

Resumen del Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión Europea al Consejo y al Parlamento Europeo sobre la creación de un centro europeo de ciberdelincuencia

(El texto completo del presente dictamen puede encontrarse en inglés, francés y alemán en el sitio web del SEPD <http://www.edps.europa.eu>)

(2012/C 336/05)

1. Introducción

1.1. Consulta al Supervisor Europeo de Protección de Datos

1. El 28 de marzo de 2012, la Comisión adoptó una Comunicación titulada «La represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia» ⁽¹⁾.

2. El SEPD destaca que el Consejo publicó sus conclusiones sobre la creación de un centro europeo de ciberdelincuencia los días 7 y 8 de junio de 2012 ⁽²⁾. El Consejo apoya los objetivos de la Comunicación, así como la creación de un centro (también llamado «EC3») en la estructura de Europol y el uso de las estructuras de este organismo para facilitar la colaboración con otros servicios encargados de la lucha contra otros tipos de delincuencia, confirma que el EC3 debe servir de punto central en la lucha contra la ciberdelincuencia, y que el EC3 cooperará de manera estrecha con las agencias y actores importantes a nivel internacional, y pide a la Comisión, previa consulta con Europol, que desarrolle el ámbito de las tareas específicas que serán necesarias para hacer que el EC3 esté operativo en 2013. Sin embargo, las Conclusiones no hacen referencia a la importancia de los derechos fundamentales y, en particular, a la protección de datos en la creación del EC3.

3. Antes de que fuera adoptada la comunicación de la Comisión, el SEPD pudo proporcionar observaciones informales sobre el proyecto de Comunicación. En sus observaciones informales, el SEPD destacó que la protección de datos constituye un aspecto esencial que debe ser tenido en cuenta en el establecimiento de un centro europeo de ciberdelincuencia (en adelante, el «EC3»). Por desgracia, la Comunicación no ha tenido en cuenta las observaciones realizadas en la fase informal. Asimismo, las Conclusiones del Consejo piden que se garantice que el Centro ya estará operativo a finales del próximo año. Por esta razón, la protección de datos debería tenerse en cuenta en los próximos pasos que se tomarán a muy corto plazo.

4. El presente dictamen aborda la importancia de la protección de datos al crear el EC3 y aporta sugerencias específicas que podrían ser consideradas durante la elaboración del pliego de condiciones del EC3 y en la revisión legislativa del marco jurídico de Europol. Por tanto, el SEPD ha adoptado por iniciativa propia el presente dictamen, sobre la base del artículo 41, apartado 2, del Reglamento (CE) n° 45/2001.

1.2. Ámbito de aplicación de la Comunicación

5. En su Comunicación, la Comisión apunta su intención de crear un Centro Europeo de Ciberdelincuencia como prioridad de la Estrategia de Seguridad Interna ⁽³⁾.

6. La Comunicación enumera de manera no exhaustiva parcelas de la ciberdelincuencia en las que se supone que se concentra el EC3: ciberdelitos cometidos por grupos de la delincuencia organizada, especialmente los que generan extensos réditos ilegales mediante el fraude en línea, ciberdelitos que provocan daños graves a sus víctimas, como la explotación sexual de menores en línea, y los ciberdelitos que afectan gravemente a infraestructuras y sistemas de información esenciales de la Unión.

7. En relación con el trabajo del Centro, la Comunicación indica cuatro funciones principales ⁽⁴⁾:

- servir de punto central de información sobre la delincuencia en Europa,
- aunar el conocimiento sobre ciberdelincuencia europea para contribuir a la capacitación de los Estados miembros,

⁽¹⁾ La ciberdelincuencia no está definida en la legislación de la UE.

⁽²⁾ Conclusiones del Consejo sobre la creación de un Centro Europeo de Ciberdelincuencia, 3172a sesión del Consejo de Justicia e Interior, Luxemburgo, 7 y 8 de junio 2012.

⁽³⁾ «La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura». COM(2010) 673 final, de 22 de noviembre de 2010. Véase también el dictamen del SEPD sobre dicha Comunicación, emitido el 17 de diciembre de 2010 (DO C 101 de 1.4.2011, p. 6).

⁽⁴⁾ Véanse las pp. 4-5.

- prestar apoyo a los Estados miembros en investigaciones de ciberdelincuencia,
- ser la voz colectiva de los investigadores de ciberdelincuencia europeos ante los organismos de orden público y el estamento judicial.

8. La información que el EC3 trata será recogida a partir del *abanico más amplio posible de fuentes públicas, privadas y abiertas*, que completen los datos policiales disponibles, y *afectaría a las actividades, los métodos y los sospechosos de la ciberdelincuencia*. Igualmente, el EC3 debe colaborar directamente con otras agencias y organismos europeos. Esto se dará mediante la participación de dichas entidades en la Junta de Programación del EC3 y también cooperando operativamente cuando sea necesario.

9. La Comisión propone que el EC3 sea la interfaz natural con el trabajo sobre ciberdelincuencia de Interpol y otras instancias policiales internacionales de ciberdelincuencia. Asociado a Interpol y a otros socios internacionales estratégicos de todo el mundo, el EC3 debe esforzarse en mejorar las respuestas coordinadas en la lucha contra la ciberdelincuencia.

