



# LA AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN

Cinta Castillo Jiménez

Profesora Asociada de Filosofía del Derecho  
Universidad de Sevilla



## sumario

### ■ INTRODUCCIÓN

#### 1 ■ OBJETIVOS DE LA AGENCIA

##### 1.1. Definiciones

#### 2 ■ ORGANIZACIÓN DE LA AGENCIA

##### 2.1. Solicitudes dirigidas a la Agencia

##### 2.2. Cláusula de revisión

##### 2.3. Sede

##### 2.4. Duración

#### 3 ■ LA PROTECCIÓN DE DATOS EN EL ÁMBITO DE LA UNIÓN EUROPEA

##### 3.1. Principios que rigen la protección de las personas a través de sus datos

##### 3.2. Sentencia 292/2002 de 30 de noviembre, del Tribunal Constitucional

##### 3.3. La protección de datos en la Constitución Europea

##### 3.4. La Comisión de las Comunidades Europeas

#### 4 ■ DIRECTIVA 2002/21/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 7 DE MARZO DE 2002, RELATIVA A UN MARCO REGULADOR COMUN DE LAS REDES Y LOS SERVICIOS DE COMUNICACIONES ELECTRÓNICAS

##### 4.1. Ámbito de aplicación, objetivo y definiciones

##### 4.2. Autoridades nacionales de reglamentación

##### 4.3. Obligaciones y misiones de las autoridades nacionales de reglamentación

##### 4.4. Resolución de litigios

##### 4.5. Revisión y Transposición

## resumen

La misión de la Agencia Europea de Seguridad de las Redes y la Información (ENISA), es ayudar a la Comunidad a obtener unos niveles particularmente altos de seguridad de las redes y de la información.

La Agencia contribuirá por lo tanto al desarrollo de una cultura de seguridad de las Redes y de la información en beneficio de los ciudadanos, los consumidores, las empresas y las organizaciones del sector público de la Unión Europea, contribuyendo así al correcto funcionamiento del mercado interior.

La Agencia ayudará a la Comisión, a los Estados miembros y a la comunidad empresarial a cumplir los requisitos de seguridad de las redes y de la información, incluida la legislación comunitaria presente y futura.

ENISA funcionará esencialmente como un Centro de asesoramiento técnico y proporcionará asistencia a los Estados miembros así como a las instituciones de la UE sobre las cuestiones vinculadas a la seguridad de las redes y de la información.

Con el fin de garantizar la realización de sus objetivos, las tareas de la Agencia consistirán principalmente en:

- \_ Acopio y análisis de datos relativos a aspectos vinculados a la seguridad y a los riesgos emergentes;
- \_ Cooperación con los distintos protagonistas creando asociaciones entre el sector público y el sector privado con empresas que ejercen sus actividades en la UE y/o a nivel mundial;
- \_ Sensibilizar a los usuarios en la problemática de la seguridad de las redes y de la información y promover métodos de evaluación de riesgos y mejores prácticas con el fin de encontrar soluciones interoperativas de gestión de los riesgos;
- \_ Seguimiento del desarrollo de las normas sobre productos y servicios en la sociedad de la información y en las redes.

## ■ INTRODUCCIÓN

En nuestra vida cotidiana, la informática y las Redes, representan un componente esencial para los ciudadanos europeos. Dada la omnipresencia de las redes de comunicación y los sistemas de información, la seguridad se ha convertido en un tema de creciente preocupación para el conjunto de la Sociedad

Más del 90% de las empresas de la Unión Europea disponen de una conexión a Internet, y la mayoría de ellas tienen su propia página web. En el año 2002, el 40% de los hogares de la U.E. disponían de conexión propia.

Los ciudadanos, las Administraciones Públicas y las empresas han recurrido a medidas tecnológicas de seguridad y a procedimientos de gestión de la seguridad, si bien, las reacciones de los Estados miembros han sido dispares e insuficientes.

Se ha producido una descoordinación que ha hecho imposible la respuesta eficaz a los problemas de seguridad.

El desarrollo exponencial de las Redes de comunicaciones y los sistemas de información han planteado la preocupación creciente para la sociedad en general, de la seguridad. Las violaciones repetidas de la seguridad de las Redes ha causado considerables perjuicios económicos, que han quebrantado la confianza de los usuarios y ha perjudicado el desarrollo del comercio electrónico.

Un ataque dirigido contra los sistemas de información clave, podría repercutir en el suministro de servicios vitales para el bienestar de los ciudadanos europeos.

No ha existido hasta ahora la cooperación transfronteriza sistemática entre los Estados miembros en cuanto a la seguridad de las Redes, y de la información, aún cuando no puede considerarse un problema aislado que afecte a un único país.

La complejidad técnica de las Redes y de los sistemas de información, la diversidad de productos y servicios que están interconectados y el gran número de agentes privados y públicos responsables de aspectos determinados amenazan con dificultar un correcto funcionamiento del mercado interior.

