Lecciones aprendidas durante la tramitación de la Directiva NIS

Félix Arteaga | Investigador principal, Real Instituto Elcano | @rielcano

Tema

El seguimiento de la elaboración de la Directiva 2016/1148 sobre la seguridad de las redes y sistemas de información de la UE y de su trasposición al Anteproyecto español proporciona lecciones de cara a la regulación futura de cuestiones de ciberseguridad.

Resumen

La Comisión Europea aprobó en julio de 2016 una Directiva con medidas y mecanismos de cooperación destinados a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[1], a la que ha seguido una Comunicación con instrucciones sobre su aplicación para facilitar su trasposición de forma homogénea en el territorio de la Unión[2].

Ha sido un ejercicio de regulación largo y complejo, del que este ARI recoge las lecciones aprendidas por el Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano que ha venido siguiendo la trasposición de la Directiva y que delimitan el entorno regulatorio de la ciberseguridad europea y española, más allá del ámbito concreto de la seguridad de redes y sistemas de información.

Análisis

La Directiva (UE) 2016/1148 sobre la seguridad de las redes y sistemas de información (Directiva NIS en sus siglas inglesas o SRI en las españolas) se adoptó el 6 de julio de 2016 para mejorar y establecer un nivel mínimo común en la resiliencia, capacidad de respuesta y la cooperación de la ciberseguridad entre todos los países miembros de la UE, así como fomentar una cultura de gestión de riesgos y notificación de incidentes entre los agentes económicos clave, como los operadores de servicios esenciales y proveedores de servicios digitales. La Directiva NIS/SRI se propuso por la Comisión en febrero de 2013 como parte de la Estrategia de Ciberseguridad de la UE y se aprobó por el Consejo Europeo y el Parlamento Europeo el 6 de julio de 2016.

En España, la trasposición condujo a un Anteproyecto de Ley, elaborado bajo la coordinación de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD) del Ministerio de Energía, Turismo y Agenda Digital (MINETAD), y

[1] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016. Entró en vigor el 8 de agosto de 2016.

[2] Comisión Europea, COM(2017)476 y Anexo de 4 de octubre de 2017, "Aprovechar al maximo la SRI. Hacia la aplicación efectiva de la Directiva (UE)2016/1148".

(cont.)

publicado en noviembre de 2017[3]. Tras el posterior trámite de audiencia pública, el Anteproyecto se encuentra a la espera de su revisión antes de convertirlo en Ley.

Es importante señalar que las obligaciones establecidas por la Directiva a los proveedores de servicios digitales transfronterizos están sujetos a una supervisión más ligera (la autoridad intervendrá ex post cuando tenga constancia del incumplimiento de la Directiva o al producirse un incidente). Sin embargo, en la práctica es un reglamento de facto ya que su aplicación ha de ser común a todos los Estados miembros. Así la Comisión aprobó en el 30 de enero de 2018 el Reglamento de Ejecución sobre la especificación de elementos y parámetros relacionados con la seguridad de las redes y sistemas de información y de requisitos para la notificación de incidentes aplicables a los proveedores de servicios digitales.

El concepto plataforma en la UE

El objetivo de la Directiva NIS/SRI de mejorar la seguridad de las redes y de los sistemas de información, no era un fin en si mismo (ciberseguridad de los Estados) sino un medio para fomentar el mercado único digital en la UE (seguridad económica) por lo que la Comisión tuvo claro en su elaboración que deberían participar también aquellos operadores privados que utilizan las redes para hacerlo posible. Son actores que gestionan las infraestructuras críticas de agua, energía, banca y finanzas, transporte, entre otros o que proporcionan a los ciudadanos europeos determinadas categorías de servicios propios de una economía digital (portales de compra online de servicios y bienes incluyendo la distribución digital de aplicaciones o programas informáticos, los buscadores online y los servicios de computación en la nube).

