establecimiento de un mecanismo de cooperación eficaz entre los Estados miembros de la UE para favorecer el logro de esta meta. Los recursos deben dedicarse principalmente a la consecución de estos dos importantes objetivos».

Y señala los puntos centrales a la hora de asegurar que el proceso no se malogre: «En el caso de la industria tecnológica, las disposiciones relativas a los denominados proveedores de servicios digitales (DSP) revisten especial interés. La Directiva pone de manifiesto claramente que existen diferencias fundamentales entre los operadores de

[9] Digital Europe Transposición de la Directiva sobre seguridad de las redes y de la información (NIS) Bruselas, 5 julio 2016. http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2228&PortalId=0&TabId=353.

servicios esenciales (OES) y los DSP. De hecho, estos últimos no deben ser considerados una infraestructura crítica como tal. Tal y como reconoce la legislación, un incidente que afectase a estos servicios digitales representaría un nivel de riesgo considerablemente inferior para la seguridad económica y pública de un país. El mantenimiento de esta distinción es esencial para poder desplegar de forma eficaz los escasos recursos de las autoridades que tendrán que supervisar y velar por el cumplimiento de las normas. En consecuencia, recomendamos prestar especial atención al ámbito de aplicación previsto para los servicios en cuestión y solicitamos a los responsables políticos que no impongan los requisitos de seguridad a sectores distintos de los identificados como DSP y OES en la legislación nacional».

Por otra parte, se debe entrar ahora en los aspectos más destacables de la Directiva NIS que van a condicionar los distintos procesos de trasposición que se vayan llevando a cabo en los Estados miembros y que por ello, habrá que tener en cuenta.

Una de las principales preocupaciones a la hora de desarrollar la Directiva NIS está constituida por los desiguales niveles de preparación de los Estados miembros en materia de ciberseguridad, por lo cual hace falta un planteamiento global. Es precisamente esa idea subyacente de fortaleza común y de que la fuerza del sistema depende de la fortaleza del más débil de los componentes de sistema, la que está entre las preocupaciones centrales de la Directiva.

Por otra parte, se debe señalar que los intereses esenciales para la seguridad quedan protegidos por el artículo 346 TFUE. Ningún Estado está obligado a facilitar información cuya divulgación se considere contraria a los intereses esenciales para su seguridad. Se asume así una cláusula general del Derecho comunitario que está represente en la regulación de la mayoría de las materias que afectan a la seguridad de los Estados.

Además, en aquellos ámbitos en los cuales la UE ya haya establecido estándares más elevados de protección que sean más específicos normativamente, estos serán *lex specialis* y prevalecerán siempre que sean más elevados que los establecidos en la Directiva NIS. Así por ejemplo, en seguridad del transporte marítimo y fluvial, los estándares fijados de notificación de ciberincidentes son mayores que los fijados por la Directiva NIS. Igual ocurre con la regulación y supervisión del sector bancario e infraestructuras de los mercados financieros, profusamente regulado por la UE, y cuya

normativa es más estricta en materia de seguridad, integridad y resiliencia de redes y sistemas que la establecida la Directiva NIS[10].

La Directiva NIS entra a regular ámbitos hasta ahora no señalados de la economía nueva digital tales como los mercados en línea, el *e-commerce*, los buscadores, o la computación en nube. No obstante, de forma algo inexplicable, con la Directiva aprobada no se establece que las empresas fabricantes de software o hardware sean incluidas en el ámbito de aplicación de la norma, lo que se antoja sorprendente, ya que es obvio que deberían ser las primeras en el cumplimiento de los requisitos básicos de seguridad y privacidad en cuanto al diseño de sus productos y servicios. Estas empresas suministran las herramientas para que todos los operadores públicos o privados puedan operar en la red de forma tal que son elemento físico básico que permite la propia existencia de la red. Además, debe tenerse en cuenta que las funciones de búsqueda limitadas al contenido de un sitio web concreto no deben quedar incluidas como motores de búsqueda en línea aunque recurran a un proveedor externo. La definición de un servicio de computación en nube de conformidad con la Directiva depende de los recursos de computación que sean compartidos por múltiples usuarios. Dado que las nubes privadas (a diferencia de las nubes públicas) se dedican a una única organización no deben ser incluidas en el ámbito de estas obligaciones[11].

