

Povzetek mnenja Evropskega nadzornika za varstvo podatkov o sporočilu Evropske komisije Svetu in Evropskemu parlamentu o ustanovitvi Evropskega centra za boj proti kibernetiski kriminaliteti

(Celotno besedilo tega mnenja je na voljo v angleškem, francoskem in nemškem jeziku na spletni strani ENVP na naslovu <http://www.edps.europa.eu>)

(2012/C 336/05)

1. Uvod

1.1 Posvetovanje z Evropskim nadzornikom za varstvo podatkov (ENVP)

1. Evropska komisija je 28. marca 2012 sprejela sporočilo z naslovom „Boj proti kriminalu v digitalni dobi: ustanovitev Evropskega centra za boj proti kibernetiski kriminaliteti“⁽¹⁾.

2. ENVP ugotavlja, da je Svet objavil sklepe o ustanovitvi Evropskega centra za boj proti kibernetiski kriminaliteti 7. in 8. junija 2012⁽²⁾. Svet potrjuje cilje sporočila, podpira ustanovitev centra (imenovanega tudi „EC3“) v okviru Europolu in uporabo sedanjih struktur za navzkrižno sodelovanje na drugih področjih kriminalitete, potrjuje, da mora EC3 delovati kot osrednja točka v boju proti kibernetiski kriminaliteti in da bo EC3 tesno sodeloval z zadevnimi agencijami in akterji na mednarodni ravni, ter Komisijo poziva, naj v posvetovanju z Europolom podrobneje opredeli obseg posebnih nalog, ki bodo potrebne, da bo lahko EC3 začel delovati do leta 2013. Vendar v sklepih nista omenjena pomen temeljnih pravic in zlasti varstvo podatkov v postopku ustanavljanja EC3.

3. ENVP je imel pred sprejetjem sporočila Komisije možnost predložiti neuradne pripombe k osnutku sporočila. V njih je poudaril, da je varstvo podatkov bistven vidik, ki ga je treba upoštevati pri vzpostavitvi Evropskega centra za boj proti kibernetiski kriminaliteti (v nadaljnjem besedilu: EC3). Žal v sporočilu niso bile upoštevane pripombe, predložene v neformalni fazi. Poleg tega se v sklepih Sveta poziva k zagotovitvi, da bo center začel delovati že do naslednjega leta. Zato je treba v naslednjih korakih, ki bodo sprejeti v že zelo kratkem času, upoštevati varstvo podatkov.

4. V tem mnenju je obravnavan pomen varstva podatkov pri ustanovitvi EC3, zagotovljeni pa so tudi posebni predlogi, ki bi jih bilo mogoče upoštevati pri oblikovanju poslovnika EC3 in zakonodajni reviziji pravnega okvira Europolu. Zato je ENVP to mnenje, ki temelji na členu 41(2) Uredbe (ES) št. 45/2001, sprejel na lastno pobudo.

1.2 Področje uporabe sporočila

5. Komisija je v sporočilu nakazala, da je ustanovitev Evropskega centra za boj proti kibernetiski kriminaliteti prednostna naloga strategije notranje varnosti⁽³⁾.

6. V sporočilu je neizčrpno naštetih več pojavnih oblik kibernetiske kriminalitete, na katere naj bi se osredotočal EC3: kibernetiska kazniva dejanja, ki so jih zagrešile organizirane kriminalne združbe, zlasti tista, ki ustvarjajo ogromne nezakonite dobičke, kot so spletne goljufije, kibernetiska kazniva dejanja, ki žrtvam povzročajo resno škodo, kot so spolno izkoriščanje otrok na spletu, in kibernetiska kazniva dejanja, ki resno vplivajo na ključne sisteme komunikacijske in informacijske tehnologije (IKT) v Uniji.