Dada la omnipresencia de las redes de comunicación y los sistemas de información, y como hemos argumentado, siendo la seguridad un tema de creciente preocupación para el conjunto de la Sociedad, es necesario dar una respuesta adecuada a las amenazas que hemos expuesto y por ello las instancias europeas nos han dotado de una Agencia encargada de la seguridad de la Redes y de la información.

La creación de esta Agencia, tiene el fin de garantizar a los usuarios el mayor grado de seguridad. Su función es de asesoramiento y coordinación de las medidas adoptadas por los Estados miembros para asegurar sus Redes y sistemas de información.

El objetivo de la Agencia es por tanto, reforzar la cooperación entre los distintos agentes que operan en el ámbito, y en particular, entre la Comisión y los Estados miembros, con el fin de prevenir riesgos y tratar los problemas de seguridad.

Así, el Reglamento (CE) nº460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, crea la Agencia Europea de Seguridad de las Redes y de la Información.

La Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo del 2002, estableció el marco regulador común de las Redes y los servicios de comunicaciones electrónicas, esta fue por tanto la Directiva marco. En ella se fijaron las misiones de las

autoridades nacionales de reglamentación, que incluyen cooperar mutuamente y con la Comisión, de una forma transparente, para garantizar el desarrollo de prácticas reglamentarias coherentes.

Con esta Directiva se pretendía contribuir a alcanzar un alto nivel en la protección de los datos personales y del derecho fundamental a la intimidad, así como, garantizar la integridad y la seguridad de las Redes públicas de comunicaciones.

Junto a esta Directiva la de 1999/93/CE contiene disposiciones sobre las normas técnicas que deben publicarse en el Diario Oficial de la Unión europea.

Los Estados miembros utilizan también normas técnicas de organismos internacionales, así como normas técnicas de facto elaboradas por la industria mundial. Es preciso por tanto que la Comisión y los Estados miembros estén al tanto de las normas técnicas que cumplen los requisitos establecidos por la legislación comunitaria.

Estas medidas relativas al mercado interior exigen distintas formas de aplicaciones técnicas y de organización por parte de los Estados miembros y de la Comisión.. Se trata de tareas técnicamente complejas sin soluciones únicas o evidentes.

La aplicación heterogénea de estos requisitos puede dar lugar a soluciones ineficaces y poner trabas al mercado interior, por tanto, esta situación exige la creación de un Centro de Conocimiento especializado en el ámbito europeo que preste servicios de orientación, asesoramiento, y cuando se solicite, asistencia dentro de sus objetivos.

A este Centro podrán recurrir el Parlamento Europeo, la Comisión y los organismos competentes designados por los Estados miembros.

Las autoridades nacionales de reglamentación, designadas en virtud de la Directiva 2002/21/CE, podrán ser nombradas por un Estado miembro como organismo competente.

El establecimiento de la Agencia Europea de Seguridad de las Redes y de la información, que en lo sucesivo llamaremos “Agencia”, debe actuar como punto de referencia e inspirar confianza, por su independencia, la calidad del asesoramiento que preste y de la información que divulgue, a la transparencia de sus procedimientos y métodos de funcionamiento y a su diligencia a la hora de desempeñar las funciones que se asignen, cooperando con los Estados miembros.

La Agencia debe apoyarse en los esfuerzos realizados a nivel nacional y comunitario y por tanto cooperar con los Estados miembros, así mismo, debe estar abierta a contactos con la industria y otros agentes interesados. Las Redes electrónicas son, en gran medida, de propiedad privada.

Es necesario que la Agencia se apoye en las informaciones facilitadas por el sector privado y trabajar en cooperación con éste. Sus funciones no deben interferir, obstaculizar ni solaparse con competencias y funciones correspondientes que se hayan encomendado a las autoridades nacionales de reglamentación.

La Decisión 2002/627/CE de la Comisión y el Comité de comunicaciones a que se refiere la Directiva 2002/21/CE, establecen el Grupo de entidades reguladoras europeas de Redes y de servicios de comunicaciones.

En cuanto a los organismos europeos de normalización, los nacionales, y el Comité permanente están regulados por la Directiva 98/34/CE del Parlamento europeo y del Consejo, por la que se establece un procedimiento de información en materia de normas y reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información.

Por último, tampoco puede interferir la Agencia en las competencias de las autoridades de supervisión de los Estados miembros, en relación con la protección de las personas físicas respecto del tratamiento de los datos personales y de la libre circulación de esos

datos. La responsabilidad reside en la autoridad estatal y autonómica de las Agencias de Protección de Datos y su correspondiente legislación.<sup>1</sup>

## 1 ■ OBJETIVOS DE LA AGENCIA

La creación de la Agencia tiene como objetivo principal, reforzar la capacidad de la Comunidad Europea, los Estados miembros y las empresas, en cuanto a la reacción y la gestión de los problemas vinculados con la seguridad de las redes y la información.

Es importante destacar también, entre los objetivos la asistencia y asesoramiento a la Comisión y los Estados miembros en las cuestiones relacionadas con la seguridad de las redes y la información.

