Mnenje Evropskega nadzornika za varstvo podatkov o sporočilu Komisije Evropskemu parlamentu in Svetu o območju svobode, varnosti in pravice za državljane

(2009/C 276/02)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

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

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

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

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 ter zlasti člena 41 uredbe –

SPREJEL NASLEDNJE MNENJE:

I. UVOD

1. Komisija je 10. junija 2009 sprejela Sporočilo Evropskemu parlamentu in Svetu o območju svobode, varnosti in pravice za državljane ([1]). ENVP je pripravil to mnenje v skladu s členom 41 Uredbe (ES) št. 45/2001.

2. Pred sprejetjem sporočila se je Komisija neuradno posvetovala z ENVP; pismo je bilo poslano 19. maja 2009. ENVP je odgovoril 20. maja 2009 in neuradno predlagal dodatne izboljšave besedila Komisije. Poleg tega je aktivno sodeloval pri pripravi pisma o večletnem programu za področje varnosti, svobode in pravice, ki ga je 14. januarja 2009 poslala Delovna skupina za policijo in pravosodje. ([2])

3. V sporočilu (prvo poglavje) je poudarjeno, da Unija „potrebuje nov večletni program, ki bi bil na podlagi napredka in izkušenj, pridobljenih iz obstoječih pomanjkljivosti, ambiciozno zasnovan v prihodnost. V tem novem programu bo treba določiti prednostne naloge za prihodnjih pet let.“ Ta večletni program (ki je že poznan kot stockholmski program) bo nadaljevanje programa iz Tampereja in haaškega programa, ki sta dala močan politični zagon območju svobode, varnosti in pravice.

4. Sporočilo naj bi zasnovalo temelje tega novega večletnega programa. ENVP v tej zvezi ugotavlja, da večletni programi kljub temu, da niso zavezujoči instrumenti, precej vplivajo na politike, ki jih institucije razvijajo na zadevnem področju, ker iz njih izvirajo številni konkretni zakonodajni in nezakonodajni ukrepi.

5. Sporočilo je treba obravnavati s tega vidika. Predstavlja novo fazo v razpravi, za katero bi lahko rekli, da se je začela junija 2008 s poročiloma t. i. skupine za prihodnost notranjih zadev, ki jo je ustanovilo predsedstvo Sveta in naj bi bila vir novih idej: „Svoboda, varnost, zasebnost – evropske notranje zadeve v odprtem svetu“ ([3]) in „Predlagane rešitve za prihodnji program EU na področju pravosodja“ ([4]).

II. GLAVNA VSEBINA MNENJA

6. To mnenje ni samo odziv na sporočilo ampak tudi prispevek ENVP k splošni razpravi o prihodnosti območja svobode, varnosti in pravice, na podlagi katere mora biti, kot je napovedalo švedsko predsedstvo EU, pripravljen nov strateški delovni program (stockholmski program) ([5]). V njem so obravnavane tudi nekatere posledice morebitnega začetka veljavnosti Lizbonske pogodbe.

7. V delu III so opisani najpomembnejše vidiki, ki so obravnavani v mnenju, v delu IV pa je ocena sporočila.

8. V delu V je obravnavano vprašanje, kako zagotoviti dosledno varstvo zasebnosti in osebnih podatkov med vse intenzivnejšo izmenjavo osebnih podatkov. Obravnavano je zlasti poglavje 2.3 sporočila, ki se nanaša na varstvo osebnih podatkov in zasebnosti, ter splošneje tudi potreba po dodatnih zakonodajnih in nezakonodajnih ukrepih za izboljšanje okvira za varstvo podatkov.

([1]) COM(2009) 262 konč. (v nadaljnjem besedilu: sporočilo).

([2]) Ni objavljeno. Delovno skupino za policijo in pravosodje je ustanovila Evropska konferenca pooblaščencev za varstvo podatkov, da bi pripravljala njena stališča na področju kazenskega pregona in v nujnih primerih delovala v njenem imenu.

([3]) Dokument Sveta št. 11657/08. V nadaljnjem besedilu „poročilo o notranjih zadevah“.

([4]) Dokument Sveta št. 11549/08 („poročilo o pravosodju“).

([5]) Delovni program vlade za EU, http://www.sweden.gov.se

9. V delu VI mnenja so obravnavane potrebe in možnosti za hrambo informacij kot sredstev v kazenskem pregonu, dostop do njih in njihovo izmenjavo, oziroma, če uporabimo izraz iz sporočila, „Evropa, ki varuje“. V četrtem poglavju sporočila je navedenih več ciljev v zvezi s pretokom informacij in tehnološkimi orodji, zlasti v podpoglavjih 4.1.2 (nadzor pretoka informacij), 4.1.3 (uporaba potrebnih tehnoloških orodij) in 4.2.3.2 (informacijski sistemi). Lahko bi rekli, da je v tej zvezi najzahtevnejši predlog za razvoj evropskega informacijskega modela (v podpoglavju 4.1.2), ki ga ENVP obravnava zelo podrobno.

10. V delu VII je na kratko obravnavano posebno vprašanje v okviru območja svobode, varnosti in pravice, ki je pomembno z vidika varstva podatkov, tj. dostop do pravnega varstva in e-pravosodje.

III. **OBRAVNAVANI VIDIKI**

11. Sporočilo in bolj na splošno prihodnost območja svobode, varnosti in pravice, oblikovano v novem večletnem programu, sta v tem mnenju analizirana zlasti z vidika potrebe po varstvu temeljnih pravic. Poleg tega mnenje temelji na prispevkih, ki jih je ENVP dal k razvoju politike EU na tem področju predvsem v okviru svoje svetovalne vloge. ENVP je sprejel že več kot trideset mnenj in pripomb o pobudah, ki izhajajo iz haaškega programa; objavljena so na spletni strani urada.

12. Pri oceni sporočila je ENVP upošteval zlasti v nadaljevanju opisane štiri vidike, ki so bistveni za prihodnost območja svobode, varnosti in pravice. Vsi imajo ključno vlogo tudi v sporočilu.

13. Prvi vidik je izjemno naraščanje števila digitalnih informacij o državljanih, ki je posledica razvoja informacijskih in komunikacijskih tehnologij ([6]). Družba postaja t. i. „družba nadzorovanja“, ki vodi digitalne evidence o skoraj vseh transakcijah in skoraj vseh dejavnostih državljanov. Tako se z uporabo oznak RFID že hitro razvijajo t. i. „internet stvari“ in „inteligentna okolja“. Vse bolj se uporablja digitalizacija telesnih značilnosti (biometrika). Svet je vse bolj povezan, organizacije za javno varnost pa imajo dostop do velikega števila potencialno koristnih informacij, kar lahko neposredno vpliva na življenje posameznikov, na katere se te informacije nanašajo.

14. Drugi vidik je internacionalizacija. Po eni strani v digitalni dobi izmenjava podatkov ni omejena z zunanjimi mejami Evropske unije, po drugi strani pa je vse bolj potrebno mednarodno sodelovanje pri številnih dejavnostih EU na področju svobode, varnosti in pravice, med drugim pri preprečevanju terorizma, policijskem in pravosodnem sodelovanju ter civilnem pravosodju in nadzoru meja.

15. Tretji vidik je uporaba podatkov pri kazenskem pregonu: zaradi terorističnih in drugih groženj, s katerimi se družba sooča v zadnjem času, imajo organi kazenskega pregona (zahteve za) več možnosti za zbiranje, hranjenje in izmenjavo osebnih podatkov. V številnih primerih so dejavno vključeni zasebniki, kot je *inter alia* razvidno iz direktive o hrambi podatkov ([7]) in različnih instrumentov v zvezi s podatki PNR ([8]).

16. Četrti vidik je prosto gibanje. Postopni razvoj območja svobode, varnosti in pravice zahteva nadaljnjo ukinitev notranjih meja in odstranitev morebitnih ovir za prosto gibanje. Novi instrumenti na tem področju v nobenem primeru ne bi smeli ponovno postavljati ovir. V tem okviru prosto gibanje vključuje na eni strani prosto gibanje oseb in na drugi strani prost pretok (osebnih) podatkov.

17. Vsi štirje vidiki kažejo, da se okolje, v katerem se uporabljajo informacije, hitro spreminja, zato ni dvoma o tem, da je potreben močan mehanizem za zaščito temeljnih pravic državljanov ter zlasti za varstvo zasebnosti in podatkov. Zato se je ENVP odločil, kot je navedeno v točki 11, v analizi največ pozornosti nameniti potrebi po varstvu.

([6]) V poročilu o notranjih zadevah je uporabljen izraz „digitalni cunami“.

