EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

MNENJE EVROPSKEGA NADZORNIKA ZA VARSTVO PODATKOV

— o predlogu Sklepa Sveta o vzpostavitvi, delovanju in uporabi druge generacije Schengenskega informacijskega sistema (SIS II) (COM(2005)230 konč.);

— o predlogu uredbe Evropskega parlamenta in Sveta o vzpostavitvi, delovanju in uporabi druge generacije Schengenskega informacijskega sistema (SIS II) (COM(2005)236 konč.), in

— o predlogu uredbe Evropskega parlamenta in Sveta o dostopu služb držav članic, pristojnih za izdajo potrdil o registraciji vozil, do druge generacije Schengenskega informacijskega sistema (SIS II) (COM(2005)237 konč.).

(2006/C 91/11)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE —

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

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

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

ob upoštevanju Uredbe (ES) št. 45/2001/ES 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 teh podatkov ter zlasti člena 41 Uredbe,

ob upoštevanju prošnje Komisije za mnenje v skladu s členom 28(2) Uredbe (ES) št. 45/2001, prejete 17. junija 2005;

SPREJEL NASLEDNJE MNENJE:

1. UVOD

1.1. Ozadje

Schengenski informacijski sistem (SIS) je obsežni IT sistem Evropske unije, ki je bil vzpostavljen kot izravnalni ukrep po odpravi kontrol na notranjih mejah znotraj Schengenskega območja. SIS pristojnim organom v državah članicah omogoča izmenjavo informacij, ki se uporabljajo pri izvajanju kontrol oseb in predmetov na zunanjih mejah ali na ozemlju in tudi pri izdaji vizumov in dovoljenj za bivanje.

Schengenska konvencija je začela veljati leta 1995 kot medvladni sporazum. SIS je bil kot del Schengenske konvencije kasneje z Amsterdamsko pogodbo vključen v okvir EU.

Nov schengenski informacijski sistem II „druge generacije“ bo zamenjal sedanji sistem in s tem omogočil širitev Schengenskega območja na nove države članice EU. Poleg tega bo v sistem uvedel nove funkcionalnosti. Schengenske določbe, pripravljene v medvladnem okviru, bodo v celoti preoblikovane v klasičnih instrumentih evropskega prava.

Evropska komisija je 1. junija 2005 predstavila tri predloge za vzpostavo SIS II. Ti predlogi zajemajo:

— predlagano uredbo, ki temelji na Naslovu IV Pogodbe ES (vizumi, azil, priseljevanje in druge politike, povezane s prostim gibanjem oseb), ki bo urejala vidike prvega stebra (priseljevanje) SIS II, v nadaljnjem besedilu „predlagana uredba“;

— predlagani sklep, ki temelji na Naslovu VI Pogodbe EU (policijsko in pravosodno sodelovanje v kazenskih zadevah) in bo urejal uporabo SIS namene iz tretjega stebra, v nadaljnjem besedilu „predlagani sklep“;

— predlagano uredbo, ki temelji na Naslovu V (transport) in posebej obravnava dostop do podatkov SIS s strani organov za registracijo vozil; ta predlog bo obravnavan ločeno (glej točko 4.6 spodaj).

V tem kontekstu je vredno omeniti, da bo Komisija v prihodnjih mesecih izdala sporočilo o interoperabilnosti in povečanem sodelovanju med informacijskimi sistemi EU (SIS, VIS, Eurodac).

SIS II sestavlja centralna podatkovna baza, imenovana „Centralni schengenski informacijski sistem“ (CS-SIS), za katero bo Komisija zagotovila operativno vodenje in je povezana z nacionalnimi dostopnimi točkami (NI-SIS), ki jih določi vsaka država članica. Vodstvo omrežja Sirene zagotavlja izmenjavo vseh dodatnih informacij (informacij, povezanih z razpisi ukrepov v SIS II, ki niso shranjeni v SIS II).

Države članice bodo v SIS II prispevale podatke o ljudeh, iskanih za prijetje, predajo ali izročitev, ljudeh, iskanih zaradi sodnih postopkov, ljudeh, ki jih je treba nadzorovati ali so predmet posebnih preverjanj, ljudeh, ki se jim zavrne vstop na zunanjih mejah ter o izgubljenih ali ukradenih predmetih. Skupek podatkov, imenovanih „razpisi ukrepov“, vnesenih v SIS, pristojnemu organu omogoči prepoznati osebo ali predmet.