Por otra parte, la Agencia deberá facilitar y fomentar la cooperación entre los agentes de los sectores público y privado y permitir, así, alcanzar un nivel de seguridad suficientemente elevado en los Estados miembros. Por último, la Comisión podrá reclamar la asistencia de la Agencia para realizar labores técnicas preparatorias para la actualización y el desarrollo de la legislación comunitaria en materia de seguridad de las redes y la información.

Con el fin de alcanzar los objetivos anteriormente mencionados, la Agencia llevará a cabo las siguientes tareas:

— Recoger la información necesaria para el análisis de los riesgos actuales y emergentes para la seguridad de las redes y los sistemas de información y proporcionar los resultados de dichos análisis a los Estados miembros y a la Comisión.

— Proporcionar al Parlamento Europeo, a la Comisión y otros órganos competentes asesoramiento y, en su caso, asistencia en relación con los objetivos que le han sido asignados.

\_ Impulsar la cooperación entre los distintos agentes que operan en el sector (por ejemplo, organización de consultas con las empresas y las universidades) y facilitar la cooperación entre la Comisión y los Estados miembros en la elaboración de métodos comunes para prevenir los problemas de seguridad.

\_ Contribuir a la sensibilización de los usuarios y a la rápida puesta a disposición de todos los usuarios de información objetiva y exhaustiva sobre los problemas de seguridad de las redes y de la información. Esto podría hacerse, por ejemplo, promoviendo intercambios de buenas prácticas sobre métodos de alerta a los usuarios.

\_ Asistir a la Comisión y a los Estados miembros en el diálogo que mantienen con las empresas para gestionar los problemas de seguridad que plantean los materiales y los programas informáticos.

\_ Realizar un seguimiento de la elaboración de normas para los productos y servicios en materia de seguridad y promover actividades de evaluación de riesgos.

\_ Contribuir a las iniciativas comunitarias destinadas a cooperar con terceros países y organizaciones internacionales para elaborar un enfoque global común sobre la problemática de la seguridad.

## 1.1. DEFINICIONES

La propuesta de la Comisión precisa determinadas definiciones como las siguientes:

«**Red**»: sistema de transmisión de datos y, en su caso, equipo de conmutación o encaminamiento y cualesquiera otros recursos que permitan la transmisión de señales por cable, radio, por medios ópticos o por otros medios electromagnéticos, incluidas las redes de satélites, las redes terrestres móviles y fijas, las redes utilizadas para las

emisiones de radio y televisión, y las redes de televisión por cable.

«**Sistema de información**»: los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, recuperados o transmitidos por los mismos en relación con su funcionamiento, uso, protección y mantenimiento.

«**Seguridad de las redes y de la información**»: la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, todos los accidentes o acciones ilegales o malintencionadas que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados y transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles.

## 2 ■ ORGANIZACIÓN DE LA AGENCIA

La estructura de la Agencia se basa en la siguiente composición:

Un Consejo de Administración compuesto de representantes de los Estados miembros y de la Comisión.

Un Director Ejecutivo nombrado por el Consejo de Administración a partir de una lista de candidatos propuestos por la Comisión.

Un grupo permanente de las partes interesadas, creado por el Director Ejecutivo y compuesto por representantes de las empresas, los consumidores y expertos universitarios. Este grupo permitirá a la Agencia acceder a los datos más recientes que puedan servir para dar respuesta a los retos que surjan en cuanto a seguridad de las redes.

## 2.1. SOLICITUDES DIRIGIDAS A LA AGENCIA

Las solicitudes de asesoramiento y asistencia destinadas a la Agencia deben dirigirse al Director Ejecutivo e ir acompañadas de información general sobre la cuestión planteada. Las solicitudes pueden ser presentadas por el Parlamento Europeo, la Comisión o un organismo competente designado por los Estados miembros (la autoridad de reglamentación nacional, por ejemplo).

A fin de que el asesoramiento y los dictámenes emitidos por la Agencia sean aceptados por los particulares, las Administraciones públicas y las empresas, debe garantizarse y reconocerse la independencia de la Agencia. A tal efecto, los miembros del Consejo de Administración, el Director Ejecutivo y los expertos externos que participen en grupos de trabajo estarán obligados a declarar que no tienen ningún interés que pudiera poner en peligro su independencia.

La Agencia debe velar por que el público y toda parte interesada reciban información objetiva, fidedigna y fácilmente accesible, en particular, por lo que se refiere al resultado de sus trabajos.

## 2.2. CLÁUSULA DE REVISIÓN

En el plazo de tres años a partir de la creación efectiva de la Agencia, la Comisión tiene previsto llevar a cabo una evaluación, a fin de:

- \_ Determinar si debe prolongarse el periodo para el que se creó la Agencia.
- \_ Evaluar las prácticas de trabajo y las repercusiones de la Agencia.
- \_ Examinar los objetivos y mecanismos establecidos.
- \_ Prever, cuando proceda, la adopción de modificaciones convenientes a la luz de la evolución de la situación institucional y jurídica de la UE y teniendo

en cuenta problemas de seguridad de más amplio alcance.

## 2.3. SEDE

La Agencia tiene su sede en Heraklion, Grecia.