([7]) Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES, UL L 105, 13.4.2006, str. 54.

([8]) Glej Sporazum med Evropsko unijo in Združenimi državami Amerike o obdelavi in prenosu podatkov iz evidence imen letalskih potnikov (Passenger Name Record, PNR) s strani letalskih prevoznikov Ministrstvu Združenih držav za domovinsko varnost (2007 Sporazum PNR), UL L 204, 4.8.2007, str. 18, in predlog okvirnega sklepa Sveta o uporabi evidence podatkov o potnikih (PNR) za kazenski pregon, COM(2007) 654 konč.

IV. **SPLOŠNA OCENA**

18. V sporočilu in stockholmskem programu so določeni cilji EU za naslednjih pet let, ki bi lahko imeli tudi dolgoročnejši učinek. ENVP ugotavlja, da je sporočilo napisano tako, da sprejetje oziroma nesprejetje Lizbonske pogodbe nanj ne bo imelo učinka. Popolnoma razume odločitev Komisije za takšen pristop, vendar hkrati obžaluje, da v sporočilu niso v celoti upoštevane dodatne možnosti, ki jih ponuja Lizbonska pogodba. V mnenju so poudarjene perspektive, ki jih daje Lizbonska pogodba.

19. Sporočilo temelji na rezultatih ukrepov EU na območju svobode, varnosti in pravice v zadnjih letih. Ti rezultati so dogodkovno pogojeni, poudarek je na ukrepih, ki razširjajo pristojnosti organov kazenskega pregona in posegajo v vsakodnevno življenje državljanov. To velja zlasti na področjih z intenzivno uporabo in izmenjavo osebnih podatkov, kjer je varstvo podatkov bistvenega pomena. Rezultati so dogodkovno pogojeni, saj zunanji dogodki, kot so 11. september ter bombna napada v Madridu in Londonu, močno vplivajo na zakonodajne dejavnosti. Prenos podatkov o potnikih v Združene države, na primer, je mogoče razumeti kot posledico 11. septembra ([9]), posledica bombnih napadov v Londonu pa je bilo sprejetje direktive o hrambi podatkov 2006/24/ES ([10]). Poudarek je bil na ukrepih, ki bolj posegajo v vsakodnevno življenje ljudi, ker se je zakonodajalec EU usmeril na ukrepe za lažjo uporabo in izmenjavo podatkov, medtem ko obravnava ukrepov za zagotovitev varstva osebnih podatkov ni bila tako nujna. Najpomembnejši zaščitni ukrep, ki je bil sprejet po treh letih razprav v Svetu, je Okvirni sklep Sveta 2008/977/PNZ o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah ([11]). Ta okvirni sklep Sveta ni v celoti zadovoljiv (glej točki 29–30).

20. Izkušnje, pridobljene v zadnjih letih, dokazujejo, da je treba pred sprejetjem novih instrumentov preučiti njihov vpliv na organe kazenskega pregona in evropske državljane. Pri tem je treba ustrezno upoštevati vpliv na zasebnost in učinkovitost kazenskega pregona; to je potrebno najprej pri pripravi in obravnavi predlogov, pa tudi izvajanje teh aktov je treba v ta namen redno pregledovati). Preučitev vplivov je bistvena tudi pred sprejetjem večletnega programa, v katerem so določeni kratkoročni cilji.

21. ENVP z zadovoljstvom ugotavlja, da je v sporočilu varstvo temeljnih pravic in zlasti osebnih podatkov opredeljeno kot eno ključnih vprašanj za prihodnost območja svobode, varnosti in pravice. V drugem poglavju sporočila je EU opredeljena kot edinstveno območje z vidika varstva temeljnih pravic, ki temeljijo na skupnih vrednotah. Prav tako je pozitivno, da je pristop k Evropski konvenciji o človekovih pravicah opredeljen kot prednostno vprašanje – celo kot prvo prednostno vprašanje v sporočilu. Pristop je pomemben za zagotovitev usklajenega in povezanega sistema za varstvo temeljnih pravic. Nenazadnje, varstvo podatkov ima v sporočilu ima pomembno mesto.

22. Ta usmeritev je dokaz, da je pomemben cilj sporočila zagotovitev varstva pravic državljanov in – s tem – bolj uravnotežen pristop. Vlade potrebujejo ustrezne instrumente za zagotovitev varnosti državljanov, vendar morajo v evropski družbi v celoti spoštovati njihove temeljne pravice. „Za državljane“ ([12]) pomeni, da mora Evropska unija ohraniti to uravnoteženost.

23. ENVP meni, da je ta uravnoteženost, vključno s potrebo po varstvu podatkov, v sporočilu zelo dobro upoštevana. Prav tako je ugotovljeno, da se je treba preusmeriti. To je pomembno, saj politike na območju svobode, varnosti in pravice ne bi smele spodbujati postopnega razvoja v družbo nadzorovanja. ENVP pričakuje, da bo Svet sprejel enak pristop v stockholmskem programu, med drugim tudi s sprejetjem smernic iz točke 25 tega mnenja.

24. To je še toliko bolj pomembno, ker je območje svobode, varnosti in pravice območje, ki „oblikuje življenjske okoliščine državljanov, zlasti zasebno področje njihove lastne odgovornosti ter politične in socialne varnosti, zavarovane s temeljnimi pravicami“, kakor je bilo poudarjeno v nedavni odločbi nemškega Zveznega ustavnega sodišča z dne 30. junija 2009, ki se nanaša na Lizbonsko pogodbo. ([13])

([9]) Sporazum PNR iz leta 2007, naveden v prejšnji opombi, in ustrezni predhodni sporazumi.

([10]) Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES, UL L 105, 13.4.2006, str. 54. Čeprav je pravna podlaga člen 95 ES, je bilo sprejetje direktive neposreden odziv na bombne napade v Londonu.

([11]) Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, UL L 350, 30.12.2008, str. 60.

([12]) Glej naslov sporočila.

([13]) Sporočilo za javnost št. 72/2009 z dne 30. junija 2009 Zveznega ustavnega sodišča Nemčije, odst. 2 (c).

25. ENVP poudarja, da bi bilo treba na takšnem območju:

— informacije med organi držav članic ter med ustreznimi evropskimi organi ali zbirkami podatkov, izmenjevati na osnovi ustreznih in učinkovitih mehanizmov, ki v celoti spoštujejo temeljne pravice državljanov in zagotavljajo vzajemno zaupanje.

— To zahteva dostopnost informacij in vzajemno priznavanje pravnih sistemov držav članic (in EU) ter usklajenost standardov za varstvo informacij, ki se lahko med drugim zagotovi s skupnim okvirom za varstvo podatkov.

— Ti skupni standardi naj se ne bi uporabljali samo v situacijah s čezemejnimi razsežnostmi. Vzajemno zaupanje je možno le, če so standardi zanesljivi in dosledno spoštovani ter ni tveganja, da bi se v primeru, če čezmejna razsežnost ne bi bila (več) prisotna, prenehali uporabljati. Poleg tega razlike med „notranjimi" in „čezmejnimi" podatki v praksi ne obstajajo, zlasti ne pri uporabi informacij ([14]).

V. **INSTRUMENTI ZA VARSTVO PODATKOV**

V.1 **Za vsestranski mehanizem za varstvo podatkov**

26. ENVP podpira strateški pristop, ki varstvu podatkov namenja pomembno mesto v sporočilu. Veliko pobud na območju svobode, varnosti in pravice dejansko temelji na uporabi osebnih podatkov in učinkovito varstvo podatkov je bistveno za njihov uspeh. Spoštovanje zasebnosti in varstvo podatkov nista samo pravna obveznost, ki je na ravni EU vse bolj priznana, ampak tudi vprašanje, ki je glede na podatke Eurobarometra ([15]) bistvenega pomena za evropske državljane. Poleg tega je omejitev dostopa do osebnih podatkov bistvena za zagotovitev zaupanja organov pregona.

27. V podpoglavju 2.3. sporočila je navedeno, da mora vsestranski mehanizem za varstvo podatkov zajemati vsa področja, ki so v pristojnosti EU ([16]). ENVP popolnoma podpira ta cilj, ne glede na to, ali bo Lizbonska pogodba začela veljati. Poleg tega ugotavlja, da takšen sistem ne pomeni nujno, da naj bi se za vse obdelave podatkov uporabljal en sam okvir. Glede na trenutno veljavne pogodbe so možnosti za sprejetje enega samega vsestranskega pravnega okvira, ki bi se uporabljal za vse obdelave, omejene zaradi strukture stebrov in dejstva, da so – vsaj v prvem stebru – podatki, ki jih obdelujejo evropske institucije, varovani na posebni pravni podlagi (člen 286 PES). Kljub temu pa ENVP opozarja, da bi z določenimi izboljšavami lahko popolnoma izkoristili možnosti, ki jih nudijo veljavne pogodbe, kot je bilo poudarjeno že v sporočilu Komisije „Izvajanje haaškega programa – pot naprej" ([17]). Ko bo začela veljati Lizbonska pogodba, bo ustrezna pravna podlaga za en sam vsestranski pravni okvir, ki se bo uporabljal za vse obdelave podatkov, člen 16 Pogodbe o delovanju EU.

