Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)

(2011/C 101/04)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 16,

Vista la Carta de los Derechos Fundamentales de la Unión Europea y, en particular, sus artículos 7 y 8,

Vista la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ([1]),

Vista la solicitud de dictamen de conformidad con el artículo 28, apartado 2, del Reglamento (CE) nº 45/2001 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos ([2]),

HA ADOPTADO EL SIGUIENTE DICTAMEN:

I. **INTRODUCCIÓN**

Descripción de la propuesta

1. El 30 de septiembre de 2010, la Comisión adoptó una propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la ENISA, la Agencia Europea de Seguridad de las Redes y de la Información ([3]).

2. La ENISA se había creado en marzo de 2004 para un período inicial de cinco años de conformidad con el Reglamento (CE) nº 460/2004 ([4]). En 2008, el Reglamento (CE) nº 1007/2008 ([5]) prorrogó el mandato correspondiente hasta marzo de 2012.

3. Tal como se desprende del artículo 1, apartado 1, del Reglamento (CE) nº 460/2004, la Agencia se creó a efectos de garantizar un nivel efectivo y elevado de seguridad de las redes y de la información en la Comunidad y con el fin de contribuir al correcto funcionamiento del mercado interior.

4. La propuesta de la Comisión tiene la intención de modernizar la Agencia, al objeto de fortalecer sus competencias, y establecer un nuevo mandato por un período de cinco años que permita la continuidad de la Agencia más allá de marzo de 2012 ([6]).

5. La propuesta de Reglamento tiene su fundamento jurídico en el artículo 114 del TFUE ([7]), que confiere competencia a la Unión para adoptar medidas encaminadas a establecer o garantizar el funcionamiento del mercado interior. El artículo 114 del TFUE sucede al artículo 95 del antiguo Tratado de la CE, en el que se fundamentó el Reglamento anterior de la ENISA ([8]).

6. La exposición de motivos que acompaña la propuesta se refiere a que la prevención y la lucha contra la delincuencia se han convertido en una competencia compartida tras la entrada en vigor del Tratado de Lisboa. Ello ha creado la posibilidad de que la ENISA desempeñe el papel de plataforma en materia de seguridad de las redes de información (SRI) de la lucha contra la ciberdelincuencia e intercambie opiniones y mejores prácticas con la ciberdefensa y con las autoridades encargadas de hacer cumplir la ley y proteger los datos.

7. En diversas ocasiones, la Comisión ha optado por proponer una ampliación de las funciones de la ENISA e incorporar a las autoridades encargadas de hacer cumplir la ley y proteger los datos como miembros de pleno derecho de su Grupo Permanente de Partes Interesadas. La nueva lista de funciones no incluye las operativas sino que actualiza y reformula las competencias actuales.

Consulta al SEPD

8. El 1 de octubre de 2010, la propuesta se envió al SEPD a título consultivo, de conformidad con el artículo 28, apartado 2, del Reglamento (CE) nº 45/2001. El SEPD se congratula de que se le haya consultado a propósito de este asunto y recomienda que se haga referencia a esta consulta en los considerandos de la propuesta, tal como suele hacerse en los textos legislativos a propósito de los que se ha consultado al SEPD con arreglo al Reglamento (CE) nº 45/2001.

9. Antes de la adopción de la propuesta, se había consultado al SEPD de manera informal y se le había facilitado una serie de observaciones asimismo informales. Sin embargo, ninguna de estas observaciones se tuvo en cuenta en la versión final de la propuesta.

