SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Resumen del Dictamen del Supervisor Europeo de Protección de Datos sobre la estrategia de ciberseguridad y la Directiva SRI 2.0

(El texto completo del presente dictamen está disponible en inglés, francés y alemán en el sitio web del SEPD, www.edps.europa.eu)

(2021/C 183/03)

El 16 de diciembre de 2020, la Comisión Europea adoptó una propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión, y por la que se deroga la Directiva (UE) 2016/1148 («la Propuesta»). Paralelamente, la Comisión Europea y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad publicaron una comunicación conjunta al Parlamento Europeo y el Consejo, titulada «La estrategia de ciberseguridad de la UE para la década digital» («la Estrategia»).

El SEPD apoya firmemente el objetivo general de la Estrategia para garantizar una internet global y abierta, con sólidas salvaguardias para los riesgos de seguridad y los derechos fundamentales, que reconozca el valor estratégico de internet y su gobernanza, y consolide la actuación de la Unión en ese sentido, en un modelo de múltiples partes interesadas.

Por esa razón, el SEPD valora satisfactoriamente el objetivo de la Propuesta de introducir cambios sistémicos y estructurales a la Directiva SRI actual para abarcar un conjunto más amplio de entidades en la Unión, con mayores medidas de seguridad, incluida la gestión obligatoria del riesgo, normas mínimas y disposiciones apropiadas de supervisión y cumplimiento. A este respecto, el SEPD considera necesario integrar plenamente a las instituciones, oficinas, órganos y agencias de la Unión en el marco global de ciberseguridad de la UE, con el fin de alcanzar un nivel uniforme de protección que incluya explícitamente a las instituciones, oficinas, órganos y agencias de la Unión en el ámbito de la Propuesta.

Además, el SEPD destaca la importancia de integrar la perspectiva de la privacidad y la protección de datos en las medidas de ciberseguridad derivadas de la Propuesta o de otras iniciativas de ciberseguridad de la Estrategia, con vistas a asegurar un enfoque integral y permitir las sinergias en la gestión de la ciberseguridad y en la protección de los datos de carácter personal que procesan. Es igualmente importante que cualquier limitación potencial del derecho a la protección de los datos de carácter personal y de la privacidad derivada de estas medidas cumpla los requisitos dispuestos en el artículo 52 de la Carta de los Derechos Fundamentales de la Unión Europea y, en particular, que se lleve a cabo mediante una medida legislativa y que sea, a la vez, necesaria y proporcionada.

El SEPD espera que la Propuesta no persiga afectar a la aplicación de la legislación de la UE que regula el tratamiento de datos de carácter personal, incluidas las funciones y poderes de las autoridades de control independientes con competencias para supervisar el cumplimiento de dichos instrumentos. Esto significa que todos los sistemas y servicios de ciberseguridad implicados en la prevención, detección y respuesta a las ciberamenazas deben ajustarse al marco actual de protección de datos y privacidad. En este sentido, el SEPD considera importante y necesario establecer una definición clara e inequívoca del término «ciberseguridad» a efectos de la Propuesta.

El SEPD formula recomendaciones concretas para garantizar que la Propuesta complementa de manera correcta y efectiva la legislación actual de la Unión en materia de protección de datos de carácter personal, en particular el RGPD y la Directiva sobre la privacidad y las comunicaciones electrónicas, implicando también al SEDP y al Consejo Europeo de Protección de Datos en caso necesario, y estableciendo mecanismos claros de colaboración entre las autoridades competentes de los distintos ámbitos normativos.

Además, las disposiciones sobre la gestión de los registros de dominios de primer nivel de internet deben definir claramente el ámbito de aplicación y las condiciones pertinentes en la legislación. El concepto de los exámenes proactivos de las redes y los sistemas de información por parte de los CSIRT también requiere más aclaraciones sobre el ámbito de aplicación y los tipos de datos personales tratados. Se llama la atención sobre los riesgos de posibles transferencias de datos no conformes relacionadas con la externalización de servicios de ciberseguridad o la adquisición de productos de ciberseguridad y su cadena de suministro.

