ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

122/2014 28 octubre de 2014

Vicente Moret Millás
Ainhoa Uribe Otalora *

LA UNIÓN EUROPEA ANTE EL RETO DE LA CIBERSEGURIDAD: LA FUTURA DIRECTIVA NIS

LA UNIÓN EUROPEA ANTE EL RETO DE LA CIBERSEGURIDAD: LA FUTURA DIRECTIVA NIS

Resumen:

La Propuesta de Directiva NIS es el primer intento serio de la UE 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. Pretende ser una respuesta coordinada y europea frente a esta nueva amenaza cuyos potenciales riesgos son innumerables. Su aprobación supondrá 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, afectando a sectores tan relevantes como la energía, la banca o la sanidad. Además, los Estados deberán adaptar sus estructuras administrativas a estas nuevas obligaciones. El Ciberespacio es un nuevo 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, tan a priori contrario a estos parámetros como es la Red.
En relación con nuestro país, España, la aprobación de la nueva Estrategia de Seguridad Nacional, y la Estrategia de Ciberseguridad Nacional en el año 2013 han supuesto un avance en este ámbito. Ahora bien, la aprobación de esta nueva Directiva NIS, supondrá la necesidad de adaptar el marco normativo y orgánico español en esta materia, siendo una magnífica ocasión para corregir algunas disposiciones que no se adaptar a este nuevo contexto normativo europeo. Así por ejemplo, será necesario designar una autoridad única de referencia y un CERT único de referencia, decisión que se ha pretendido orillar mediante la articulación de un sistema de rotación al frente de esta responsabilidad por parte de los distintos actores estatales con competencias en esta materia. Esta configuración del liderazgo de la ciberseguridad en España, deberá cambiar a la luz de lo que dispone el texto de la propuesta de Directiva en estos momentos.

Vicente Moret Millás
Ainhoa Uribe Otalora

Abstract:

The proposed NIS Directive is the first European Union serious attempt to address the challenge of cybersecurity in the current context in which there is a constant concern for security in cyberspace, especially after increasingly frequent security incidents, in many cases caused by government agents. The new Directive is intended to become a coordinated European response to this new threat whose potential risks are innumerable. Its adoption will suppose a very significant number of new obligations, both for Member States and for certain actors, included most of the biggest operators, affecting such important sectors as energy, banking and healthcare.
In addition, States should adapt their administrative structures to these new obligations. Cyberspace is a new field in which those actors who are equipped with the most advanced and effective tools to protect their citizens and their national interests will have a great advantage over those who do not take too seriously the issues related to cybersecurity. That´s the reason why it´s necessary to be at the forefront of this effort, aimed to attain a higher degree of security, certainty and legality.
In relation with our country, Spain, the adoption of the new National Security Strategy and the National Cyber Security Strategy in 2013, is a milestone in this approach. However, in the adoption of this new directive NIS, it will be necessary to adapt the Spanish regulatory and organizational framework, in order to correct some provisions that are not adapted to the new European regulatory context.

Palabras clave:

Directiva NIS; Directiva relativa a la Seguridad de las Redes y de la Información; Ciberseguridad; Ciberdefensa; Estrategia de Ciberseguridad Nacional; Estrategia Nacional de Seguridad; Red de Cooperación.

Keywords:

NIS Directive; Directive on Network Information Security ; Cybersecurity; Cyberdefense; National Cybersecurity Strategy; National Security Strategy; Cooperation Network.

Vicente Moret Millás
Ainhoa Uribe Otalora

AUMENTAR LOS NIVELES DE CIBERSEGURIDAD: UNA TAREA URGENTE E IMPRESCINDIBLE

La auténtica revolución que el uso masivo de las nuevas tecnologías está suponiendo en todas las esferas de las actividades humanas, ya sean económicas, políticas o sociales, hace que el contexto mundial haya cambiado en la última década. Se trata de un nuevo entorno que además es global. Ahora bien, al lado de las inmensas oportunidades que para el progreso humano suponen estas nuevas tecnologías, aparecen nuevos peligros y amenazas que proceden del también ciberespacio. Es una experiencia continua, que una misma tecnología admite usos diversos, unos beneficiosos para las personas, y otros no tanto, en función de cual sea la intencionalidad que mueve a los individuos u organizaciones que usan esa tecnología. Estas amenazas adoptan diversas formas y pueden tener distintas procedencias. También su gravedad es diversa atendiendo a las posibles consecuencias que pueden ir, desde la comisión de un simple delito en la red, hasta el uso del ciberespacio como nuevo escenario para el enfrentamiento militar entre Estados.