Evaluación general

10. El SEPD destaca que la seguridad del tratamiento de datos es un elemento crucial de la protección de los mismos ([9]). A este respecto, acoge con satisfacción el objetivo de la propuesta de reforzar las funciones de la Agencia para que pueda cumplir más eficazmente sus tareas y responsabilidades actuales y, al mismo tiempo, ampliar su ámbito de

([1]) DO L 281 de 23.11.1995, p. 31.
([2]) DO L 8 de 12.1.2001, p. 1.
([3]) COM(2010) 521 final.
([4]) DO L 77 de 13.3.2004, p. 1.
([5]) DO L 293 de 31.10.2008, p. 1.
([6]) Con el objetivo de evitar un vacío jurídico, por si el procedimiento legislativo en el Parlamento Europeo y en el Consejo se prolongara más allá de la expiración del actual mandato, la Comisión adoptó, el pasado 30 de septiembre de 2010, una segunda propuesta de modificación del Reglamento (CE) nº 460/2004 cuya intención es únicamente prorrogar el plazo del mandato vigente durante 18 meses. Véase COM(2010) 520 final.
([7]) Véase más arriba.
([8]) El 2 de mayo de 2006, el Tribunal de Justicia desestimó un recurso de anulación del Reglamento anterior (CE) nº 460/2004 que impugnaba su fundamento jurídico (asunto C-217/04).
([9]) Los requisitos en materia de seguridad se recogen en los artículos 22 y 35 del Reglamento (CE) nº 45/2001, los artículos 16 y 17 de la Directiva 95/46/CE y los artículos 4y 5 de la Directiva 2002/58/CE.

actividad. El SEPD acoge asimismo con satisfacción la inclusión de las autoridades de protección de datos y las autoridades encargadas de hacer cumplir la ley como partes interesadas de pleno derecho. Considera que la prórroga del mandato de la ENISA es una manera de fomentar a nivel europeo la gestión profesional y racional de las medidas de seguridad de los sistemas de información.

11. La valoración global de la propuesta es positiva. Sin embargo, la propuesta de Reglamento adolece en varios puntos de falta de claridad o exhaustividad, lo que suscita cierta preocupación desde el punto de vista de la protección de datos. Estas cuestiones se explicarán y analizarán en el próximo capítulo del presente dictamen.

II. **OBSERVACIONES Y RECOMENDACIONES**

Las funciones ampliadas que desempeñará la ENISA no están suficientemente claras

12. Las funciones ampliadas de la Agencia, que se refieren a la participación de las autoridades encargadas de hacer cumplir la ley y proteger los datos, se formulan de una manera muy general en el artículo 3 de la propuesta. La exposición de motivos es más explícita al respecto. Se refiere a la ENISA como «interfaz» con las autoridades encargadas de hacer cumplir la ley responsables de la lucha contra la ciberdelincuencia y se le atribuyen tareas de índole no operativa vinculadas a los aspectos relacionados con la lucha contra la ciberdelincuencia. Sin embargo, tales funciones no se incluyen, o sólo se mencionan en términos muy generales, en el artículo 3.

13. Con el fin de evitar toda inseguridad jurídica, la propuesta de Reglamento debe ser clara e inequívoca acerca de las funciones de la ENISA. Como se ha indicado, la seguridad del tratamiento de datos es un elemento crucial de la protección de los mismos. La ENISA desempeñará una función cada vez más importante en ese ámbito. Los ciudadanos, las instituciones y los diversos órganos han de tener claro en qué tipo de actividades podría participar la Agencia. Tal extremo sería aún más importante si entre las competencias de la ENISA se incluyera el tratamiento de datos personales (véanse los puntos 17 a 20 más adelante).

14. El artículo 3, apartado 1, letra k), de la propuesta establece que la Agencia desempeñará las funciones que le confieran los actos legislativos de la Unión. El SEPD tiene dudas sobre esta cláusula abierta, ya que crea una posible laguna que podría afectar la coherencia del instrumento jurídico y podría asimismo dar lugar a una «desviación de uso» de la Agencia.

15. Una de las funciones a las que se refiere el artículo 3, apartado 1, letra k), de la propuesta se contempla en la Directiva 2002/58/CE ([1]). En esta se establece que la Comisión está obligada a consultar a la Agencia sobre las medidas técnicas de ejecución aplicables a las notificaciones en el contexto de las violaciones de datos. El SEPD recomienda que esta actividad de la Agencia se describa con mayor detalle, adscribiéndola asimismo al ámbito de la seguridad. Habida cuenta de la posible repercusión que la ENISA podría tener en el desarrollo de políticas en este ámbito, tal actividad debería ocupar una posición más clara y más prominente dentro de la propuesta de Reglamento.