SIS II razvija nove značilnosti: razširjen dostop do SIS (Europol, Eurojust, državni tožilci, organi za registracijo vozil), medsebojno povezovanje razpisov ukrepov, dodajanje novih kategorij podatkov, vključno z biometričnim podatki (prstni odtisi in fotografije), kot tudi tehnično platformo za izmenjavo z vizumskim informacijskim sistemom. Te dodatne dejavnosti so več let razvnemale razprave glede spremembe namena SIS, in sicer s kontrolnega orodja na obveščevalni in preiskovalni sistem.

1.2. **Splošna ocena predlogov**

1. Evropski nadzornik za varstvo podatkov (ENVP) pozdravlja dejstvo, da so ga vprašali za mnenje na podlagi člena 28(2) Uredbe (ES) št. 45/2001. Vendar je treba glede na obvezen značaj člena 28(2) to mnenje navesti v preambuli besedil.

2. ENVP iz več razlogav pozdravlja predloge. Preoblikovanje medvladne strukture v instrumente evropskega prava prinaša številne pozitivne posledice: pravna vrednost pravil, ki urejajo SIS II, bo jasnejša, Sodišče Evropskih skupnosti bo imelo pristojnosti za interpretacijo prvega stebra pravnih instrumentov, Evropski parlament bo vsaj delno udeležen (čeravno nekoliko pozno).

3. Poleg tega predlogi vsebinsko zajemajo pomemben del, posvečen varstvu podatkov, nekateri od teh pa so dobrodošle izboljšave v primerjavi s sedanjim stanjem. Zlasti lahko omenimo ukrepe za zaščito žrtev kraje identitete, razširitev Uredbe 45/2001 na dejavnosti Komisije v zvezi z obdelavo podatkov v okviru dejavnostih iz naslova VI, boljšo opredelitev razlogov za razspis ukrepov za posameznike v zvezi z zavrnitvijo vstopa.

4. Očitno je tudi, da je bila oblikovanju osnutkov predlogov namenjena velika pozornost; ti so zapleteni, vendar so odraz inherentne zapletenosti sistema, ki ga urejajo. Večina opomb v tem mnenju skuša razjasniti dopolnjujoče določbe, vendar ne bo zahtevala popolnega preoblikovanja.

Vendar se lahko kljub tej v celoti pozitivni oceni izrazi nekatere zadržke, zlasti naslednje:

1. Pogosto je težko razbrati namen besedila; velika škoda je, da mu ni priložen obrazložitveni memorandum. Ker so ti dokumenti zelo zapleteni, bi moral biti ta memorandum osnovna zahteva. Ker ga ni, se mora bralec v nekaterih primerih zateči k ugibanju.

2. Poleg tega je škoda, da ni bilo narejene študije o presoji vplivov. Dejtvo, da prva različica sistema že velja, tega ne opravičuje, saj so med prejšnjim in novim sistemom velike razlike. Med drugim bi bilo treba bolje razmisliti o vplivu uvedbe biometričnih podatkov.

3. Pravni okvir varstva podatkov je zelo zapleten; temelji na kombinirani uporabi *lex generalis* in *lex specialis*. Treba bi bilo zagotoviti, da obstoječi okvir varstva podatkov v Direktivi 95/46/ES in Uredbi 45/2001 v celoti ostane v veljavi, tudi ko se oblikuje posebni zakonodajni akt. Kombinirana uporaba različnih pravnih instrumentov ne bi smela voditi v neskladja med nacionalnimi sistemi v zvezi s temeljnimi vidiki, niti ne bi smela oslabiti sedanje ravni varstva podatkov.

4. Dostop s strani številnih novih organov, ki ne sodijo v prvotne „namene kontrol oseb in predmetov“ bi morali spremljati strožji nadzorni ukrepi.

5. Predlogi večinoma temeljijo na drugih pravnih instrumentih, ki se še pripravljajo (nekateri še niso bili niti predlagani). ENVP razume, da je sprejemanje predpisov v zapletenem in nenehno razvijajočem se okolju težavno; vendar meni, da z vidika posledic za zadevne osebe in pravne negotovosti, ki jo povzroča, to ni sprejemljivo.

6. Pri dodeljevanju pristojnosti med države članice in Komisijo obstajajo nejasnosti. Jasnost je najpomembnejša, saj ni le nujna za nemoteno delovanje sistema, ampak je tudi osnovna zahteva za zagotovitev celovitega nadzora sistema.