El SEPD acoge con satisfacción el llamamiento en favor del fomento del uso del cifrado, y en particular del cifrado de extremo a extremo, y reitera su posición sobre el cifrado como tecnología crítica e insustituible para una protección eficaz de los datos y la privacidad, cuya elusión privaría al mecanismo de cualquier capacidad de protección debido a su posible uso ilícito y pérdida de confianza en los controles de seguridad. A tal fin, debe aclararse que nada de lo dispuesto en la Propuesta debe interpretarse como un respaldo al debilitamiento del cifrado de extremo a extremo a través de «puertas traseras» o soluciones similares.

1. **INTRODUCCIÓN Y ANTECEDENTES**

1. El 16 de diciembre de 2020, la Comisión Europea adoptó una propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión y por la que se deroga la Directiva (UE) 2016/1148 ([1]) (en lo sucesivo, «la Propuesta»).

2. En la misma fecha, la Comisión Europea y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad publicaron una Comunicación conjunta al Parlamento Europeo y el Consejo, titulada «La estrategia de ciberseguridad de la UE para la década digital» («la Estrategia») ([2]).

3. La Estrategia tiene por objeto reforzar la autonomía estratégica de la Unión en los ámbitos de la ciberseguridad y mejorar su resiliencia y su respuesta colectiva, así como construir una internet global y abierta con potentes salvaguardias para hacer frente a los riesgos para la seguridad y los derechos y libertades fundamentales de las personas en Europa ([3]).

4. La Estrategia contiene propuestas de iniciativas normativas, de inversión y políticas en tres ámbitos de actuación de la UE: (1) resiliencia, soberanía tecnológica y liderazgo, (2) creación de capacidades operativas para prevenir, disuadir y responder, y (3) promover un ciberespacio mundial y abierto.

5. La Propuesta constituye una de las iniciativas reguladoras de la Estrategia y, en particular, en el ámbito de la resiliencia, la soberanía tecnológica y el liderazgo.

6. Según la exposición de motivos, el objetivo de la Propuesta es modernizar el marco jurídico vigente, es decir, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo («Directiva SRI») ([4]). La Propuesta tiene por objeto basarse en la actual Directiva SRI y derogar la que fue la primera legislación de la UE en materia de ciberseguridad y que establece medidas jurídicas para impulsar el nivel general de ciberseguridad en la Unión. La Propuesta tiene en cuenta el aumento de la digitalización del mercado interior en los últimos años y la evolución del panorama de amenazas a la ciberseguridad, amplificado desde el inicio de la crisis del Covid-19. La Propuesta tiene por objeto abordar varias deficiencias detectadas en la Directiva SRI y aumentar el nivel de ciberresiliencia de todos aquellos sectores, públicos y privados, que desempeñan una función importante para la economía y la sociedad.

7. Los principales elementos de la Propuesta son:

   (i) la ampliación del ámbito de aplicación de la actual Directiva SRI añadiendo nuevos sectores basados en su criticidad para la economía y la sociedad;

   (ii) el endurecimiento de los requisitos de seguridad para las empresas y entidades cubiertas, imponiendo un enfoque de gestión de riesgos que proporcione una lista mínima de elementos básicos de seguridad que deben aplicarse;

   (iii) la gestión la seguridad de las cadenas de suministro y las relaciones con los proveedores exigiendo a las empresas individuales que gestionen los riesgos de ciberseguridad en las cadenas de suministro y las relaciones con los proveedores;

   (iv) La mejora de la cooperación entre las autoridades de los Estados miembros y con las instituciones, oficinas, órganos y agencias de la Unión en el ámbito de las actividades relacionadas con la ciberseguridad, incluida la gestión de crisis cibernéticas.

8. El 14 de enero de 2021, el SEPD recibió una solicitud de consulta formal de la Comisión Europea sobre la «Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión y por la que se deroga la Directiva (UE) 2016/1148».