16. Asimismo, el SEPD recomienda la inclusión de una referencia a la Directiva 1999/5/CE ([2]) en el considerando 21, habida cuenta de la función concreta de la ENISA a la que se refiere el artículo 3, apartado 1, letra c), de la presente propuesta de asistir a los Estados miembros y a las instituciones y organismos europeos en sus esfuerzos por recopilar, analizar y difundir datos sobre la seguridad de las redes y de la información. Ello debería fomentar los ejercicios de promoción de la ENISA en favor de las mejores prácticas y técnicas en materia de SRI (seguridad de las redes de información), toda vez que ilustraría mejor las posibles interacciones constructivas entre la Agencia y los organismos de normalización.

Debe aclararse si la Agencia tratará datos personales

17. La propuesta no aclara si entre las funciones de la Agencia podría incluirse el tratamiento de datos personales. Por ello, la propuesta no se remite a un fundamento jurídico específico para el tratamiento de datos personales, en el sentido del artículo 5 del Reglamento (CE) nº 45/2001.

18. Sin embargo, algunas de las funciones asignadas a la Agencia podrían entrañar (al menos hasta cierto punto) el tratamiento de datos personales. No se descarta, por ejemplo, que el análisis de incidentes de seguridad y violaciones de datos o el desempeño de funciones no operativas en la lucha contra la ciberdelincuencia pueda entrañar la recopilación y el análisis de datos personales.

19. El considerando 9 de la propuesta se refiere a las disposiciones de la Directiva 2002/21/CE ([3]), que establecen que, en su caso, la Agencia recibirá la notificación de las autoridades nacionales de reglamentación en el caso de que se detecten violaciones de seguridad. El SEPD recomienda que se pormenorice más la propuesta en lo que atañe a las notificaciones que se vayan a transmitir a la ENISA y al modo en que la Agencia debe responder a las mismas. Igualmente, la propuesta debe abordar las repercusiones en materia de tratamiento de datos personales que podrían desprenderse del análisis de tales notificaciones (en su caso).

([1]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) DO L 201 de 31.7.2002, p. 37.

([2]) Directiva 1999/5/CE del Parlamento Europeo y del Consejo de 9 de marzo de 1999 sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad, DO L 91 de 7.4.1999, p. 10 y, en particular, el artículo 3, apartado 3, letra c), de la misma.

([3]) 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 (Directiva marco, DO L 108 de 24.4.2002, p. 33).

20. El SEPD invita al legislador a que aclare si las actividades de la ENISA que se enumeran en el artículo 3 —y, en caso afirmativo, cuáles— entrañarán el tratamiento de datos personales.

Deben establecerse las normas de seguridad interna de la ENISA

21. Aunque la ENISA desempeña una función importante en el debate sobre la seguridad de las redes de información en Europa, la propuesta apenas se refiere al establecimiento de las medidas de seguridad de la propia Agencia (tengan éstas relación con el tratamiento de datos personales o no).

22. El SEPD considera que la ENISA se hallará en una posición aún mejor para fomentar las buenas prácticas en relación con la seguridad del tratamiento de datos si la propia Agencia aplica con rigor tales medidas de seguridad internamente. Ello fomentará que la Agencia sea reconocida no sólo como centro de conocimientos especializados, sino, asimismo, como un punto de referencia en la aplicación práctica de las mejores técnicas disponibles (MTD) en el ámbito de la seguridad. La pugna por lograr la excelencia en cuanto a las prácticas en materia de seguridad debería integrarse, pues, en el Reglamento que rige los procedimientos de trabajo de la Agencia. El SEPD recomienda, por lo tanto, que se añada una disposición en este sentido a la propuesta, con arreglo a la que, por ejemplo, se exija que la Agencia aplique las mejores técnicas disponibles, a saber, los procedimientos de seguridad más eficaces y avanzados y sus correspondientes métodos de funcionamiento.