Hasta hace poco la red por su propia naturaleza no había prestado atención a los aspectos relativos a su seguridad. Esto ya ha cambiado y constituye una preocupación creciente el constatar que hay un nuevo espacio, de enorme importancia para la vida de los ciudadanos de todos los países, que no está sometido, como sí lo están el resto de los ámbitos de actividad humana de una u otra forma, a la esfera de competencias del Estado, y por tanto de su herramienta de acción que es la Ley. No se debe olvidar que cuando la fuerza de la ley está ausente de un determinado ámbito, es la ley de la fuerza o el crimen simplemente, el que acaba por ocupar el puesto que corresponde a la norma. Y esta circunstancia no se puede permitir en los Estados Democráticos de Derecho, ni en el ámbito de la Unión Europea. Por ello, todos los Estados occidentales están estableciendo mecanismos legales y estructuras administrativas de seguridad que permitan aumentar las garantías en este ámbito frente a los posibles ataques que desde las organizaciones criminales, terroristas, o desde otros Estados, pudiesen afectar a los derechos y libertades de los ciudadanos, a su seguridad, o a los sistemas y redes de las infraestructuras críticas y de la Defensa Nacional. Aunque debe señalarse que por la propia naturaleza del contexto que se pretende regular y controlar, no es esta una tarea fácil. La dificultad radica en el objeto que se pretende regular, ya que nada hay más ubicuo, mutable y globalizado que las nuevas tecnologías de la información, que además se alojan en un medio que muchas veces no es una realidad física sino virtual. No obstante, esas dificultades no deben disuadir a Gobiernos y Parlamentos de intentar, con todas las cautelas y salvedades, asegurar mediante normas un cierto nivel mínimo de certezas jurídicas y legales.

Vicente Moret Millás
Ainhoa Uribe Otalora

LA NUEVA DIRECTIVA NIS

Haciéndose eco de esta imperiosa necesidad, el pasado 13 de marzo de 2014, el Parlamento Europeo aprobó la propuesta de Directiva relativa a la Seguridad de las Redes y de la Información[1], estando pendiente su aprobación final por el Consejo que se prevé se produzca a finales de 2014 o principios de 2015. Se trata de una norma europea de especial trascendencia, tanto por la relevancia de la materia que pretende regular, como por la imperiosa necesidad de coordinar las actuaciones de los Estados miembros de la Unión en aras a dar una respuesta netamente europea a los desafíos cruciales planteados por la seguridad en el Ciberespacio. Es una cuestión que va a condicionar múltiples aspectos de la vida de los ciudadanos europeos, por las múltiples implicaciones que la ciberseguridad supone desde el punto de vista económico, social, o en el plano de la defensa de los derechos fundamentales. No son menos importantes a este respecto las implicaciones geopolíticas relativas con las relaciones entre Estados, e incluso relativas a un nuevo tipo de enfrentamiento que ya se denomina ciberguerra.