Además, se coloca sobre los hombros de los Estados la difícil tarea de elaborar la lista de entidades que cumplen con los criterios para ser calificados como operadores de servicios esenciales. Ello supone asentar como criterio definitorio para establecer la competencia de cada Estado, el hecho de que ese Estado sea la sede de una organización estable que represente a esa entidad o empresa. Se trata de una labor decisiva a la hora de poder someter a ese operador de servicios esenciales a la normativa de un Estado miembro u otro. Es importante señalar la obligación de los Estados de identificar a los operadores de servicios esenciales antes del 9 de noviembre de 2018. No obstante, la Comisión podrá adoptar directrices para que la elaboración de la lista se haga en toda la UE en términos comparables y con un planteamiento coherente.

[10] Borja Francisco Larrumbide. La Directiva de Seguridad de las Redes y de la Información (NIS). Parte 1 de 2. Situación Economía Digital. BBVA Research. Abril 2016.
[11] Digital Europe, *op. cit.*

Para no imponer una carga financiera y administrativa desproporcionada a los operadores de servicios esenciales y a los proveedores de servicios digitales, los requisitos han de ser proporcionados en relación con los riesgos que presenta la red y el sistema de información en cuestión, y tener en cuenta el estado de la técnica. En el caso de los proveedores de servicios digitales, esos requisitos no deben aplicarse ni a las microempresas ni a las pequeñas empresas. Tal y como se definen estas en la recomendación 2003/361, es decir; microempresa menos de 10 asalariados y un volumen de negocios anual de menos de 2 millones de euros, y tampoco a pequeñas empresas; menos de 250 asalariados y menos de 250 millones de volumen de negocios anual.

Esta diferenciación en cuanto a las obligaciones que afrontan las empresas del sector según su tamaño ha sido señalada como una posible debilidad del sistema dado que muchas de estas empresas TIC trabajan como proveedores para empresas más grandes que sí están incluidas en el ámbito de aplicación de la Directiva. Eso significa que podrían ser el eslabón débil a través del cual se podría ver comprometida la ciberseguridad del conjunto. Para ello sería imprescindible que de alguna manera esas empresas que contratan a proveedores de servicios obliguen a estos a cumplir unas obligaciones estandarizadas en materia de ciberseguridad.

Por otra parte, para calificar un incidente como relevante debe tenerse en cuenta el posible efecto perturbador significativo sobre un número considerable de usuarios que confían en dicho servicio. Esta prescripción general se acabaría materializando en cada uno de los sectores atendiendo a ciertos parámetros tales como el volumen o proporción en el total de la energía nacional que suponga un proveedor; el volumen de viajeros en el caso del transporte aéreo, o la importancia sistémica en el caso de entidades financieras. Ahora bien, los proveedores de servicios digitales deben ser supervisados a posteriori por la autoridad competente de forma tal que esa intervención se produzca cuando exista constancia de que se ha producido un incidente, o de que ese proveedor no cumple con la normativa al respecto. Es evidente que con esta limitación se da cumplimiento al principio general que preside el Derecho comunitario que impide una intervención ilimitada y previa de la autoridad pública de carácter previo. Al contrario, se establece como principio general una intervención posterior y limitada sin que pueda darse un control general previo en ningún caso. La Directiva pone de relieve que la actuación de las autoridades consiste en una supervisión a posteriori reactiva y, en

consecuencia, las autoridades competentes no tienen ninguna obligación general de supervisar y únicamente deben actuar si tienen pruebas de que se está infringiendo la normativa. La Directiva NIS establece claramente que las autoridades no poseen competencias de auditoría y no pueden emitir instrucciones vinculantes, con lo cual estas limitaciones también deberán respetarse a escala nacional en el momento en el cual se produzca la trasposición a las normativas nacionales.

No obstante, la notificación de incidentes está a la espera para su desarrollo de los actos de ejecución que pueda adoptar la Comisión Europea, la cual deberá publicarlos antes de 9 agosto de 2017. Tampoco existe ningún tipo de criterio asentado sobre el solapamiento en las obligaciones de notificación de las distintas regulaciones como NIS y el futuro Reglamento General de Protección de Datos —*GDPR*, acrónimo del inglés *General Data Protection Regulation*—. Del mismo modo, no se ha tenido en cuenta la posibilidad de que algunos operadores críticos estén sujetos a la notificación simultánea a distintos Reguladores nacionales e internacionales. En el caso de un banco español, por ejemplo, una fuga de datos personales es un incidente significativo se tendría que notificar simultáneamente al regulador nacional de protección de datos, al Regulador competente en infraestructura crítica, al Ministerio del Interior y al Banco Central Europeo. Todos estos retos ponen en evidencia la gran cantidad de Reguladores que pueden estar exigiendo las mismas responsabilidades, creando solapamientos regulatorios y, por lo tanto, añadiendo mayor complejidad y costes para las empresas y gobiernos. Un mecanismo único de notificación al estilo *«one-stop-shop»* permitiría mejorar la eficacia en las notificaciones, así como la reducción del coste y la complejidad del mismo[12].