## 2.4. DURACIÓN

La Agencia será operativa del 14 de marzo de 2004 al 31 de diciembre de 2008. La cláusula de revisión va a garantizar que durante el tiempo previsto de existencia de la Agencia, se evalúe su funcionamiento y la necesidad de su permanencia de manera continua, para perfeccionarla y adaptar su funcionamiento a las necesidades que garanticen la seguridad de las Redes en el espacio europeo.

## 3 ■ LA PROTECCIÓN DE DATOS EN EL ÁMBITO DE LA UNIÓN EUROPEA

En el ámbito europeo, la mayoría de los Estados cuentan con regulaciones sobre protección de datos, adaptadas al ordenamiento europeo sobre la protección de las personas físicas respecto a la protección de sus datos personales y de la libre circulación de éstos, según acordó el Parlamento y el Comité el 24 de octubre de 1995.

La Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos<sup>2</sup>, creó el Grupo de Trabajo sobre protección de las personas, este grupo tiene la obligación de facilitar a la Comisión, al Parlamento Europeo y al Consejo un informe anual sobre el estado de protección de las personas físicas con respecto al tratamiento de los datos de carácter personal en la Comunidad y en terceros países.

El grupo se compone de representantes de las autoridades nacionales independientes encargadas de la protección de datos y un representante de la Comisión.

Una de las funciones principales del Grupo de Trabajo es la de formular dictámenes sobre el nivel de protección en la Unión y en los terceros países, y emitir recomendaciones sobre cualquier cuestión referente a la protección de las personas con respecto al tratamiento de los datos personales.

Tomando la Directiva como punto de partida y teniendo en cuenta las disposiciones de otros textos internacionales sobre la protección de datos, debemos referirnos a un núcleo de principios de contenido de protección de datos y requisitos de procedimiento y de aplicación cuyo cumplimiento debe considerarse un requisito mínimo para juzgar la adecuada protección.

El grado de riesgo para el interesado, en caso de transferencia internacional supone un factor importante para determinar los requisitos concretos en un caso determinado.

No podemos perder la visión de la Sociedad de la Información y de la economía interrelacionadas a nivel mundial, fruto de la globalización, donde las tecnologías de la información y de las comunicaciones desempeñan un papel decisivo en la transformación en todos sus aspectos. Vivimos en el albor de una nueva era, donde el músculo es sustituido por el conocimiento, la presencia física de un objeto por lo intangible y la materialidad por la realidad virtual<sup>9</sup>.

### 3.1. PRINCIPIOS QUE RIGEN LA PROTECCIÓN DE LAS PERSONAS A TRAVÉS DE SUS DATOS

Los principios fundamentales de la protección de las personas a través de sus datos personales son:

— La finalidad con que se recaban y usan los datos como principio de limitación de objetivos. Los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia.

— La proporcionalidad y la calidad. Los datos deben ser exactos y estar actualizados, deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

— La transparencia en la información, y en la recogida de los datos. Debe informarse a los interesados sobre el objetivo del tratamiento, así como de la identidad del responsable del fichero.

— La seguridad. El responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos y establecidas en la Ley.

La aplicación del ordenamiento europeo protege la creación de archivos usando datos recopilados a través de Internet, la transferencia a través de la red y la agrupación e interconexión de tales archivos conectados a través de ella. Entendiéndose por dato personal toda información concerniente a una persona física, identificada directa o indirectamente, así como a las imágenes y sonidos digitalizados.

La Ley de la Sociedad de la información define el procesamiento, como cualquier operación o serie de operaciones realizadas y aplicadas a los datos personales como son, la recolección, grabación, organización, almacenamiento, adaptación, extracción, consulta, uso, comunicación, transmisión, radiodifusión o cualquier otro medio de provisión de datos, correspondencia o interconexión, borrado o destrucción de los datos.

La solicitud de información en Internet, la consulta de archivos de datos personales, el intercambio de mensajes en grupos de interés, y una gran cantidad

de operaciones son consideradas como procesamiento en red.

Los países de la Unión Europea garantizan a los titulares de la información, el derecho de acceso, conocer la identidad del responsable del fichero, y el uso que se dará a los datos procesados, así como, el derecho a corregir la información incorrecta o incompleta.

Cuando se transmite un mensaje que contiene datos personales, a través de Internet es el emisor y no la parte que ofrece el servicio el responsable del procesamiento.

El proveedor del servicio es responsable del proceso adicional, necesario para cumplir su labor.

### 3.2. SENTENCIA 292/2002 DE 30 DE NOVIEMBRE, DEL TRIBUNAL CONSTITUCIONAL

A partir de la Sentencia 292/2000 del Tribunal Constitucional, la protección de los datos de carácter personal adquiere en España el carácter de derecho fundamental independiente del derecho a la intimidad.

Esta Sentencia establece que la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede al ámbito propio del derecho fundamental a la intimidad reconocido en el art. 18.1 CE, y que se traduce en el derecho de control sobre los datos relativos a la propia persona.