23. Este planteamiento permitirá a la Agencia asesorar sobre la idoneidad práctica de determinadas técnicas para ofrecer las garantías de seguridad necesarias. Por otra parte, la aplicación de estas MTD debe dar prioridad a las que permitan garantizar la seguridad y, al mismo tiempo, minimizar en lo posible el impacto sobre la privacidad. Deberían elegirse las técnicas que mejor se adecuen al concepto de la «privacidad desde el diseño».

24. Aunque el planteamiento sea menos ambicioso, el SEPD recomienda, como mínimo, que el Reglamento contenga los siguientes requisitos: i) la creación de una política de seguridad interna derivada de una evaluación global del riesgo que tenga en cuenta las normas internacionales y las mejores prácticas en los Estados miembros, ii) el nombramiento de un responsable de seguridad encargado de la aplicación de la política que cuente con los recursos y la autoridad adecuados, iii) la aprobación de esta política después de un examen detallado de los riesgos residuales y los controles propuestos por el Consejo de Administración, y iv) una revisión periódica de la política en la que se establezca con claridad la periodicidad de los plazos fijados y los objetivos de tal revisión.

Deben definirse mejor los canales de cooperación con las autoridades de protección de datos (incluido el SEPD) y el Grupo de Trabajo del Artículo 29

25. Como ya se ha indicado, el SEPD acoge con satisfacción la prórroga del mandato de la Agencia y cree que las autoridades de protección de datos pueden beneficiarse mucho de la existencia de la Agencia (y ésta de los conocimientos de dichas autoridades). Dada la convergencia natural y lógica entre la seguridad y la protección de los datos, la Agencia y las autoridades de protección de datos están, de hecho, llamadas a colaborar estrechamente.

26. Los considerandos 24 y 25 contienen una referencia a la propuesta de Directiva comunitaria sobre la ciberdelincuencia e indican que la Agencia debe actuar como enlace con las autoridades encargadas de hacer cumplir la ley y, asimismo, con las autoridades de protección de datos a propósito de los aspectos de seguridad de la información de la lucha contra la ciberdelincuencia ([1]).

27. La propuesta también debería establecer cauces y mecanismos concretos de colaboración que i) garanticen la *coherencia* de las actividades de la Agencia con las de las autoridades de protección de datos y ii) permitan una *estrecha cooperación* entre la primera y las últimas.

28. Con respecto a la *coherencia*, el considerando 27 se refiere explícitamente a que las funciones de la Agencia no deben entrar en conflicto con las autoridades de protección de datos de los Estados miembros. El SEPD acoge con satisfacción esta referencia, pero señala que en ella no se le cita ni se menciona al Grupo de Trabajo del Artículo 29. El SEPD recomienda al legislador que incluya en la propuesta una disposición similar de no injerencia con respecto a estas dos instituciones. Ello creará un entorno de trabajo más claro para todas las partes y debería asimismo delimitar los canales y mecanismos de colaboración que permitan a la Agencia asistir a las diversas autoridades de protección de datos y al Grupo de Trabajo del Artículo 29.

29. Por consiguiente, en lo que se refiere a la *estrecha cooperación*, el SEPD acoge con satisfacción la inclusión de una representación de las autoridades de protección de datos en el Grupo Permanente de Partes Interesadas que asesorará a la Agencia en el desempeño de sus actividades. Recomienda que se mencione explícitamente que esa representación de las autoridades nacionales de protección de datos sea designada por la Agencia sobre la base de una propuesta del Grupo de Trabajo del Artículo 29. Asimismo, agradecería que se incluyera una referencia que previera la asistencia del SEPD, en calidad de tal, a las reuniones en la que vayan a debatirse temas pertinentes para la cooperación con el Supervisor Europeo de Protección de Datos. Por otra parte, el SEPD recomienda que la Agencia (asesorada por el Grupo Permanente de Partes Interesadas y contando con el beneplácito del Consejo de Administración) establezca grupos de trabajo *ad hoc* en cuanto a los temas en los que la protección de datos y la seguridad se solapen en el marco de esta iniciativa de estrecha cooperación.