10. En términos prácticos, lo que la Comisión propone es crear este EC3 como parte de Europol. El EC3 *formará parte de Europol* ⁽¹⁾ y, por lo tanto, se regirá por el régimen jurídico de Europol ⁽²⁾.

11. Según la Comisión Europea ⁽³⁾, las principales novedades que el EC3 propuesto aportaría a las actuales actividades de Europol serán: (i) aumentar los recursos para recoger información de las distintas fuentes de la manera más eficaz (ii) intercambiar información con los socios distintos de los servicios represivos (principalmente del sector privado).

1.3. Puntos esenciales del dictamen

12. El SEPD pretende con el presente dictamen:

- pedir a la Comisión que aclare el ámbito de aplicación de las actividades del EC3, en la medida en que éstas sean pertinentes para la protección de datos,
- valorar las actividades previstas en el contexto del actual marco jurídico de Europol, en especial su compatibilidad con el mismo,
- destacar los aspectos relevantes en que el legislador debe introducir más detalles en el contexto de la futura revisión del marco jurídico de Europol para garantizar un mayor nivel de protección de datos.

13. El presente dictamen está organizado de la siguiente manera. La parte 2.1 aborda el motivo por el cual la protección de datos constituye un elemento esencial de la creación del EC3. La parte 2.2 trata la compatibilidad de los objetivos establecidos para el EC3 en la Comunicación con el mandato legal de Europol. La parte 2.3 trata la cooperación con el sector privado y los socios internacionales.

3. Conclusiones

50. El SEPD considera la lucha contra la ciberdelincuencia una piedra angular en la construcción de la seguridad y la protección en el espacio digital, así como para generar la confianza necesaria. El SEPD señala que el cumplimiento de los sistemas de protección de datos debe considerarse una parte integral de la lucha contra la ciberdelincuencia y no como un elemento de disuasión de su eficacia.

51. La Comunicación hace referencia a la creación de un nuevo Centro Europeo de Ciberdelincuencia dentro de Europol, mientras que desde hace unos años ya existe un Centro de Ciberdelincuencia de Europol. El SEPD recibiría con agrado una mayor claridad en relación con las nuevas capacidades y actividades que diferenciarán el nuevo EC3 del Centro de Ciberdelincuencia de Europol existente.

⁽¹⁾ Tal como recomienda el estudio de viabilidad publicado en febrero de 2012 que evalúa las distintas opciones disponibles (estatuto, organización por parte de Europol, propiedad/formar parte de Europol, Centro virtual). http://ec.europa.eu/home-affairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf

⁽²⁾ Decisión del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol) (2009/371/JAI).

⁽³⁾ Comunicado de prensa de 28 de marzo. «Frequently Asked Questions: the new European Cybercrime Centre» (Preguntas frecuentes: el nuevo Centro Europeo de Ciberdelincuencia) Referencia: MEMO/12/221 Fecha: 28.3.2012 <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/221> (disponible en inglés).

52. El SEPD recomienda que se definan de manera clara las competencias del EC3 y que no sólo se establezcan haciendo referencia al concepto de «delincuencia informática» incluida en la legislación actual de Europol. Asimismo, la definición de las competencias y de las garantías de protección de datos del EC3 debe formar parte de la revisión de la legislación de Europol. Hasta que la nueva legislación de Europol sea aplicable, el SEPD recomienda que la Comisión establezca dichas competencias y garantías de protección de datos en el pliego de condiciones del Centro, lo cual debe incluir:

- una definición clara de cuáles son las funciones de tratamiento de datos (en particular, las investigaciones y las actividades de apoyo operativo) en que el personal del Centro podría comprometerse, de manera independiente o en colaboración con los equipos conjuntos de investigación, y
- procedimientos claros que, por un lado, garanticen el respeto de los derechos individuales (incluido el derecho a la protección de datos) y, por otro, ofrezcan garantías de que las pruebas han sido obtenidas de manera legal y pueden utilizarse ante un tribunal.

53. El SEPD considera que los intercambios de datos personales del EC3 con el «abanico más amplio posible de fuentes públicas, privadas y abiertas» conllevan riesgos específicos para la protección de datos ya que siempre implicarán el tratamiento de datos obtenidos con fines comerciales así como transferencias internacionales de datos. La actual Decisión de Europol trata estos riesgos y establece que, en general, Europol debe intercambiar datos directamente con el sector privado y con organizaciones internacionales específicas únicamente en circunstancias muy concretas.

54. En este contexto, y dada la importancia de estas dos actividades del EC3, el SEPD recomienda que se ofrezcan las garantías adecuadas de protección de los datos, en cumplimiento de lo dispuesto en las disposiciones existentes en la Decisión de Europol. Dichas garantías deben incorporarse en el pliego de condiciones para que puedan ser elaboradas por el equipo de establecimiento del EC3 (y posteriormente en el marco jurídico revisado de Europol) y, en ningún caso, deberían implicar un nivel inferior de protección de datos.

Hecho en Bruselas, el 29 de junio de 2012.

Peter HUSTINX
Supervisor Europeo de Protección de Datos