La propuesta de Directiva, cuya aprobación va a tener una gran repercusión interna en la forma en la cual los Estados miembros regulan y ejecutan políticas públicas relativas a la ciberseguridad, persigue un fin esencial: obligar a los Estados miembros a estar más preparados en cuanto a la garantía de la seguridad de sus redes y de la información contenida en estas. No obstante, no es esta la primera vez que la Unión Europea se ha aproximado a esta decisiva materia. Ya la *Directiva marco para la lucha contra los ciberataques y la armonización del derecho penal de los estados miembros y cooperación en la persecución penal*, que entró en vigor en octubre de 2003, se ocupó de la materia, recogiendo gran parte de los aspectos que a su vez fueron incluidos en el *Convenio de Budapest* aprobado por el Consejo de Europa el mismo año. Así mismo, la actuación de la Unión Europea no se ciñe sólo al ámbito de la regulación, ya que en 2004 se crea la *Agencia Europea para la Seguridad de las Redes y de la Información* (ENISA). No obstante, en la actualidad las estrategias y políticas de la Unión Europea al respecto, vienen establecidas en la *Estrategia de Ciberseguridad de la Unión Europea* aprobada en el año 2013 y de la cual la propuesta de Directiva NIS es directa consecuencia.

[1] Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:ES:PDF

Vicente Moret Millás
Ainhoa Uribe Otalora

La propuesta de Directiva NIS resalta la importancia de esta materia, y las negativas consecuencias que tiene para las sociedades actuales un inadecuado nivel de ciberseguridad.

La propuesta de Directiva insiste en la necesidad de entrar a regular este ámbito, dada la actual descoordinación y desprotección que afecta a muchas de estas redes y sistemas en algunos países de la UE. En definitiva, y así se señala, en último extremo el valor esencial que está en juego y que es preponderante sobre todos los demás es la promoción y la protección de los derechos fundamentales de los ciudadanos europeos.

El primer rasgo destacable de esta propuesta de norma es su enorme ámbito de aplicación y por tanto la sujeción a la misma de una multitud de actores públicos y privados en los términos en los cuales se redactada a día de hoy. Se considera necesario exigir a ciertos agentes que son: Operadores de infraestructuras críticas, Proveedores clave de servicios de la sociedad de la información, y las Administraciones Públicas, la adopción de las medidas oportunas para gestionar los riesgos de seguridad, y notificar asimismo, los incidentes graves a las autoridades nacionales competentes. La justificación de la extensión de estas obligaciones se encuentra en que la falta de seguridad en las redes de información puede llegar a comprometer servicios vitales de nuestras sociedades, generando cuantiosas pérdidas financieras, así como incidiendo negativamente en el bienestar de la sociedad.

La propuesta de Directiva NIS señala que los riesgos proceden de los incidentes relacionados con la seguridad, tales como errores humanos, fenómenos naturales, fallos técnicos o ataques malintencionados. Además al tratarse de instrumentos de comunicación sin fronteras, los sistemas de información digitales —y en particular Internet— están interconectados entre los Estados miembros, y contribuyen decisivamente a facilitar la circulación transfronteriza de bienes, servicios y personas. Por ello, un problema grave de estos sistemas en un Estado miembro puede afectar a otros Estados miembros y a la UE en su conjunto. Por todo ello, la resiliencia y la estabilidad de las redes y los sistemas de información revisten suma importancia para la realización del mercado único digital y el buen funcionamiento del mercado interior, así como, y de modo más trascendente, para la salvaguarda de los derechos fundamentales y las libertades públicas de los ciudadanos de la Unión Europea.

Por otra parte, la propia propuesta de Directiva señala que la situación actual en la UE en esta materia es reflejo del planteamiento meramente voluntario seguido hasta el momento, y no ofrece protección suficiente frente a incidentes y riesgos relacionados con la SRI de forma homogénea en toda la Unión. Se afirma que las capacidades y mecanismos de SRI actuales son sencillamente insuficientes para seguir el ritmo de unas amenazas en rápida

mutación y garantizar un nivel elevado de protección igual en todos los Estados miembros. El problema radica en que los niveles de capacidad y preparación de los Estados miembros son muy distintos y dan lugar a enfoques fragmentados en el seno de la UE. Al estar las redes y sistemas interconectados, la SRI global de la UE se ve perjudicada por esos Estados miembros cuyo nivel de protección es insuficiente. Ello además repercute negativamente en la creación de lazos de confianza entre los propios Estados, requisito previo para la cooperación y el intercambio de información. Por todo lo anterior, la Directiva fija una serie de objetivos, siendo el primero de ellos, establecer la obligación de que todos los Estados actúen para que exista un nivel mínimo de capacidades nacionales, mediante la designación de autoridades competentes en materia de Ciberseguridad, la creación de equipos de respuesta a emergencias informáticas (CERT), y la adopción de estrategias y planes de cooperación nacionales en el ámbito de la Seguridad de las Redes y la Información.