([1]) Propuesta de Directiva relativa a los ataques contra los sistemas de información, por la que se deroga la Decisión marco 2005/222/JAI del Consejo, COM(2010) 517 final.

30. Por último, con el fin de evitar cualquier posible malentendido, el SEPD recomienda que se emplee el término «autoridades de protección de datos» en lugar de «autoridades encargadas de proteger la intimidad» y se aclare cuáles son tales autoridades mediante la inclusión de una referencia al artículo 28 de la Directiva 95/46/CE y al SEPD, tal como se establece en el capítulo V del Reglamento (CE) nº 45/2001.

No está claro qué beneficiarios pueden solicitar la asistencia de la ENISA

31. El SEPD observa una incoherencia en la propuesta de Reglamento con respecto a quién puede solicitar la asistencia de la ENISA. De los considerandos 7, 15, 16, 18 y 36 de la propuesta se desprende que la ENISA está facultada para asistir a los organismos de los Estados miembros y a la Unión en su conjunto. Sin embargo, el artículo 2, apartado 1, se refiere únicamente a la Comisión y a los Estados miembros, mientras que el artículo 14 limita la capacidad de presentar solicitudes de asesoramiento a: i) el Parlamento Europeo, ii) el Consejo, iii) la Comisión y iv) cualquier organismo competente designado por un Estado miembro, dejando al margen algunas de las instituciones, órganos, organismos y oficinas de la Unión.

32. El artículo 3 de la propuesta es más específico y contempla diferentes tipos de asistencia en función del tipo de beneficiario: i) la recolección y el análisis de datos sobre seguridad de la información (en el caso de los Estados miembros y las instituciones y órganos europeos), ii) el análisis del estado de la red y la seguridad de la información en Europa (en el caso de los Estados miembros y las instituciones europeas), iii) la promoción de la gestión de riesgos y las buenas prácticas de seguridad (en toda la Unión y en los Estados miembros), iv) el desarrollo de una capacidad en materia de detección, análisis y respuesta en relación con la seguridad de las redes y de la información (en las instituciones y órganos europeos) y v) la colaboración en el diálogo y la cooperación con terceros países (en el caso de la Unión).

33. El SEPD invita al legislador a subsanar esta incoherencia y a adaptar las disposiciones mencionadas. En este sentido, el SEPD recomienda que el artículo 14 se modifique de manera que incluya, de hecho, todas las instituciones, órganos, organismos y oficinas de la Unión y que sea claro en cuanto al tipo de asistencia que puedan solicitar las distintas entidades de la Unión (en caso de que el legislador pretenda establecer tal diferenciación). En el mismo sentido, se recomienda que ciertas entidades públicas y privadas puedan solicitar la asistencia de la Agencia, si la asistencia solicitada alberga un potencial claro desde una perspectiva europea y es conforme a los objetivos de la Agencia.

Funciones del Consejo de Administración

34. En la exposición de motivos se describen las competencias ampliadas del Consejo de Administración en cuanto a su función de supervisión. El SEPD se felicita de esta ampliación de funciones y recomienda la inclusión de varios aspectos relativos a la protección de los datos entre las competencias del Consejo de Administración. Además, el SEPD recomienda que el Reglamento especifique de forma inequívoca quién está facultado para: i) establecer medidas para la aplicación del Reglamento (CE) nº 45/2001 por la Agencia, incluidas las relativas al nombramiento de un responsable de la protección de datos, ii) aprobar la política de seguridad y las posteriores revisiones periódicas de la misma, y iii) establecer el protocolo de cooperación con las autoridades de protección de datos y las autoridades encargadas de hacer cumplir la ley.