La libertad informática se traduce en el derecho a controlar el uso de los datos personales insertos en un programa informático, a través del "habeas data" y comprende entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.

El derecho fundamental a la protección de datos, atribuye a su titular facultades para imponer a terceros

la realización u omisión de determinados comportamientos regulada por Ley que desarrolla los arts. 18.4, 81.1 y 53.1 de la CE.

El derecho a la intimidad como derecho fundamental, protege frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, para impedir su tráfico ilícito y lesivo para su dignidad y derecho como afectado.

En definitiva, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno y el derecho a la protección de datos garantiza a los individuos el poder de disposición sobre sus datos.

Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías, así como el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidos de dicha información.

Para que el titular de la información pueda disponer de sus datos, es imprescindible que sepa que datos son los que se conocen, quiénes los poseen y con qué fin.

El derecho a la protección de datos personales es más amplio que el propio derecho a la intimidad, porque si bien, este se extiende a los bienes de la personalidad que pertenecen al ámbito de la vida privada y permite el pleno ejercicio de los derechos de la persona.

El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos datos que sean relevantes en el ejercicio de los derechos de la persona, sean o no derechos constitucionales, por

tanto sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado.

El objeto de protección del derecho fundamental a la protección de datos alcanza a los datos personales públicos, es decir todos aquellos que identifiquen o permitan la identificación de su titular, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole que constituya una amenaza para el titular.

Otra peculiaridad del derecho fundamental a la protección de datos es la de atribuir al titular de los datos un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad. Estos deberes jurídicos se materializan en derechos como el de consentimiento del titular, el de información sobre el destino de los datos, el derecho de acceso y el de rectificación y cancelación, en definitiva todos los que garantizan el poder de disposición sobre los datos personales por parte de su titular.

Podemos concluir, que el derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los propios datos personales que faculta a la persona a decidir cuales de estos datos esta dispuesto a proporcionar a un tercero, ya sea el Estado o un particular.

Por tanto, los elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales, son los derechos que garantizan la información, el acceso y el poder oponerse a la posesión y uso.

La autodeterminación informativa nace como la expresión máxima de control sobre los datos personales que puede tener el interesado. Tras la Sentencia del Tribunal Constitucional Alemán de 1983 por la que se declaraba inconstitucional algunos aspecto de la Ley del Censo.

A través del derecho de información y acceso, de rectificación y de cancelación de la información se hace posible el ejercicio de la autodeterminación que no es total, pues no podemos desaparecer de los bancos de datos de las Administraciones a las que nos vemos obligados a prestar nuestros datos personales. Pero que permite en los demás casos controlar que información tienen los demás sobre nosotros y cual queremos que tengan.

Existe un cauce procesal para llevar a cabo la autodeterminación informativa conocido como “Habeas Data”, que permite el conocimiento de la información que tienen sobre nosotros y que permite a partir de esa información ejercer el resto de los derechos incluidos en la Ley de Protección de Datos. El instrumento por el que se hace posible el ejercicio de los derechos, es la Agencia de Protección de Datos, a través de la cual se hacen las consultas y las reclamaciones en todo lo que concierne a la protección del derecho fundamental de la intimidad personal.

### 3.3 LA PROTECCIÓN DE DATOS EN LA CONSTITUCIÓN EUROPEA

La Constitución europea recoge la protección de datos como un Derecho fundamental “ARTÍCULO I-51. Protección de datos de carácter personal.

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. La ley o ley marco europea establecerá las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

## PARTE II

### CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN

#### ARTÍCULO II-68. Protección de datos de carácter personal:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad-independiente.

### 3.4 LA COMISIÓN DE LAS COMUNIDADES EUROPEAS

Recomendación de la Comisión de 23/7/2003 sobre las notificaciones, los plazos y las consultas previstos en el artículo 7 de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicación electrónicos

De conformidad con el nuevo marco regulador de las redes y los servicios de comunicación electrónicos, las autoridades nacionales de reglamentación tienen la obligación de contribuir al desarrollo del mercado interior, especialmente cooperando entre ellas y con la Comisión, de manera transparente, con objeto de velar por el desarrollo de una práctica reguladora coherente y por la aplicación coherente de las disposiciones de las Directivas que constituyen el nuevo marco regulador.

Con objeto de garantizar que las decisiones nacionales no afecten negativamente al mercado único o a los objetivos del nuevo marco regulador, las autoridades nacionales de reglamentación deben notificar a la Comisión y a las demás autoridades nacionales de reglamentación los proyectos de medidas mencionados en el apartado 3 del artículo 7 de la Directiva 2002/21/CE (Directiva marco).

Como requisito suplementario, las autoridades nacionales de reglamentación deben obtener la autorización de la Comisión en el caso de las obligaciones cubiertas por el segundo párrafo del apartado 3 del artículo 8 de la Directiva 2002/19/CE (Directiva acceso), lo que constituye un procedimiento distinto.