Además, se establece la obligación de crear una nueva red de cooperación que garantice una coordinación segura y eficaz y, en particular, un intercambio coordinado de información y unas labores de detección y respuesta a escala de la UE. A través de esta red, los Estados miembros deberán intercambiar información y cooperar para hacer frente a las amenazas e incidentes. Se incide asimismo, en la necesidad de proceder a la progresiva implantación de una cultura de gestión de riesgos, así como a garantizar el intercambio de información entre los sectores público y privado. Las empresas de los sectores críticos concretos antes citados y las Administraciones Públicas deberán evaluar los riesgos a los que se enfrentan, y adoptar medidas adecuadas y proporcionadas para garantizar la Ciberseguridad. Uno de los aspectos más destacados de toda la Directiva por las evidentes repercusiones que tiene, es el relativo a la obligación de esas empresas, de notificar a las autoridades competentes todos los incidentes que supongan un peligro grave para el funcionamiento de sus redes y sistemas de información y comprometan de forma significativa la continuidad de los servicios críticos o el suministro de mercancías.

Por otra parte, la Directiva tiene como objetivo cubrir sectores de actividad en el ámbito de las tecnologías de la información, que hasta este momento habían escapado a la regulación por parte de la normativa europea. Afirma la propia propuesta de Directiva, que a los agentes que gestionan infraestructuras críticas o prestan servicios esenciales para el funcionamiento de nuestras sociedades no se les han impuesto las oportunas obligaciones de adoptar medidas de gestión de riesgos ni de intercambiar información con las autoridades competentes. El actual marco regulador europeo solamente obliga a las empresas de telecomunicaciones a adoptar medidas de gestión de riesgos y a notificar los incidentes graves. No obstante, hay muchos otros sectores cuyo desarrollo depende de las TIC y que, por tanto, deberían también prestar la debida atención a la Seguridad de las Redes

de Información. Entre estos sectores críticos para el buen funcionamiento de la actividad económica y en general de nuestras sociedades, la Directiva NIS señala: Las entidades financieras y crediticias; Los mercados de valores; La generación, transporte y distribución de energía; Los transportes aéreo, ferroviario y marítimo; El sector de la sanidad; Los servicios de Internet; y las Administraciones Públicas.

Por tanto, una de las consecuencias más relevantes de la aprobación de esta propuesta de Directiva será, en los términos en los cuales está hoy redactada, la imposición de una serie de obligaciones nuevas a algunas de las empresas más importantes de la Unión Europea. De la lectura conjunta de la propuesta de Directiva, se extrae que los sujetos obligados a cumplir esta nueva normativa son, entre otros, los siguientes: Pasarelas de pago por Internet; Redes sociales; Motores de búsqueda; Servicios de computación en nube; Tiendas de aplicaciones. En el ámbito de la energía, serían: Proveedores de gas y electricidad, Gestores de redes de distribución de gas o electricidad y minoristas para consumidores finales, Gestores de redes de transporte de gas natural y gestores de almacenamiento, Gestores de redes de transporte de electricidad, Oleoductos de transporte de crudo y almacenamiento de crudo, Operadores de los mercados del gas y la electricidad, Operadores de producción de crudo y gas natural, e instalaciones de refinado y tratamiento.

También en cuanto a los transportes la lista de obligados sería enorme: Compañías aéreas, Compañías de transporte marítimo, Compañías ferroviarias, Aeropuertos, Puertos, Operadores de control de la gestión del tráfico, y Servicios logísticos auxiliares. En el sector financiero están incluidas, y es aplicable por tanto esta normativa, a las entidades de crédito y a las Infraestructuras de los mercados financieros, es decir las bolsas. Por último, en el Sector sanitario también estarían incluidos los entornos de asistencia sanitaria; hospitales y clínicas privadas, y otras entidades que prestan asistencia sanitaria. En definitiva, este prolijo listado es una muestra de las múltiples y relevantes consecuencias que la aprobación de esta Directiva supondrá para las Administraciones Públicas de todos los Estados miembros y para las grandes empresas de los sectores antes citados que operan en el ámbito de la Unión Europea.

Por otra parte, es necesario conocer las nuevas obligaciones que para Administraciones y empresas se prevén en la nueva normativa pendiente de aprobación. A nivel de principio general, los Estados miembros deberán garantizar un elevado nivel común de seguridad de las redes y los sistemas de información en sus territorios, lo cual impone adoptar una estrategia nacional de Seguridad de las Redes de Información.

Una de las cuestiones más difíciles de articular será la obligación de que cada Estado miembro designe una única autoridad nacional competente en esta materia. Estas autoridades nacionales, supervisarán la aplicación de la presente Directiva a escala nacional y contribuirán a una aplicación coherente de la misma en toda la Unión. Ello es así porque la mayoría de los Estados miembros disponen de varios organismos e instituciones dedicados a la protección de la seguridad en el ciberespacio, con una evidente fragmentación de competencias que en algunos casos por la propia naturaleza de la red es casi imposible delimitar con precisión. Es el caso de España, ya que sólo en la Administración General del Estado hay cuatro Ministerios que disponen de organismos específicos de ciberseguridad. Esta necesidad de nombrar un *primus interpares* puede acarrear dificultades que probablemente deban ser superadas por la decisión que se adopte al respecto al máximo nivel.

Po otra parte, cada Estado miembro tiene que crear un único equipo de respuesta a emergencias informáticas (CERT) responsable de la gestión de incidentes y riesgos de acuerdo con un procedimiento claramente definido previamente. La norma regula profusamente las características de estos CERT, buscando asegurar la confidencialidad, integridad, disponibilidad y autenticidad de la información que reciba, así como su ubicación en lugares seguros, y la continuidad en su funcionamiento mediante la creación de sistemas redundantes. Las tareas encomendadas a estos CERT de referencia son las más decisivas: supervisar incidentes a escala nacional; difundir alertas tempranas; y sobre todo la respuesta a los incidentes graves incluidos los ciberataques procedan de donde procedan. También tiene la obligación de entablar relaciones de cooperación con el sector privado, para lo cual se fomentará la adopción y utilización de prácticas comunes o normalizadas mediante protocolos.

LA RED DE COOPERACIÓN

Uno de los aspectos más relevantes de la Propuesta de Directiva es la creación de un nuevo mecanismo de cooperación entre Estados que se denomina *Red de cooperación*. Se trata de articular un nuevo sistema de cooperación entre las autoridades competentes de cada Estado, con el objeto de colaborar contra los riesgos e incidentes que afecten a las redes y los sistemas de información. El fin último de esta red será mantener una comunicación constante entre la Comisión y las autoridades competentes de cada Estado, que además contará con la asistencia y colaboración de la Agencia Europea de Seguridad de las Redes y de la Información («ENISA»). El instrumento normativo central en cuanto a las actuaciones a

desarrollar en esta materia será el Plan de cooperación de la Unión Europea en materia de SRI, en el cual se describirán los procedimientos y protocolos para las actuaciones en el marco de esta Red. Con ella se trata de concertar una respuesta homogénea a las amenazas que puedan surgir desde el ciberespacio, difundiendo alertas tempranas sobre riesgos e incidentes, así como cooperar e intercambiar información con el Centro Europeo de Ciberdelincuencia de EUROPOL y con otros organismos europeos pertinentes, en particular en los sectores de la protección de datos, la energía, los transportes, la banca, la bolsa y la sanidad.

En definitiva, se puede afirmar que el corazón de esta Propuesta de Directiva es precisamente poner en marcha esta Red que pretende dar una respuesta homogénea y coordinada por parte de todos los Estados miembros, siendo esta la principal motivación de la propia Propuesta de Directiva. Se insiste en la regulación de esta Red de cooperación, en la necesidad de asegurar la creación de un sistema seguro de intercambio de información que es calificada de delicada y confidencial, reservándose la Comisión la decisión de admitir o no a los Estados miembros como parte integrante de la Red, según se cumplan o no los criterios que la propia Comisión fije en cuanto a la seguridad de las infraestructuras de comunicación, su resiliencia, y la capacidad del CERT de referencia nacional. Por tanto, no todos los Estado miembros tendrán acceso a esa red, que es sin duda la innovación más destacada de la nueva normativa.

Ahora bien, no todo son obligaciones aplicables a los Gobiernos y Administraciones Públicas de la Unión Europea. La propuesta de Directiva, supone también una serie de obligaciones concretas para las empresas privadas antes enumeradas. De hecho se impone a estos actores la obligatoriedad de que notifiquen a la autoridad nacional de referencia los incidentes que tengan efectos significativos en la seguridad de los servicios básicos que prestan. Por tanto, precisamente por ser los prestadores de esos servicios públicos básicos, sus obligaciones son mayores que las de otros sectores de actividad, dado que su actividad tiene una incidencia directa en los demás servicios prestados por otros operadores y agentes y que, además, en el caso de las Administraciones Públicas especialmente son servicios logados a derechos fundamentales de los ciudadanos. Debe señalarse que las obligaciones antes citadas las microempresas, definidas por la Comisión como aquellas que ocupan a menos de 10 personas, y cuyo volumen de negocios anual, o cuyo balance general anual, no supere los 2 millones de euros.

No obstante, lo más relevante es la atribución de una serie de poderes que los Estados miembros deben otorgar a las autoridades competentes designadas en cada país para ente otras facultades someter a todos los sujetos, ya sean públicos o privados, a auditorias de seguridad así como a impartir instrucciones vinculantes. Esto supondría la creación de un nuevo centro generador de normas cuyo rango y ámbito deberían especificarse. Por ello, también la propuesta afecta a la estructura institucional y orgánica de la propia Comisión Europea con la creación de un nuevo Comité con el objeto de asistir a la Comisión, en el funcionamiento del cual se aplicarían los procedimientos de comitología, es decir, que la Comisión deberá consultar cada vez que va a adoptar un acto de ejecución en esta materia.

En relación con nuestro país, España, la aprobación de la nueva Estrategia de Seguridad Nacional, y la Estrategia de Ciberseguridad Nacional en el año 2013 han supuesto un avance en este ámbito. Ahora bien, la aprobación de esta nueva Directiva NIS, supondrá la necesidad de adaptar el marco normativo y orgánico español en esta materia, siendo una magnífica ocasión para corregir algunas disposiciones que no se adaptar a este nuevo contexto normativo europeo. Así por ejemplo, será necesario designar una autoridad única de referencia y un CERT único de referencia, decisión que se ha pretendido orillar mediante la articulación de un sistema de rotación al frente de esta responsabilidad por parte de los distintos actores estatales con competencias en esta materia. Esta configuración del liderazgo de la ciberseguridad en España, deberá cambiar a la luz de lo que dispone el texto de la propuesta de Directiva en estos momentos.

CONCLUSIONES

Como se ha ido explicando, la Propuesta de Directiva NIS es el primer intento serio de la UE 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. Pretende ser una respuesta coordinada y europea frente a esta nueva amenaza cuyos potenciales riesgos son innumerables. Su aprobación supondrá 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, afectando a sectores tan relevantes como la energía, la banca o la sanidad. Además, los Estados deberán adaptar sus estructuras administrativas a estas nuevas obligaciones. En el caso de España será necesario revisar y adaptar la recientemente aprobada Estrategia de Ciberseguridad Nacional para cumplir con las nuevas obligaciones que impone la nueva Propuesta de Directiva. El Ciberespacio es un nuevo

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, tan a priori contrario a estos parámetros como es la Red.

Vicente Moret Millás
Ainhoa Uribe Otalora ***
Letrado Cortes Generales y Profesora Titular CEUSanPablo