La pluralidad de actores públicos y privados, llevó a la Comisión a fomentar un mecanismo de coordinación transversal (Plataforma NIS) para asegurar que la Directiva atendía también a los intereses económicos en juego y no sólo a los intereses de ciberseguridad de las administraciones públicas [4]. Como resultado, y junto a representantes de las instituciones comunitarias, la Plataforma NIS congregó a representantes públicos y privados de más de 130 organizaciones para identificar las mejores prácticas relacionadas con la gestión del riesgo, la coordinación de incidentes e intercambio de información y la investigación e innovación en los respectivos grupos de trabajo.

La Directiva NIS/SRI fija los resultados a obtener, pero son los Estados miembros los que deciden cómo conseguirlos, por lo que su efectividad no dependía tanto de su entrada en vigor, el 8 de mayo de 2018, como de la forma en la que esos Estados traspusieran su mandato y mecanismos. Para armonizar las trasposiciones y su

[3] MINETAD, Anteproyecto de Ley sobre la Seguridad de las Redes y Sistemas de Información, 29 de noviembre de 2017.

[4] La Fundación ESYS describe los orígenes de esta Plataforma en la Estrategia de Ciberseguridad de la UE, la Asociación Público-Privada Europea para la Resiliencia (EP3R) y el Grupo de Expertos del Art. 13 (de la Directiva 2009/140/CE de Telecomunicaciones). Previamente, la Dirección General de Redes de Comunicación, Contenidos y Tecnología convocó una encuesta de opinión a la que respondieron 180 representantes públicos, privados e independientes cuyos resultados se describen "La trasposición de la Directiva NIS al ordenamiento jurídico español: una perspectiva empresarial", septiembre 2017, pp. 37-39 y 65-71, respectivamente.

implementación posterior, la Directiva creó un Grupo de Cooperación compuesto por representantes de los Estados miembros, la Comisión y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), otra plataforma de coordinación, aunque de carácter público a la que la Directiva recomienda, cuando sea necesario, buscar la cooperación de los operadores de servicios esenciales y proveedores de servicios digitales.

Como resultado de lo anterior, la lección a aprender sería la de que las decisiones de regulación sobre la ciberseguridad en la UE cuentan con un ecosistema de actores públicos y privados. Cada uno de ellos, para defender sus intereses, debe buscar capacidad de influencia en todas las fases de la regulación, desde la elaboración a la implementación, con una actitud proactiva y participativa. La influencia sobre cualquier aspecto de regulación y gobernanza en la UE se juega en Bruselas, en el entorno comunitario de la Comisión, del Parlamento Europeo, Consejo de Europa y de ENISA, por lo que los actores públicos y privados deben articular mecanismos de influencia para interactuar con las instituciones comunitarias y con el resto de actores.

Uno de los problemas que reconoce la Directiva, es la necesidad de que los operadores y proveedores públicos y privados articulen mejor su cooperación con mecanismos que simplifiquen y agilicen la interlocución. La necesidad de coordinación, en su variante interadministrativa, afecta particularmente a los Estados descentralizados ya que aumenta el número de autoridades competentes potenciales y dificulta la designación de un punto de contacto único. En el ámbito privado, existen asociaciones como la Organización para la Ciberseguridad Europea (ECSO en sus siglas inglesas) que aglutinan los intereses de grandes compañías, PYME, start-ups, centros tecnológicos, universidades, operadores y representantes de las administraciones regionales y locales implicadas en el desarrollo del Mercado Único Digital, la industria de ciberseguridad europea, su I+D+i y la seguridad de las redes y sistemas de información. Se pueden encontrar asociaciones similares para el sector específicos, como los operadores de telecomunicaciones (Groupe Special Mobile Association, GSMA y European Telecommunications Network Operators' Association ETNO), o la industrial digital (Digital Europe), entre otros que se ocupan de intereses globales o sectoriales.