3. CONCLUSIONES

77. En vista de lo anterior, el SEPD formula las recomendaciones siguientes:

Respecto a la Estrategia de ciberseguridad

— que se tenga en cuenta que el primer paso para mitigar los riesgos para la protección de datos y la privacidad asociados a las nuevas tecnologías para mejorar la ciberseguridad, como la inteligencia artificial, consiste en aplicar los requisitos de protección de datos desde el diseño y por defecto establecidos en el artículo 25 del RGPD, lo que ayudará a integrar las salvaguardias adecuadas, como la seudonimización, el cifrado, la exactitud de los datos y la minimización de datos, en el diseño y el uso de estas tecnologías y sistemas;

— que se tenga en cuenta la importancia de integrar la perspectiva de privacidad y protección de datos en las políticas y normas relacionadas con la ciberseguridad, así como en la gestión tradicional de la ciberseguridad, a fin de garantizar un enfoque integral y permitir sinergias a las organizaciones públicas y privadas a la hora de gestionar la ciberseguridad y proteger la información que procesan sin que se multipliquen inútilmente los esfuerzos;

— que se consideren y planifiquen los recursos que deben utilizar las instituciones de la Unión para reforzar su capacidad en materia de ciberseguridad, también respetando plenamente los valores de la Unión;

— que se tengan en cuenta las dimensiones de privacidad y protección de datos de la ciberseguridad invirtiendo en políticas, prácticas y herramientas en las que la perspectiva de privacidad y protección de datos se integre en la gestión tradicional de la ciberseguridad y se integren salvaguardias efectivas de protección de datos en el tratamiento de datos personales en actividades de ciberseguridad;

Respecto al ámbito de aplicación de la Estrategia y de la Propuesta a las instituciones, oficinas, órganos y agencias de la Unión

— que se tengan en cuenta las necesidades y el papel de las instituciones de la UE para que se integren en este marco general de ciberseguridad a escala de la UE en calidad de entidades que gozan del mismo nivel elevado de protección que las de los Estados miembros;

— que se incluyan explícitamente en el ámbito de aplicación de la Propuesta las instituciones, oficinas, órganos y agencias de la Unión.

Respecto a la relación con la legislación vigente de la Unión en materia de protección de datos personales

— que se aclare en el artículo 2 de la Propuesta que la legislación de la Unión para la protección de los datos personales, en particular el RGPD y la Directiva sobre la privacidad y las comunicaciones electrónicas, se aplica a todo tratamiento de datos personales que entre en el ámbito de aplicación de la Propuesta (solo en contextos específicos);

— que se aclare también en un considerando pertinente que la Propuesta no pretende afectar a la aplicación de la legislación vigente de la UE que regula el tratamiento de datos personales, incluidas las funciones y competencias de las autoridades de control independientes competentes para supervisar el cumplimiento de dichos instrumentos.

Respecto a la definición de ciberseguridad

— que se aclare el uso diferenciado de los términos «ciberseguridad» y «seguridad de las redes y sistemas de información», y se utilice el término «ciberseguridad» en general y la expresión «seguridad de las redes y sistemas de información» únicamente cuando lo permita el contexto (por ejemplo, un contexto puramente técnico, sin tener en cuenta las repercusiones en los usuarios de sistemas y otras personas).

Respecto a los nombres de dominio y los datos de registro («datos WHOIS»)

— que se precise claramente qué se entiende por «información pertinente» a efectos de identificación y se contacte a los titulares de los nombres de dominio y los puntos de contacto que administran los nombres de dominio en el marco de los dominios de nivel superior;

— que se aclare con mayor detalle qué categorías de datos de registro del dominio de datos (que no constituyen datos personales) deben ser objeto de publicación;

— que se aclare en mayor medida qué entidades (públicas o privadas) pueden constituir «solicitantes de acceso legítimos»;

— que se aclare si los datos personales en poder de los registros de dominio de nivel superior y de las entidades que prestan servicios de registro de dominio de nivel superior también deben ser accesibles para las entidades situadas fuera del EEE y, en caso afirmativo, se establezcan claramente las condiciones, limitaciones y procedimientos para dicho acceso, teniendo también en cuenta, en su caso, los requisitos del artículo 49, apartado 2, del RGPD;

— que se introduzcan más aclaraciones sobre lo que constituye una solicitud «lícita y debidamente justificada» sobre la base de la cual se concederá el acceso y en qué condiciones.

