

Rezumatul Avizului Autorității Europene pentru Protecția Datelor referitor la Comunicarea Comisiei Europene către Consiliu și Parlamentul European privind instituirea unui Centru european de combatere a criminalității informatice

(Textul integral al acestui aviz poate fi consultat în limbile engleză, franceză și germană pe site-ul AEPD <http://www.edps.europa.eu>)

(2012/C 336/05)

1. Introducere

1.1. Consultarea AEPD

1. La 28 martie 2012, Comisia a adoptat o comunicare intitulată „Combaterea criminalității în era digitală actuală: instituirea unui Centru european de combatere a criminalității informatice” ⁽¹⁾.

2. AEPD observă că Consiliul a publicat Concluziile sale privind instituirea unui Centru european de combatere a criminalității informatice la 7 și 8 iunie 2012 ⁽²⁾. Consiliul susține obiectivele comunicării, sprijină instituirea centrului (denumit, de asemenea, „EC3”) în cadrul Europol și utilizarea structurilor existente pentru activități comune în legătură cu alte domenii de criminalitate, confirmă că EC3 ar trebui să servească drept punct de convergență în combaterea criminalității informatice și că EC3 va coopera strâns cu agențiile și actorii relevanți la nivel internațional și invită Comisia să participe la consultări cu Europol în vederea elaborării în continuare a sferei sarcinilor specifice care vor fi necesare pentru ca EC3 să devină funcțional până în 2013. Totuși, concluziile nu fac referire la importanța drepturilor fundamentale, în special la protecția datelor, în cadrul instituirii EC3.

3. Înainte de adoptarea comunicării Comisiei, Autorității Europene pentru Protecția Datelor i s-a dat posibilitatea de a prezenta observații informale cu privire la proiectul de comunicare. În observațiile sale informale, AEPD a subliniat că protecția datelor este un aspect esențial care trebuie luat în considerare în înființarea Centrului european de combatere a criminalității informatice (denumit în continuare, „EC3”). Din păcate, Comisia nu a luat în considerare observațiile prezentate în etapa informală. În plus, în concluziile Consiliului se solicită să se asigure că centrul va fi deja funcțional până anul viitor. Din acest motiv, protecția datelor ar trebui să fie luată în considerare în cadrul următoarelor etape care vor fi parcurse deja într-un termen foarte scurt.

4. Prezentul aviz abordează importanța protecției datelor în momentul instituirii EC3 și oferă propuneri specifice care ar putea fi luate în considerare în cursul stabilirii mandatului EC3 și în cadrul revizuirii legislative a cadrului juridic al Europol. Prin urmare, acționând din proprie inițiativă, AEPD a adoptat prezentul aviz în temeiul articolului 41 alineatului (2) din Regulamentul (CE) nr. 45/2001.

1.2. Domeniul de aplicare al comunicării

5. În comunicarea sa, Comisia își exprimă intenția de a institui Centrul european de combatere a criminalității informatice ca prioritate a Strategiei de securitate internă ⁽³⁾.

6. Comunicarea enumeră, sub forma unei liste neexhaustive, mai multe aspecte majore ale criminalității informatice pe care EC3 va trebui să se concentreze: acte de criminalitate informatică comise de către grupurile de criminalitate organizată, în special acele acte care generează profituri considerabile obținute din săvârșirea de infracțiuni, cum ar fi fraudă online, acte de criminalitate informatică ce aduc prejudicii grave victimelor lor, cum ar fi exploatarea sexuală a copiilor pe internet, precum și acte de criminalitate informatică îndreptate împotriva infrastructurii critice și a sistemelor informatice (TIC) ale Uniunii.

7. În ceea ce privește activitatea centrului, comunicarea prezintă patru sarcini principale ⁽⁴⁾:

- să fie punctul de convergență, la nivel european, al informațiilor privind criminalitatea informatică;
- să pună în comun expertiza europeană în materie de combatere a criminalității informatice pentru a sprijini statele membre în consolidarea propriilor capacități;

⁽¹⁾ Criminalitatea informatică nu este definită în legislația UE.

⁽²⁾ Concluziile Consiliului privind instituirea unui Centru european de combatere a criminalității informatice – a 3172-a reuniune a Consiliului Justiție și Afaceri Interne de la Luxemburg, 7 și 8 iunie 2012.

⁽³⁾ Strategia de securitate internă a UE în acțiune: cinci pași către o Europă mai sigură. COM(2010) 673 final, 22 noiembrie 2010. A se vedea, de asemenea, avizul AEPD privind această comunicare, emis la 17 decembrie 2010 (JO C 101, 1.4.2011, p. 6).

⁽⁴⁾ Comunicare, pp. 4 și 5.

- să ofere sprijin statelor membre în cadrul investigațiilor privind criminalitatea informatică;
- să devină purtătorul de cuvânt al investigatorilor europeni privind criminalitatea informatică la nivelul autorităților de aplicare a legii și al sistemului judiciar.

8. Informațiile prelucrate de EC3 vor fi colectate *dintr-un număr foarte mare de surse publice, private și deschise*, îmbogățind astfel datele de care dispune poliția și vor *viza activitățile metodele și persoanele suspectate de criminalitate informatică*. EC3 va colabora, de asemenea, în mod direct, cu alte agenții și organisme europene. Această colaborare va avea loc prin participarea acestor entități în cadrul comitetului de gestionare a programului EC3, precum și prin cooperarea operativă, după caz.