1.3. **Struktura mnenja**

Mnenje ima naslednjo strukturo: najprej pojasni pravni okvir, ki velja za SIS II. Nato povzame opredelitev namena SIS II in elementov, ki so bistveno drugačni od sedanjega sistema. Točka 5 vsebuje komentarje o posameznih vlogah Komisije in držav članic z vidika delovanja SIS II. Točka 6 obravnava pravice oseb, na katere se podatki nanašajo, točka 7 pa nadzor na nacionalni ravni in na ravni ENVP ter sodelovanje med nadzorniki. V točki 8 so navedene nekatere pripombe in predlagane možne spremembe v zvezi z varnostjo; točki 9 in 10 obravnavata komitologijo in interoperabilnost. In končno, v povzetku zaključkov so poudarjeni glavni zaključki vsake točke.

2. USTREZNI PRAVNI OKVIR

2.1. **Ustrezni okvir varstva podatkov SIS II**

Predlogi se nanašajo na Direktivo 95/45/ES, Konvencijo 108 in Uredbo 45/2001 kot njihov pravni okvir varstva podatkov. Relevantni so tudi drugi instrumenti.

Z namenom razjasnitve tega konteksta in da spomnimo, katere so glavne sklicne točke našega pregleda, je koristno našteti naslednje:

— Spoštovanje zasebnega življenja je v Evropi zagotovljeno že od sprejetja Konvencije o varstvu človekovih pravic in temeljnih svoboščin leta 1950 (v nadaljnjem besedilu: „ECHR“) s strani Sveta Evrope. Člen 8 ECHR določa „pravico do spoštovanja zasebnega in družinskega življenja“.

  V skladu s členom 8(2) je vsako vmešavanje s strani javne oblasti v izvrševanje te pravice dovoljeno le, če je to „določeno z zakonom“ in „nujno v demokratični družbi“ za zaščito pomembnih interesov. V sodni praksi Evropskega sodišča za človekove pravice so zaradi teh pogojev nastale dodatne potrebe na področju kakovosti pravne podlage za vmešavanje, sorazmernosti vsakega ukrepa ter potrebe po ustreznih nadzornih ukrepih za preprečevanje zlorabe.

— Pravica do spoštovanja zasebnega življenja in varstvo osebnih podatkov sta bila določena pred kratkim v členih 7 in 8 Listine o temeljnih pravicah Evropske unije. V skladu s členom 52 Listine se priznava, da so te pravice lahko omejene, če so izpolnjeni podobni pogoji, kot veljajo v skladu s členom 8 ECHR.

— Člen 6(2) Pogodbe EU določa, da Unija spoštuje temeljne pravice, zajamčene z ECHR.

Tri besedila, ki se izrecno uporabljajo za predloge SIS II, so:

— Konvencija Sveta Evrope št. 108 z dne 28. januarja 1981 o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (v nadaljnjem besedilu *„Konvencija 108“*) vsebuje osnovna načela za varstvo posameznikov pri obdelavi osebnih podatkov. Vse države članice so Konvencijo 108 ratificirale. Uporablja se tudi za dejavnosti, ki se izvajajo na policijskem in pravosodnem področju. Konvencija 108 je trenutno sistem varstva podatkov, ki se uporablja za Konvencijo SIS, skupaj s Priporočilom Odbora ministrov Sveta Evrope št. R(87)15 z dne 17. septembra 1987, ki ureja uporabo osebnih podatkov v policijskem sektorju.

— Direktivi 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, str. 31). Ta direktiva bo v nadaljnjem besedilu imenovana *„Direktiva 95/46/ES“*. Velja omeniti, da v večini držav članic nacionalna zakonodaja za izvajanje direktive zajema tudi dejavnosti v zvezi z obdelavo podatkov, ki se izvajajo na področju policije in pravosodja.

— Uredba (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 (UL L 8, str. 1). Ta uredba bo v nadaljnjem besedilu imenovana *„Uredba 45/2001“*.

Razlaga Direktive 95/46/ES in Uredbe 45/2001 mora biti odvisna delno od ustrezne sodne prakse Evropskega sodišča za človekove pravice, v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin (ECHR) iz leta 1950. Drugače povedano, direktivo in uredbo si je treba razlagati v luči temeljnih pravic v toliko, kolikor zadevata obdelavo osebnih podatkov, zaradi katerih se lahko kratijo temeljne svoboščine, zlasti pravica do zasebnosti. To sledi tudi iz sodne prakse Sodišča Evropskih skupnosti. ([1])

([1]) V tem kontekstu je koristno omeniti sodbo Sodišča v zadevi Österreichischer Rundfunk in drugi (združene zadeve C-465/00, C-138/01 in C-139/01, sodba z dne 20. maja 2003, občna seja, (2003) PSES I-4989). Sodišče je obravnavalo avstrijski zakon, ki določa prenos podatkov o plačah uslužbencev javnega sektorja Avstrijskemu računskemu sodišču ter njihovo naknadno objavo. V svoji sodbi je Sodišče zabeležilo številne kriterije iz člena 8 Evropske konvencije o varstvu človekovih pravic, naj bi se uporabljali pri uporabi Direktive 95/46/ES, kolikor ta direktiva dovoljuje določene omejitve pri pravici do zasebnosti.