Aplicabilidad del Reglamento (CE) nº 45/2001

35. Aunque se trata de una exigencia recogida ya en el Reglamento (CE) nº 45/2001, el SEPD sugiere incluir en el artículo 27 el nombramiento de un responsable de la protección de datos, toda vez que se trata de un punto de particular importancia al que debe acompañar una disposición relativa al rápido establecimiento de las normas de desarrollo referidas al alcance de las funciones y competencias encomendadas a dicho responsable de conformidad con el artículo 24, apartado 8, del Reglamento (CE) nº 45/2001. Más concretamente, el artículo 27 podría formularse del modo siguiente:

1) La información personal que la Agencia solicite a los candidatos de conformidad con el presente Reglamento se tratará con arreglo a lo dispuesto en el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

2) El Consejo de Administración adoptará las medidas para la aplicación del Reglamento (CE) nº 45/2001 por la Agencia, incluidas las relativas al responsable de la protección de datos de la misma.

36. En caso de que resulte necesario remitirse a un fundamento jurídico específico para el tratamiento de datos personales, tal como se ha analizado en los puntos 17 a 20, aquél debería aclarar las garantías, limitaciones y condiciones necesarias y adecuadas conforme a las que se llevaría a cabo dicho tratamiento.

III. **CONCLUSIONES**

37. La valoración global de la propuesta es positiva y el SEPD acoge con satisfacción la prórroga del mandato de la Agencia y la ampliación de sus funciones a través de la inclusión de las autoridades de protección de datos y las autoridades encargadas de hacer cumplir la ley como partes interesadas de pleno derecho. El SEPD considera que la continuidad de la Agencia promoverá a nivel europeo la gestión profesional y racional de las medidas de seguridad relativas a los sistemas de información.

38. El SEPD recomienda que, para evitar toda inseguridad jurídica, se aclare la propuesta en lo que atañe a la ampliación de las funciones de la Agencia y, en particular, de las relativas a la participación de las autoridades encargadas de hacer cumplir la ley y las autoridades de protección de datos. Asimismo, el SEPD llama la atención sobre la laguna que podría crear la inclusión de una disposición en la propuesta que permita la asignación de nuevas funciones a la Agencia a través de cualquier otro acto legislativo de la Unión, sin restricción adicional alguna.

39. El SEPD insta al legislador a que aclare si las actividades de la ENISA —y, en caso afirmativo, cuáles— entrañarán el tratamiento de datos personales.

40. El SEPD recomienda incluir disposiciones sobre el establecimiento de una política de seguridad de la propia Agencia, con el fin de reforzar su función de promoción de la excelencia en las prácticas de seguridad y de la «privacidad desde el diseño», integrando el uso de las mejores técnicas disponibles en materia de seguridad con el respeto de los derechos de protección de los datos personales.

41. Los canales de cooperación con las autoridades de protección de datos, incluidos el SEPD y el Grupo de Trabajo del Artículo 29, deben definirse mejor con el objetivo de garantizar la coherencia y una cooperación estrecha.

42. El SEPD invita al legislador a resolver algunas incoherencias en lo que respecta a las restricciones expresadas en el artículo 14, relativo a la capacidad de solicitar la asistencia de la Agencia. En particular, el SEPD recomienda suprimir tales restricciones y disponer que todas las instituciones, órganos, organismos y oficinas de la Unión estén facultados para solicitar la asistencia de la Agencia.

43. Por último, el SEPD recomienda que las competencias ampliadas del Consejo de Administración incorporen ciertos aspectos concretos que podrían mejorar las garantías de adhesión a las buenas prácticas en el seno de la Agencia en lo que respecta a la seguridad y la protección de los datos. Entre otros, se propone incluir el nombramiento de un responsable de la protección de datos y la aprobación de las medidas encaminadas a la correcta aplicación del Reglamento (CE) nº 45/2001.

Hecho en Bruselas, el 20 de diciembre de 2010.

Giovanni BUTTARELLI

Supervisor Europeo de Protección de Datos Adjunto