28. ENVP ugotavlja, da je v vsakem primeru bistveno zagotoviti usklajenost pravnega okvira za varstvo podatkov, po potrebi z uskladitvijo in konsolidacijo različnih pravnih instrumentov, ki se uporabljajo na območju svobode, varnosti in pravice.

V skladu z veljavnimi pogodbami

29. Prvi korak je bilo nedavno sprejetje okvirnega sklepa Sveta 2008/977/PNZ ([18]), čeprav ta pravni instrument v bistvu ni vsestranski okvir, ker njegove določbe niso splošno uporabne. Ne uporabljajo se v notranjih primerih, ko osebni podatki izvirajo iz države članice, ki jih uporablja. Če se države članice ne bodo odločile za vključitev notranjih primerov v nacionalno izvedbeno zakonodajo – kar se verjetno ne bo zgodilo –, bo ta omejitev zmanjšala dodano vrednost okvirnega sklepa Sveta.

30. Drugi razlog, zaradi katerega ENVP meni, da Okvirni sklep Sveta 2008/977/PNZ ne vsebuje zadovoljivega okvira za varstvo podatkov na območju svobode, varnosti in pravice, je dejstvo, da več bistvenih določb ni v skladu z Direktivo 95/46/ES. V skladu z veljavnimi pogodbami bi drugi korak lahko bila razširitev področja uporabe in povezava okvirnega sklepa Sveta z navedeno direktivo.

31. Dodatni zagon pri uresničevanju vsestranskega mehanizma za varstvo podatkov bi lahko dosegli z določitvijo jasne dolgoročne vizije, ki bi lahko vključevala splošen in usklajen pristop za določitev zbiranja in izmenjave podatkov – ter uporabo obstoječih zbirk podatkov – in hkrati

([14]) ENVP je podrobno obravnaval to zadnjo točko v mnenju z dne 19. decembra 2005 o Predlogu okvirnega sklepa Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (COM(2005) 475 konč.), UL C 47, 25.2.2006 str. 27., odst. 30–32.

([15]) Varstvo podatkov v Evropski uniji – mnenje državljanov – analitično poročilo, *Flash Eurobarometer Series 225*, januar 2008, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) Glej tudi prednostna vprašanja sporočila.

([17]) COM(2006) 331 konč., 28. junija 2006.

([18]) Glej opombo 11.

jamstva za varstvo podatkov. Na ta način bi preprečili nepotrebno prekrivanje in podvajanje instrumentov (in s tem obdelave osebnih podatkov). To bi tudi pospešilo usklajevanje politik EU na zadevnem področju ter okrepilo zaupanje državljanov v način, kako javni organi ravnajo z njihovimi podatki. ENVP priporoča Svetu, naj v stockholmskem programu potrdi, da je potrebna jasna dolgoročna vizija.

32. Nadalje ENVP priporoča, da bi bilo treba oceniti že sprejete ukrepe na tem področju, njihovo konkretno izvajanje in učinkovitost, ter nanje pogledati v pravi luči. Pri tej oceni bi bilo treba ustrezno upoštevati njihov učinek na zasebnost in učinkovitost kazenskega pregona. Če bi se v teh ocenah izkazalo, da se z nekaterimi ukrepi ne dosegajo predvideni rezultati ali rezultati niso sorazmerni s predvidenimi cilji, bi bilo treba razmisliti o naslednjem:

— Najprej o spremembi ali razveljavitvi ukrepov, če se izkaže, da niso upravičeni in ne prinašajo dodane vrednosti za organe kazenskega pregona in evropske državljane.

— Nato bi bilo treba preučiti možnosti za boljšo uporabo obstoječih ukrepov.

— Novi zakonodajni ukrepi naj bi bili predlagani šele v tretji fazi, če bi se izkazalo, da so potrebni za uresničevanje zastavljenih ciljev. Novi instrumenti naj bi bili sprejeti samo v primeru, če bi prinašali jasno in konkretno dodano vrednost za organe kazenskega pregona in evropske državljane.

ENVP priporoča, naj se v stockholmskem programu navede sistem za oceno obstoječih ukrepov.

33. Nenazadnje pa je treba posebej poudariti pomen doslednejšega izvajanja obstoječih zaščitnih ukrepov v skladu s sporočilom Komisije o nadaljevanju delovnega programa za boljše izvajanje direktive o varstvu podatkov ([19]) in predlogov ENVP v mnenju o tem sporočilu ([20]). V okviru tretjega stebra Komisija žal nima možnosti, da bi začela postopke v primeru kršitev.

V skladu z Lizbonsko pogodbo

34. V Lizbonski pogodbi je predviden resnično vsestranski okvir za varstvo podatkov. V členu 16.2 Pogodbe o delovanju Evropske unije je določeno, da Evropski parlament in Svet po rednem zakonodajnem postopku določata pravila v zvezi z obdelavo osebnih podatkov s strani institucij, organov, uradov in agencij Unije ter držav članic in zasebnih strank v okviru dejavnosti s področja uporabe prava Unije.

35. Glede na to, da je v sporočilu vsestranskemu mehanizmu za varstvo podatkov namenjeno pomembno mesto, ENVP meni, da je namen Komisije predlagati pravni okvir, ki se bo uporabljal za vse obdelave podatkov. ENVP v celoti podpira ta cilj, ki zagotavlja večjo skladnost sistema in pravno varstvo ter s tem učinkovitejše varstvo podatkov. Zlasti pa bi se s takšnim sistemom izognili težavam pri ločevanju med stebri, ki nastanejo, kadar se podatki, zbrani za komercialne namene v zasebnem sektorju, uporabljajo za namene kazenskega pregona. Ločnica med stebri dejansko ne ustreza popolnoma resničnosti, kar dokazujeta tudi odločbi Sodišča v zvezi s PNR ([21]) in hrambo podatkov ([22]).

36. ENVP predlaga, da se to načelo vsestranskega mehanizma za varstvo podatkov poudari v stockholmskem programu, saj dokazuje, da takšen mehanizem ni samo prednostna naloga, ampak je nujen glede na različne prakse pri obdelavi podatkov. Predlaga, da se v stockholmski program kot prednostna naloga vključi potreba po novem zakonodajnem okviru, ki bo *inter alia* nadomestil tudi Okvirni sklep Sveta 2008/977/PNZ.

37. ENVP poudarja, da vsestranski mehanizem za varstvo podatkov, ki temelji na splošnem zakonodajnem okviru, ne izključuje sprejetja dodatnih predpisov za varstvo podatkov v policijskem in pravosodnem sektorju. V teh dodatnih predpisih bi lahko upoštevali posebne potrebe na področju kazenskega pregona, kot je predvideno v izjavi št. 21, ki je priložena Lizbonski pogodbi. ([23])

V.2 **Preoblikovanje načel varstva podatkov**

38. V sporočilu je ugotovljeno, da tehnološke spremembe vplivajo na komunikacijo med posamezniki ter javnimi in zasebnimi organizacijami. Komisija meni, da je zato treba preoblikovati številna temeljna načela varstva podatkov.

([19]) COM(2007) 87 konč. z dne 7. marca 2007.

([20]) Mnenje z dne 25. julija 2007, OJ C 255, 27.10.2007, str. 1, zlasti točka 30.

([21]) Sodba Sodišča z dne 30. maja 2006, Evropski parlament proti Svetu Evropske unije (C-317/04) in Komisiji Evropskih skupnosti (C-318/04), združeni zadevi C-317/04 in C-318/04, Zbirka odločb, [2006], stran I-4721.

([22]) Odločba sodišča z dne 10. februarja 2009, Irska proti Evropskemu parlamentu in Svetu Evropske unije, zadeva C-301/06, še ni objavljena.

([23]) Glej izjavo št. 21 o varstvu osebnih podatkov na področju pravosodnega sodelovanja v kazenskih zadevah in policijskega sodelovanja, dodano sklepni listini Medvladne konference, ki je sprejela Lizbonsko pogodbo, UL C 115, 9.5.2008, str. 345.