7. V zvezi z delom centra so v sporočilu navedene štiri glavne naloge⁽⁴⁾:

— delovati kot osrednja evropska informacijska točka v boju proti kibernetiski kriminaliteti,

— združevati strokovna znanja v Evropi o kibernetiski kriminaliteti, da bi podprl države članice pri krepitvi zmogljivosti,

⁽¹⁾ Kibernetiska kriminaliteta ni opredeljena v zakonodaji EU.

⁽²⁾ Sklepi Sveta o ustanovitvi Evropskega centra za boj proti kibernetiski kriminaliteti, 3172. zasedanje Sveta za pravosodje in notranje zadeve, Luxembourg, 7. in 8. junija 2012.

⁽³⁾ Izvajanje strategije notranje varnosti EU: pet korakov k varnejši Evropi. COM(2010) 673 konč. z dne 22. novembra 2010. Glej tudi mnenje ENVP o tem sporočilu, izdano 17. decembra 2010, (UL C 101, 1.4.2011, str. 6).

⁽⁴⁾ Sporočilo, str. 4 in 5.

- zagotavljati podporo državam članicam pri preiskovanju kibernetске kriminalitete,
- postati mora skupni glas evropskih preiskovalcev kibernetске kriminalitete iz vseh organov kazenskega pregona in pravosodnih organov.

8. Informacije, ki jih bo obdeloval EC3, se bodo zbirale iz številnih javnih, zasebnih in prosto dostopnih virov, s čimer bi se obogatili podatki, ki so na voljo policiji, *nanašale pa se bodo na dejavnosti in metode kibernetске kriminalitete ter osumljence*. EC3 bo poleg tega neposredno sodeloval z drugimi evropskimi agencijami in organi. To bo potekalo prek sodelovanja teh subjektov v programskem odboru EC3 ter operativnega sodelovanja, kadar je to primerno.

9. Komisija predlaga, naj bi bil EC3 naravni vmesnik za sodelovanje z Interpolom in drugimi mednarodnimi policijskimi enotami na področju boja proti kibernetски kriminaliteti. EC3 bi si moral poleg tega v partnerstvu z Interpolom in drugimi strateškimi partnerji po svetu prizadevati za izboljšanje usklajenih odzivov v boju proti kibernetски kriminaliteti.

10. Komisija v praksi predlaga, naj se EC3 oblikuje kot sestavni del Europolu. EC3 bo *sestavni del Europolu* ⁽¹⁾, zato bo zanj veljala pravna ureditev Europolu ⁽²⁾.

11. V skladu z Evropsko komisijo ⁽³⁾ bosta glavni novosti, ki ju bo v zvezi s sedanjimi dejavnostmi Europolu povzročila predlagana ustanovitev EC3, naslednji: (i) več sredstev za učinkovitejše zbiranje informacij iz različnih virov in (ii) izmenjava informacij s partnerji, ki niso le organi kazenskega pregona (predvsem iz zasebnega sektorja).

1.3 Osrednja tema mnenja

12. ENVP v tem mnenju Komisijo poziva, naj:

- pojasni obseg dejavnosti EC3, če so pomembne za varstvo podatkov,
- oceni predvidene dejavnosti v okviru sedanje pravne ureditve Europolu, zlasti njihovo skladnost s to ureditvijo,
- poudari pomembne vidike, v zvezi s katerimi bi moral zakonodajalec vključiti dodatne podrobnosti v okviru prihodnjega pregleda Europolove pravne ureditve za zagotovitev višje ravni varstva podatkov.

13. Mnenje je strukturirano na naslednji način. V delu 2.1 je pojasnjeno, zakaj je varstvo podatkov bistven del oblikovanja EC3. Del 2.2 obravnava skladnost ciljev, ki so bili v sporočilu določeni za EC3, s pristojnostmi Europolu. V delu 2.3 je obravnavano sodelovanje z zasebnim sektorjem in mednarodnimi partnerji.

3. Sklepne ugotovitve

50. ENVP meni, da je boj proti kibernetски kriminaliteti temelj za vzpostavitev varnosti v digitalnem prostoru in zagotavljanje potrebnega zaupanja. Ugotavlja, da je treba skladnost z ureditvami varstva podatkov šteti za sestavni del boja proti kibernetски kriminaliteti in ne za dejavnik, ki zmanjšuje učinkovitost.

51. Sporočilo se sklicuje na ustanovitev novega Evropskega centra za boj proti kibernetски kriminaliteti v okviru Europolu, čeprav Europolov center za boj proti kibernetски kriminaliteti obstaja že vrsto let. ENVP bi bil zadovoljen, če bi se zagotovila podrobnejša pojasnila glede novih zmogljivosti in dejavnosti, ki bodo nov EC3 razlikovale od sedanjega Europolovega centra za boj proti kibernetски kriminaliteti.

⁽¹⁾ Kot je bilo priporočeno v študiji izvedljivosti, objavljeni februarja 2012, v kateri so bile ocenjene različne razpoložljive možnosti (nespremenjeno stanje, vodil bi ga Europol, center bi bil v lasti oziroma del Europolu, virtualni center). http://ec.europa.eu/home-affairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf

⁽²⁾ Sklep Sveta z dne 6. aprila 2009 o ustanovitvi Evropskega policijskega urada (Europol) (2009/371/PNZ).

⁽³⁾ Sporočilo za javnost z dne 28. marca 2012. Pogosto zastavljena vprašanja: novi Evropski center za boj proti kibernetски kriminaliteti. Sklic: MEMO/12/221. Datum: 28.3.2012. <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/221>

52. ENVP svetuje, da je treba jasno opredeliti pristojnosti EC3 in ni dovolj, da so samo navedene s sklicevanjem na pojem „računalniški kriminal“ iz veljavne zakonodaje o Europolu. Tudi opredelitev pristojnosti in zaščitnih ukrepov za varstvo podatkov v zvezi z EC3 mora biti del pregleda zakonodaje o Europolu. ENVP priporoča, naj Komisija do začetka veljavnosti nove zakonodaje o Europolu v poslovniku centra opredeli takšne pristojnosti in zaščitne ukrepe za varstvo podatkov. Ti bi lahko vključevali:

- jasno opredelitev, pri katerih nalogah obdelave podatkov (zlasti preiskavah in dejavnostih operativne podpore) bi lahko sodelovalo osebje centra, samostojno ali v sodelovanju s skupnimi preiskovalnimi skupinami, in
- jasne postopke, ki po eni strani zagotavljajo spoštovanje posameznih pravic (vključno s pravico do varstva podatkov), po drugi strani pa zagotavljajo jamstva, da so bili dokazi pridobljeni zakonito in jih je mogoče uporabiti na sodišču.

53. ENVP meni, da izmenjave osebnih podatkov med EC3 in „številnimi javnimi, zasebnimi in prosto dostopnimi akterji“ pomenijo posebna tveganja za varstvo podatkov, saj pogosto vključujejo obdelavo podatkov, ki se zbirajo za trgovinske namene, in mednarodne prenose podatkov. Ta tveganja so obravnavana v veljavnem Sklepu o ustanovitvi Europa, ki določa, da Europol načeloma ne sme izmenjevati podatkov neposredno z zasebnim sektorjem, s posebnimi mednarodnimi organizacijami pa le v zelo konkretnih okoliščinah.

54. ENVP glede na navedeno in zaradi pomena teh dveh dejavnosti za EC3 priporoča, da je treba v skladu z veljavnimi določbami iz Sklepa o ustanovitvi Europa zagotoviti ustrezne zaščitne ukrepe za varstvo podatkov. Te zaščitne ukrepe je treba vključiti v poslovník, ki ga bo opredelila skupina za ustanovitev EC3 (in pozneje v revidirani pravni okvir Europa), vendar nikakor ne smejo znižati ravni varstva podatkov.

V Bruslju, 29. junija 2012

Peter HUSTINX

Evropski nadzornik za varstvo podatkov