Respecto al «escaneado proactivo de redes y sistemas de información» por parte del CSIRT

— que se delimiten claramente los tipos de escaneado proactivo que se puede solicitar a los CSIRT y se identifiquen las principales categorías de datos personales que figuran en el texto de la Propuesta.

Respecto a la externalización y la cadena de suministro

— que se tengan en cuenta las características que permiten la aplicación efectiva del principio de protección de datos desde el diseño y por defecto, al evaluar las cadenas de suministro de tecnología y sistemas de tratamiento de datos personales;

— que se tengan en cuenta los requisitos específicos del país de origen que puedan representar un obstáculo para el cumplimiento de la legislación de la UE en materia de privacidad y protección de datos, al evaluar los riesgos de la cadena de suministro de los servicios, sistemas o productos de TIC;

— que se incluya en el texto jurídico la consulta obligatoria del CEPD a la hora de definir las características mencionadas y, en caso necesario, en la evaluación coordinada sectorial de riesgos mencionada en el considerando 46;

— que se recomiende que se mencione en un considerando que los productos de ciberseguridad de código abierto (software y hardware), incluido el cifrado de código abierto, podrían ofrecer la transparencia necesaria para mitigar los riesgos específicos de la cadena de suministro.

Respecto al cifrado

— que se aclare en el considerando 54 que nada de lo dispuesto en la Propuesta debe interpretarse como un respaldo al debilitamiento del cifrado de extremo a extremo a través de «puertas traseras» o soluciones similares.

Respecto a las medidas de gestión de riesgos en materia de ciberseguridad

— que se incluya tanto en los considerandos como en la parte sustantiva de la Propuesta el concepto de que la integración de la perspectiva de privacidad y protección de datos en la gestión tradicional de los riesgos en materia de ciberseguridad garantizará un enfoque integral y permitirá sinergias con las organizaciones públicas y privadas a la hora de gestionar la ciberseguridad y proteger la información que tratan sin una multiplicación inútil de esfuerzos;

— que se añada en el texto jurídico la obligación de que ENISA consulte al CEPD cuando elabore el asesoramiento pertinente.

Respecto a las infracciones relacionadas con datos personales

— que se modifique el texto «en un plazo de tiempo razonable», en el artículo 32, apartado 1, por «sin demora indebida».

Respecto al Grupo de cooperación

— que se incluya en el texto jurídico la participación del CEPD en el Grupo de cooperación, teniendo en cuenta el vínculo entre las tareas de este Grupo y el marco de protección de datos.

Respecto a la competencia y la territorialidad

— que se aclare en el texto jurídico que la Propuesta no afecta a las competencias de las autoridades de control de la protección de datos en virtud del RGPD;

— que se proporcione una base jurídica exhaustiva para la cooperación y el intercambio de información entre las autoridades competentes y de control, cada una de ellas dentro de sus respectivos ámbitos de competencia;

— que se aclare que las autoridades de control competentes en virtud de la Propuesta deberán poder facilitar, a petición de las autoridades de control competentes en virtud del Reglamento (UE) 2016/679 o por propia iniciativa, cualquier información obtenida en el contexto de cualquier auditoría e investigación relacionada con el tratamiento de datos personales, y se incluya una base jurídica explícita a tal efecto.

Bruselas, 11 de marzo de 2021.

Wojciech Rafał WIEWIÓROWSKI

(1) Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión y por la que se deroga la Directiva (UE) 2016/1148, COM (2020) 823 final.
(2) La estrategia de ciberseguridad de la UE para la década digital, JOIN (2020) 18 final.
(3) Véase el capítulo I. INTRODUCCIÓN, página 4, de la Estrategia.
(4) Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1).