39. ENVP pozitivno ocenjuje te cilje sporočila. Izredno koristna bi bila ocena učinkovitosti teh načel z vidika tehnoloških sprememb. Najprej je treba opozoriti, da preoblikovanje in potrditev načel varstva podatkov ni zmeraj neposredno povezano s tehnološkim razvojem. Lahko bi bilo potrebno tudi iz drugih razlogov, navedenih v delu III, kot so internacionalizacija, vse večja uporaba podatkov za namene kazenskega pregona in prosto gibanje.

40. Poleg tega ENVP meni, da bi bila ta ocena lahko vključena v javno posvetovanje, ki ga je napovedala Komisija na konferenci „Osebni podatki – večja uporaba, večja zaščita“ 19. in 20. maja 2009. To javno posvetovanje bi lahko dalo pomembne rezultate ([24]). ENVP predlaga, naj Svet v stockholmskem programu in Komisija v javnih izjavah o posvetovanju poudarita povezavo med cilji sporočila iz podpoglavja 2.3 in javnim posvetovanjem o prihodnosti varstva podatkov.

41. Takšna ocena bi lahko vključevala naslednje točke:

— Osebni podatki na območju svobode, varnosti in pravice so lahko zelo občutljivi; to velja med drugim za podatke o kazenskih obsodbah, policijske podatke in biometrične podatke, kot so prstni odtisi in profili DNK.

— Obdelava takšnih podatkov lahko ima neprijetne posledice za posameznike, na katere se podatki nanašajo, zlasti glede na to, da imajo organi kazenskega pregona pooblastila za prisilne ukrepe. Poleg tega je spremljanje in analiziranje podatkov vse bolj avtomatizirano, pogosto brez človeškega posredovanja. Tehnologija omogoča uporabo podatkovnih zbirk z osebnimi podatki za splošna iskanja (ruderjenje in profiliranje podatkov itd.) Treba bi bilo jasno določiti pravne obveznosti, na katerih temelji obdelava podatkov.

— Zakonodaja v zvezi z varstvom podatkov temelji na tem, da se lahko podatki zbirajo za posebne namene in se ne morejo uporabljati na način, ki ni združljiv s temi nameni. Uporaba za druge namene bi lahko bila dovoljena samo, če je tako določeno v zakonu in potrebno za zaščito določenih javnih interesov, kot so tisti iz člena 8.2. EKČP.

— Treba je spoštovati načelo omejitve namena, kar lahko vpliva na sedanje trende pri uporabi podatkov. Za namene kazenskega pregona se uporabljajo podatki, ki jih zasebna podjetja v telekomunikacijskem, prometnem in finančnem sektorju zbirajo za komercialne namene. Poleg tega se uporabljajo, na primer na področju priseljevanja in nadzorovanja meja, obsežni informacijski sistemi. Dovoljene so povezave in dostop do podatkovnih zbirk, kar pomeni razširitev osnovnega namena, za katerega so bili podatki zbrani. Treba je preučiti sedanje trende, po potrebi tudi možne prilagoditve in/ali dodatne zaščitne ukrepe.

— Poleg načel varstva podatkov, ki so navedeni v sporočilu, bi bilo treba v oceni upoštevati, da je treba zagotoviti preglednost obdelave, ki omogoča posameznikom, na katere se podatki nanašajo, uveljavljanje pravic. Preglednost je zelo problematično vprašanje na področju kazenskega pregona, zlasti zato ker jo je treba presojati glede na tveganja za preiskave.

— Treba bi bilo tudi najti rešitve za izmenjavo podatkov s tretjimi državami.

42. V oceni bi bilo treba tudi preučiti možnosti za zagotovitev večje učinkovitosti uresničevanja načel varstva podatkov. V tej zvezi bi bilo koristno, da bi se usmerili na instrumente, ki lahko povečajo odgovornosti upravljavcev podatkov. Ti bi morali omogočati popolno odgovornost upravljavcev podatkov za njihovo upravljanje. V tej zvezi je koristen pojem „upravljanje podatkov“, ki zajema vsa pravna, tehnična in organizacijska sredstva, s katerimi organizacije zagotavljajo popolno odgovornost za način ravnanja s podatki, kot je načrtovanje in nadzor, uporaba zvočne tehnologije, primerno usposabljanje osebja, revizije skladnosti itd.

V.3 **Tehnologije, ki spoštujejo zasebnost (privacy aware technologies)**

43. ENVP je zadovoljen, da je v podpoglavju 2.3 sporočila navedeno certificiranje za varstvo zasebnosti. Poleg tega bi lahko navedli tudi načelo spoštovanja zasebnosti pri načrtovanju sistemov (privacy by design) in potrebo po določitvi najboljših razpoložljivih tehnologij za varstvo podatkov v okviru EU.

44. ENVP meni, da bi s spoštovanjem zasebnosti pri načrtovanju sistemov in tehnologijami, ki spoštujejo zasebnost, lahko zagotovili boljše varstvo in učinkovitejšo uporabo informacij. ENVP predlaga dve možnosti nadaljnjega razvoja, ki se ne izključujeta:

— certificiranje za varstvo zasebnosti in podatkov ([25]) za razvijalce in uporabnike informacijskih sistemov, ki je lahko financirano iz sredstev EU in podprto z zakonodajo EU ali ne,

([24]) Delovna skupina za varstvo podatkov iz člena 29, v kateri sodeluje ENVP, se je odločila, da si bo intenzivno prizadevala prispevati k temu javnemu posvetovanju.

([25]) Primer takega sistema je Evropski pečat zaupnosti.

— pravna obveznost razvijalcev in uporabnikov informacijskih sistemov, da uporabljajo sisteme, ki so skladni z načelom zasebnosti pri načrtovanju. V ta namen bi bilo morda treba razširiti področje uporaba zakonodaje na področju varstva podatkov, da bi bili razvijalci sistemov odgovorni za sisteme, ki jih razvijajo. ([26])

ENVP predlaga, da se ti možnosti navedeta v stockholmskem programu.

V.4 **Zunanji vidiki**

45. V sporočilu sta obravnavana tudi razvoj in promocija mednarodnih standardov za varstvo podatkov. V tem času se izvajajo številne dejavnosti, med drugim v okviru mednarodne konference pooblaščencev za zasebnost in varstvo podatkov, katerih namen je priprava izpolnljivih in splošno uporabnih standardov. Na tej podlagi bi lahko v bližnji prihodnosti sprejeli mednarodni sporazum. ENVP predlaga, da se te dejavnosti podprejo v stockholmskem programu.

46. V sporočilu je navedeno tudi sklepanje dvostranskih sporazumov na podlagi napredka, doseženega v sodelovanju z Združenimi državami. Tudi ENVP meni, da je potreben jasen pravni okvir za prenos podatkov v tretje države in je zato pozdravil skupna prizadevanja organov EU in ameriških oblasti v okviru skupine na visoki ravni v zvezi s čezatlantskim instrumentom za varstvo podatkov, hkrati pa je poudaril, da je treba pojasniti posebna vprašanja in jim nameniti več pozornosti ([27]). S tega stališča so zanimive tudi pobude iz poročila o notranjih zadevah v zvezi z evroatlantskim območjem svobode, varnosti in pravice, o katerem naj bi se EU v skladu s tem poročilom odločila do leta 2014. Takšno območje ne bi moglo obstajati brez ustreznih jamstev za varstvo podatkov.

47. ENVP meni, da bi bilo treba z evropskimi standardi za varstvo podatkov, ki temeljijo na konvenciji Sveta Evrope št. 108 o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov ([28]) ter sodni praksi Sodišča Evropskih skupnosti in Sodišča za človekove pravice, določiti raven varstva podatkov v splošnem sporazumu z Združenimi državami o varstvu in izmenjavi podatkov. Takšen splošni sporazum bi lahko bil temelj za posebne sporazume o izmenjavi osebnih podatkov. To je še toliko bolj pomembno glede na cilj iz podpoglavja 4.2.1 sporočila, v katerem je določeno, da mora EU skleniti sporazum o policijskem sodelovanju, kadar je to potrebno.

48. ENVP popolnoma razume, da je treba okrepiti mednarodno sodelovanje, včasih tudi z državami, ki ne zagotavljajo varstva temeljnih pravic. Kljub temu ([29]) je nujno upoštevati, da bi takšno mednarodno sodelovanje še povečalo obseg zbiranja in mednarodnega prenosa podatkov. Zato je bistveno, da za zbiranje in prenos osebnih podatkov prek meja Unije veljajo načela poštene in zakonite obdelave – kot tudi splošna načela predpisanega postopka – in da se osebni podatki posredujejo tretjim državam ali mednarodnim organizacijam samo, če zadevne tretje strani zagotovijo ustrezno stopnjo varstva ali druge primerne zaščitne ukrepe.

49. Nazadnje ENVP priporoča, da se v stockholmskem programu poudari pomen splošnih sporazumov z Združenimi državami in drugimi tretjimi državami o varstvu in izmenjavi podatkov, ki morajo temeljiti na ravni varstva, ki je zajamčena na ozemlju EU. V širšem smislu ENVP opozarja na pomen aktivne promocije spoštovanja temeljnih pravic in zlasti varstva podatkov v odnosih s tretjimi državami in mednarodnimi organizacijami. ([30]) Poleg tega bi lahko v stockholmskem programu na splošno navedli, da je treba pri izmenjavi podatkov s tretjimi državami zagotoviti ustrezno raven varstva podatkov ali druge zaščitne ukrepe v teh tretjih državah.

VI. **UPORABA INFORMACIJ**

VI.1 **Za evropski informacijski model**

50. Boljša izmenjava informacij je najpomembnejši politični cilj Evropske unije na območju svobode, varnosti in pravice. V podpoglavju 4.1.2 sporočila je poudarjeno, da je varnost v Evropski uniji odvisna od učinkovitih mehanizmov za izmenjavo informacij med nacionalnimi organi in drugimi evropskimi akterji. Da je poudarek na izmenjavi informacij, je logično glede na to, da ni evropskih policijskih sil, evropskega sistema za kazensko pravosodje in evropskega nadzora meja. Ukrepi, ki se nanašajo na informacije, so

([26]) Uporabniki informacij so zajeti v zakonodajo o varstvu podatkov kot upravljavci ali obdelovalci podatkov.

([27]) Glej mnenje ENVP z dne 11. novembra 2008 o končnem poročilu Kontaktne skupine na visoki ravni EU-ZDA za izmenjavo informacij ter varstvo zasebnosti in osebnih podatkov, UL C 128, 6.6.2009, str. 1.

([28]) ETS št. 108, 28.1.1981.

([29]) Glej pismo ENVP z dne 28. novembra 2005 o sporočilu Komisije o zunanjih vidikih območja svobode, varnosti in pravice na spletni strani urada.

([30]) Nedavna sodna praksa glede seznamov teroristov so dokaz, da so jamstva potrebna – tudi v odnosih z Združenimi državami – da se zagotovi skladnost ukrepov za preprečevanje terorizma s standardi EU o temeljnih pravicah (združeni zadevi C-402/05 P in C-415/05 P, Kadi and Al Barakaat Foundation proti Svetu, odločba z dne 3. septembra 2008, še ni objavljena.

torej bistveni prispevek Evropske unije, ki omogoča organom držav članic obravnavo čezmejnega kriminala in učinkovito varstvo zunanjih meja. Vendar pa ne prispevajo samo k varnosti državljanov ampak tudi k njihovi svobodi – prosto gibanje oseb je bilo v tem mnenju je že omenjeno – in pravici.

51. Prav zato je bilo v haaški program vključeno načelo dostopnosti, v skladu s katerim ne bi smelo biti ovir pri prenosu informacij, ki so potrebne za boj proti kriminalu, preko notranjih meja EU. Nedavne izkušnje dokazujejo, da je bila uvedba tega načela v zakonodajne ukrepe težavna. Svet ni sprejel predloga Komisije za okvirni sklep Sveta z dne 12. oktobra 2005 o izmenjavi informacij v skladu z načelom dostopnosti ([31]). Države članice niso bile pripravljene v celoti sprejeti posledic izvajanja načela dostopnosti. Namesto tega so bili sprejeti bolj omejeni instrumenti ([32]), kot je Sklep Sveta 2008/615/PNZ z dne 23. junija 2008 o poglobitvi čezmejnega sodelovanja, zlasti na področju boja proti terorizmu in čezmejnemu kriminalu (sklep k Prümski pogodbi) ([33]).

52. Čeprav je bilo načelo dostopnosti bistvo haaškega programa, se je Komisija, kot kaže, odločila za zmernejši pristop. Da bi dodatno spodbudili izmenjavo informacij med organi držav članic, je predvidela uvedbo evropskega informacijskega modela. Švedsko predsedstvo EU zagovarja enak pristop ([34]). Predstavilo bo predlog strategije za izmenjavo informacij. Svet je že začel pripravljati ambiciozni projekt v zvezi s strategijo Evropske unije za upravljanje informacij, ki je tesno povezana z evropskim informacijskim modelom. ENVP z velikim zanimanjem spremlja ta prizadevanja in poudarja, da je v navedenih projektih treba posebno pozornost nameniti vidiku varstva podatkov.

Evropski informacijski model in varstvo podatkov

53. Najprej je treba poudariti, da prihodnost območja svobode, varnosti in pravice ne bi smela biti tehnološko pogojena, tj. da bi bilo treba nove tehnološke možnosti, ki so skoraj neomejene, zmeraj preverjati glede na ustrezna načela varstva podatkov in jih uporabljati samo v primeru, če so skladna s temi načeli.

54. ENVP ugotavlja, da informacijski model, ki ga predlaga Komisija, ni samo tehnološki model: ima tudi velike zmogljivosti za strateško analizo ter boljše zbiranje in obdelavo operativnih informacij. Prav tako priznava, da bi moral biti model skladen z načeli varstva podatkov, hkrati pa bi bilo treba upoštevati vidike, ki se navezujejo na politiko, kot so načela za zbiranje, izmenjavo in obdelavo informacij.

55. Bistveni so – in bodo tudi v prihodnje – informacijska tehnologija in pravni pogoji. ENVP pozitivno ocenjuje izhodišče sporočila, v skladu s katerim evropski informacijski model ne sme temeljiti na tehničnih vidikih. Bistveno je, da se informacije zbirajo, izmenjujejo in obdelujejo samo, če je to dejansko potrebno zaradi varnosti in so upoštevana načela varstva podatkov. ENVP se tudi popolnoma strinja, da je treba določiti mehanizem za nadaljnje ukrepanje, tj. preverjanje izmenjave informacij. Predlaga, naj Svet navedene elemente podrobno obravnava v stockholmskem programu.

56. V tej zvezi ENVP poudarja, da varstva podatkov, katerega cilj je zaščita državljanov, ne bi smeli obravnavati kot škodljivega za upravljanje podatkov. Zagotavlja pomembna orodja za boljšo hrambo, dostopnost in izmenjavo informacij. Pravica posameznika, na katerega se podatki nanašajo, do obveščenosti o tem, kateri podatki v zvezi z njim se obdelujejo, in pravica do popravka nepravilnih podatkov lahko prispevata k večji točnosti podatkov v sistemih za upravljanje podatkov.

57. Zakonodaja na področju varstva podatkov v bistvu vpliva na naslednje: podatke je mogoče uporabiti za posebne in upravičene namene; če namen ni točno določen, se ne smejo uporabljati. V prvem primeru se lahko zgodi, da je treba sprejeti dodatne zaščitne ukrepe.

58. Kljub temu pa ima ENVP kritično pripombo, ker je v sporočilu „opredelitev prihodnjih potreb“ v veliki meri obravnavana kot del informacijskega modela. Poudarja, da bi bilo tudi v prihodnje pri razvoju informacijskih sistemov treba upoštevati načelo omejitve namena ([35]). To je eno najpomembnejših jamstev, ki ga sistem za varstvo podatkov zagotavlja državljanu. Ta mora imeti možnost, da je vnaprej seznanjen z namenom, za katerega se zbirajo njegovi podatki, in zagotovilo, da se bodo uporabljali, predvsem v prihodnosti, izključno za ta namen. To jamstvo je določeno celo v členu 8 Listine o temeljnih pravicah Unije. Načelo omejitve namena omogoča izjeme – ki so zlasti primerne na območju svobode, varnosti in pravice –, vendar te izjeme ne smejo določati oblike sistema.

([31]) COM(2005) 490 konč.
([32]) Z vidika dostopnosti sklep k Prümski pogodbi vključuje daljnosežne določbe o uporabi biometričnih podatkov (DNK in prstni odtisi).
([33]) UL L 210, 6.8.2008, str. 1.
([34]) Glej delovni program vlade za EU iz opombe 5, str. 23.
([35]) Glej točko 41.

Izbira prave arhitekture

59. Najprej je treba izbrati pravo arhitekturo sistema za izmenjavo informacij. Da je to pomembno, je ugotovljeno tudi v sporočilu (podpoglavje 4.1.3), žal pa se nanaša samo na interoperabilnost.

