SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Resumen ejecutivo del Dictamen del Supervisor Europeo de Protección de Datos sobre la difusión y el uso de tecnologías de vigilancia intrusiva

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

(2016/C 79/04)

El SEPD trata en el presente dictamen los problemas de protección de datos y de intimidad que plantean la difusión y el uso de tecnologías de vigilancia intrusiva. El uso de dichas herramientas implica por defecto el tratamiento de datos personales y una posible intrusión; el principal objetivo de las herramientas de vigilancia intrusiva es infiltrarse de forma remota en los sistemas de TI (normalmente a través de internet) para controlar de forma encubierta las actividades de dichos sistemas y, con el tiempo, enviar datos al usuario de dichas herramientas.

A pesar de que dichas herramientas pueden ser instrumentos para un uso legítimo (y regulado) por parte de los órganos policiales o de las agencias de inteligencia, también pueden utilizarse como «caballos de Troya» para eludir las medidas de seguridad en las comunicaciones electrónicas y el tratamiento de datos.

La tensión entre un uso positivo de las herramientas TIC y las consecuencias negativas que dicho mal uso de la tecnología pueda tener en los derechos humanos y, en especial, en la protección de los datos personales y la intimidad, es una cuestión que debe ser tratada tanto por las políticas nacionales y europeas como por todos los actores implicados en el sector de las TIC (desarrolladores, proveedores de servicio, vendedores, corredores, distribuidores y usuarios).

En el presente dictamen, el SEPD se propone abordar la amenaza que representa el uso de tecnologías de vigilancia intrusiva mediante las siguientes acciones:

— Debe realizarse una evaluación de las normas europeas existentes en materia de TIC, con el objetivo de aumentar la protección de los derechos humanos, en especial en caso de exportación de tecnología de vigilancia o de intercepción y de servicios relacionados.

— Deben someterse a una regulación adecuada el uso y la difusión (incluso dentro de la UE) de las herramientas de vigilancia y de intercepción, así como de los servicios relacionados, teniendo en cuenta el riesgo potencial de vulneración de derechos fundamentales, en particular de los derechos de intimidad y de protección de datos.

— El Consejo de la UE, el Parlamento Europeo, la Comisión Europea y la DG EAC deberán desarrollar políticas coherentes y más efectivas respecto de la exportación de herramientas de vigilancia intrusiva en el contexto de tecnologías de doble uso, a escala internacional y de la UE.

— Las políticas actualizadas deberán regular los ataques y las vulnerabilidades de «día 0» para evitar un uso que pueda vulnerar derechos fundamentales.

— Las políticas europeas en materia de ciberseguridad deben tener en cuenta la difusión de las tecnologías de intercepción y de vigilancia y abordar de forma específica esta cuestión en el marco de la legislación adecuada.

— Deberán promoverse inversiones en seguridad en internet e iniciativas para integrar la privacidad desde el diseño en las nuevas soluciones tecnológicas.

— Deberá ponerse en práctica un enfoque coherente para conceder protección internacional a los denunciantes que contribuyan a revelar violaciones de derechos humanos a través del uso de las tecnologías de intercepción y de vigilancia.

Hecho en Bruselas, el 15 de diciembre de 2015.

Giovanni BUTTARELLI

Supervisor Europeo de Protección de Datos