La Comisión ofrecerá a las autoridades nacionales de reglamentación, cuando así lo soliciten, la oportunidad de examinar cualquier proyecto de medida, antes de su notificación formal de conformidad con el artículo 7 de la Directiva 2002/21/CE (Directiva marco) se ofrecerá lo antes posible a la autoridad nacional de reglamentación de que se trate la oportunidad de expresar sus opiniones en relación con las cuestiones planteadas por la Comisión.

La Directiva 2002/21/EC (Directiva marco) establece ciertos plazos obligatorios para el estudio de las notificaciones en base al Artículo 7.

Para facilitar y garantizar la eficacia del mecanismo de cooperación y consulta establecido en el artículo 7 de la Directiva 2002/21/CE (Directiva marco) y en interés de la seguridad jurídica, se necesitan unas normas claras en lo referente al proceso de notificación, al examen por la Comisión de las notificaciones y al cálculo de los plazos legales a los que se ha hecho referencia anteriormente.

Asimismo sería beneficioso aclarar algunas cuestiones procedimentales en el contexto del segundo párrafo del apartado 3 del artículo 8 de la Directiva 2002/19/CE (Directiva acceso).

Para simplificar y acelerar el examen de los proyectos de medidas notificados, es deseable que las autoridades nacionales de reglamentación utilicen un formato estándar para sus notificaciones (formulario de notificación abreviado).

El Grupo de entidades reguladoras europeas creado por la Decisión 2002/627/CE de la Comisión, de 29 de julio de 2002, ha reconocido la necesidad de estas medidas. Para cumplir los objetivos fijados en el artículo 8 de la Directiva 2002/21/CE (Directiva marco) y, en particular, responder a la necesidad de velar por el desarrollo de prácticas reguladoras coherentes y por la aplicación coherente de dicha Directiva, es esencial que se respete íntegramente el mecanismo de notificación previsto en su artículo 7 y que éste sea lo más eficaz posible.

El Comité de Comunicaciones ha emitido su dictamen de conformidad con el apartado 2 del artículo 22 de la Directiva 2002/21/CE (Directiva marco), y en este sentido recomienda:

Los términos definidos en la Directiva 2002/21/CE (Directiva marco) [y en las Directivas específicas] tendrán el mismo significado.

Además, por "Recomendación sobre mercados pertinentes" se entenderá la Recomendación de la Comisión de [11 de febrero de 2003] sobre mercados pertinentes de productos y servicios de comunicaciones electrónicas susceptibles de reglamentación previa.

- "Notificación", se entenderá la notificación a la Comisión por una autoridad nacional de reglamentación de un proyecto.

2. Las notificaciones deberán realizarse, cuando sea posible, por medio de correo electrónico y con solicitud de acuse de recibo. Se supondrá que el destinatario de los documentos enviados a través del correo electrónico los recibe el mismo día de su transmisión.

3. Las notificaciones surtirán efectos a partir de la fecha en la que la Comisión las registre. La fecha de registro será la del día en el que la Comisión reciba la notificación completa.

La fecha de registro de la notificación, el asunto de la notificación y los documentos que se adjunten con ella se pondrán en conocimiento de todas las autoridades nacionales de reglamentación a través del sitio en Internet de la Comisión y de medios electrónicos.

4. La notificación deberá redactarse en cualquiera de las lenguas oficiales de la Comunidad. El formulario abreviado de notificación correspondiente podrá redactarse en una lengua distinta de la del proyecto de medida para facilitar la consulta efectiva de las demás autoridades nacionales de reglamentación.

Toda observación formulada o decisión adoptada por la Comisión de conformidad se redactará en la lengua del proyecto de medida notificado, y se traducirá, siempre que sea posible, a la lengua utilizada en el formulario de notificación abreviado.

5. Los proyectos de medidas notificados por una autoridad nacional de reglamentación deberán ir acompañados de la documentación necesaria para que la Comisión lleve a cabo sus misiones. Los proyectos de medidas deberán motivarse suficientemente.

6. Las notificaciones deberán incluir los siguientes datos:

6.1.-el mercado de productos o servicios pertinente,

6.2.-el mercado geográfico de referencia,

6.3.-las empresas más importantes en el mercado

6.4.-los resultados del análisis del mercado pertinente, en especial los relativos a la existencia o inexistencia de una competencia efectiva en él, así como las razones

6.5.- en su caso, las empresas que tengan, individual o junto con otras, un peso significativo en mercado en el sentido del artículo 14 de la Directiva 2002/21/CE (Directiva marco) y los argumentos, pruebas o cualquier otra información de hecho pertinente en apoyo de tal designación,

6.6.- los resultados de las consultas públicas previas que se hubieran llevado a cabo por la autoridad nacional de reglamentación,

6.7.- el dictamen emitido por la órgano nacional de defensa de la competencia, cuando se haya emitido,

6.8.- pruebas que demuestren que en el momento de la notificación a la Comisión, se adoptaron las medidas apropiadas para notificar el proyecto de la medida a las autoridades nacionales de reglamentación de todos los demás Estados miembros,

6.9.- en el caso de notificaciones de proyectos de medidas que entren en el ámbito de aplicación de los artículos 5 u 8 de la Directiva 2002/19/CE (Directiva acceso) o del artículo 16 de la Directiva 2002/22/CE (Directiva servicio universal), las obligaciones de reglamentación específicas propuestas para hacer frente a la falta de competencia efectiva en el mercado de que se trate o, en el caso de que se considere que existe una competencia efectiva en dicho mercado y ya se hayan impuesto esas obligaciones, las medidas propuestas para retirarlas.