En cuanto a los aspectos organizativos jurídico-públicos, los Estados miembros pueden designar a una o más autoridades nacionales responsables. Estas serán las responsables de la supervisión del cumplimiento de la Directiva. No obstante, sí es obligatoria la existencia de un solo punto de contacto nacional que coordine las cuestiones relacionadas con la seguridad de las redes y la cooperación transfronteriza. Este aspecto que ha sido uno de los aspectos más complicados a la hora de la aprobación de la Directiva, supone que los Estados deberán adaptar sus estructuras a

[12] Borja Francisco Larrumbide, *op. cit.*

esa obligación de punto de referencia nacional único, lo cual va a suponer en muchos casos la necesidad de introducir cambios normativos y organizativos.

En consonancia con todo lo anteriormente expuesto, la competencia judicial respecto de los proveedores de servicios digitales debe atribuirse al Estado miembro en el cual el operador tenga su establecimiento principal, que es a su vez el lugar en el cual el proveedor tiene su domicilio social dentro de la UE. Por establecimiento, se entiende el ejercicio real y efectivo de una actividad mediante una organización estable. Ahora bien, si el proveedor de servicios no dispone de esa organización estable en la UE deberá designar un representante, que debe serlo de forma expresa por el proveedor de servicios, autorizándolo a actuar por cuenta suya. Así, se recomienda desde la Unión Europea la trasposición en este aspecto: «En lo que respecta a la jurisdicción, los DSP deberán poder acogerse a la legislación vigente en el país de su establecimiento principal, incluso en aquellos casos en los que estén involucradas las autoridades competentes de varios países. En lo referente a la supervisión, las autoridades competentes deberán seguir un enfoque a posteriori en lugar de imponer una obligación general de vigilancia de los DSP. Es más, deberán centrarse en los resultados y mantener la distinción entre los OES y los DSP, no sometiendo a estos últimos a los requisitos no previstos por la Directiva, como auditorías e instrucciones vinculantes»[13].

En caso de que los Proveedores de Servicios Digitales dispongan de redes y sistemas de información en países distintos del de la ubicación de su establecimiento principal, la Directiva prevé la colaboración de las autoridades nacionales competentes. Sin embargo, la legislación aplicable sigue siendo la del Estado en el cual radica su establecimiento principal por lo cual son exclusivamente responsables ante la autoridad competente en dicha jurisdicción, quien actuará como su interlocutor.

No obstante, la Directiva no entra en ciertos aspectos en los cuales se podría haber avanzado, en concreto aspectos relativos a la cooperación en materia penal. Está materia está sometida a un intenso debate en relación con el acceso a información alojada en servidores o redes o equipos situados en el territorio de Estados por parte de autoridades de otros Estados[14].

La cuestión central es si las potestades investigadoras de estas autoridades nacionales son suficientes para poder llevar acabo intrusiones en esos sistemas de información

[13] Digital Europe, *op. cit.*

[14] García Mexía, Pablo. «La maraña digital europea». La Ley en la Red. Blogs ABC. 13/Mayo/2015.

incluso sin el consentimiento de los Estados en los cuales esa información que se pretende obtener está situada. La aplicación del principio de territorialidad que preside las relaciones internacionales debería ser la base que permita la persecución de las actividades delictivas cuando en estas se utilizan, de algún modo, instrumentos o medios que actúan en el ciberespacio. Un número creciente de delitos implican la necesidad de recabar pruebas electrónicas y por ello el acceso transfronterizo a los datos es relevante no solo para la investigación de los delitos cibernéticos, sino ya para la mayoría de los delitos, debido sobre todo a la ubicuidad de internet como medio de comunicar y a de almacenar información[15].

No es el contenido ni el ámbito apropiado para abordar en su totalidad esta compleja cuestión la Directiva NIS, pero no habría estado de más contener en su texto alguna referencia a esta materia.

Conclusiones

La aparición de nuevos actores y riesgos de naturaleza heterogénea en el ciberespacio ha motivado que muchos Estados de nuestro entorno geopolítico estén llevando a cabo una profunda revisión y transformación de sus políticas de seguridad y defensa. Los Estados llevan a cabo así su función más antigua, la de proporcionar seguridad a sus ciudadanos. Si bien esas agresiones no son cruentas de por sí, sus efectos sobre las vidas de las personas y sus derechos son absolutamente reales[16].

En este nuevo empeño el Derecho internacional ya está contribuyendo a «civilizar» estas amenazas de carácter internacional contra estabilidad internacional y estatal de muchos países[17].

Se pude afirmar que la directiva no es una especie de panacea que va a traer como por arte de magia una seguridad sin fisuras de nuestras redes y sistemas. No obstante, tampoco sería adecuado despreciar o minusvalorar su impacto. Es un importante paso que constituye el primer intento sistemático y coordinado de regular la ciberseguridad en la Unión Europea. Y ello por varios motivos.

[15] Moret Millás, Vicente. El desarrollo de mecanismos internacionales de cooperación para combatir el ciberterrorismo. Estado de la cuestión. Revista de Privacidad y Derecho Digital. Núm. 3. P. 132.
[16] Gómez de Ágreda, Ángel. El ciberespacio como escenario de conflicto. Identificación de las amenazas. Monografías del CESEDEN. NÚM. 126. Ministerio de Defensa. 2011. P. 180.
[17] Defending the digital frontier. The Economist. 14 jul 2014.

En primer lugar, porque supone atribuir a la ciberseguridad la caracterización de sector regulado de la actividad económica con lo que ello supone de intervención normativa de la UE al igual que en otros sectores como la energía o las telecomunicaciones. Es un primer paso hacia la creación de un marco regulador europeo de la ciberseguridad que además tiene fecha límite, ya que antes de 21 meses desde la aprobación de la Directiva (5 de julio de 2016) deben ser completadas las trasposiciones nacionales.

Por otra parte, al regular mediante una Directiva y no mediante un reglamento, se utiliza un instrumento que atribuye a los Estados la responsabilidad de regular y ejecutar lo regulado sobre la base de unas orientaciones generales fijadas en la Directiva. No debe olvidarse que la Directiva es una disposición normativa de Derecho comunitario que vincula a los Estados de la Unión, o en su caso al Estado destinatario, en la consecución de resultados u objetivos concretos en un plazo determinado, dejando sin embargo a las autoridades internas competentes la debida elección de la forma y los medios adecuados a tal fin. Por tanto la responsabilidad en la implementación de las políticas de ciberseguridad sigue recayendo en ámbito de los Estados miembros.

Esta iniciativa debe situarse en el más amplio escenario de la Estrategia para el Mercado Digital Único Europeo la cual sostiene que creando un mercado único digital conectado, se pueden generar hasta unos 250.000 millones de euros de crecimiento adicional en Europa en los próximos 5 años, creando cientos de miles de nuevos puestos de trabajo, especialmente para los solicitantes de empleo más jóvenes, y una pujante sociedad basada en el conocimiento[18].

Todo este espectacular crecimiento no será posible si no se consigue un adecuado nivel de ciberseguridad. Aunque sin duda la Directiva NIS es un gran paso para la mejora de la ciberseguridad, la Comisión Europea junto con ENISA deben todavía despejar muchos interrogantes, muchas cuestiones no resueltas para la aplicación de esta Directiva lo cual deberá producirse mediante normas y guías que especifiquen y estandaricen procedimientos de cooperación y articulen mecanismos operativos y funcionales.

Por otra parte, el concepto que mejor define esta política es la inmensa transversalidad de la Directiva, que por otra parte es consustancial a la propia ubicuidad que ha alcanzado la red y las tecnologías de la información. En cuanto al marco normativo nacional, se impone ahora la enorme tarea de adaptar la normativa ya vigente y dispersa

[18] http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuId=FTU_5.9.4.html

a esta nueva norma transversal en materia de ciberseguridad. Además, debe tenerse en cuenta que la Directiva NIS no es una directiva de seguridad en sí misma, sino una norma que establece los mecanismos para establecer medidas de seguridad, mediante la armonización, la coordinación y colaboración entre los diferentes actores estatales y agentes y entidades privados.

En cuanto a la posición de España, estamos en una posición de salida mejor que la de otros países por la adopción de diversa normativa y de la Estrategia Nacional de Ciberseguridad, con lo cual la trasposición de la NIS no debe ser complicada. Incluso desde un punto de vista tecnológico y operativo, España es uno de los pocos Estados de la UE que tiene el sistema de registro de datos de pasajeros aéreos (PNR) preparado.