60. ENVP poudarja drug vidik: v okviru evropskega informacijskega modela morajo biti zahteve za varstvo podatkov sestavni del razvoja sistema in ne samo nujen pogoj za njegovo zakonitost ([36]). Treba je upoštevati načelo spoštovanja zasebnosti pri načrtovanju sistemov in določiti „najboljše razpoložljive tehnologije“ ([37]), kot je navedeno v točki 43. Evropski informacijski model mora temeljiti na teh konceptih. Natančneje to pomeni, da bi morali pri razvoju informacijskih sistemov, oblikovanih za namene javne varnosti, zmeraj upoštevati načelo spoštovanja zasebnosti pri načrtovanju sistemov. ENVP priporoča, naj Svet te elemente vključi v stockholmski program.

Interoperabilnost sistemov

61. ENVP poudarja, da interoperabilnost ni samo tehnično vprašanje, ampak vpliva tudi na varstvo državljanov in zlasti podatkov. Z vidika varstva podatkov ima interoperabilnost sistemov, če je dobro izvedena, jasne prednosti, saj preprečuje podvajanje hrambe. Prav tako pa je jasno, da lahko dejstvo, da sta dostop do podatkov ali njihova izmenjava tehnično omogočena, velikokrat spodbudi *de facto* dostopanje do podatkov ali njihovo izmenjavo. Drugače povedano: interobilnost predstavlja določeno tveganje za povezavo podatkovnih zbirk, ki imajo različne namene ([38]). Lahko vpliva na stroge omejitve namena podatkovnih zbirk.

62. Na kratko, samo dejstvo, da je izmenjava digitalnih informacij med interoperabilnimi podatkovnimi zbirkami ali združevanje teh zbirk izvedljivo, ne upravičuje izjem pri spoštovanju načela omejitve namena. V konkretnih primerih bi morala interoperabilnost temeljiti na jasnih in previdnih političnih odločitvah. ENVP predlaga, da se to navede v stockholmskem programu.

VI.2 **Uporaba informacij, ki so bile zbrane za druge namene**

63. V sporočilu ni izrecno obravnavana ena najpomembnejših teženj v zadnjih letih, tj. uporaba podatkov, zbranih za poslovne namene v zasebnem sektorju, za namene kazenskega pregona. Ta težnja ni opazna samo pri prenosu elektronskih sporočil in podatkov o potnikih, ki letijo v (nekatere) tretje države ([39]), ampak tudi v finančnem sektorju. Kot primer lahko navedemo Direktivo 2005/60/ES Evropskega parlamenta in Sveta z dne 26. oktobra 2005 o preprečevanju uporabe finančnega sistema za pranje denarja in financiranje terorizma ([40]). Drug dobro znan primer, o katerem je bilo veliko razprav, se nanaša na Združenje za svetovne finančne telekomunikacije med bankami (SWIFT) ([41]), ki obdeluje osebne podatke za namene programa nadzora nad financiranjem terorizma, ki ga izvaja finančno ministrstvo ZDA.

64. ENVP meni, da je te težnje treba posebej obravnavati v stockholmskem programu. Lahko bi rekli, da predstavljajo odstopanja od načela omejitve namena in pogosto močno posegajo v zasebnost, saj uporaba teh podatkov lahko razkrije veliko informacij o vedenju posameznikov. V vseh primerih, kjer se predlagajo takšni ukrepi, mora biti zelo jasno dokazano, da je takšen ukrep poseganja v zasebnost potreben. Če dokazi obstajajo, je treba zagotoviti, da bodo v celoti zaščitene pravice posameznikov.

65. ENVP meni, da se osebni podatki, zbrani v poslovne namene, lahko uporabljajo za namene kazenskega pregona samo pod strogimi pogoji, kot so:

— podatki se uporabljajo za natančno določene namene, kot je preprečevanje terorizma ali hudih kaznivih dejanj, ki se določijo za vsak primer posebej,

— podatki naj bi se prenašali raje po metodi „*push*“ in ne po metodi „*pull*“ ([42]),

([36]) Glej „Smernice in merila za razvoj, izvajanje in uporabo tehnologij za boljše varovanje zasebnosti“ iz projekta PRISE (http://www.prise.oeaw.ac.at).

([37]) Najboljše razpoložljive tehnologije pomenijo najučinkovitejše in najbolje razvite dejavnosti ter njihove metode delovanja, ki kažejo praktično primernost posameznih tehnologij, s katerimi se načeloma lahko zagotovi, da bodo sistemi informacijske tehnologije in njihove aplikacije skladni z načeli varstva zasebnosti in podatkov ter z varnostnimi zahtevami, določenimi v regulativnem okviru EU.

([38]) Glej tudi pripombe ENVP v zvezi s sporočilom Komisije o interoperabilnosti evropskih podatkovnih zbirk z dne 10. marca 2006, objavljeno na spletni strani http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

([39]) Glej točko 15.

([40]) UL L 309, 25.11.2005, str. 15.

([41]) Glej Mnenje 10/2006 o obdelavi osebnih podatkov Družbe za svetovne medbančne finančne telekomunikacije (SWIFT), ki ga je pripravila Delovna skupina iz člena 29.

([42]) Pri metodi „*push*“ (potisk) upravljavec podatkov pošlje („potisne“) podatke na zahtevo organa kazenskega pregona. Pri metodi „*pull*“ (poteg) ima organ kazenskega pregona dostop do podatkovne zbirke upravljavca in izloči („potegne“) informacije iz podatkovne zbirke. V tem primeru upravljavec težje prevzame odgovornost.

— zahteve za podatke bi morale biti sorazmerne in ozko usmerjene ter temeljiti na sumu v zvezi z določenimi osebami,

— treba bi se bilo izogibati rutinskim iskanjem, rudarjenju podatkov in profiliranju,

— vsaka uporaba podatkov za namene kazenskega pregona bi morala biti zabeležena, da se omogoči učinkovit nadzor njihove uporabe s strani posameznikov, ki uveljavljajo svoje pravice, organov za varstvo podatkov in sodnih organov.

VI.3 **Informacijski sistemi in organi EU**

Informacijski sistemi s centralizirano ali decentralizirano hrambo ([43])

66. V zadnjih letih se je število informacijskih sistemov na območju svobode, varnosti in pravice, ki temeljijo na zakonodaji EU, zelo povečalo. Včasih so sprejete odločitve o vzpostavitvi sistema s centralizirano hrambo podatkov na evropski ravni, v drugih primerih je v zakonu predvidena samo izmenjava informacij med nacionalnimi podatkovnimi zbirkami. Schengenski informacijski sistem je verjetno najboljši primer sistema s centralizirano hrambo. Sklep Sveta 2008/615/PNZ (sklep k Prümski pogodbi) ([44]) je z vidika varstva podatkov najpomembnejši primer sistema z decentralizirano hrambo, saj predvideva obsežno izmenjavo biometričnih podatkov med organi držav članic.

67. V sporočilu je prikazano, da se bo ta težnja vzpostavljanja novih sistemov ohranila. Prvi primer, ki je opisan v podpoglavju 4.2.2, je informacijski sistem, ki razširja Evropski sistem za izmenjavo informacij med kazenskimi evidencami (ECRIS) na državljane držav, ki niso članice EU. Komisija je že naročila raziskavo v zvezi s pripravo evropskega spiska državljanov tretjih držav (EICTCN), ki bi lahko bil v prihodnosti osnova za centralizirano podatkovno zbirko. Drugi primer je izmenjava informacij o posameznikih v registrih plačilne nesposobnosti iz drugih držav članic, ki imajo decentralizirano hrambo, v okviru e-pravosodja (podpoglavje 3.4.1 sporočila).

68. Decentraliziran sistem bi imel določene prednosti z vidika varstva podatkov. Preprečuje podvojeno hrambo podatkov na ravni organov držav članic in v centraliziranem sistemu, hkrati je tudi jasno določena odgovornost za te podatke, saj je upravljavec organ države članice, nadzor pa lahko izvajajo pravosodni organi in organi za varstvo podatkov na ravni držav članic. Pomanjkljivosti tega sistema pa se kažejo pri izmenjavi podatkov z drugimi pristojnimi organi, na primer pri zagotavljanju, da se podatki redno posodabljajo tako v državi izvora kot v namembni državi ter da obe državi izvajata učinkovit nadzor. Še bolj zapleteno je zagotavljanje odgovornosti za tehnični sistem za izmenjavo. Te pomanjkljivosti je mogoče odpraviti z odločitvijo za centralizirani sistem, za katerega bi bili vsaj deloma (na primer za tehnično infrastrukturo) odgovorni evropski organi.

69. V tej zvezi bi bilo treba pripraviti vsebinska merila za odločanje o tem, ali naj bi bili sistemi centralizirani ali decentralizirani, in zagotoviti jasne in previdne politične odločitve v konkretnih primerih. Ta merila bi lahko prispevala k delovanju sistemov in k varstvu podatkov državljanov. ENVP predlaga, da se priprava navedenih meril vključi med cilje stockholmskega programa.

Obsežni informacijski sistemi

70. V podpoglavju 4.2.3.2 sporočila je na kratko opisana prihodnost obsežnih informacijskih sistemov, poudarek pa je na schengenskem informacijskem sistemu (SIS I) in vizumskem informacijskem sistemu (VIS).

71. V podpoglavju 4.2.3.2. je navedeno tudi, da bo poleg programov za registrirane potnike vzpostavljen tudi sisteme elektronskega evidentiranja vstopov na ozemlje držav članic in izstopov z njega. Komisija je ta sistem napovedala že prej, in sicer kot del „svežnja ukrepov o upravljanju meja“, ki je bil pripravljen na pobudo podpredsednika Frattinija ([45]). ENVP je v predhodnih pripombah ([46]) precej kritično ocenil ta predlog, ker v njem ni bilo v zadostni meri dokazano, da je poleg že obstoječih obsežnih sistemov potreben tudi ta sistem, ki bi močno posegal v zasebnost državljanov. Ugotavlja, da ni dodatnih dokazov o potrebnosti takšnega sistema in zato predlaga Svetu, naj te pobude ne vključi v stockholmski program.

72. V tej zvezi želi ENVP opozoriti na svoja mnenja o različnih pobudah na področju izmenjave informacij v EU ([47]), v katerih je navedel številne predloge in pripombe v zvezi z vplivom uporabe obsežnih podatkovnih zbirk na varstvo podatkov v EU. Med drugim je posebej poudaril, da je

([43]) Centralizirana hramba v tej zvezi pomeni hrambo na centralni evropski ravni, decentralizirana pa hrambo na ravni držav članic.
([44]) Glej opombo 33.
([45]) Sporočilo Komisije „Priprava naslednjih ukrepov pri upravljanju meja v Evropski uniji“, 13.2.2008, COM(2008) 69.
([46]) Predhodne pripombe ENVP v zvezi s tremi sporočili Komisije o upravljanju meja (COM(2008) 69, COM(2008) 68 in COM(2008) 67), 3.3.2008 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf
([47]) Še zlasti Mnenje z dne 23. marca 2005 o predlogu uredbe Evropskega parlamenta in Sveta o Vizumskem informacijskem sistemu (VIS) in izmenjavi podatkov o vizumih za kratkoročno prebivanje med državami članicami, UL C 181, 23.7.2005, str. 13 in Mnenje z dne 19. oktobra 2005 o treh predlogih v zvezi z drugo generacijo Schengenskega informacijskega sistema (SIS II), UL C 91, 19.4.2006, str. 38.

pred pripravo predlogov ali sprejetjem ukrepov na tem področju treba zagotoviti močne in po meri oblikovane zaščitne ukrepe ter da so sorazmerne ocene vpliva nujne. ENVP je zmeraj zagovarjal pravilno uravnoteženost, usklajeno s pravili varstva podatkov, med varnostnimi zahtevami in varstvom zasebnosti posameznikov, katerih podatki so vneseni v sisteme. Enako stališče je zavzel v vlogi nadzornika centralnih delov sistema.

73. Poleg tega želi ENVP ob tej priložnosti poudariti, da je potreben dosleden pristop k celotni izmenjavi informacij v EU z vidika pravne doslednosti, tehnične usklajenosti in enotnega nadzora obstoječih sistemov in sistemov v razvoju. Dejansko je danes bolj kot kdaj prej jasno, da je potrebna pogumna in celovita vizija glede načina izmenjave informacij v EU in prihodnjih obsežnih informacijskih sistemov. Samo na tej osnovi je mogoče ponovno obravnavati sistem elektronskega evidentiranja vstopov na ozemlje držav članic in izstopov z njega.

74. ENVP predlaga, naj se med cilje stockholmskega programa vključi razvoj takšne vizije, ki bi morala vključevati tudi morebiten začetek veljavnosti Lizbonske pogodbe in njen vpliv na sisteme, ki temeljijo na pravni podlagi prvega in tretjega stebra.

75. V sporočilu je navedena tudi ustanovitev nove agencije, ki naj bi bila pristojna tudi za sistem elektronskega evidentiranja vstopov in izstopov. Medtem je Komisija sprejela predlog za ustanovitev te agencije. ([48]) ENVP načeloma podpira ta predlog, ker zagotavlja učinkovitejše delovanje teh sistemov, vključno z varstvom podatkov, in bo pravočasno pripravil mnenje o njem.

Europol in Eurojust

76. Vloga Europola je v sporočilu navedena na več mestih; poudarjeno je, da je njegova prednostna naloga osrednja vloga pri usklajevanju, izmenjavi informacij in usposabljanju strokovnjakov. Poleg tega so v podpoglavju 4.2.2. omenjene nedavne spremembe pravnega okvira za sodelovanje med Eurojustom in Europolom in najavljena prihodnja prizadevanja za nadaljnjo krepitev Eurojusta, zlasti v zvezi s preiskavami na področju čezmejnega organiziranega kriminala. ENVP v celoti podpira te cilje pod pogojem, da bodo ustrezno upoštevani zaščitni ukrepi za varstvo podatkov.

([48]) Predlog Komisije z dne 24. junija 2009 za uredbo Evropskega parlamenta in Sveta o ustanovitvi Agencije za operativno upravljanje schengenskega informacijskega sistema (SIS II), vizumskega informacijskega sistema (VIS), EURODAC in drugih obsežnih informacijskih sistemov na področju svobode, varnosti in pravice COM(2009) 293/2).

77. V tej zvezi ENVP pozitivno ocenjuje nov osnutek sporazuma med Europolom in Eurojustom ([49]), katerega cilj je izboljšati in okrepiti vzajemno sodelovanje ter zagotoviti učinkovito izmenjavo informacij med obema organoma. V tem osnutku ima ključno vlogo učinkovito varstvo podatkov.

VI.4 **Uporaba biometričnih podatkov**

78. ENVP ugotavlja, da v sporočilu ni obravnavano vprašanje vse intenzivnejše uporabe biometričnih podatkov v različnih pravnih instrumentih Evropske unije o izmenjavi informacij, med drugim tudi v instrumentih o vzpostavitvi obsežnih informacijskih sistemov. To je obžalovanja vredno, ker je vprašanje zelo pomembno in občutljivo z vidika varstva podatkov in zasebnosti.

79. Čeprav ENVP priznava, da ima uporaba biometričnih podatkov določene prednosti, neprestano poudarja, da lahko takšna uporaba bistveno vpliva na pravice posameznikov, na katere se podatki nanašajo, in zato predlaga vključitev strogih zaščitnih ukrepov pri uporabi biometričnih podatkov v posameznih sistemih. V tej zvezi daje koristne podatke, zlasti glede upravičenosti in omejitev uporabe biometričnih podatkov, nedavna odločba Sodišča za človekove pravice v zadevi *S. and Marper proti Združenemu Kraljestvu* ([50]). Zlasti pri uporabi informacij o DNK se lahko razkrijejo občutljive informacije o posameznikih; pri tem je treba upoštevati, da se tehnične možnosti pridobivanja informacij iz DNK še razvijajo. V primeru uporabe biometričnih podatkov v obsežnih informacijskih sistemih so težave tudi zaradi nepravilnosti pri zbiranju in primerjavi teh podatkov. Zato bi morala EU kot zakonodajalec omejiti njihovo uporabo.

80. Drugo vprašanje, ki se zastavlja v zadnjih letih, se nanaša na uporabo prstnih odtisov otrok in starejših oseb, zaradi pomanjkljivosti biometričnih sistemov pri uporabi za ti starostni skupini. ENVP je predlagal poglobljeno raziskavo, v kateri naj bi določili natančnost sistemov ([51]). Za otroke je predlagal starostno omejitev 14 let, ki naj bi veljala, če v raziskavi ne bodo pridobljeni drugačni dokazi. ENVP predlaga, da se to vprašanje vključi v stockholmski program.

([49]) Osnutek sporazuma, ki ga je odobril Svet, morata podpisati obe strani. Glej register Sveta na spletni strani http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf http://register.consilium.europa.eu/pdf/en/09/st10/st10107.en09.pdf

([50]) Združeni zadevi 30562/04 in 30566/04, S. and Marper proti Združenemu kraljestvu, odločba z dne 4. decembra 2008, ESČP še ni objavljena.

([51]) Mnenje z dne 26. marca 2008 o predlogu uredbe Evropskega parlamenta in Sveta o spremembi Uredbe Sveta (ES) št. 2252/2004 o standardih za varnostne značilnosti in biometrične podatke v potnih listih in potovalnih dokumentih, ki jih izdajo države članice, UL C 200, 6.8.2008, str. 1.

81. Glede na navedeno ENVP predlaga, da bi bilo koristno razviti vsebinska merila za uporabo biometričnih podatkov, s katerimi bi zagotovili, da so bodo podatki uporabljali samo, kadar je to potrebno in primerno ter v skladu z načeli sorazmernosti in kadar zakonodajalec predhodno dokaže jasen, točno določen in zakonit namen uporabe. Natančneje rečeno: uporaba biometričnih podatkov in podatkov o DNK ne bi smela biti dovoljena, če je mogoče doseči enake učinke z uporabo drugih manj občutljivih informacij.

VII. **DOSTOP DO PRAVNEGA VARSTVA IN E-PRAVOSODJE**

82. Uporaba tehnologij bo pripomogla tudi k boljšemu pravosodnemu sodelovanju. Podpoglavje 3.4.1 sporočila se nanaša na e-pravosodje, ki naj bi državljanom zagotavljalo lažji dostop do pravnega varstva. Projekt vključuje spletni portal z informacijami in video-konferencami kot del pravnega postopka. Poleg tega predvideva izvajanje pravnih postopkov po elektronski poti ter povezavo nacionalnih registrov, kot so na primer registri plačilne nesposobnosti. ENVP ugotavlja, da v sporočilu niso navedene nove pobude v zvezi z e-pravosodjem, ampak so samo povzeti ukrepi, ki se že izvajajo. ENVP sodeluje pri izvajanju nekaterih od njih na podlagi mnenja z dne 19. decembra 2008 o sporočilu Komisije z naslovom „Za evropsko strategijo na področju e-pravosodja“. ([52])

83. e-pravosodje je ambiciozen projekt in ga je treba v celoti podpreti. Učinkovito lahko izboljša evropski pravosodni sistem in pravno varstvo državljanov. Je pomemben prispevek k razvoju evropskega območja pravice. Ocena je torej pozitivna, vendar lahko kljub temu navedemo nekaj pripomb:

— pri razvoju tehnoloških sistemov e-pravosodja bi bilo treba upoštevati načelo spoštovanja zasebnosti pri načrtovanju sistemov. Kot že rečeno, je v zvezi z evropskim informacijskim sistem bistveno, da se izbere prava arhitektura,

— pri povezavi in interoperabilnosti sistemov bi bilo treba upoštevati načelo omejitve namena,

— natančno bi bilo treba določiti odgovornosti različnih akterjev,

— vnaprej bi bilo treba analizirati, kakšne posledice za posameznike lahko ima povezovanje nacionalnih registrov, ki vsebujejo občutljive osebne podatke, kot so registri plačilne nesposobnosti.

VIII. **ZAKLJUČNE UGOTOVITVE**

84. ENVP z zadovoljstvom ugotavlja, da je v sporočilu poudarjeno varstvo temeljnih pravic in zlasti osebnih podatkov, ki je eno ključnih vprašanj za prihodnost območja svobode, varnosti in pravice. ENVP meni, da je v sporočilu pravilno upoštevana uravnoteženost med potrebami po ustreznih instrumentih za zagotovitev varnosti državljanov in varstvu človekovih pravic. Ugotavlja, da bi bilo treba bolj poudariti varstvo osebnih podatkov.

85. ENVP v celoti podpira podpoglavje 2.3 sporočila, v katerem je opredeljena potreba po vsestranskem mehanizmu za varstvo podatkov, ki bi vključeval vsa področja, ki so v pristojnosti EU, ne glede na začetek veljavnosti Lizbonske pogodbe. V tej zvezi priporoča, da se:

— v stockholmskem programu navede, da je potrebna jasna dolgoročna vizija o takšnem vsestranskem mehanizmu,

— ocenijo že sprejeti ukrepi na tem področju ter njihovo dejansko izvajanje in učinkovitost, pri čemer se upošteva vpliv na zasebnost in učinkovitost kazenskega pregona,

— v stockholmski program kot prednostna naloga vključi potreba po novem zakonodajnem okviru, ki bo *inter alia* nadomestil tudi Okvirni sklep Sveta 2008/977/PNZ.

86. ENVP pozitivno ocenjuje namero Komisije o preoblikovanju načel varstva podatkov, ki mora biti povezana z javnim posvetovanjem, ki ga je napovedala Komisija na konferenci „Osebni podatki – večja uporaba, večja zaščita?“ 19. in 20. maja 2009. Z vidika vsebine ENVP poudarja pomen načela omejitve namena, ki je temelj zakonodaje o varstvu podatkov; hkrati poudarja, da bi bilo treba zlasti preučiti možnosti za izboljšanje učinkovitosti uporabe načel varstva podatkov z instrumenti, ki bi lahko okrepili odgovornost upravljavcev.

87. Treba bi bilo spodbujati upoštevanje „načela spoštovanja zasebnosti pri načrtovanju sistemov“ in uporabo tehnologij, ki spoštujejo zasebnost, in sicer:

— s certificiranjem za varstvo zasebnosti in podatkov za razvijalce in uporabnike informacijskih sistemov,

— s pravno obveznostjo razvijalcev in uporabnikov informacijskih sistemov, da uporabljajo sisteme, ki so skladni z načelom zasebnosti pri načrtovanju.

88. V zvezi z zunanjimi vidiki varstva podatkov ENVP priporoča, da se:

— v stockholmskem programu poudari pomen splošnih sporazumov z Združenimi državami in drugimi tretjimi državami o varstvu in izmenjavi podatkov,

([52]) Mnenje ENVP z dne 19. decembra 2008 o Sporočilu Komisije z naslovom „Za evropsko strategijo na področju e-pravosodja“, UL C 128, 6.6.2009, str. 13.

— aktivno spodbuja spoštovanje temeljnih pravic in zlasti varstva podatkov v odnosih s tretjimi državami in mednarodnimi organizacijami,

— v stockholmskem programu navede, da je treba pri izmenjavi podatkov s tretjimi državami zagotoviti ustrezno raven varstva podatkov ali druge zaščitne ukrepe v teh tretjih državah.

89. ENVP z zanimanjem spremlja razvoj strategije EU za upravljanje informacij in evropskega informacijskega modela ter poudarja, da je treba v teh projektih nameniti pozornost elementom, ki se nanašajo na varstvo podatkov; hkrati predlaga podrobnejšo obravnavo teh elementov v stockholmskem programu. Arhitektura sistemov za izmenjavo informacij bi morala temeljiti na „načelu spoštovanja zasebnosti pri načrtovanju sistemov“ in „najboljših razpoložljivih tehnologijah“.

90. Dejstvo, da je izmenjava digitalnih informacij med interoperabilnimi podatkovnimi zbirkami ali združevanje teh zbirk tehnično izvedljivo, ne upravičuje izjem glede spoštovanja načela omejitve namena. V konkretnih primerih bi morala interoperabilnost temeljiti na jasnih in previdnih političnih odločitvah. ENVP predlaga, da se to navede v stockholmskem programu.

91. ENVP meni, da bi moralo biti organom kazenskega pregona dovoljeno, da uporabljajo podatke, ki se zbirajo za poslovne namene, samo pod zelo strogimi pogoji, navedenimi v točki 65 tega mnenja.

92. Drugi predlogi v zvezi z uporabo osebnih podatkov:

— Treba bi bilo razviti vsebinska merila za odločanje o tem, ali naj bi bili sistemi centralizirani ali decentralizirani, in vključiti razvoj teh meril med cilje stockholmskega programa.

— Vzpostavitev sistema elektronskega evidentiranja vstopov na ozemlje držav članic in izstopov z njega poleg programov za registrirane potnike ne bi smela biti vključena v stockholmski program.

— Treba bi bilo podpreti krepitev Europola in Eurojusta ter novi sporazum med obema organoma, ki je bil pripravljen pred kratkim.

— Treba bi bilo razviti vsebinska merila za uporabo biometričnih podatkov, s katerimi bi zagotovili, da so bodo podatki uporabljali samo, kadar je to potrebno in primerno ter v skladu z načeli sorazmernosti in zakonodajalec predhodno dokaže jasen, točno določen in zakonit namen uporabe. Uporaba podatkov o DNK ne bi smela biti dovoljena, če je mogoče doseči enak učinek z uporabo drugih manj občutljivih informacij.

93. ENVP podpira projekt e-pravosodje in je pripravil nekaj predlogov za njegovo izboljšanje (glej točko 83).

V Bruslju, 10. julija 2009

Peter HUSTINX

Evropski nadzornik za varstvo podatkov