La actuación regulatoria de los distintos actores reside en su capacidad de influir proactivamente en el ecosistema regulatorio de Bruselas, manteniendo de forma sostenida su contribución en él, diversificando sus operaciones e interacciones de influencia, recabando y analizando la inteligencia disponible y aportando sus propuestas para liderar la transformación del ecosistema digital en Europa. En el ecosistema regulatorio, y además de los actores institucionales, gubernamentales y las asociaciones mencionadas, participan activamente empresas individuales afectas por las distintas iniciativas regulatorias que dispongan de la adecuada presencia y recursos de influencia.

El concepto plataforma en España

La trasposición de la Directiva NIS/SRI depende de las peculiaridades legislativas de cada país, su organización administrativa y la cultura de cooperación que tengan. En el caso español, la elaboración del Anteproyecto ha sido un largo ejercicio intergubernamental complicado por la diversidad de actores gubernamentales

implicados. Cada uno de los participantes en el Grupo Interministerial creado para la trasposición tenía sus propios intereses respecto a la seguridad de las redes y sistemas de información, especialmente aquellos que aspiraban a ser nominados como autoridades competentes. El Grupo Interministerial mantuvo contactos informales con algunos actores privados, aunque no participaron formalmente en la elaboración del Anteproyecto.

La colaboración informal en materia de ciberseguridad se beneficia de la positiva experiencia previa de cooperación público-privada en relación a las infraestructuras críticas que cubrió todo el proceso legislativo incluida la Ley y el Reglamento de Protección de Infraestructuras Críticas. Una colaboración que se ha formalizado en la Mesa de Coordinación creada en el CNPIC para canalizar el apoyo y seguimiento de las medidas adoptadas, donde participa un representante de cada uno de los sectores estratégicos identificados en la Ley 8/2011 para la protección de las infraestructuras críticas[5].

La expectativa de trasposición de la Directiva generó mucha inquietud entre los operadores de servicios esenciales y los proveedores de servicios digitales, preocupaciones ya que el sector privado valoró que el Anteproyecto sobrepasaba lo establecido en la Directiva sobre la notificación de incidentes, al incluir criterios de difícil objetivación como la importancia de los sistemas afectados y el daño reputacional que pueden generar inseguridad jurídica. Igualmente, el sector privado ha mostrado su preocupación ante la multiplicidad de autoridades competentes, el solapamiento de regulaciones y la necesidad de una armonización del régimen de notificaciones debido a la casuística y variedad de regulaciones y autoridades que pueden concurrir en el curso de la gestión de un incidente dado. La inquietud y el interés condujeron a reflexiones públicas, que contaron con la comprensión y colaboración de la SESIAD y del resto de actores gubernamentales. También a reflexiones privadas, entre las que destaca la presentación, en septiembre de 2017, de la encuesta realizada por la Fundación Empresa Seguridad y Sociedad (ESYS) entre los profesionales privados responsables de aplicar las medidas resultantes de la trasposición de la Directiva NIS/SRI y que expuso las percepciones, positivas y negativas, sobre la trasposición antes de que se hiciera público el texto del Anteproyecto[6].

La interacción directa tuvo que esperar a que la publicación del Anteproyecto por la SESIAD abriera el trámite de audiencia pública al que se incorporaron las propuestas y recomendaciones individuales de los operadores de servicios esenciales y proveedores de servicios digitales y las colectivas de algunas fundaciones[7]. El Real Instituto Elcano, dentro su programa sobre Ciberpolítica también participó en la valoración del Anteproyecto y presentó sus propias recomendaciones. Entre ellas se extraen las

[5] Ley 8/2011 sobre medidas para la protección de las infraestructuras críticas de 28 de abril.

[6] Los resultados figuran en la mencionada publicación de la Fundación ESYS, pp. 105-151.

[7] Entre otras, la Fundación Barredá, Seguridad de las redes y sistemas de información: comentarios al borrador del Anteproyecto de Ley NIS, *Seguritecnia*, enero 2018.

conclusiones que tienen una proyección reguladora o de gobernanza más allá del ámbito concreto de la Directiva NIS/SRI.

En primer lugar, y comprendiendo el lógico interés y competencia de la Administración en regular la ciberseguridad, la reserva de regulación no debe ir más allá de los límites propios de la seguridad nacional. Los contenidos de la Directiva NIS/SRI no pertenecen a ese ámbito, porque sus riesgos no afectan a la misma sino a la seguridad pública como reconoce la Memoria de Impacto Normativo del Anteproyecto. Si no se tiene en cuenta que sólo una parte de la regulación en materia de ciberseguridad afecta al núcleo esencial de la seguridad nacional, se corre el riesgo de que la lógica interministerial prime la seguridad y la simplicidad frente a los intereses económicos y la diversidad. La relación público-privada en la regulación es normalmente asimétrica porque los actores públicos dominan la colaboración. Pero un exceso de asimetría que prime la segurización frente a los intereses económicos de operadores y proveedores o la propia dinámica competitiva de los agentes europeos en un mercado globalizado puede poner en peligro el desarrollo del mercado digital único y de la sociedad de la información de Europa. La ciberseguridad es un medio para ese fin y no un fin en sí mismo, por lo que en el futuro debería ir adoptando un enfoque de supervisión menos excluyente del protagonismo privado.

En segundo lugar, y como resultado del enfoque anterior, la participación del sector privado en los trabajos del Grupo Interministerial ha sido informal, a posteriori y alejado de la voluntad de la Directiva de que la cooperación público-privada fuera “esencial” (art. 35.). Incluso admitiendo por razones de urgencia, que el sistema intergubernamental seguido sea más rápido que cualquier otro más inclusivo, el sector privado debe ir ganando protagonismo en regulaciones futuras que afectan a sus intereses económicos por razones prácticas y de competencia, así como, por razones prácticas, porque disponen de más recursos humanos y materiales que el sistema gubernamental de ciberseguridad para elaborar, debatir y evaluar los resultados de la regulación. Como la propia Directiva apuntaba, una mayor seguridad y nuevas funciones obligan al sector público a habilitar mayores medios, pero las limitaciones presupuestarias y de plantilla -que no las de competencia profesional- limitan los recursos del sector público disponibles para esa función regulatoria. Esta necesidad se va a hacer patente, por ejemplo, en la trasposición de la Directiva NIS/SRI, donde el Proyecto y -probablemente la Ley- remiten numerosas cuestiones importantes a su desarrollo reglamentario posterior, por lo que es imprescindible una mayor cooperación entre los sectores público y privado desde el inicio de la regulación reglamentaria, en lugar de ser informados al final, tanto por razones prácticas como de competencia.

En tercer lugar, la Administración tiende a simplificar su función sancionadora recurriendo únicamente a instrumentos coactivos sin incentivar ni recompensar las iniciativas del sector privado para cumplir los objetivos de la trasposición, ni el proceso de acomodación normativa de los operadores. El talante proactivo y colaborador ha dado buenos resultados y se ha visto reflejado en el curso de los últimos años en la elaboración e implantación de la regulación de las infraestructuras críticas, así como en las importantes inversiones, planes de prevención y contingencia para la prevención de potenciales ciberataques o incidentes basados en un modelo de gestión de riesgos e impactos llevados a cabo por el sector privado. El enfoque del régimen sancionador es importante porque si difiere significativamente del de otros países europeos puede crear

agravios, diferencias competitivas y situaciones de arbitraje entre agentes en el mercado europeo. Por eso no debe limitarse a la penalización de las trasgresiones sino a incentivar la reputación de la marca española de ciberseguridad, para lo que es necesario incentivar la contribución de operadores y proveedores y evitar daños reputacionales irreparables. En el mismo sentido, la relación público-privada tras la notificación de incidentes deber velar por la reputación del notificante, estableciendo mecanismos que le tengan al tanto de la evolución de un incidente que afecte a sus intereses económicos e imagen.

En cuarto lugar, y en la expectativa de una colaboración público-privada más formal, sistematizada y fluida en el futuro, se debería reforzar la interlocución privada en dos ámbitos. Por un lado, se debería potenciar el reconocimiento de los jefes de seguridad de la información (CISOs) de los operadores de servicios esenciales y los proveedores de servicios digitales como interlocutores privilegiados de las autoridades competentes, algo que ha ocurrido ya con figuras similares como los delegados de protección de datos o los responsables y delegados de seguridad de infraestructuras críticas. Por otro, se precisa una mejor articulación de la interlocución entre actores privados en asociaciones nacionales, genéricas o sectoriales. En concreto, la colaboración público-privada demanda una articulación estructurada a cuatro niveles: privado, público, europeo y técnico. En este sentido, el sector privado de la ciberseguridad debería de fomentar la formación de un tejido asociativo capaz de responder a la altura de la interlocución público-privada que se desea en el plano nacional, primero, y en el europeo después[8].

Conclusiones

La regulación de las cuestiones vinculadas a la ciberseguridad en Europa precisa de una mayor participación de todos los actores, públicos y privados, lo que está dando lugar a ecosistemas/plataformas de colaboración público–privada trasversales de coordinación. Florecen entre las administraciones públicas de los niveles nacional y europeo y engloban, en distinta proporción, a actores públicos, industrias de variados tamaños, operadores, centros tecnológicos, universidades, think-tanks, entre otros.

Están tomando conciencia de su capacidad y responsabilidad colegisladora y se organizan para influir en los procesos regulatorios con su presencia y participación en los foros de decisiones legislativas y en todas sus fases previas, de elaboración, implantación y revisión. Tienen a su favor su mayor capacidad para adaptarse a la evolución tecnológica y cuentan con mayores recursos para contrastar mejores prácticas internacionales y aportar propuestas regulatorias a las administraciones.

La ciberseguridad española ya tiene constancia de los dividendos positivos que la colaboración público-privada en materia de regulación de infraestructuras críticas ha dado en España y en el ámbito europeo, donde la legislación española se ha constituido en la referencia de otros procesos legislativas nacionales y de la propia Comisión. Para

[8] De momento, la cultura de asociación, clústeres y ecosistemas se ha desarrollado más en el ámbito de algunas Comunidades Autónomas que en el nacional, y más para ámbitos tecnológicos y de innovación generales que para el ámbito concreto de la ciberseguridad. Ver Félix Arteaga, "La Cuarta Revolución Industrial: un enfoque de seguridad nacional", DT 12/2018, mayo de 2018.

reforzar este potencial de influencia regulatoria en la UE, la cooperación público-privada debe articularse mejor a nivel nacional. El sector público, debe abrirse a mecanismos de participación ordinarios más inclusivos y menos asimétricos, aprovechando los recursos privados para compensar sus carencias reguladoras, centrándose en la supervisión. El sector privado debe mejorar la cooperación interna (privada-privada) simplificando y fortaleciendo la interlocución si desea que la Administración le conceda mayor protagonismo, especialmente si tiene vocación de constituir algún día una marca española de ciberseguridad que beneficie a industrias y proveedores nacionales. La interlocución público-privada no puede limitarse al territorio nacional, sino que debe replicarse en Bruselas, reforzando la interlocución directa entre los representantes permanentes de las administraciones e industrias en la capital belga y las autoridades comunitarias responsables.

Por consiguiente, el modelo de gobernanza y la remodelación de la cooperación público-privada en España deben adaptarse con agilidad al nuevo modelo de gobernanza europeo que se está articulando para gestionar la ciberseguridad, incluido el reforzamiento de la Agencia ENISA, y al modelo de gobernanza que se debe crear en España aprovechando la revisión de la Estrategia de Ciberseguridad Nacional, incluida la creación de una Agencia que pueda catalizar la cooperación público-privada.