El único punto en el cual habría que hacer un esfuerzo clarificador es en el de la designación de las autoridades nacionales competentes, dado que existe un conjunto de órganos estatales con competencias repartidas en la materia y pertenecientes a distintos Ministerios.

Otro de los aspectos más críticos y complejos a la hora de trasponer la Directiva será establecer un régimen sancionador que se aplique cuando se produzca un incumplimiento por parte de alguna de las empresas incluidas en el ámbito de aplicación marcado en la Directiva.

Cada Estado deberá establecer un régimen de sanciones aplicables en caso de incumplimiento de las disposiciones nacionales aprobadas, asimismo adoptará todas las medidas necesarias para garantizar su aplicación.

Esta regulación por tanto deberá respetar y cumplir los principios del derecho administrativo sancionador general.

Esto supone que este régimen sancionador deberá contar con, al menos, una regulación con rango de ley para fijar los principios esenciales de esta potestad en el ámbito de la ciberseguridad, así como la tipificación de las conductas descritas como infractoras por la videncia del principio de tipicidad. Este principio obliga a evitar incluir infracciones genéricas o vagas y exige que la acción u omisión esté concretada con precisión. Así mismo, deberá esa norma con rango de ley fijar las sanciones que se impondrán.

Además y posteriormente una norma de rango reglamentario deberá regular el concreto procedimiento sancionador, así como graduar las sanciones previamente fijadas por ley.

No obstante, deberá tenerse en cuenta que para poder sancionar esas conductas infractoras la Administración competente deberá tener la capacidad de investigar esos

casos de incumplimiento. Por lo tanto, deberá tener las herramientas y el conocimiento adecuado para poder realizar esas evaluaciones del nivel de ciberseguridad y exigir las medidas necesarias en los sistemas de información de las empresas. También se podrán exigir auditorías de ciberseguridad a realizar por terceros. A falta de tener más información, existen dudas acerca de cuáles van a ser las exigencias respecto a las medidas de seguridad mínimas, si se basarán en estándares o auditorías internacionalmente reconocidas como ISO 27001, NIST o SSAE16 o si, por lo contrario, asistiremos a la creación de nuevos estándares[19]. Tampoco se conoce si estos estándares y auditorías serán comunes en toda la Unión Europea o si cada país adoptará los suyos propios, creando una mayor fragmentación.

No obstante, nada de lo que establece la Directiva, que responde al loable objetivo de incrementar la ciberseguridad en la UE, será posible sin una tarea insoslayable que es la de la colaboración intensa entre sector público y privado, entre actores institucionales y empresas. Dada la naturaleza de este ámbito sin esa colaboración estrecha no habrá posibilidad de éxito.

En definitiva, el ciberespacio se ha convertido ya en el lugar en el cual se va a decidir en gran medida la prosperidad y seguridad de los países en el futuro próximo.

Será un ámbito en el cual aquellos actores que estén dotados de las herramientas más avanzadas y eficaces para proteger a sus ciudadanos y a sus intereses nacionales contarán con una gran ventaja respecto a aquellos que no tomen demasiado en serio las cuestiones relacionadas con la ciberseguridad, por lo cual conviene estar a la cabeza de este esfuerzo necesario por alcanzar unas más altas dosis de seguridad, certezas y legalidad en ese ámbito.

Es especialmente relevante que la acción del Estado se despliegue en este nuevo ámbito de actuación de los poderes públicos.

Y esta actividad, solo se podrá llevar a cabo desde la norma jurídica, que en un Estado de Derecho siempre debe preceder a la actividad de los poderes públicos, marcando así las líneas generales y también los límites a su actuación, porque lo necesario es una ciberseguridad que resulte respetuosa de los derechos y libertades[20].

[19] Borja Francisco Larrumbide, *op. cit.*

[20] García Mexía, Pablo. «Safe Harbor: Más olfato, más Europa, más humildad». La Ley en la Red. Blogs ABC. 23/oct/2015.

Esta nueva obligación es desde la aprobación de la Directiva NIS de una obligación ya impuesta por el Derecho comunitario en cumplimiento de la cual no solo deberíamos, como país, quedarnos en el cumplimiento de mínimos, si no ir un poco más allá, creando un sólido sistema institucional que asegure en lo posible un razonable nivel de ciberseguridad.

*Vicente Moret Millás**
Letrado Cortes Generales
Letrado comisión mixta seguridad nacional.