9. Comisia propune ca EC3 să fie interfața naturală între activitățile Europol în materie de criminalitate informatică și alte unități polițienești internaționale de combatere a criminalității informatice. De asemenea, EC3 ar trebui, în parteneriat cu Interpol și alți parteneri strategici din lume, să depună eforturi pentru îmbunătățirea coordonării răspunsurilor în materie de combatere a criminalității informatice.

10. În termeni practici, Comisia propune crearea EC3 ca parte a Europol. EC3 va *face parte din Europol* ⁽¹⁾ și, prin urmare, va fi plasat sub regimul juridic al Europol ⁽²⁾.

11. Potrivit Comisiei Europene ⁽³⁾, principalele noutăți pe care le va aduce EC3 în activitățile actuale ale Europol vor fi: (i) creșterea resurselor în vederea colectării mai eficiente a informațiilor din diferite surse; și (ii) schimbul de informații cu parteneri din afara comunității de aplicare a legii (în special din sectorul privat).

1.3. Obiectivul avizului

12. Prin prezentul aviz, AEPD intenționează:

- să solicite Comisiei să clarifice sfera activităților EC3, în măsura în care acestea sunt relevante pentru protecția datelor;
- să evalueze activitățile prevăzute în contextul cadrului juridic al Europol, în special compatibilitatea acestora cu cadrul;
- să sublinieze aspectele relevante în legătură cu care legislatorul ar trebui să introducă mai multe detalii în contextul viitoarei revizuirii a regimului juridic al Europol pentru asigurarea unui nivel mai ridicat al protecției datelor.

13. Avizul este organizat după cum urmează. Partea 2.1 explică de ce protecția datelor este un element esențial în crearea EC3. Partea 2.2 se referă la compatibilitatea obiectivelor prevăzute pentru EC3 în comunicare cu mandatul legal al Europol. Partea 2.3 se referă la cooperarea cu sectorul privat și cu partenerii internaționali.

3. Concluzii

50. AEPD consideră că lupta împotriva criminalității informatice este o piatră de temelie în consolidarea securității și siguranței în spațiul digital și în generarea încrederii necesare. AEPD observă că respectarea regimurilor de protecție a datelor ar trebui să fie considerată o parte integrantă a combaterii criminalității informatice și nu un element care îi împiedică eficacitatea.

51. Comunicarea face referire la instituirea unui nou Centru european de combatere a criminalității informatice în cadrul Europol, având în vedere că un Centru Europol de combatere a criminalității informatice există de mai mulți ani. AEPD ar saluta o mai mare claritate cu privire la noile competențe și activități care vor face distincția între noul EC3 și Centrul Europol de combatere a criminalității informatice existent.

⁽¹⁾ Astfel cum se recomandă în studiul de fezabilitate publicat în februarie 2012 în care sunt evaluate diferite opțiuni disponibile (*statu quo*, găzduit de Europol, deținut de/parte din Europol, centru virtual). http://ec.europa.eu/home-affairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf

⁽²⁾ Decizia Consiliului din 6 aprilie 2009 privind înființarea Oficiului European de Poliție (Europol) (2009/371/JAI).

⁽³⁾ Comunicat de presă din 28 martie. Întrebări frecvente: noul Centru european de combatere a criminalității informatice: MEMO/12/221. Data: 28.3.2012. <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/221>

52. AEPD recomandă definirea clară a competențelor EC3, în loc ca acestea să fie doar prezentate prin referirea la conceptul de „criminalitate informatică” inclus în actuala legislație privind Europol. De asemenea, definițiile competențelor și garanțiilor privind protecția datelor în cadrul EC3 ar trebui să fie incluse în revizuirea legislației referitoare la Europol. Până în momentul în care noua legislație Europol va deveni aplicabilă, AEPD recomandă Comisiei să stabilească aceste competențe și garanții privind protecția datelor în mandatul centrului. Acestea ar putea include:

- o definiție clară a sarcinilor de prelucrare a datelor (în special, anchetele și activitățile de sprijin operativ) în care se poate implica personalul centrului, în mod individual sau în colaborare cu echipe comune de anchetă; precum și
- proceduri clare care, pe de o parte, asigură respectarea drepturilor individuale (inclusiv dreptul la protecția datelor) și, pe de altă parte, oferirea de garanții că probele au fost obținute în mod legal și pot fi utilizate în instanță.

53. AEPD consideră că schimbul de date cu caracter personal între EC3 și „numărul foarte mare de surse publice, private și deschise” prezintă riscuri specifice în materie de protecție a datelor, deoarece va implica de multe ori prelucrarea de date colectate în scop comercial și transferuri internaționale de date. Aceste riscuri sunt abordate în actuala Decizie privind Europol, care stabilește că, în general, Europol nu ar trebui să realizeze schimburi directe de date cu sectorul privat și cu organizații internaționale specifice decât în circumstanțe foarte concrete.

54. În acest context și având în vedere importanța acestor două activități pentru EC3, AEPD recomandă introducerea unor garanții adecvate privind protecția datelor în conformitate cu dispozițiile existente din Decizia privind Europol. Aceste garanții ar trebui să fie integrate în mandatul care va fi elaborat de echipa responsabilă de instituirea EC3 (și, ulterior, în cadrul juridic revizuit al Europol) și ar trebui să nu genereze în niciun caz un nivel mai scăzut de protecție a datelor.

Adoptat la Bruxelles, 29 iunie 2012.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor
