EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Mnenje Evropskega nadzornika za varstvo podatkov o predlogu sklepa Evropskega parlamenta in Sveta o oblikovanju večletnega programa Skupnosti za zaščito otrok, ki uporabljajo internet in druge komunikacijske tehnologije

(2009/C 2/02)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti in zlasti člena 286 Pogodbe,

ob upoštevanju Listine o temeljnih pravicah Evropske unije in zlasti člena 8 Listine,

ob upoštevanju Direktive 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ([1]),

ob upoštevanju Uredbe (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov ([2]) ter zlasti člena 41 Uredbe,

ob upoštevanju zaprosila za mnenje v skladu s členom 28(2) Uredbe (ES) št. 45/2001, ki ga je 4. marca 2008 prejel od Evropske komisije –

SPREJEL NASLEDNJE MNENJE:

I. UVOD

Posvetovanje z evropskim nadzornikom za varstvo podatkov (ENVP)

1. Komisija je 4. marca 2008 poslala ENVP predlog sklepa Evropskega parlamenta in Sveta o oblikovanju večletnega programa Skupnosti za zaščito otrok, ki uporabljajo internet in druge komunikacijske tehnologije, (v nadaljnjem besedilu „predlog“) da bi se z njim posvetovala v skladu s členom 28(2) Uredbe (ES) št. 45/2001. V preambuli sklepa bi bilo treba to posvetovanje izrecno omeniti.

Predlog in njegovo ozadje

2. Nov večletni program (v nadaljnjem besedilu „program“) je bil predložen kot naslednik programov „Varnejši internet (1999–2004)“ in „Varnejši internet Plus (2005–2008)“.

3. V njem so opredeljene štiri smernice:

   — zmanjševanje nezakonite vsebine in obravnava škodljivega vedenja na spletu,

   — spodbujanje varnejšega spletnega okolja,

   — zagotavljanje ozaveščenosti javnosti,

   — vzpostavitev baze znanja.

4. Program naj bi bil usklajen z ustreznimi politikami, programi in ukrepi Skupnosti, ki naj bi jih tudi dopolnjeval. Glede na številne veljavne regulativne ukrepe na področju zaščite otrok v zvezi z novimi tehnologijami je ta program usmerjen bolj v ukrepanje kot urejanje. Poudarek je na učinkovitosti in uspešnosti pobud, ki jih je treba sprejeti, ter na prilagajanju razvoju novih tehnologij. S tega vidika predvideva okrepljeno izmenjavo informacij in najboljših praks.

5. Program se kot okvirni instrument ne poglablja v podrobnosti ukrepov, ki jih je treba sprejeti, temveč omogoča javne razpise za zbiranje predlogov in ponudb v skladu s štirimi opredeljenimi smernicami.

Bistveni elementi mnenja

6. Program je na splošno naravnan na obravnavo zaščite otrok, ki uporabljajo internet in druge komunikacijske tehnologije, brez posebnega poudarka na vidikih zasebnosti tega vprašanja ([3]). ENVP cilj predloga sicer v celoti podpira, v tem mnenju pa želi osvetliti te vidike zasebnosti.

([1]) UL L 281, 23.11.1995, str. 31.
([2]) UL L 8, 12.1.2001, str. 1.

([3]) Nekaj navedb glede zasebnosti je mogoče zaslediti v oceni učinka (3.2.2 Posebna tveganja: razkritje osebnih podatkov; 3.3 Ciljne skupine; 5.2 Analiza učinka političnih možnosti), vendar pa niso razdelane v večji meri.

7. Po mnenju ENVP je bistvenega pomena, da se načrtovane pobude uskladijo z obstoječim pravnim okvirom, kakor je naveden v predlogu ([1]), zlasti pa z Direktivo 2000/31/ES o elektronskem poslovanju, Direktivo 2002/58/ES o zasebnosti in elektronskih komunikacijah ter Direktivo 95/46/ES o varstvu podatkov ([2]).

8. Varstvo osebnih podatkov bi bilo treba upoštevati v zvezi z različnimi vidiki in različnimi akterji, ki so udeleženi v programu: seveda je glavno vprašanje varstvo osebnih podatkov otrok, vendar pa to vprašanje ni edino – upoštevati je treba tudi osebne podatke posameznikov in vsebine, ki se nadzorujejo zaradi zaščite otrok.

9. V tem mnenju se ta vprašanja obravnavajo na naslednji način:

   — v poglavju II se vzpostavlja povezava med varstvom podatkov in varnostjo otrok, pri čemer je poudarjeno, da je varstvo podatkov otrok nujno potrebno zaradi večje varnosti in preprečevanja zlorab,

   — v poglavju III mnenja je poudarjeno, da je obdelava osebnih podatkov neločljivo povezana tudi s prijavljanjem, filtriranjem ali blokiranjem sumljivih vsebin ali oseb na internetu:

      — v prvi točki se analizira vprašanje prijavljanja sumljivih oseb ali dejstev z vidika varstva podatkov,

      — druga točka je posvečena vlogi tehničnih orodij,

      — v zadnji točki se obravnava odgovornost sektorja glede na njegovo nadzorovanje podatkov uporabnikov in podatkov o vsebini.

II. VARSTVO OSEBNIH PODATKOV IN VARNOST OTROK

10. ENVP v celoti podpira cilj programa in opredeljene smernice, da bi okrepili zaščito otrok, ki uporabljajo internet. Zlasti zmanjšanje nezakonitih ali škodljivih vsebin ter dviganje ozaveščenosti otrok in drugih akterjev sta odločilna ukrepa, ki bi ju bilo treba dodatno razviti.

11. ENVP želi opozoriti, da je ustrezno varstvo osebnih podatkov otrok bistveni predukrep za zagotovitev varnosti pri uporabi interneta. Ta medsebojna povezanost zasebnosti in varnosti otrok je izrecno navedena v nedavni deklaraciji Odbora ministrov o „zaščiti dostojanstva, varnosti in zasebnosti otrok, ki uporabljajo internet“ ([3]). V deklaraciji je navedeno, da je za dobro počutje otrok nujno, da imajo pravico do dostojanstva, posebne zaščite in skrbi ter do „zaščite pred vsemi oblikami diskriminacije ali pred samovoljnimi ali nezakonitimi posegi v njihovo zasebnost ter pred nezakonitimi napadi na njihovo čast in ugled“.

12. V deklaraciji je kot primer tveganja, povezanega z zaščito zasebnosti otrok, navedena možnost sledenja dejavnostim otrok, zaradi katerih bi lahko bili ti izpostavljeni kriminalnim dejavnostim, na primer nadlegovanju zaradi spolnih namenov ali drugim nezakonitim dejavnostim. Tudi izdelava profilov in hramba osebnih podatkov v zvezi z dejavnostmi otrok sta prikazana kot možni izvor tveganja za zlorabe, na primer za poslovne namene ali pri iskanju izobraževalnih ustanov ali morebitnih delodajalcev. Deklaracija zato poziva k odstranitvi ali izbrisu vsebin ali sledi, ki jih otroci pustijo na internetu, v sprejemljivo kratkem roku, pa tudi k razvoju in spodbujanju obveščenosti otrok, zlasti o ustrezni uporabi orodij, ki zagotavljajo dostop do informacij, k razvijanju kritične analize vsebin in usvajanju ustreznih komunikacijskih spretnosti.

13. ENVP podpira te ugotovitve. Zlasti se mu zdi bistvenega pomena, da se dvigne ozaveščenost otrok glede tveganja, povezanega s spontanim posredovanjem osebnih podatkov, kot so pravo ime, starost ali kraj bivanja.

14. Točka 3 ukrepov ([4]), ki so predlagani v večletnem programu, je posebej posvečena „Zagotavljanju ozaveščanja javnosti“ z dejavnostmi za otroke, starše, skrbnike in učitelje, in sicer glede priložnosti in tveganj, povezanih z uporabo internetnih tehnologij in „načinov, kako na spletu ostati varen“. V predlogu sta med načini navedena tudi razširjanje ustreznih informacij in zagotavljanje kontaktnih točk, kjer starši in otroci lahko dobijo odgovore na vprašanja o tem, kako na spletu ostati varen; gre za uporabni orodji, v kateri bi bilo treba izrecno vključiti to razsežnost varstva osebnih podatkov otrok.

15. ENVP želi poudariti, da so v tem okviru ustrezni sogovorniki organi za varstvo podatkov. Ti bi morali biti omenjeni v predlogu, zlasti kjer ta predvideva spodbujanje sodelovanja in izmenjavo informacij, izkušenj in dobrih praks na ravni držav in na evropski ravni ([5]).

([1]) Obrazložitveni memorandum, 2.1. Zakonodajni okvir; Povzetek ocene učinka, 1.2 Trenutno stanje: zakonodaja.

([2]) — Direktiva 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu („Direktiva o elektronskem poslovanju“) (UL L 178, 17.7.2000, str. 1),
— Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37),
— Direktiva 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31).

([3]) Deklaracija Odbora ministrov z dne 20. februarja 2008, sprejeta na 1018. seji namestnikov ministrov; na voljo na naslovu: „wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)&Ver=0001“.

([4]) Priloga 1, Dejavnosti, točka 3.

([5]) Priloga 1, Dejavnosti, točka 1.

16. Kot ponazoritev zadnjih ukrepov, ki so bili v tem oziru sprejeti v državah članicah ali v državah članicah EGP, se lahko omeni več pobud. Švedski organ za varstvo podatkov vsako leto izvaja raziskavo o odnosu mladine do interneta in nadzora, organ za varstvo podatkov Združenega kraljestva ([1]) pa je prav tako izvedel raziskavo med 2000 otroci, starimi od 14 do 21 let. Norveški organ za varstvo podakov je skupaj z ministrstvom za izobraževanje januarja 2007 začel izobraževalno kampanjo za šole ([2]). Na Portugalskem sta organ za varstvo podatkov in ministrstvo za izobraževanje podpisala protokol o spodbujanju kulture za varstvo podatkov na internetu in zlasti družbenih mrežah ([3]). V okviru tega projekta so socialne mreže na Portugalskem vgradile vmesnik in vpeljale maskoto za otroke, stare od 10 do 15 let.

17. Ti primeri ponazarjajo aktivno in odločilno vlogo, ki jo imajo organi za varstvo podatkov pri zaščiti otrok na internetu, ter potrebo, da se otroci izrecno vključijo v večletni program kot sogovorniki.

III. VARSTVO OSEBNIH PODATKOV IN PRAVICE DRUGIH ZAINTERESIRANIH STRANI

I. *Prijavljanje in izmenjava informacij*

18. V prvi točki predloga („Zmanjševanje nezakonite vsebine in obravnava škodljivega vedenja na spletu“ ([4])) se kot eden glavnih ukrepov navaja zagotovitev kontaktnih točk za prijavljanje nezakonitih vsebin in škodljivega vedenja na spletu. Nesporno je, da je za učinkovito zoperstavljanje nezakonitim vsebinam ali škodljivemu vedenju o njih treba obvestiti pristojne organe. Kontaktne točke v zvezi z zaščito otrok so bile dejansko že vzpostavljene, obstajajo pa tudi, na primer, za boj proti neželeni elektronski pošti ([5]).

19. Ne glede na to pa ENVP ugotavlja, da je pojem škodljivih vsebin še nejasen: nikjer ni navedeno, kdo je odgovoren za opredelitev škodljive vsebine in v skladu s kakšnimi merili naj bi jo opredelil kot takšno. To je še toliko bolj zaskrbljujoče zaradi posledic, ki bi jih morebitna prijava takšne vsebine imela.

20. Poleg tega in kot je bilo že povedano, v okviru programa, kakršen je sedanji, niso na kocki le osebni podatki otrok, temveč tudi osebni podatki vseh posameznikov, na katere se na takšen ali drugačen način nanašajo informacije, ki krožijo po omrežju. Lahko bi šlo, na primer, za osebo, ki je osumljena neprimernega vedenja ali je prijavljena kot osumljena, ali pa tudi za osebo, ki prijavi sumljivo vedenje ali vsebino ali pa žrtvo zlorabe. Čeprav so te informacije potrebne zaradi učinkovitosti sistema prijavljanja, pa je po mnenju ENVP pomembno opozoriti, da jih je vedno treba obravnavati v skladu z načeli varstva podatkov.

21. Nekatere kočljive podatke bi morda bilo treba celo posebej zaščititi, saj bi lahko veljali za občutljive podatke v smislu člena 8 Direktive 95/46/ES. To bi lahko veljalo za podatke, povezane s kršitelji in tudi z žrtvami zlorab, zlasti v primeru otroške pornografije. Treba je ugotoviti, da je bilo treba na ravni držav spremeniti zakonodajo na področju varstva podatkov v zvezi z nekaterimi sistemi prijavljanja, da bi omogočili obdelavo pravosodnih podatkov osumljenih storilcev ali žrtev ([6]). ENVP vztraja pri tem, da je treba pri vzpostavljajočih se sistemih prijavljanja upoštevati obstoječi okvir varstva podatkov. Pri uskladitvi s tem okvirom so odločilni elementi izkazan javni interes in zagotovila glede nadzorovanja sistema, načeloma s strani organov kazenskega pregona.

II. *Vloga tehničnih orodij z vidika zasebnosti*

22. Uporaba tehničnih orodij se spodbuja kot ena od rešitev za obravnavanje nezakonitih vsebin in škodljivega ravnanja ([7]). Primeri takšnih orodij so navedeni v oceni učinka ([8]), vključno z orodji za ugotavljanje starosti, prepoznavanje obrazov (s čimer lahko organi kazenskega pregona ugotavljajo istovetnost žrtev) ali tehnologijami za filtriranje. V skladu s predlogom bi bilo treba ta orodja bolje prilagoditi praktičnim potrebam in ustreznim zainteresiranim stranem omogočiti dostop do njih.

23. ENVP se je že jasno zavzel ([9]) za uporabo novih tehnologij, da bi okrepili varstvo pravic posameznikov. Po njegovem mnenju bi moralo biti načelo spoštovanja zasebnosti že pri načrtovanju neločljiv del tehnološkega razvoja, ki zadeva obdelavo osebnih podatkov. ENVP zaradi tega zelo spodbuja pripravo projektov, s katerimi bi se tehnologije razvijale v tem smislu.

24. Bistvenega pomena je razvoj sistemov, v okviru katerih se bo kar najbolj omejilo razkrivanje osebnih podatkov otrok, s čimer jim bo zagotovljena zanesljiva zaščita, ustrezno temu pa tudi možnost, da uporabljajo nova orodja informacijske družbe, na primer družbene mreže, na varnejši način.

([1]) Glej „www.ico.gov.uk/youngpeople“
([2]) Glej „www.dubestemmer.no“
([3]) Glej „dadus.cnpd.pt“
([4]) Priloga 1 predloga.
([5]) Glej na primer spletno stran, ki so jo v te namene postavili belgijski organi: www.ecops.be
([6]) Glej člen 3(6) belgijskega zakona o varstvu podatkov z dne 8. decembra 1992 v zvezi z obdelavo podatkov s strani centra za prijavljanje pogrešanih ali spolno zlorabljenih otrok.
([7]) Priloga 1, Dejavnosti, točka 1.
([8]) Ocena učinka, točka 3.1.
([9]) Letno poročilo ENVP za leto 2006, del 3.5.1 Tehnološki razvoj.

25. Vseeno pa je treba opozoriti, da imajo tehnološka orodja lahko različne učinke na posameznike, odvisno od načina njihove uporabe. Če se uporabljajo za filtriranje ali blokiranje informacij, lahko otrokom preprečijo dostop do morebitno škodljivih vsebin, nekomu drugemu pa dostop do informacij, do katerih je upravičen.

26. Tudi če je tu najpomembnejše vprašanje pravica dostopa do informacij, so z vidika zasebnosti še vedno prisotne posledice. Filtriranje, zlasti najnovejši razvoj v zvezi z njim, tj. uporaba upravljanja identitete, lahko dejansko deluje na podlagi določenih meril, vključno z osebnimi podatki, na primer starostjo posameznika, priključenega na omrežje (da se prepreči dostop odraslih ali otrok do posebnih vsebin), vsebino informacij in podatki o prometu, povezani z identiteto avtorja informacij. Odvisno od tega, kako bodo te osebne informacije (samodejno) obdelane, bi za zadevne posameznike to lahko imelo posledice v zvezi z njihovo pravico do internetnega komuniciranja.

27. Filtriranje ali orodje za blokiranje, s katerima se nadzoruje dostop do omrežij, je treba torej uporabljati previdno in pri tem upoštevati njune možne škodljive učinke ter v celoti izkoristiti možnosti za okrepitev zasebnosti, ki jih ponuja tehnologija.

28. ENVP pozdravlja natančno razlago iz ocene učinka ([1]), v skladu s katero naj nobena od predlaganih možnosti ne bi okrnila pravice do zasebnosti in svobode izražanja. Strinja se tudi s tam navedenim stališčem, da je eden od glavnih ciljev spodbujanje vloge uporabnika, tj. „ozaveščanje za sprejemanje boljših odločitev in ustreznih ukrepov“, da bi zaščitili otroke ([2]).

III. *Odgovornost ponudnikov storitev*

29. V predlogu velja sodelovanje med vsemi zainteresiranimi strani za nujen element pri krepitvi zaščite otrok, ki uporabljajo komunikacijske tehnologije. Predlog ([3]) predvideva v zvezi s temi zainteresiranimi stranmi sodelovanje in pritegnitev sektorja, zlasti v okviru samoregulacije.

30. Glede na to, da je ta gospodarski sektor odgovoren za zagotavljanje telekomunikacijskih storitev in storitev v zvezi z vsebinami, bi lahko imel določen vpliv na prijavljanje, filtriranje ali blokiranje informacij, kadar te veljajo za nezakonite ali škodljive. Možno pa je, da bi se s pravnega vidika lahko sprožile razprave o tem, do kakšnega obsega bi mu dejansko lahko zaupali takšno nalogo.

31. Seveda je z vidika ozaveščanja otrok in drugih zadevnih akterjev, na primer staršev ali učiteljev, sodelovanje sektorja seveda dobrodošlo. Bistven vidik odgovornosti ponudnikov vsebin je tudi vzpostavljanje alarmnih sistemov in določitev moderatorjev za internetne strani, ki lahko izključijo neprimerne vsebine.

32. V zvezi s ponudniki *telekomunikacijskih* storitev je mogoče razpravljati o vprašanju spremljanja telekomunikacij, najsi bo to z vidika nadzora vsebin, zaščitenih s pravicami intelektualne lastnine, kot tudi drugih nezakonitih vsebin. V zvezi s tem se zastavlja vprašanje vpletenosti poslovnega akterja, ki ponuja posebno (telekomunikacijsko) storitev, v okolju, v katerem naj načeloma ne bi deloval, tj. pri nadzoru vsebin telekomunikacij. ENVP opozarja, da takšnega nadzora načeloma ne bi smeli opravljati ponudniki storitev, nikakor pa ga ne bi smeli opravljati sistematično. Kadar je to potrebno zaradi posebnih okoliščin, bi to načeloma morala biti naloga organov kazenskega pregona.

33. Delovna skupina iz člena 29 je v mnenju z dne 18. januarja 2005 opozorila, da v zvezi s tem vprašanjem ([4]) v skladu s členom 15 Direktive 2000/31/ES o elektronskem poslovanju ponudnikom storitev informacijske družbe ni mogoče naložiti sistematične obveznosti nadzora in sodelovanja. (…) Kakor je navedeno v členu 8 direktive o varstvu podatkov, se podatki v zvezi s prekrški, kazenskimi obsodbami ali varnostnimi ukrepi lahko obdelujejo le pod strogimi pogoji, ki jih uveljavijo države članice. Medtem ko je jasno, da ima posameznik pravico do obdelave pravosodnih podatkov v postopku pravdnega spora, v katerem je sam udeležen, pa načelo ne dopušča, da bi tretje strani temljito preiskovale, zbirale ali na enem mestu združevale osebne podatke, zlasti in vključno s splošnim sistematičnim raziskovanjem, na primer s pregledovanjem interneta (…). Takšna preiskava spada v pristojnost pravosodnih organov.

34. Na področju, kjer gre za svobodo govora, dostop do informacij, zasebnost in druge temeljne pravice, se zaradi vpletenosti zasebnih akterjev zastavlja vprašanje sorazmernosti uporabljenih sredstev. Evropski parlament je pred kratkim sprejel resolucijo, v kateri je poudaril, da je treba najti rešitev, ki bo v skladu s temeljnimi pravicami posameznikov ([5]). V točki 23 resolucije je navedel, da „je internet obsežna platforma za kulturno izražanje, dostop do znanja in demokratično udeležbo pri evropskemu ustvarjanju, ki z informacijsko družb povezuje generacije; [Parlament] poziva Komisijo in države članice, naj se izogibajo sprejemanju ukrepov, ki so v nasprotju z državljanskimi svoboščinami in človekovimi pravicami ter z načeli sorazmernosti, učinkovitosti in odvračanja, kot je na primer prekinitev dostopa do interneta“.

([1]) Ocena učinka, točka 5.2.

([2]) V tem smislu naj bi filtre vklopili starši, možno pa bi jih bilo tudi izklopiti, tako da bi odrasli v celoti nadzorovali učinke filtriranja.

([3]) Uvodna izjava 8 preambule; Priloga 1.4, točka 1; Povzetek ocene učinka, točka 3.1.

([4]) Delovni dokument Delovne skupine iz člena 29 o vprašanjih varstva podatkov, povezanih s pravicami intelektualne lastnine, WP 104.

([5]) Resolucija Evropskega parlamenta z dne 10. aprila 2008 o kulturnih industrijah v Evropi (2007/2153(INI)), točka 23.

35. ENVP meni, da je treba uravnotežiti legitimen cilj boja proti nezakonitim vsebinam in ustrezno naravo uporabljenih sredstev. Opozarja, da bi moral biti vsakršen ukrep nadzorovanja telekomunikacijskih omrežij, če je to potrebno v posebnih primerih, naloga organov kazenskega pregona.

IV. **SKLEP**

36. ENVP podpira predlog za večletni program za zaščito otrok, ki uporabljajo internet in druge komunikacijske tehnologije. Pozdravlja dejstvo, da naj bi se ta program osredotočil na razvoj novih tehnologij in na pripravo konkretnih ukrepov za okrepitev učinkovitosti zaščite otrok.

37. ENVP opozarja, da je varstvo osebnih podatkov bistveni predpogoj za varnost otrok na internetu. Preprečiti je treba zlorabo osebnih podatkov otrok, in sicer z uporabo smernic, predlaganih v programu, zlasti pa z naslednjim:

— zagotoviti ozaveščenost otrok in drugih zainteresiranih strani, na primer staršev in učiteljev,

— spodbuditi oblikovanje najboljših praks v sektorju,

— spodbuditi razvoj tehnoloških orodij, ustreznih z vidika zasebnosti,

— spodbuditi izmenjavo dobrih praks in praktičnih izkušenj med ustreznimi organi, tudi med organi za varstvo podatkov.

38. Pri pripravi teh ukrepov ne bi smeli spregledati dejstva, da zaščita otrok poteka v okolju, kjer bi lahko bile ogrožene pravice drugih. Kakršnokoli pobudo za zbiranje, blokiranje ali prijavljanje informacij bi bilo treba sprejeti le ob spoštovanju temeljnih pravic vseh vpletenih posameznikov in v skladu s pravnim okvirom za varstvo podatkov. ENVP zlasti opozarja, da bi moralo biti nadzorovanje telekomunikacijskih omrežij, če je to potrebno v posebnih okoliščinah, naloga organov kazenskega pregona.

39. ENVP ugotavlja, da je ta program splošni okvir za nadaljnje konkretne ukrepe. Meni, da so nekatere ugotovitve iz tega mnenja le prvi korak in bi jih lahko v skladu s smernicami iz programa v praksi še nadalje razvili v zvezi s projekti, ki jih je še treba vzpostaviti. Priporoča, da se pri opredelitvi teh praktičnih projektov k sodelovanju pritegnejo organi za varstvo podatkov. Sklicuje se tudi na dejavnosti Delovne skupine iz člena 29 v zvezi s tem vprašanjem, zlasti pa tudi na potekajoče delo delovne skupine za družbene mreže ([1]).

V Bruslju, 23. junij 2008

Peter HUSTINX

Evropski nadzornik za varstvo podatkov

([1]) Glej delovni dokument št. 1/2008 z dne 18. februarja 2008 o varstvu osebnih podatkov otrok, WP 147, za bolj splošni pregled pa delovni program delovne skupine za leti 2008–2009, vključno v zvezi z družbenimi mrežami, na voljo na naslovu: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm