I

(Resolucije, priporočila in mnenja)

MNENJA

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Mnenje Evropskega nadzornika za varstvo podatkov o osnutku predloga okvirnega sklepa Sveta o uporabi evidence podatkov o potnikih (PNR) za namene kazenskega pregona

(2008/C 110/01)

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 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 ([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 ter zlasti člena 41 Uredbe ([2]),

ob upoštevanju zaprosila za mnenje v skladu s členom 28(2) Uredbe (ES) št. 45/2001, ki ga je 13. novembra 2007 prejel od Komisije –

SPREJEL NASLEDNJE MNENJE:

I. UVOD

Posvetovanje z Evropskim nadzornikom za varstvo podatkov (ENVP)

1. Komisija je ENVP poslala osnutek predloga okvirnega sklepa Sveta o uporabi evidence podatkov o potnikih (PNR) za namene kazenskega pregona (v nadaljevanju „predlog“), da bi se z njim posvetovala v skladu s členom 28(2) Uredbe (ES) št. 45/2001.

2. Predlog se nanaša na obdelavo podatkov PNR v okviru EU in je tesno povezan z drugimi sistemi zbiranja in uporabe podatkov o potnikih, zlasti s sporazumom med EU in ZDA iz julija 2007. Takšni sistemi so za ENVP zelo zanimivi, decembra 2006 pa je že imel priložnost zadevnim zainteresiranim stranem ([3]) poslati nekaj začetnih pripomb k vprašalniku Komisije glede načrtovanega sistema EU za PNR. ENVP izraža zadovoljstvo zaradi posvetovanja s Komisijo. ENVP meni, da bi bilo treba to mnenje navesti v preambuli sklepa Sveta.

Predlog in njegovo ozadje

3. Namen predloga je uskladitev določb držav članic o obveznostih letalskih prevoznikov, ki opravljajo lete na ozemlje ali z ozemlja vsaj ene države članice, glede posredovanja podatkov PNR pristojnim organom za namene preprečevanja terorističnih kaznivih dejanj in organiziranega kriminala ter boja proti njim.

4. Evropska unija je z ZDA in s Kanado sklenila sporazum o posredovanju podatkov PNR za namene primerjanja. Prvi sporazum, ki je bil z ZDA sklenjen maja 2004, je bil

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

([3]) Vključno z državami članicami, organi za varstvo podatkov in združenji letalskih prevoznikov. Vprašalnik je bil sestavljen v zvezi s pripravo presoje učinka zadevnega predloga s strani Evropske komisije.

nadomeščen z drugim sporazumom julija 2007 ([1]). Julija 2005 je bil sklenjen podoben sporazum s Kanado ([2]). Poleg tega se bodo v kratkem začela pogajanja med EU in Avstralijo glede sporazuma o izmenjavi podatkov PNR, pa tudi Južna Koreja zahteva podatke PNR za lete na njeno ozemlje, ne da bi bila v tej fazi načrtovana pogajanja na evropski ravni.

5. V okviru EU predlog dopolnjuje Direktivo Sveta 2004/82/ES ([3]) o dolžnosti prevoznikov, da posredujejo podatke o potnikih, označene kot predhodne informacije o potnikih (podatki API), zaradi boja proti nezakonitemu priseljevanju in izboljšanja mejne kontrole. Države članice bi morale prenesti to direktivo v notranjo zakonodajo najpozneje do 5. septembra 2006. Vendar pa vse države članice še niso zagotovile njenega izvajanja.

6. V nasprotju s podatki API, ki naj bi pripomogli k identifikaciji posameznikov, bi podatki PNR iz predloga bili v pomoč pri ocenjevanju tveganja v zvezi z osebami, pridobivanju obveščevalnih podatkov ter ugotavljanju povezav med znanimi in neznanimi osebami.

7. Predlog zajema naslednje glavne elemente:

— predlog predvideva, da dajejo letalski prevozniki pristojnim organom držav članic na voljo podatke PNR za namene preprečevanja terorističnih kaznivih dejanj in organiziranega kriminala ter boja proti njim,

— v predlogu je predvideno, da se v vsaki državi članici imenuje enota za informacije o potnikih (EIP), pristojna za zbiranje podatkov PNR od letalskih prevoznikov (ali imenovanih posrednikov) in za ocenjevanje tveganja v zvezi s potniki,

— informacije, ocenjene skladno s tem, bodo posredovane pristojnim organom v posameznih državah članicah. Te informacije se bodo izmenjevale z drugimi državami članicami glede na posamezne primere in za navedene namene,

— za posredovanje podatkov državam zunaj Evropske unije veljajo dodatni pogoji,

— podatki se hranijo trinajst let, od česar osem let v mirujoči podatkovni zbirki,

— obdelavo podatkov bo urejal (osnutek) okvirnega sklepa Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (v nadaljevanju „okvirni sklep o varstvu podatkov“) ([4]),

— odbor, ki ga bodo sestavljali predstavniki držav članic, bo Komisiji pomagal pri vprašanjih protokolov in šifriranja ter v zvezi z merili in prakso pri ocenah tveganja,

— sklep bo pregledan v treh letih po začetku veljavnosti.

Bistveni elementi mnenja

8. Predlog, ki ga obravnava ENVP v okviru posvetovanja, je nadaljnji korak proti rutinskemu zbiranju podatkov o posameznikih, ki načeloma niso osumljeni kaznivih dejanj. Kot že povedano, se ta premik odvija na mednarodni in evropski ravni.

9. ENVP ugotavlja, da sta tudi Delovna skupina iz člena 29 in Delovna skupina za policijo in pravosodje predložili skupno mnenje o predlogu ([5]). ENVP podpira navedeno mnenje. V pričujočem mnenju je izpostavljenih in nadalje obravnavanih več dodatnih vprašanj.

10. Čeprav so v mnenju ENVP analizirani vsi pomembni vidiki predloga, se največ pozornosti namenja štirim glavnim vprašanjem.

— Prvo od teh je vprašanje legitimnosti načrtovanih ukrepov. Vprašanje namena, potrebnosti in sorazmernosti predloga se ocenjuje glede na merila iz člena 8 Listine o temeljnih pravicah Evropske unije.

— V mnenju se analizira tudi vprašanje prava, ki se uporablja za predlagano dejavnost obdelovanja podatkov. Še posebno pozornost si zasluži področje uporabe okvirnega sklepa o varstvu podatkov v razmerju do uporabe zakonodaje o varstvu podatkov iz prvega stebra. Obravnava se tudi vprašanje posledic ureditve, ki se uporablja za varstvo podatkov, glede uveljavljanja pravic posameznikov, na katere se nanašajo podatki.

([1]) Sporazum med Evropsko unijo in Združenimi državami Amerike o obdelavi in posredovanju podatkov iz evidence imen letalskih potnikov (PNR) s strani letalskih prevoznikov ministrstvu Združenih držav za domovinsko varnost (MDV) (Sporazum PNR iz leta 2007) (UL L 204, 4.8.2007, str. 18).

([2]) Sporazum med Evropsko skupnostjo in Vlado Kanade o obdelavi in prenosu predhodnih podatkov o potnikih in podatkov o evidenci imen letalskih potnikov (UL L 82, 21.3.2006, str. 15).

([3]) Direktiva Sveta 2004/82/ES z dne 29. aprila 2004 o dolžnosti prevoznikov, da posredujejo podatke o potnikih (UL L 261, 6.8.2004, str. 24).

([4]) Zadnji osnutek tega predloga je na razpolago v registru Sveta pod številko dokumenta 16397/07.

([5]) Skupno mnenje o predlogu okvirnega sklepa Sveta o uporabi evidence podatkov o potnikih (PNR) za namene kazenskega pregona, ki ga je Komisija predložila 6. novembra 2007; Delovna skupina iz člena 29 je mnenje sprejela 5. decembra 2007, Delovna skupina za policijo in pravosodje pa 18. decembra 2007, WP 145, WPPJ 01/07.

— V mnenju se nato obravnava narava prejemnikov podatkov na ravni držav. Posebni pomisleki nastanejo zlasti glede narave EIP, posrednikov in pristojnih organov, imenovanih za ocenjevanje tveganja ter analiziranje podatkov o potnikih, saj v predlogu niso natančneje opredeljeni v tem oziru.

— Četrto vprašanje je povezano s pogoji prenosa podatkov v tretje države. Ni pojasnjeno, kateri pogoji se bodo za takšne prenose uporabljali v primeru, če obstajajo različna pravila: bodo to pogoji prenosa v skladu z zadevnim predlogom, skupaj s pogoji iz okvirnega sklepa o varstvu podatkov, ali pogoji, določeni z obstoječimi mednarodnimi sporazumi (z ZDA in Kanado).

11. V zadnjem delu se obravnavajo druga vsebinska vprašanja, vključno s pozitivnimi ukrepi glede varstva podatkov, a tudi dodatni pomisleki, izhajajoči iz predloga.

II. LEGITIMNOST PREDLAGANEGA UKREPA

12. Da bi analizirali legitimnost predlaganih ukrepov v skladu s temeljnimi načeli varstva podatkov, zlasti členom 8 evropske listine o temeljnih pravicah ter členi 5 do 8 Konvencije Sveta Evrope št. 108 ([1]), je treba jasno opredeliti namen načrtovanega obdelovanja osebnih podatkov, da bi ocenili njegovo nujnost in sorazmernost. Treba bi se bilo prepričati, ali za dosego predvidenega namena morda ne obstaja drugo sredstvo, ki bi manj posegalo v zasebnost.

Opredelitev namena

13. Iz besedila predloga in njegove presoje vpliva je razvidno, da cilj ni samo identifikacija znanih teroristov ali znanih storilcev kaznivih dejanj, vpletenih v organizirani kriminal, s primerjanjem njihovih imen z imeni na seznamih, ki jih vodijo organi kazenskega pregona. Namen je pridobivanje obveščevalnih podatkov v zvezi s terorizmom ali organiziranim kriminalom, bolj podrobno pa „ocenjevanje tveganja v zvezi s posameznimi osebami, pridobivanje obveščevalnih podatkov ter povezovanje znanih in neznanih oseb“ ([2]). Podobno je opisan namen v členu 3(5) predloga – šlo naj bi predvsem za „identifikacijo oseb, ki so *ali bi lahko bile* vpletene v teroristično kaznivo dejanje ali kaznivo dejanje, povezano z organiziranim kriminalom, *ter njihovih sodelavcev*“.

14. S tem razlogom naj bi pojasnili, da podatki API ne zadostujejo za dosego načrtovanega namena. Kot je že bilo povedano, naj bi podatki API pripomogli k identifikaciji posameznikov, medtem ko podatki PNR temu niso namenjeni, vendar pa bi bile podrobnosti iz teh podatkov v pomoč pri ocenjevanju tveganja v zvezi z osebami, pridobivanju obveščevalnih podatkov ter ugotavljanju povezav med znanimi in neznanimi osebami.

15. Namen načrtovanih ukrepov ne vključuje le zajetja *znanih* oseb, temveč tudi odkrivanje oseb, ki *bi lahko* ustrezale merilom predloga.

Pri identifikaciji teh oseb imata v projektu osnovno vlogo ocena tveganja in ugotavljanje vzorcev. Uvodna izjava 9 predloga izrecno navaja, da je treba podatke hraniti „dovolj dolgo, da dosežejo svoj namen, in sicer razvoj kazalnikov tveganja ter opredelitev potovalnih in vedenjskih vzorcev“.

16. Tako opisan namen je torej dvostopenjski: prva stopnja zajema globalni cilj, tj. boj proti terorizmu in organiziranemu kriminalu, druga stopnja pa vključuje sredstva in ukrepe, neobhodno potrebne za dosego tega cilja. Medtem ko se zdi boj proti terorizmu in organiziranemu kriminalu kot namen dovolj jasen in legitimen, pa bi se dalo o sredstvih, ki se uporabijo za dosego tega namena, še razpravljati.

Ugotavljanje vzorcev in ocena tveganja

17. V predlogu se ne omenja, na kakšen način se bodo ugotavljali vzorci in kako bo opravljena ocena tveganja. V presoji vpliva je pojasnjeno, da bodo podatki PNR uporabljeni za analizo podatkov o potnikih „glede na kombinacijo lastnosti in vedenjskih vzorcev za namene priprave ocene tveganja. Kadar potnik ustreza določeni oceni tveganja, je lahko identificiran kot visoko tvegan potnik“ ([3]).

18. Osumljene osebe bi lahko izbrali glede na dejanske elemente suma iz njihovih podatkov PNR (na primer, stik s sumljivo potovalno agencijo, navedba glede ukradene kreditne kartice) in tudi na podlagi „vzorcev“ ali abstraktnega profila. Na podlagi potovalnih vzorcev bi seveda lahko sestavili različne standardne profile „običajnih potnikov“ ali „sumljivih potnikov“. Ti profili bi omogočili nadaljnjo preiskavo potnikov, ki ne spadajo v „kategorijo običajnih potnikov“, toliko bolj, če je njihov profil povezan z drugimi sumljivimi elementi, na primer ukradeno kreditno kartico.

19. Čeprav ni mogoče sklepati, da bi bili potniki vzeti na tarčo zaradi svoje vere ali drugih občutljivih podatkov, pa se ne glede na to zdi, da bi bili predmet preiskave na podlagi mešanih dejanskih in abstraktnih podatkov, *vključno* s standardnimi vzorci in abstraktnimi profili.

([1]) Konvencija Sveta Evrope z dne 28. januarja 1981 o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov.

([2]) Obrazložitveni memorandum predloga, poglavje I.

([3]) Presoja vpliva, poglavje 2.1, „Opredelitev težave“.

20. O tem, ali bi takšna vrsta preiskave lahko štela za izdelavo profilov, bi se dalo razpravljati. Izdelava profilov bi vključevala „računalniško podprto metodo z uporabo podatkovnega rudarjenja v podatkovnem skladišču, s čimer se omogoči ali naj bi se omogočilo, da se z določeno mero verjetnosti, in torej tudi z nekaj dovoljenega odstopanja, posameznik uvrsti v posebno kategorijo, da bi v zvezi s to osebo sprejeli individualne ukrepe“ ([1]).

21. ENVP je seznanjen s trenutno potekajočimi razpravami glede opredelitve izdelave profilov. Ne glede na to, ali se uradno prizna, da je cilj predloga *izdelava profilov* o potnikih, pa bistveno vprašanje niso opredelitve, temveč posledice za posameznike.

22. Glavni pomislek ENVP se nanaša na dejstvo, da bodo odločitve o posameznikih sprejete na podlagi vzorcev in meril, določenih z uporabo podatkov o potnikih na splošno. Tako bi bile lahko odločitve o posamezniku sprejete tako, da bi kot referenco (vsaj deloma) uporabili vzorce, ki izhajajo iz podatkov *drugih* posameznikov. Odločitve bodo torej sprejete glede na abstrakten okvir, kar bi lahko zelo vplivalo na posameznike, na katere se nanašajo podatki. Posamezniki se izredno težko branijo pred takšnimi odločitvami.

23. Poleg tega je predvideno, da se opravi ocena tveganja, če ni enotnih standardov za identifikacijo osumljencev. ENVP ima resne dvome glede pravne varnosti celotnega postopka filtriranja, saj so po njegovem mnenju merila, po katerih bodo pregledali vsakega potnika, slabo opredeljena.

24. ENVP opozarja na sodno prakso Evropskega sodišča za človekove pravice, po kateri mora biti notranje pravo dovolj natančno, da državljanom pove, v kakšnih okoliščinah in pod kakšnimi pogoji smejo javni organi shranjevati podatke o njihovem zasebnem življenju in jih uporabiti. Podatki „bi morali biti dostopni zadevni osebi, učinki glede njih pa predvidljivi“. Predpis je „predvidljiv“, „če je opredeljen dovolj natančno, da lahko vsak posameznik – če je treba, ob ustreznem nasvetu – usmerja svoje ravnanje“ ([2]).

25. Kot zaključek naj navedemo, da je treba zadevni predlog skrbno preučiti predvsem zaradi tovrstnih tveganj. Medtem ko je splošen namen boja proti terorizmu in organiziranemu kriminalu sam po sebi jasen in legitimen, pa se zdi, da samo bistvo obdelave podatkov, ki se bo izvajala, ni dovolj opredeljeno in upravičeno. ENVP zato poziva zakonodajalca EU, naj pred sprejetjem okvirnega sklepa razjasni to vprašanje.

Nujnost

26. Kot je prikazano zgoraj, ukrepi očitno posegajo v zasebnost. Po drugi strani pa njihova koristnost še zdaleč ni dokazana.

27. Presoja vpliva predloga se osredotoča na to, kako bi vzpostavili PNR EU na najboljši način, in ne toliko na to, koliko je takšna PNR sploh potrebna. V presoji se navajajo sistemi PNR ([3]), ki so vzpostavljeni v drugih državah, tj. v ZDA in Združenem kraljestvu. Vendar pa lahko obžalujemo, da dejstva in podatki, povezani s temi sistemi, niso dovolj natančni. V signalnem sistemu Združenega kraljestva se poroča o „številnih aretacijah“ v zvezi z „različnimi kaznivimi dejanji“, ne da bi pri tem natančno pojasnili povezavo s terorizmom ali organiziranim kriminalom. Glede programa v ZDA ni navedenih nobenih podrobnosti, razen da „je EU lahko ocenila vrednost podatkov PNR in spoznala njihove zmožnosti za namene kazenskega pregona“.

28. Ne le, da *v predlogu* ni dovolj natančnih informacij o konkretnih rezultatih takšnih sistemov PNR, tudi poročila, ki so jih objavile *druge agencije*, na primer GAO (Government Accountability Office) v Združenih državah Amerike, v tej fazi ne potrjujejo učinkovitosti ukrepov ([4]).

([1]) Ta opredelitev izhaja iz nedavne študije Sveta Evrope o izdelavi profilov. *L'application de la Convention 108 au mécanisme de profilage, Eléments de réflexion destinés au travail futur du Comité consultatif* (T-PD), Jean-Marc Dinant, Christophe Lazaro, Yves Poullet, Nathalie Lefever, Antoinette Rouvroy, november 2007 (še ni objavljeno). Glej tudi opredelitev po Leeju Bygravu: „Na splošno je izdelava profilov postopek ugotavljanja sklopa značilnosti (tipično vedenjskih) o posamezniku ali kolektivnem subjektu in nato obravnava tega posameznika/subjekta (ali drugih oseb/subjektov) v luči teh značilnosti. Postopek izdelave profilov je kot tak sestavljen iz dveh glavnih elementov: (i) izdelava profila – postopek ugotavljanja profila; (ii) uporaba profila – postopek obravnave oseb/subjektov glede na ta profil“. L. A. BYGRAVE, *Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, Computer Law & Security Report, 2001, vol. 17, str. 17–24: http://www.austlii.edu.au/au/journals/PLPR/2000/40.html.

([2]) Rotaru proti Romuniji, št. 28341/95, odstavki 50, 52 in 55. Glej tudi Amann proti Švici, št. 27798/95, odstavek 50 in naslednji.

([3]) Presoja vpliva, poglavje 2.1, „Opredelitev težave“.

([4]) Glej na primer poročilo, ki ga je maja 2007 vladna služba Združenih držav za nadzor javne porabe (GAO) predložila na zahtevo kongresa: „*Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues remain*“), http://www.gao.gov/new.items/d07346.pdf.

29. ENVP meni, da je treba dodatno oceniti tehnike, s katerimi se ob uporabi orodij za rudarjenje podatkov in vedenjskih vzorcev ocenjuje tveganje, ki ga predstavljajo posamezniki, koristnost tehnik pa je treba jasno opredeliti v okviru boja proti terorizmu, še preden se uporabijo v tako velikem obsegu.

Sorazmernost

30. Da bi ugotovili razmerje med poseganjem v zasebnost posameznika in nujnostjo ukrepa ([1]), se upoštevajo naslednji elementi:

— ukrepi veljajo za vse potnike, ne glede na to, ali jih organi kazenskega pregona preiskujejo ali ne. Gre za proaktivno iskanje v obsegu, kakršnega še ni bilo,

— odločitve glede posameznikov lahko temeljijo na abstraktnih profilih, kar vključuje tudi precejšnje dovoljeno odstopanje,

— narava ukrepov, ki naj bi se sprejeli za posameznika, je povezana s kazenskim pregonom: posledice v smislu izključitve ali prisile torej precej bolj posegajo v zasebnost kot v drugih primerih, na primer pri goljufiji s kreditnimi karticami ali marketingu.

31. Skladnost z načelom sorazmernosti ne pomeni le, da je predlagan ukrep učinkovit, temveč tudi, da predvideni namen predloga ne more biti dosežen z uporabo instrumentov, ki bi manj posegali v zasebnost. Učinkovitost načrtovanih ukrepov ni bila dokazana. Skrbno je treba preveriti obstoj drugih možnosti, preden se uvedejo dodatni/novi ukrepi za obdelavo osebnih podatkov. Po mnenju ENVP takšna izčrpna presoja ni bila opravljena.

32. ENVP želi opozoriti na druge velike sisteme za spremljanje gibanja posameznikov v EU in na njenih mejah, ki že delujejo ali pa bodo v kratkem vpeljani, predvsem vizumski informacijski sistem ([2]) in schengenski informacijski sistem ([3]). Medtem ko glavni cilj teh instrumentov ni boj proti terorizmu ali organiziranemu kriminalu, pa imajo organi kazenskega pregona oziroma bodo imeli do neke mere dostop do njih v širšem okviru boja proti kriminalu ([4]).

33. Drug primer zadeva razpoložljivost osebnih podatkov, ki so vključeni v državne policijske podatkovne zbirke – zlasti biometričnih podatkov – v okviru Prümske pogodbe, podpisane maja 2005 in razširjene na vse države članice Evropske unije ([5]).

34. Vsem tem različnim instrumentom je skupno, da omogočajo globalno spremljanje gibanja posameznikov, čeprav z drugačnega vidika. Način, na katerega že lahko prispevajo k boju proti posebnim oblikam kriminala, vključno s terorizmom, bi bilo treba poglobljeno in izčrpno analizirati, preden bi se odločili za uvedbo nove oblike sistematičnega pregledovanja vseh oseb, ki z letalom odhajajo iz EU ali tja prihajajo. ENVP priporoča, naj Komisija opravi takšno analizo kot nujen korak v zakonodajnem postopku.

Sklep

35. Glede na povedano ENVP navaja naslednje sklepe glede legitimnosti predlaganih ukrepov. Razvijanje različnih podatkovnih zbirk brez globalnega pogleda na dejanske rezultate in pomanjkljivosti:

— je v nasprotju z racionalno zakonodajno politiko, po kateri se novi instrumenti ne smejo sprejeti, dokler že obstoječi niso bili v celoti izvedeni in so se izkazali za nezadostne ([6]),

— bi lahko sicer pomenilo korak proti popolnemu nadzoru družbe.

36. Boj proti terorizmu je vsekakor lahko legitimen razlog za uporabo izjem od temeljnih pravic do zasebnosti in varstva podatkov. Da pa se ga utemelji, je treba nujnost posega v zasebnost podpreti z jasnimi in nespornimi

([1]) V skladu s členom 9 Konvencije št. 108 „so omejitve določb v 5., 6. in 8. členu te konvencije dopustne, kadar so predpisane v zakonu pogodbenice ob upoštevanju temeljnih vrednot demokratične družbe. V tem okviru so omejitve dopustne zaradi:
1. zaščite državne varnosti, javne varnosti, denarnih interesov države ali zatiranja kriminala;
2. zaščite dajalcev (posameznikov) podatkov ali pravic in svoboščin drugih."

([2]) Odločba Sveta 2004/512/ES z dne 8. junija 2004 o vzpostavitvi vizumskega informacijskega sistema (VIS) (UL L 213, 15.6.2004, str. 5); predlog uredbe Evropskega parlamenta in Sveta o Vizumskem informacijskem sistemu (VIS) in izmenjavi podatkov o vizumih za kratkoročno prebivanje med državami članicami, COM(2005) 835 konč.; predlog sklepa Sveta o dostopu organov držav članic, odgovornih za notranjo varnost, in Europola do Vizumskega informacijskega sistema (VIS) za iskanje podatkov v namen preprečevanja, odkrivanja in preiskovanja terorističnih dejanj in drugih hudih kaznivih dejanj, COM(2005) 600 konč.

([3]) Glej zlasti Sklep Sveta 2007/533/PNZ z dne 12. junija 2007 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II) (UL L 205, 7.8.2007).

([4]) O tem vprašanju glej: Mnenje Evropskega nadzornika za varstvo podatkov o predlogu sklepa Sveta o dostopu organov držav članic, odgovornih za notranjo varnost, in Europola do Vizumskega informacijskega sistema (VIS) za iskanje podatkov v namen preprečevanja, odkrivanja in preiskovanja terorističnih dejanj in drugih hudih kaznivih dejanj (COM (2005) 600 konč.) (UL C 97, 25.4.2006, str. 6).

([5]) Glej mnenji ENVP o prümskih sklepih: Mnenje z dne 4. aprila 2007 o pobudi petnajstih držav članic z namenom sprejetja Sklepa Sveta o poglobitvi čezmejnega sodelovanja, zlasti na področju boja proti terorizmu in čezmejnemu kriminalu (UL C 169, 21.7.2007, str. 2) in Mnenje z dne 19. decembra 2007 o pobudi Zvezne republike Nemčije z namenom sprejetja Sklepa Sveta o izvajanju Sklepa 2007/…/PNZ o poglobitvi čezmejnega sodelovanja, zlasti na področju boja proti terorizmu in čezmejnemu kriminalu (dostopno na naslovu: http://www.edps.europa.eu).

([6]) Tak sklep je ENVP že večkrat izrazil, nazadnje v svojem mnenju z dne 25. julija 2007 o izvajanju direktive o varstvu podatkov (UL C 255, 27.10.2007, str. 1).

elementi ter dokazati sorazmernost obdelave podatkov. To je še toliko bolj potrebno v primeru večjega poseganja v zasebnost posameznikov, kakor je to predvideno v predlogu.

37. Ugotovimo lahko le, da v predlogu ni takšnih utemeljitvenih elementov ter da preizkus glede nujnosti in sorazmernosti ne vzdrži.

38. ENVP vztraja, da je preizkus glede nujnosti in sorazmernosti, kot je opisano zgoraj, bistvenega pomena. Je neobhodni pogoj za uveljavitev zadevnega predloga. Vse nadaljnje opombe ENVP v tem mnenju je treba brati v luči tega predpogoja.

III. PRAVO, KI SE UPORABLJA – UVELJAVLJANJE PRAVIC POSAMEZNIKOV, NA KATERE SE NANAŠAJO PODATKI

Pravo, ki se uporablja

39. Analiza se v nadaljevanju osredotoča na tri točke:

— opis različnih korakov v predlogu predvidene obdelave podatkov, da bi ugotovili, katero pravo se uporablja na vsaki stopnji,

— omejitve predloga okvirnega sklepa Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, in sicer glede področja uporabe in pravic posameznikov, na katere se nanašajo podatki,

— bolj splošna analiza vprašanja, do kakšne mere se lahko instrument tretjega stebra uporablja za podatke zasebnih subjektov, ki se obdelujejo v okviru prvega stebra.

Pravo, ki se uporablja v različnih fazah obdelave podatkov

40. Člen 11 predloga navaja, da „[d]ržave članice zagotovijo, da se Okvirni sklep Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (…), uporablja za obdelavo osebnih podatkov v skladu s tem okvirnim sklepom“.

41. Vendar pa kljub tej določbi ni jasno, do kakšne mere se bo okvirni sklep o varstvu podatkov, ki je sicer instrument tretjega stebra Pogodbe EU, uporabljal za podatke, ki jih obdelujejo letalski prevozniki, zbirajo EIP in nadalje uporabljajo drugi pristojni organi.

42. Prva faza obdelave osebnih podatkov, ki jo predvideva predlog, je obdelava s strani letalskih prevoznikov, ki morajo podatke PNR dati na razpolago nacionalnim EIP, načeloma z uporabo sistema *push*. Po besedilu predloga in presoje vpliva ([1]) bi lahko sklepali, da bi letalski prevozniki lahko podatke pošiljali posrednikom tudi v neprečiščeni obliki. Dejavnost letalskih prevoznikov poteka primarno v komercialnem okolju, za katerega velja nacionalna zakonodaja o varstvu podatkov, ki uveljavlja Direktivo 95/46/ES ([2]). Vprašanja o pravu, ki se uporablja, se bodo pojavila, kadar se zbrani podatki uporabljajo v namene kazenskega pregona ([3]).

43. Podatke bi nato filtriral posrednik (da bi jim dal obliko in izključil podatke PNR, ki niso vključeni na seznam podatkov, zahtevanih po predlogu) ali pa bi bili poslani neposredno EIP. Posredniki bi lahko bili tudi iz zasebnega sektorja, kot je denimo tudi SITA, ki deluje kot posrednik v okviru sporazuma o PNR s Kanado.

44. Kar zadeva EIP, ki so odgovorne za oceno tveganja za celotni skup podatkov, ni jasno, kdo bo odgovoren za obdelavo. Pri njej bi lahko sodelovali carinski in mejni organi in ne nujno organi kazenskega pregona.

45. Nadaljnje pošiljanje prečiščenih podatkov „pristojnim“ organom bi se verjetno odvijalo v okviru kazenskega pregona. Predlog navaja, da „[p]ristojni organi vključujejo samo organe, ki so pristojni za preprečevanje terorističnih kaznivih dejanj in organiziranega kriminala ali boj proti njim“.

46. Pri pomikanju naprej skozi faze obdelave so udeleženi akterji in načrtovani namen vse tesneje povezani s policijskim in pravosodnim sodelovanjem v kazenskih zadevah. Vendarle pa v predlogu ni izrecno navedeno, kdaj natančno se bo uporabil okvirni sklep o varstvu podatkov. Po besedilu bi lahko celo sklepali, da se uporablja za obdelavo podatkov v celoti in tudi za letalske prevoznike ([4]). Vendar pa okvirni sklep o varstvu osebnih podatkov že sam po sebi vsebuje nekatere omejitve.

([1]) Člen 6(3) predloga in v presoji vpliva priloga A „Način posredovanja podatkov s strani prevoznikov“.

([2]) Direktiva 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 (UL L 281, 23.11.1995, str. 31).

([3]) Glej v zvezi s tem posledice sodbe glede PNR. Sodba Sodišča z dne 30. maja 2006, Evropski parlament proti Svetu (C-317/04) in Komisiji (C-318/04), združeni zadevi C-317/04 in C-318/04, Zbirka odločb (2006), točka 56.

([4]) Člen 11 predloga. Glej tudi uvodno izjavo 10 preambule: „Okvirni sklep Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (…), je treba uporabljati za vse podatke, obdelane v skladu s tem okvirnim sklepom. Pravice posameznika, na katerega se podatki nanašajo, v zvezi s tako obdelavo, kot so pravica do informacij, pravica do dostopa, pravica do popravka, izbrisa in zamrznitve ter pravica do odškodnine in pravnih sredstev, morajo biti tiste iz navedenega okvirnega sklepa.“

47. Glede na to ENVP načelno dvomi v to, da bi se naslov VI Pogodbe EU lahko uporabil kot pravna podlaga za rutinske pravne obveznosti in za namene kazenskega pregona akterjev iz zasebnega sektorja. Poleg tega se je ustrezno vprašati tudi, ali se lahko naslov VI Pogodbe EU uporabi kot pravna podlaga za pravne obveznosti javnih organov, ki načeloma ne spadajo v okvir sodelovanja na področju kazenskega pregona. Ti dve vprašanji se v tem mnenju obravnavata v nadaljevanju.

Omejitve okvirnega sklepa o varstvu podatkov

48. Besedilo predloga okvirnega sklepa Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, vsebuje najmanj dve pomembni omejitvi glede področja uporabe.

49. Prvič, področje uporabe okvirnega sklepa o varstvu podatkov je v okvirnem sklepu dobro opredeljeno: uporablja se „le za podatke, ki jih pristojni organi zbirajo ali obdelujejo za namen preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvajanja kazni“ ([1]).

50. Drugič, okvirni sklep o varstvu podatkov naj se ne bi uporabljal za podatke, ki se obdelujejo samo na ravni države, temveč je omejen na izmenjavo podatkov med državami članicami in njihovo nadaljnje posredovanje tretjim državam ([2]).

51. Okvirni sklep o varstvu podatkov ima tudi nekatere slabosti v primerjavi z Direktivo 95/46/ES, zlasti precejšnjo izjemo od načela o omejitvi namena. Kar zadeva načelo o namenu, je v predlogu namen jasno omejen na obdelavo podatkov v okviru boja proti terorizmu in organiziranemu kriminalu. Vendar pa okvirni sklep o varstvu podatkov dopušča tudi obdelavo za širše namene. V takšnem primeru naj bi *lex specialis* (predlog) prevladal nad *lex generalis* (okvirni sklep o varstvu podatkov) ([3]). To bi bilo treba v besedilu predloga izrecno poudariti.

52. Zaradi tega ENVP priporoča, da bi predlogu dodali naslednjo določbo: „Osebni podatki, ki jih letalski prevozniki posredujejo v skladu s tem okvirnim sklepom, se smejo obdelovati le za namene boja proti terorizmu in organiziranemu kriminalu. Izjeme, predvidene z ozirom na načelo o namenu v okvirnem sklepu Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, se ne uporabljajo“.

53. Na koncu ENVP ugotavlja, da je pravna varnost v zvezi z ureditvijo varstva podatkov, ki se uporablja za različne akterje v projektu, zlasti pa za letalske prevoznike in druge akterje iz prvega stebra, precej pomanjkljiva, najsi gre za pravila iz predloga, pravila iz okvirnega sklepa o varstvu podatkov ali pa nacionalno zakonodajo za uveljavitev Direktive 95/46/ES. Zakonodajalec bi moral jasno navesti, v katerem trenutku obdelave se bodo ta različna pravila uporabljala.

Pogoji uporabe pravil za prvi oziroma tretji steber

54. ENVP v osnovi dvomi v dejstvo, da bi instrument tretjega stebra ustvarjal rutinske pravne obveznosti za namene kazenskega pregona akterjev iz zasebnega ali javnega sektorja, ki načeloma ne spadajo v okvir sodelovanja na področju kazenskega pregona.

55. Na tem mestu bi lahko naredili primerjavo z dvema drugima primeroma, v katerih je zasebni sektor sodeloval pri hrambi oziroma pošiljanju podatkov z vidika kazenskega pregona, in sicer:

— *primer ZDA-PNR, kjer je bilo predvideno, da bi letalski prevozniki sistematično pošiljali podatke PNR organom kazenskega pregona*. Sodišče je v sodbi v primeru PNR izključilo, da bi bila Skupnost pristojna za sklenitev sporazuma o PNR. Ena od utemeljitev je bila, da prenos podatkov PNR Uradu za carinsko in mejno zaščito Združenih držav Amerike (Urad CBP) predstavlja obdelavo, katere predmet je javna varnost in dejavnosti države na področju kazenskega prava ([4]). V tem primeru je bila obdelava *sistematično* posredovanje podatkov Uradu CBP za razliko od naslednjega primera.

— *Splošna hramba podatkov s strani operaterjev elektronskih komunikacij*. Glede na pristojnost Skupnosti, da določi takšen čas hrambe, je mogoče videti razliko z zadevo ZDA-PNR v tem, da Direktiva 2006/24/ES ([5]) predvideva le obveznost hrambe, pri čemer podatki ostanejo pod nadzorom operaterjev. Sistematičen prenos podatkov organom kazenskega pregona ni predviden. Zaključimo lahko, da v kolikor podatki ostanejo pod nadzorom izvajalcev storitev, so ti odgovorni tudi za spoštovanje obveznosti v zvezi z varstvom osebnih podatkov posameznika, na katerega se ti podatki nanašajo.

([1]) Uvodna izjava 5(a), različica okvirnega sklepa o varstvu podatkov z dne 11. decembra 2007.

([2]) Člen 1.

([3]) V zvezi s tem vprašanjem bi bilo treba skrbno pretehtati in razpravljati o besedilu člena 27b zadnjega osnutka okvirnega sklepa o varstvu podatkov v tretjem stebru.

([4]) Sodba Sodišča z dne 30. maja 2006, Evropski parlament proti Svetu (C-317/04) in Komisiji (C-318/04), združeni zadevi C-317/04 in C-318/04, Zbirka odločb (2006), točka 56.

([5]) 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).

56. V zadevnem predlogu o PNR EU morajo letalski prevozniki sistematično dati na razpolago podatke PNR za vse potnike. Vendar pa se ti podatki organom kazenskega pregona ne pošiljajo neposredno v neprečiščeni obliki, pač pa jih je mogoče poslati posredniku in preden se izbrani podatki pošljejo pristojnim organom, jih oceni tretja oseba, katere status je nejasen.

57. Poglavitni del obdelave podatkov se odvija v sivi coni ob vsebinski povezavi s prvim in tudi s tretjim stebrom. Kakor je nakazano v poglavju IV, pa narava akterjev, ki obdelujejo podatke, ni jasna. Letalski prevozniki očitno niso organi pregona, medtem ko so posredniki lahko tudi subjekti iz zasebnega sektorja. Tudi glede EIP, ki naj bi bile javni organ, je treba poudariti, da nimajo vsi javni organi narave in pristojnosti, da bi rutinsko opravljali naloge kazenskega pregona.

58. Običajno so dejavnosti kazenskega pregona jasno ločene od dejavnosti zasebnega sektorja, pri čemer naloge kazenskega pregona opravljajo posebej temu namenjeni organi, zlasti policija, zasebni subjekti pa so od primera do primera naprošeni, da tem organom pregona pošljejo osebne podatke. Sedaj obstaja tendenca, da bi k sodelovanju za namene kazenskega pregona sistematično pritegnili zasebne subjekte, zaradi česar se pojavlja vprašanje, kateri okvir za varstvo podatkov (prvi ali tretji steber) velja za pogoje za takšno sodelovanje: ali bi bilo treba pravila utemeljiti na naravi nadzornika podatkov (zasebni sektor) ali na predvidenem namenu (kazenski pregon)?

59. ENVP je že opozoril na tveganje pravne vrzeli med dejavnostmi iz prvega in tretjega stebra ([1]). Zares je zelo nejasno, ali dejavnosti zasebnih podjetij, ki so na nek način povezane z uveljavljanjem kazenskega prava, spadajo v področje ukrepanja zakonodajalca Evropske unije v skladu s členi 30, 31 in 34 PEU.

60. Če se splošni okvir (tj. prvi steber) ne bi uporabljal, bi imel izvajalec storitev težko nalogo, da razlikuje znotraj svojih zbirk podatkov. Pod sedanjo ureditvijo je jasno, da mora nadzornik podatkov zagotavljati varstvo podatkov oseb, na katere se ti podatki nanašajo, v enaki meri ne glede na namene, ki upravičujejo hrambo podatkov. Zaradi tega bi se bilo torej treba izogniti temu, da bi se za obdelavo podatkov s strani izvajalcev storitev za različne namene uporabljali različni okviri za varstvo podatkov.

([1]) Glej Mnenje evropskega nadzornika za varstvo podatkov o Sporočilu Komisije Evropskemu parlamentu in Svetu o nadaljevanju delovnega programa za boljše izvajanje Direktive o varstvu podatkov (UL C 255, 27.10.2007, str. 1). Glej tudi Letno poročilo za leto 2006, str. 47.

Uveljavljanje pravic posameznikov, na katere se nanašajo podatki

61. Če bi se na nacionalni ravni uporabljale različne pravne ureditve, bi to imelo zelo velik učinek predvsem na uveljavljanje pravic posameznikov, na katere se nanašajo podatki.

62. V preambuli predloga je navedeno, da je treba v okviru okvirnega sklepa o varstvu podatkov zagotoviti pravice do informacij, dostopa, popravkov, izbrisa, zamrznitve ter odškodnine in pravnih sredstev. Vendar pa ta navedek ne odgovori na vprašanje, kateri nadzornik je pristojen za odgovarjanje na zahteve posameznikov, na katere se nanašajo podatki.

63. Medtem ko bi informacije o obdelavi letalski prevozniki lahko posredovali, pa je dostop do podatkov ali njihovo popravljanje bolj zapleteno vprašanje. Ti dve pravici sta po okvirnem sklepu o varstvu podatkov zares omejeni. Kakor je bilo že povedano, ni gotovo, ali bi lahko izvajalca storitev, na primer letalskega prevoznika, zavezali k temu, da bi omogočal pravico dostopa in pravico do popravljanja podatkov, ki jih ima, različno glede na uporabljen namen (komercialni namen ali namen kazenskega pregona). Lahko bi utemeljevali, da bi bilo ti dve pravici treba uveljavljati pri EIP ali drugih določenih pristojnih organih. Vendar pa v predlogu ni drugih navedb v tem smislu in, kot je že bilo povedano, prav tako ni jasno, ali bodo ti organi (vsaj EIP) organi kazenskega pregona, ki običajno izvajajo postopke v zvezi z omejenim (po možnosti posrednim) dostopom.

64. Posameznik bi bil lahko soočen tudi z različnimi prejemniki podatkov, kar zadeva EIP, saj se podatki dejansko res pošiljajo EIP v državi odhoda/prihoda leta, lahko pa tudi EIP v drugih državah članicah, odvisno od primera. Poleg tega je mogoče, da več držav članic ustanovi ali določi le eno in skupno EIP. Posameznik, na katerega se nanašajo podatki, bi se v takšnem primeru morda moral pritožiti pri organu druge države članice. Pri tem spet ni jasno, ali bodo veljali nacionalni predpisi glede varstva podatkov (ki naj bi bili usklajeni na ravni EU) ali pa se bo upoštevala posebna zakonodaja v zvezi s kazenskim pregonom (glede na nezadostno uskladitev v tretjem stebru na ravni držav).

65. Isto vprašanje velja v zvezi z dostopom do podatkov, ki jih obdelujejo posredniki, katerih status je nejasen in s katerimi lahko hkrati sodelujejo letalski prevozniki iz različnih držav EU.

66. ENVP obžaluje, da uveljavljanje teh temeljnih pravic posameznikov, na katere se nanašajo podatki, še vedno ostaja negotovo. Poudarja, da se lahko takšno stanje pripiše predvsem dejstvu, da se takšne obveznosti naložijo subjektom, katerih glavna naloga sicer ni kazenski pregon.

Sklep

67. ENVP meni, da bi bilo treba v predlogu jasno navesti, katera pravna ureditev se uporablja v posameznih fazah obdelave in pri katerem akterju oziroma organu je treba zaprositi za dostop ali se pritožiti. ENVP opozarja, da bi morale biti v skladu s členom 30(1)(b) PEU določbe o varstvu podatkov ustrezne in zajemati celo vrsto postopkov za obdelavo, določenih v predlogu. Preprosto sklicevanje na okvirni sklep o varstvu podatkov ne zadostuje zaradi omejenega področja uporabe tega okvirnega sklepa in omejitve pravic v njem. V zvezi s sodelovanjem organov kazenskega pregona bi se morala pravila iz okvirnega sklepa o varstvu podatkov uporabljati vsaj za celotno obdelavo, predvideno po predlogu, da bi zagotovili usklajeno uporabo načel o varstvu podatkov.

IV. **NARAVA PREJEMNIKOV**

68. ENVP ugotavlja, da v predlogu ni posebej razložena narava prejemnikov osebnih podatkov, ki jih zbirajo letalski prevozniki, torej niti posrednikov niti enot za informacije o potnikih in niti pristojnih organov. Treba je poudariti, da je narava prejemnika neposredno povezana z vrsto zagotovil glede varstva podatkov, po katerih se ravna ta prejemnik. Razlika med zagotovili, ki jih določajo zlasti pravila za prvi in tretji steber, je že bila omenjena. Bistvenega pomena je, da se razjasni, katero ureditev naj bi uporabljali vsi zadevni akterji, vključno z nacionalnimi vladami, organi kazenskega pregona, organi za varstvo podatkov in nadzorniki podatkov ter posamezniki, na katere se nanašajo podatki.

Posredniki

69. V predlogu ni navedeno, kakšno naravo imajo posredniki ([1]). Prav tako ni podrobno razložena vloga posrednikov kot nadzornikov ali obdelovalcev podatkov. Iz prakse se zdi, da bi se subjektu iz zasebnega sektorja, na primer računalniškemu sistemu rezervacij ali drugemu subjektu, prav lahko zaupala naloga zbiranja podatkov PNR neposredno od letalskih prevoznikov in njihovo posredovanje EIP. Na takšen način se obdelujejo podatki v okviru sporazuma o PNR s Kanado. Za obdelavo podatkov je odgovorna družba SITA ([2]). Vloga posrednika je odločilna, saj bi ta lahko bil odgovoren za filtriranje/preoblikovanje podatkov, ki jih letalski prevozniki posredujejo v neprečiščeni obliki ([3]). Tudi če bi posredniki morali izbrisati obdelane podatke, potem ko so jih posredovali EIP, pa je že sama obdelava zelo občutljiva – posledica faze posrednikov je vzpostavitev dodatne podatkovne zbirke, v kateri so zbrane ogromne količine podatkov, med drugim, glede na predlog, tudi občutljivih podatkov (posredniki morajo v takšnem primeru te občutljive podatke izbrisati). Zaradi tega ENVP priporoča, da posredniki ne bi bili vključeni v obdelavo podatkov o potnikih, razen če se natančno opredelijo njihova narava in naloge.

Enote za informacije o potnikih

70. EIP imajo odločilno vlogo pri identificiranju oseb, ki so ali bi lahko bile udeležene pri terorizmu ali organiziranemu kriminalu ali povezane z njima. Glede na predlog bodo odgovorne za oblikovanje kazalnikov tveganja in zagotavljanje obveščevalnih podatkov o potovalnih vzorcih ([4]). Če je ocena tveganja utemeljena na standardiziranih potovalnih vzorcih in ne na stvarnih dokazih, povezanih s konkretnim primerom, lahko analiza šteje za proaktivno preiskavo. ENVP poudarja, da je takšna vrsta obdelave načeloma strogo urejena z zakonodajo države članice (če je že ne prepoveduje), za obdelavo pa so odgovorni posebni javni organi, katerih delovanje je prav tako strogo urejeno.

71. EIP je torej zaupana zelo občutljiva obdelava podatkov, ne da bi bili v predlogu natančneje opredeljeni njihova narava in pogoji, pod katerimi bi izvajale to pristojnost. Čeprav bo to nalogo verjetno opravljal vladni organ, po možnosti carinska ali mejna kontrola, pa predlog ne prepoveduje izrecno, da bi države članice njeno opravljanje zaupale obveščevalnim službam ali celo kakšnemu obdelovalcu. ENVP poudarja, da preglednost in jamstva, ki veljajo za obveščevalne službe, niso vedno enaka tistim, ki držijo za tradicionalne organe kazenskega pregona. Odločilna je podrobna opredelitev narave EIP, saj bo to imelo neposredne posledice glede pravnega okvira, ki se uporablja, in zahtev v zvezi z nadzorom. ENVP meni, da je treba v predlog vključiti dodatno določbo za podrobno opredelitev posebnih lastnosti EIP.

([1]) Člen 6 predloga.

([2]) Družbo SITA je leta 1949 ustanovilo 11 letalskih prevoznikov. SITA INC (Information, Networking Computing) je komercialna družba, ki ponuja rešitve z dodano vrednostjo za sektor zračnega prometa, SITA SC pa ponuja omrežne storitve na podlagi sodelovanja.

([3]) Presoja vpliva, priloga A, „Način posredovanja podatkov s strani prevoznikov“.

([4]) Člen 3 predloga.

Pristojni organi

72. Iz člena 4 predloga bi lahko sklepali, da podatke lahko prejme kateri koli organ, ki je pristojen za preprečevanje terorističnih kaznivih dejanj in organiziranega kriminala ali za boj proti njim. Medtem ko je namen jasno opredeljen, pa narava organa ni. V predlogu ni predvideno, da bi bili prejemniki omejeni le na organe kazenskega pregona.

Kot že prej v zvezi z EIP je odločilnega pomena, da se zadevni občutljivi podatki obdelujejo v okolju, za katerega velja jasen pravni okvir. To veliko bolj drži, na primer, za organe kazenskega pregona kot pa za obveščevalne službe. Glede na elemente rudarjenja podatkov in proaktivnega iskanja iz predloga pa ni mogoče izključiti, da te obveščevalne službe ali kakršne koli druge vrste organov ne bodo sodelovale pri obdelovanju podatkov.

Sklep

73. ENVP na splošno ugotavlja, da je uveljavitev sistema PNR EU postala še težja, saj imajo organi kazenskega pregona glede na nacionalno pravo držav članic različne pristojnosti v zvezi z obveščevalnimi podatki, davki, priseljevanjem ali policijo. To je še dodatni razlog za priporočilo, da je treba v predlogu precej bolj natančno opredeliti naravo omenjenih akterjev in jamstva glede nadzorovanja opravljanja njihovih nalog. V predlog bi bilo treba vključiti dodatne določbe, da bi natančno določili pristojnosti in pravne obveznosti posrednikov, EIP in drugih pristojnih organov.

V. **POGOJI ZA POSREDOVANJE PODATKOV TRETJIM DRŽAVAM**

74. V predlogu je določenih nekaj varoval v zvezi s posredovanjem podatkov PNR v tretje države ([1]). Zlasti je izrecno določeno, da se za posredovanje podatkov uporablja okvirni sklep o varstvu podatkov, določena je omejitev na poseben namen in potreba po soglasju države članice v primeru nadaljnjega posredovanja podatkov drugi tretji državi. Posredovanje mora biti tudi v skladu z nacionalno zakonodajo zadevne države članice in z vsemi veljavnimi mednarodnimi sporazumi.

75. Nerazjasnjenih pa je še veliko vprašanj, predvsem v zvezi z naravo soglasja, pogoji za uporabo okvirnega sklepa o varstvu podatkov ter vprašanje „vzajemnosti“ v primeru pošiljanja podatkov tretjim državam.

([1]) Člen 8 predloga.

Narava soglasja

76. Država članica izvora mora dati izrecno soglasje za posredovanje podatkov iz tretje države v drugo tretjo državo. V predlogu ni opredeljeno, pod kakšnimi pogoji bo dano to soglasje in kdo ga bo dal niti ali bi morali pri tej odločitvi sodelovati tudi nacionalni organi za varstvo podatkov. ENVP meni, da bi moral biti način, kako bo soglasje dano, skladen vsaj z nacionalnim pravom, ki določa pogoje za posredovanje osebnih podatkov v tretje države.

77. Poleg tega soglasje države članice ne bi smelo prevladati nad načelom, po katerem mora država prejemnica zagotoviti ustrezno raven varstva podatkov pri predvideni obdelavi. Ti pogoji bi morali biti kumulativni, kakor so tudi v okvirnem sklepu o varstvu podatkov (člen 14). ENVP zato predlaga, da se členu 8(1) doda točka (c) z besedilom: „in (c) tretja država zagotavlja ustrezno raven varstva pri predvideni obdelavi podatkov“. ENVP v tem oziru opozarja, da je treba vzpostaviti mehanizme, ki glede ustreznosti zagotavljajo skupne standarde in usklajene odločitve ([2]).

Uporaba okvirnega sklepa o varstvu podatkov

78. Predlog se sklicuje na pogoje in varovala iz okvirnega sklepa o varstvu podatkov, izrecno pa navaja tudi nekatere pogoje, zlasti omenjeno soglasje zadevne države članice in omejitev namena na preprečevanje terorističnih kaznivih dejanj in organiziranega kriminala ter boj proti njim.

79. Okvirni sklep o varstvu podatkov določa pogoje za prenos osebnih podatkov v tretje države, in sicer glede omejitve namena, narave prejemnikov, soglasja države članice in načela o ustreznosti. Predvideva pa tudi odstopanja od teh pogojev za prenos, in sicer so zakoniti veljavni interesi, zlasti pomembni javni interesi, lahko zadostna podlaga za prenos, tudi če našteti pogoji niso izpolnjeni.

80. Kakor je že bilo omenjeno v poglavju III tega mnenja, ENVP meni, da je treba v besedilu predloga jasno navesti, da bolj natančna jamstva iz predloga prevladajo nad splošnimi pogoji – in izjemami – iz okvirnega sklepa o varstvu podatkov, kjer se uporablja.

([2]) Mnenje ENVP z dne 26. junija 2007 o Predlogu okvirnega sklepa Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, točke 27 do 30 (UL C 139, 23.6.2007, str. 1).

Vzajemnost

81. V predlogu se obravnava vprašanje morebitnih „zahtev v zameno“, ki bi jih države lahko predložile EU, da bi od nje dobile podatke PNR za lete iz EU na njihovo ozemlje. Če EU zahteva podatke iz podatkovnih zbirk letalskih prevoznikov teh tretjih držav, ker opravljajo lete v EU oziroma iz EU, bi lahko te tretje države isto zahtevale od letalskih prevoznikov iz EU, vključno s podatki državljanov EU. Čeprav Komisija meni, da ta možnost ni „zelo verjetna“, pa jo vseeno upošteva. V tem oziru je v predlogu omenjeno, da se v sporazumih z ZDA in Kanado predvideva takšna vzajemna obravnava, „ki bi se lahko uveljavila samodejno“ ([1]). ENVP ima dvome glede pomena takšne samodejne vzajemnosti in uporabe varoval za takšne prenose, še posebno ob upoštevanju obstoja ustrezne ravni varstva v zadevni državi.

82. Treba bi bilo razlikovati med tretjimi državami, ki so z EU že sklenile sporazum, in državami, s katerimi še ni takšnega sporazuma.

Države, ki nimajo sporazuma z EU

83. ENVP ugotavlja, da bi lahko vzajemnost privedla do tega, da bi se osebni podatki pošiljali državam, ki ne morejo dati nobenih zagotovil glede demokratičnih standardov in ustrezne ravni varstva podatkov.

84. V presoji vpliva so navedeni še drugi elementi glede pogojev prenosa podatkov v tretje države. Poudarjene so prednosti sistema PNR EU, v katerem podatke filtrirajo EIP. Pristojnim organom držav članic in domnevno tudi tretjim državam naj bi se pošiljali le izbrani podatki o osumljenih posameznikih (in ne podatki v neprečiščeni obliki) ([2]). ENVP priporoča, da bi se v besedilu predloga to vprašanje razjasnilo. Preprost navedek v presoji vpliva pa ne zagotavlja potrebnega varstva.

85. Izbiranje podatkov bi prispevalo k temu, da se kar najbolj zmanjša vpliv na zasebnost potnikov, treba pa je opozoriti, da načela o varstvu podatkov segajo precej dlje od tega, da se čim bolj zmanjša količina podatkov, saj vključujejo tudi načela glede potrebnosti, preglednosti in uveljavljanja pravic posameznikov, na katere se nanašajo podatki, vsa ta pravila pa je treba upoštevati pri ugotavljanju, ali tretja država zagotavlja ustrezno raven varstva.

Države, ki imajo z EU dvostranski sporazum

86. V presoji vpliva je navedeno, da bo takšna obdelava zagotovila, da bo EU lahko „vztrajala pri nekaterih standardih in zagotovila doslednost pri takšnih dvostranskih sporazumih s tretjimi državami. Zagotovila bo tudi možnost, da se od tretjih držav, s katerimi ima EU sporazum, zahteva vzajemnost, kar danes sicer ni možno“ ([3]).

87. Iz teh opažanj izhaja vprašanje, kako bo predlog vplival na obstoječa sporazuma s Kanado in ZDA. Pogoji dostopa do podatkov so v teh sporazumih dejansko precej bolj prožni, saj podatki niso predmet podobnega izbiranja, preden se pošljejo zadevnima tretjima državama.

88. V presoji vpliva je navedeno, da „se v primerih, ko ima EU s tretjo državo mednarodni sporazum o izmenjavi/prenosu podatkov iz PNR v to tretjo državo, takšni sporazumi ustrezno upoštevajo. Prevozniki bi morali podatke PNR poslati enotam za informacije o potnikih v skladu z običajno prakso v okviru sedanjega ukrepa. EIP, ki sprejme te podatke, jih pošlje pristojnemu organu tretje države, s katero je takšen sporazum sklenjen“ ([4]).

89. Medtem ko se zdi, da je po eni strani cilj predloga prenos *le izbranih* podatkov pristojnim organom v EU ali zunaj nje, pa je v presoji vpliva, preambuli predloga (uvodna izjava 21) in členu 11 navedeno, da je treba ustrezno upoštevati obstoječe sporazume. Iz tega bi lahko sklepali, da bi lahko bilo filtriranje podatkov veljavno le za sporazume, ki se bodo sklenili v prihodnje. S tega vidika bi lahko predvidevali, da bo dostop do podatkov v neprečiščeni obliki še vedno praviloma veljal za dostop, na primer, organov ZDA do podatkov PNR – v skladu z določbami sporazuma med EU in ZDA, vzporedno in glede na posamezen primer pa bi lahko prišlo tudi do prenosa podatkov v ZDA, tj. posebnih podatkov, ki jih izberejo EIP, vključno s podatki, ki zadevajo lete v ZDA, a ne omejeno le nanje.

90. ENVP obžaluje, da ta odločilni poudarek predloga ni dovolj razjasnjen. Meni, da je izredno pomembno, da so pogoji za prenos podatkov PNR v tretje države jasni in da za podatke velja usklajena raven varstva. Poleg tega bi bilo treba zaradi pravne varnosti vključiti podrobnosti glede zagotovil, ki veljajo za prenos podatkov, v predlog kot tak in ne le v presojo vpliva, kot je to sedaj.

([1]) Obrazložitveni memorandum predloga, poglavje 2.
([2]) Presoja vpliva, poglavje 5.2, „Varstvo zasebnosti“.
([3]) Presoja vpliva, poglavje 5.2, „Odnosi s tretjimi državami“.
([4]) Presoja vpliva, Priloga A, „Organi, ki prejemajo podatke od enot za informacije o potnikih“.

VI. **DRUGA VSEBINSKA VPRAŠANJA**

Avtomatizirana obdelava podatkov

91. ENVP ugotavlja, da predlog izrecno izključuje, da bi enote za informacije o potnikih in pristojni organi držav članic sprejeli izvršilne ukrepe zgolj na podlagi avtomatizirane obdelave podatkov PNR ali rasnega ali etičnega porekla, verskih ali filozofskih prepričanj, političnih mnenj ali spolne usmerjenosti osebe ([1]).

92. Takšno pojasnilo je dobrodošlo, saj se tako omeji nevarnost samovoljnih ukrepov proti posameznikom. ENVP pa vseeno ugotavlja, da je pojasnilo omejeno na *izvršilne ukrepe* EIP ali pristojnih organov. Sedanja različica besedila ne izključuje avtomatiziranega filtriranja posameznikov glede na standardne profile, prav tako ne preprečuje avtomatiziranega sestavljanja seznamov osumljenih oseb in sprejemanja takšnih ukrepov, kot je razširjeni nadzor, če ti ukrepi ne štejejo za izvršilne ukrepe.

93. ENVP meni, da je pojem *izvršilnih ukrepov* preveč nedoločen in da se nobena odločitev glede posameznikov načeloma ne bi smela sprejeti *le* zaradi avtomatizirane obdelave njihovih podatkov ([2]). ENVP priporoča, da se besedilo ustrezno spremeni.

Narava podatkov

94. V predlogu je v členu 5(2) navedena pomembna podrobnost, in sicer da letalskim prevoznikom ni treba zbirati ali hraniti drugih podatkov, kakor so podatki, zbrani za prvotne komercialne namene.

95. Še vedno pa je treba dodatno razložiti več vidikov obdelave teh podatkov:

— Podatki, ki jih je treba dati na razpolago in so našteti v prilogi 1 predloga, so zelo obširni, seznam pa je podoben seznamu podatkov, ki so na voljo organom ZDA po sporazumu med EU in ZDA. Glede narave nekaterih podatkov, ki se zahtevajo, so organi za varstvo podatkov že večkrat izrazili dvome, zlasti Delovna skupina iz člena 29 ([3]).

— Iz besedila presoje vpliva ([4]) in člena 6(3) predloga bi lahko sklepali, da bi letalski prevozniki lahko podatke posrednikom pošiljali tudi v neprečiščeni obliki. V prvi fazi se podatki, ki se pošljejo tretji strani, celo ne bi omejevali v skladu s podatki PNR, naštetimi v prilogi 1 predloga.

— V zvezi z obdelovanjem občutljivih podatkov, čeprav bi se ti podatki lahko odstranili v fazi posrednikov, še vedno ostaja vprašanje, ali je zares potrebno, da letalski prevozniki pošiljajo podatke iz odprtih rubrik.

V tem oziru ENVP podpira poudarke iz mnenja WP29.

Metoda prenosa podatkov PNR

96. Letalski prevozniki s sedežem zunaj EU morajo EIP ali posrednikom posredovati podatke po metodi *push*, če imajo za to tehnično infrastrukturo. Če je nimajo, bodo morali dovoliti, da se podatki črpajo z metodo *pull*.

97. Zadevni letalski prevozniki pošiljajo podatke na različne načine, zaradi česar se bo pojavilo še več težav v zvezi z nadzorom skladnosti prenosa podatkov PNR s pravili o varstvu podatkov. Zaradi tega obstaja tudi tveganje, da bo izkrivljena konkurenca med letalskimi prevozniki iz EU in zunaj nje.

98. ENVP opozarja, da je metoda *push*, ki letalskim prevoznikom omogoča, da nadzorujejo vrsto poslanih podatkov in okoliščine prenosov, edina dopustna metoda z ozirom na sorazmernost obdelave. Poleg tega mora vsebovati dejanski „*push*“, tj. podatki se posredniku ne smejo poslati v neprečiščeni obliki, temveč jih je treba filtrirati že v prvi fazi obdelave. Nedopustno je, da bi se nepotrebni podatki – in podatki, ki niso vključeni v prilogo 1 predloga – pošiljali tretji strani, čeprav bi ta takoj izbrisala te podatke.

Hramba podatkov

99. Člen 9 predloga predvideva petletno obdobje hrambe podatkov PNR in dodatno osemletno obdobje, v katerem naj bi se podatki hranili v „mirujoči“ podatkovni zbirki, ki bo dostopna pod omejenimi pogoji.

([1]) Uvodna izjava 20 ter člen 3(3) in (5) predloga.

([2]) V tem oziru glej člen 15(1) Direktive 95/46/ES. Direktiva prepoveduje takšne avtomatizirane odločitve v primerih, ko bi lahko imele posledice za posameznika. Glede na kontekst predloga pa je zelo verjetno, da bodo odločitve v okviru kazenskega pregona imele precejšnje posledice za posameznike, na katere se nanašajo podatki. Tudi sekundarni pregledi lahko vplivajo na posameznika, na katerega se nanašajo podatki, zlasti če se ti ukrepi večkrat izvajajo.

([3]) Glej zlasti Mnenje št. 5/2007 z dne 17. avgusta 2007 o nadaljnjem spremljanju sporazuma med Evropsko unijo in Združenimi državami Amerike o obdelavi in prenosu podatkov iz evidence podatkov o potnikih (PNR) s strani letalskih prevoznikov ministrstvu Združenih držav za domovinsko varnost, sklenjenem julija 2007, WP 138.

([4]) Presoja vpliva, priloga A, „Način posredovanja podatkov s strani prevoznikov“.

100. ENVP se sprašuje, kakšna je razlika med tema dvema vrstama podatkovnih zbirk. Vprašanje je, ali je mirujoča podatkovna zbirka zares arhiv z različnimi metodami shranjevanja in priklica podatkov. Večina pogojev za dostop do mirujoče podatkovne zbirke dejansko vsebuje varnostne zahteve, ki bi se lahko uporabljale tudi za „podatkovno zbirko, v kateri se podatki hranijo pet let".

101. Celotno trajanje hrambe, tj. 13 let, je v vsakem primeru pretirano. V presoji vpliva je ta čas utemeljen s potrebo, da se pripravijo kazalci tveganja ter opredelijo potovalni in vedenjski vzorci ([1]), učinkovitost katerih je treba še dokazati. Medtem ko je očitno, da se lahko med preiskavo, ki še teče, podatki hranijo toliko časa, kot je to potrebno v posameznem primeru, pa nikakor ni mogoče upravičiti trinajstletne hrambe podatkov vseh potnikov, če ni nikakršnega suma.

102. ENVP ugotavlja tudi, da tega obdobja hrambe ne podpirajo niti odgovori držav članic na vprašalnik Komisije, v skladu s katerimi naj bi bilo zahtevano povprečno trajanje hrambe tri leta in pol ([2]).

103. Poleg tega bi lahko obdobje 13 let primerjali s petnajstletnim obdobjem hrambe iz zadnjega sporazuma z Združenimi državami. ENVP razume, da je bilo to dolgo obdobje hrambe odobreno le zaradi velikih pritiskov vlade ZDA, da bi bilo obdobje precej daljše od treh let in pol, česar ne Svet ne Komisija nista zagovarjala v nobeni fazi. Nobenega razloga pa ni, da bi takšen kompromis, ki je bil upravičen le kot nujni rezultat pogajanj, prenesli v pravni instrument na ravni EU.

Vloga odbora držav članic

104. Odbor držav članic, ustanovljen po členu 14 predloga, bo pristojen za varnostna vprašanja, vključno s protokolom in šifriranjem podatkov PNR, pa tudi za smernice glede skupnih splošnih meril, metod in prakse za ocene tveganja.

105. Razen teh navedb pa predlog ne vsebuje drugih elementov ali meril glede konkretnih pogojev in okvira za postopek ocene tveganja. V presoji vpliva je omenjeno, da bodo v končni fazi merila odvisna od obveščevalnih podatkov, ki jih imajo posamezne države članice in se neprestano razvijajo. Ocena tveganja naj bi se tako izvajala brez enotnih standardov za identifikacijo osumljencev. Zaradi tega se zdi negotovo, v kakšnem obsegu bo odbor držav članic lahko s tega vidika imel vlogo.

Varovanje

106. V predlogu je podrobno opisana vrsta varnostnih ukrepov ([3]), ki naj bi jih v zvezi z varstvom podatkov sprejeli EIP, posredniki in drugi pristojni organi. Glede na pomen podatkovne zbirke in občutljivost obdelave podatkov ENVP meni, da bi se moral subjekt, ki obdeluje podatke, držati predvidenih ukrepov, obenem pa tudi uradno sporočiti kakršno koli kršitev varnosti.

107. ENVP je seznanjen s projektom za vzpostavitev takšnega postopka obveščanja na področju elektronskih komunikacij na evropski ravni. Priporoča, da bi takšno varovalo vključili v zadevni predlog in se v tem oziru navezuje na sistem za kršitve varnosti, ki je bil vzpostavljen v Združenih državah v zvezi z državnimi agencijami ([4]). Do nezgod na področju varnosti lahko pride na katerem koli področju dejavnosti v zasebnem in javnem sektorju, kakor se je pokazalo nedavno, ko je britanska uprava izgubila celotne podatkovne zbirke državljanov ([5]). Obsežne podatkovne zbirke, kakor je zbirka, ki se predvideva po predlogu, bi bile prve na prednostnem seznamu uporabnikov takšnega sistema opozarjanja.

Klavzula o pregledu in časovni omejitvi veljavnosti

108. ENVP ugotavlja, da naj bi se v treh letih po začetku veljavnosti okvirnega sklepa izvedel pregled na podlagi poročila, ki ga pripravi Komisija. Ugotavlja, da bo v tem pregledu na podlagi informacij, ki jih priskrbijo države članice, posebna pozornost namenjena varovalom za varstvo podatkov, pregledani pa bodo tudi izvajanje metode „*push*", hramba podatkov in kakovost ocene tveganja. Da bi bil takšen pregled izčrpen, bi moral zajemati rezultate analize statističnih podatkov, izdelanih na podlagi obdelave podatkov PNR. V te statistične podatke bi morali poleg elementov, navedenih v členu 18 predloga, vključiti tudi statistične podrobnosti glede identifikacije oseb, ki predstavljajo veliko tveganje, na primer merila za takšno identifikacijo ter konkretne rezultate vsakršnih ukrepov kazenskega pregona, ki izhajajo iz identifikacije.

([1]) Presoja vpliva, Priloga A, „Obdobje hrambe podatkov".
([2]) Presoja vpliva, priloga B.
([3]) Člen 12 predloga.
([4]) Glej zlasti prispevke ameriške delovne skupine za ugotavljanje kraje identitete (*Identity Theft Task Force*), http://www.idtheft.gov/.
([5]) Glej povezavo na spletno stran britanskega davčnega in carinskega urada Njenega Veličanstva (*HM Revenue and Customs*): http://www.hmrc.gov.uk/childbenefit/update-faqs.htm. Glej tudi: http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm.

109. ENVP je v tem mnenju že omenil pomanjkanje konkretnih elementov, s katerimi bi ugotovili, ali je predlagani sistem zares potreben. Vseeno pa meni, da bi bilo treba okvirni sklep v primeru, da začne veljati, dopolniti vsaj še s klavzulo o časovni omejitvi njegove veljavnosti. Okvirni sklep bi bilo treba po poteku treh let razveljaviti, če ne bi bilo elementov, ki bi podprli njegovo nadaljevanje.

Učinek na druge pravne instrumente

110. V končnih določbah je v predlogu naveden pogoj glede nadaljnje uporabe že obstoječih dvostranskih ali večstranskih sporazumov ali ureditev. Ti instrumenti se lahko uporabljajo le, če so združljivi s cilji predlaganega okvirnega sklepa.

111. ENVP ima dvome glede področja uporabe te določbe. Kot je bilo že omenjeno v poglavju V pod „Vzajemnost“, ni jasno, kakšen učinek bo ta določba imela na vsebino sporazumov s tretjimi državami, na primer na sporazum z ZDA. Po drugi strani prav tako ni jasno, ali bi določba lahko imela učinek na pogoje uporabe instrumentov s širšim področjem uporabe, na primer na konvencijo Sveta Evrope št. 108. Ker gre za različna institucionalna ozadja in različne udeležene akterje, ni veliko možnosti za napačno razlago, ne glede na to pa bi se bilo treba izogniti vsakršnemu tveganju v zvezi z njo in v predlogu jasno navesti, da predlog nima učinka na instrumente s širšim področjem uporabe, zlasti na tiste, katerih predmet je varstvo temeljnih pravic.

VII. **SKLEP**

112. ENVP izpostavlja glavne učinke v zvezi z varstvom podatkov iz zadevnega predloga. V analizi se osredotoča na štiri temeljna vprašanja, ki jih sproža predlog, in vztraja, da je treba ta vprašanja izčrpno obravnavati. V sedanjih okoliščinah predlog ni skladen s temeljnimi pravicami, zlasti s členom 8 Listine o temeljnih pravicah Evropske unije, in ne bi smel biti sprejet.

113. Da bi se ravnali po zgoraj navedenih pripombah, zlasti v zvezi s preizkusom legitimnosti, je v tem mnenju navedenih nekaj predlogov za besedilo, ki bi jih moral zakonodajalec upoštevati. Zlasti je treba navesti točke 67, 73, 77, 80, 90, 93, 106, 109 in 111 tega mnenja.

Legitimnost predlaganih ukrepov

114. Medtem ko je splošen namen boja proti terorizmu in organiziranemu kriminalu sam po sebi jasen in legitimen, pa samo bistvo obdelave podatkov, ki se bo izvajala, ni dovolj opredeljeno in upravičeno.

115. ENVP meni, da je treba dodatno oceniti tehnike, s katerimi se ocenjuje tveganje, ki ga predstavljajo posamezniki, in sicer z uporabo orodij za rudarjenje podatkov in vedenjskih vzorcev, njihovo koristnost pa je treba jasno opredeliti v okviru boja proti terorizmu, še preden se uporabijo v tako velikem obsegu.

116. Opiranje na različne podatkovne zbirke brez celotnega pogleda na dejanske rezultate in pomanjkljivosti:

— je v nasprotju z racionalno zakonodajno politiko, po kateri se novi instrumenti ne smejo sprejeti, dokler obstoječi niso bili v celoti uveljavljeni in so se izkazali za nezadostne,

— bi lahko sicer pomenilo korak proti popolnemu nadzoru družbe.

117. Boj proti terorizmu je vsekakor lahko legitimen razlog za uporabo izjem od temeljnih pravic do zasebnosti in varstva podatkov. Da pa se ga utemelji, je treba nujnost poseganja podpreti z jasnimi in nespornimi elementi ter dokazati sorazmernost obdelave. To je še toliko bolj potrebno v primeru večjega poseganja v zasebnost posameznikov, kot je to predvideno v predlogu.

118. V predlogu ni takšnih utemeljitvenih elementov, preizkus glede nujnosti in sorazmernosti pa ne vzdrži.

119. ENVP vztraja, da je preizkus glede nujnosti in sorazmernosti, kot je opisano zgoraj, bistvenega pomena. Je neobhodni pogoj za uveljavitev predloga.

Pravni okvir, ki se uporablja

120. ENVP ugotavlja, da je pravna varnost v zvezi z ureditvijo, ki se uporablja za različne akterje v projektu, zlasti pa za letalske prevoznike in druge akterje iz prvega stebra, zelo pomanjkljiva, najsi gre za pravila iz predloga, pravila iz okvirnega sklepa o varstvu podatkov ali pa nacionalno zakonodajo za uveljavitev Direktive 95/46/ES. Zakonodajalec bi moral jasno navesti, v katerih fazah obdelave podatkov se bodo ta različna pravila uporabljala.

121. Trenutna tendenca je, da bi bili zasebni subjekti sistematično zavezani k sodelovanju za namene kazenskega pregona, zaradi česar se pojavlja vprašanje, kateri okvir za varstvo podatkov (prvi ali tretji steber) velja za pogoje za takšno sodelovanje: ni jasno, ali bi morala pravila temeljiti na naravi nadzornika podatkov (zasebni sektor) ali na predvidenem namenu (kazenski pregon).

122. ENVP je že izpostavil tveganje pravne vrzeli med dejavnostmi iz prvega in tretjega stebra ([1]). Zares je zelo nejasno, ali dejavnosti zasebnih podjetij, ki so na nek način povezane z uveljavljanjem kazenskega prava, spadajo v področje ukrepanja zakonodajalca Evropske unije v skladu s členi 30, 31 in 34 PEU-ja.

123. Zaradi tega bi se bilo treba izogniti temu, da bi se za obdelavo podatkov s strani izvajalcev storitev za različne namene uporabljali različni okviri za varstvo podatkov, zlasti če upoštevamo težave, ki bi jih to povzročilo v zvezi z uveljavljanjem pravic posameznikov, na katere se nanašajo podatki.

Narava prejemnikov

124. V predlogu bi bilo treba posebej razložiti naravo prejemnikov osebnih podatkov, ki jih zbirajo letalski prevozniki, najsi bodo to posredniki, enote za informacije o potnikih ali pristojni organi.

125. Narava prejemnika, v določenih primerih bi to lahko bili akterji iz zasebnega sektorja, je neposredno povezana z vrsto zagotovil za varstvo podatkov, ki veljajo za zadevnega prejemnika. Bistvenega pomena je, da se vsem udeleženim akterjem pojasni, katera ureditev naj bi se uporabljala, vključno z zakonodajalcem, organi za varstvo podatkov in nadzorniki podatkov ter posamezniki, na katere se nanašajo podatki.

Prenos podatkov v tretje države

126. ENVP poudarja, da je treba zagotoviti, da država prejemnica zagotavlja ustrezno stopnjo varstva. Izraža tudi dvom glede pomena načela „vzajemnosti“ iz predloga in njegove uporabe za države, ki že imajo sporazum z EU, na primer Kanada in ZDA. Meni, da je izredno pomembno, da so pogoji za prenos podatkov PNR v tretje države jasni in da za podatke velja usklajena raven varstva.

Druga vsebinska vprašanja

127. ENVP opozarja zakonodajalca tudi na posebne vidike predloga, ki jih je treba natančneje razjasniti ali v zvezi s katerimi je treba bolje upoštevati načelo varstva podatkov. Zlasti gre pri tem za naslednje vidike:

— pogoje, pod katerimi se sprejemajo avtomatizirane odločitve, bi bilo treba omejiti,

— treba bi bilo zmanjšati količino obdelovanih podatkov,

— prenos podatkov bi se moral opreti le na metodo „*push*“,

— obdobje hrambe podatkov je pretirano in neupravičeno dolgo,

— vloga odbora držav članic bi bila lahko natančneje opredeljena v zvezi z njegovimi vodili glede „ocene tveganja“,

— v varnostne ukrepe bi bilo treba vključiti postopek o „obveščanju o kršitvah varnosti“,

— v pregled sklepa bi bilo treba vključiti klavzulo o časovni omejitvi njegove veljavnosti,

— v predlogu bi bilo treba jasno navesti, da nima učinka na instrumente s širšim področjem uporabe, in sicer tiste, katerih predmet je varstvo temeljnih pravic.

Končne ugotovitve

128. ENVP ugotavlja, da zadevni predlog nastaja v trenutku, ko se bo institucionalni okvir Evropske unije spremenil v osnovi. Posledice lizbonske pogodbe na področju odločanja bodo temeljnega pomena, zlasti glede vloge Parlamenta.

129. Ob upoštevanju neprecedenčnega učinka predloga z vidika temeljnih pravic ENVP priporoča, da se predlog ne sprejme v okviru sedanjega okvira pogodb, temveč da se zanj uporabi postopek soodločanja, predviden po novi pogodbi. To bi utrdilo pravno podlago, na kateri bi se sprejemali odločilni ukrepi, predvideni v predlogu.

([1]) Glej Mnenje evropskega nadzornika za varstvo podatkov o Sporočilu Komisije Evropskemu parlamentu in Svetu o nadaljevanju delovnega programa za boljše izvajanje Direktive o varstvu podatkov (UL C 255, 27.10.2007, str. 1). Glej tudi Letno poročilo za leto 2006, str. 47.