7. En los casos en que un proyecto de medida defina, a los efectos del análisis del mercado, un mercado de referencia distinto de los que figuran en la Recomendación sobre mercados pertinentes de productos y servicios, las autoridades nacionales de reglamentación deberán motivar suficientemente los criterios utilizados para dicha definición del mercado.

8. Las notificaciones realizadas de conformidad con el segundo párrafo del apartado 3 del artículo 8 de la Directiva 2002/19/CE (Directiva acceso) también deberán motivar adecuadamente por qué deben

imponerse a los agentes con un peso significativo en el mercado obligaciones distintas de las enumeradas en sus artículos 9 a 13.

9. Las notificaciones que caigan en el ámbito de aplicación del apartado 5 del artículo 8 de la Directiva 2002/19/CE (Directiva acceso) también deberán motivar adecuadamente por qué son necesarias las medidas previstas para cumplir los compromisos internacionales.

10. Las notificaciones que incluyan la información pertinente en el sentido del apartado 6, se supondrán completas. En los casos en que la notificación, incluidos los documentos que se adjunten con ella, proporcione una información incompleta sobre un aspecto importante, la Comisión dispondrá de un plazo de 5 días hábiles a partir de la fecha de recepción para informar de ello a la autoridad nacional de reglamentación interesada, especificando en qué medida considera que la notificación resulta incompleta. No se registrará la notificación mientras la autoridad nacional de reglamentación de que se trate no proporcione la información necesaria.

11. En el caso de que la Comisión formule observaciones de conformidad con el apartado 3 del artículo 7 de la Directiva 2002/21/CE (Directiva marco), comunicará dichas observaciones, por medios electrónicos, a la autoridad nacional de reglamentación interesada y las publicará en su sitio Internet.

12. Cuando la Comisión, al aplicar el apartado 4 del artículo 7 de la Directiva 2002/21/CE (Directiva marco) considere que un proyecto de medida podría obstaculizar el mercado único o albergue serias dudas en cuanto a su compatibilidad con el Derecho comunitario y, en particular, con los objetivos enumerados en el artículo 8 de la Directiva 2002/21/CE

13. Las autoridades nacionales de reglamentación podrán, en todo momento, retirar el proyecto de medida notificado, en cuyo caso la medida notificada

se suprimirá del registro. La Comisión publicará una notificación apropiada a tal efecto en su sitio Internet.

14.- Cuando una autoridad nacional de reglamentación que haya recibido observaciones de la Comisión o de otra autoridad nacional de reglamentación de conformidad con el apartado 3 del artículo 7 de la Directiva 2002/21/CE (Directiva marco).

#### **4 ■ DIRECTIVA 2002/21/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 7 DE MARZO DE 2002, RELATIVA A UN MARCO REGULADOR COMÚN DE LAS REDES Y LOS SERVICIOS DE COMUNICACIONES ELECTRÓNICAS**

La Directiva marco forma parte del «paquete sobre telecomunicaciones» ideado para refundir el marco regulador de las telecomunicaciones existente y hacer más competitivo el sector de las comunicaciones electrónicas. Este nuevo marco regulador está integrado por esta Directiva y por otras cuatro directivas específicas:

la Directiva relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva de autorización);

la Directiva relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva de acceso);

la Directiva relativa al servicio universal (Directiva de servicio universal);

la Directiva relativa al tratamiento de los datos personales (Directiva de intimidad y comunicaciones electrónicas).

A esta lista hay que añadir la Decisión relativa a un marco regulador de la política del espectro radioeléctrico.

#### **4.1 AMBITO DE APLICACIÓN, OBJETIVO Y DEFINICIONES**

La Directiva tiene por objetivo establecer un marco armonizado para la regulación de las redes y los servicios de comunicaciones electrónicas. Constituye la piedra angular del paquete de medidas y contiene disposiciones horizontales al servicio de las otras medidas que lo integran: ámbito de aplicación y grandes principios, definiciones básicas, disposiciones generales sobre las *autoridades nacionales de reglamentación (ANR)*, nuevo concepto de peso significativo en el mercado y normas de concesión de ciertos recursos esenciales, como las radiofrecuencias, los números o los derechos de paso.

Habida cuenta de la convergencia tecnológica y de la necesidad de una normativa horizontal para el conjunto de las infraestructuras, el nuevo marco no se limita ya a las redes y los servicios de telecomunicaciones, sino que se refiere al conjunto de las redes y servicios de comunicaciones electrónicas. Están incluidas, por ejemplo, las redes de telecomunicaciones fijas y móviles, las redes de televisión por cable o por satélite y las redes eléctricas en la medida en que se utilizan para prestar servicios de comunicaciones electrónicas.

Se excluyen, por el contrario, los contenidos de los servicios prestados a través de las redes de comunicaciones electrónicas, como los contenidos difundidos o los servicios financieros. Lo mismo ocurre con los equipos terminales de telecomunicaciones.

La Directiva define una serie de términos relativos a las comunicaciones electrónicas, entre los que figuran:

«red de comunicaciones electrónicas»: los sistemas de transmisión que permiten el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas y móviles, redes utilizadas para la radiodifusión sonora y

televisiva y redes de televisión por cable;

«servicio de comunicaciones electrónicas»: el prestado por lo general a cambio de una remuneración y que consiste en el transporte de señales a través de redes de comunicaciones electrónicas, excluidos los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos;

«recursos asociados»: aquellos recursos asociados con una red o un servicio de comunicaciones electrónicas que permitan el suministro de servicios a través de dicha red o servicio; incluyen los sistemas de acceso condicional –medida técnica que supedita el acceso a un servicio protegido de radio o televisión al abono o a otra forma de autorización previa– y las guías electrónicas de programas.

#### 4.2 AUTORIDADES NACIONALES DE REGLAMENTACIÓN

Los Estados miembros garantizarán la independencia de las ANR, velando por que sean jurídicamente distintas y funcionalmente independientes de todas las entidades suministradoras de redes, equipos o servicios de comunicaciones electrónicas.

Derecho de recurso. A nivel nacional deberá existir un mecanismo eficaz en virtud del cual cualquier usuario o empresa suministradora de redes o servicios de comunicaciones electrónicas que esté afectado por una decisión de una ANR pueda recurrir ante un organismo independiente.

Imparcialidad y transparencia. Los Estados miembros deberán velar por que las ANR ejerzan sus competencias de manera imparcial y transparente. Deberán también garantizar que, cuando las ANR tengan intención de adoptar medidas que incidan significativamente en el mercado, apliquen mecanismos de

consulta de las partes interesadas.

#### 4.3 OBLIGACIONES Y MISIONES DE LAS AUTORIDADES NACIONALES DE REGLAMENTACIÓN (ANR), MISIONES DE CARÁCTER GENERAL

Con el fin de fomentar la competencia en el suministro de redes de comunicaciones electrónicas, las ANR deberán:

- \_ velar por que los usuarios obtengan el máximo beneficio en cuanto a posibilidades de elección, precio y calidad;
- \_ promover la inversión en materia de infraestructura y fomentar la innovación;
- \_ promover un uso eficiente y una gestión eficaz de las radiofrecuencias y de los recursos de numeración.

Las ANR contribuirán también al desarrollo del mercado interior:

- \_ fomentando el establecimiento y desarrollo de las redes transeuropeas y la interoperabilidad de los servicios;
- \_ garantizando que no se dispense un trato discriminatorio a las empresas suministradoras de redes y servicios de comunicaciones electrónicas;
- \_ cooperando mutuamente y con la Comisión Europea para garantizar el desarrollo de prácticas reglamentarias coherentes y la aplicación coherente del nuevo marco regulador del sector de las telecomunicaciones.

Por último, las ANR tienen por misión promover los intereses de los ciudadanos europeos, en particular:

- \_ velando por que todos dispongan de acceso al servicio universal especificado en la Directiva 2002/22/CE de servicio universal ;

\_ garantizando la disponibilidad de procedimientos sencillos y poco onerosos para la resolución de litigios;

\_ contribuyendo a garantizar un alto nivel de protección de los datos personales y de la intimidad (Directiva de intimidad y comunicaciones electrónicas).

#### 4.4 RESOLUCIÓN DE LITIGIOS

La resolución de los litigios entre empresas suministradoras de redes o servicios de comunicaciones electrónicas en un mismo Estado miembro correrá a cargo de la ANR afectada, que adoptará una decisión vinculante en el plazo de cuatro meses. En caso de litigio transfronterizo que oponga a partes establecidas en distintos Estados miembros, cualquiera de las partes podrá someter el litigio a las ANR afectadas, que coordinarán sus esfuerzos para la resolución del litigio.

#### 4.5 REVISIÓN Y TRANSPOSICIÓN

La obligación de revisión de la Directiva y la transposición a la legislación de los países miembros, garantizan la actualización permanente del objeto de la Directiva, que no es otro que establecer el marco regulador común de las Redes y los servicios de comunicaciones electrónicas.

A más tardar a los tres años de la fecha de aplicación, la Comisión Europea informará al Parlamento Europeo y al Consejo del funcionamiento y la aplicación de la Directiva. Los Estados miembros deberán adoptar y publicar las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo dispuesto en la Directiva ■

#### Notas

1 Castillo Jiménez M<sup>a</sup> Cinta, Derecho y Conocimiento, vol.2 “La sociedad de la información y los Derechos fundamentales” Universidad de Huelva, 2004.

2 M. Heredero Higuera, *La Directiva comunitaria de protección de datos de carácter personal*, Aranzadi, Madrid, 1997.

3 Domingo Carbajo Vasco, *Informe sobre el impacto del comercio electrónico en la fiscalidad española*.