Komisija je 4. oktobra 2005 izdala „Predlog okvirnega sklepa Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah“ ([1]) (v nadaljnjem besedilu „*osnutek okvirnega sklepa*“). Ta okvirni sklep naj bi nadomestil Konvencijo 108 kot referenčno zakonodajo za osnutek sklepa SIS II, ki bo verjetno vplival na sistem varstva podatkov v tem kontekstu (glej točko 2.2.5. spodaj).

2.2. **Pravni sistem varstva podatkov SIS II**

2.2.1. *Splošna opomba*

Zakonodajno podlago, ki je potrebna za ureditev SIS II, sestavljajo ločeni instrumenti; vendar pa, kot je navedeno v uvodnih izjavah, ta „ne vpliva na načelo, da SIS II predstavlja enoten informacijski sistem, ki mora tudi delovati enotno. Zato morajo biti nekatere določbe teh instrumentov identične“.

Struktura obeh dokumentov je v osnovi enaka, saj so poglavja I-III v obeh besedilih skoraj identična. Dejstvo, da je treba na SIS II gledati kot na enotni informacijski sistem z dvema različnima pravnima bazama, se odraža tudi v – dokaj zapletenemu – sistemu varstva podatkov.

Sistem varstva podatkov je delno določen v samih predlogih, kot „*lex specialis*“, te predloge pa dopolnjujejo različni referenčni zakonodajni akti („*lex generalis*“) za vsak sektor (Komisija in države članice v prvem stebru, države članice v tretjem stebru).

Zaradi te stukture se postavlja vprašanje, kako obravnavati specializirane sklope pravil v njihovem odnosu do splošnega prava. V tem primeru ENVP v „posebnem pravilu“ vidi uporabo „splošnega pravila“. Posledično mora biti *lex specialis* vedno v skladu z *lex generalis;* izboljšuje (specificira ali dopolnjuje) *lex generalis*, vendar ni zasnovan kot njegova izjema.

Glede vprašanja, katero pravilo naj se uporablja v posameznih primerih, ima načelno *lex specialis* prednost; če ne vsebuje predpisov ali ti niso jasni, pa mora biti sklic na *lex generalis*.

Glede na to strukturo poznamo tri različne kombinacije *lex generalis* in *lex specialis*. To lahko povzamemo na naslednji način:

2.2.2. *Sistem, ki velja za Komisijo*

Kjer je udeležena Komisija, se uporablja Uredba 45/2001, vključno z vlogo ENVP, če se dejavnosti izvajajo v okviru prvega (predlagana uredba) ali tretjega stebra (predlagani sklep). Uvodna izjava 21 predlaganega sklepa določa: „Uredba (ES) št. 45/2001 (…) se uporablja pri obdelavi osebnih podatkov s strani Komisije, kadar se ta obdelava izvaja pri izvajanju aktivnosti, ki v celoti ali delno spadajo v področje zakonodaje Skupnosti. Del obdelave osebnih podatkov v SIS II spada v področje zakonodaje Skupnosti.“

Za to obstajajo praktični razlogi: kar zadeva Komisijo, bi bilo izredno težko določiti, ali se podatki obdelujejo v okviru dejavnosti, ki spadajo v prvi ali tretji steber zakonodaje.

Poleg tega uporaba enega samega pravnega instrumenta za vse dejavnosti Komisije v kontekstu SIS II ni samo bolj smiselna iz praktičnega vidika, ampak tudi izboljšuje doslednost (zagotavlja, v skladu z uvodno izjavo 21 predlagane uredbe „dosledno in homogeno izvajanje pravil glede varstva temeljnih pravic in svoboščin posameznika glede obdelave osebnih podatkov“). Zato ENVP pozdravlja potrditev Komisije, da se Uredba 45/2001 uporablja za vse dejavnosti obdelave podatkov Komisije v SIS II.

2.2.3. *Sistem, ki velja za države članice*

Kar zadeva države članice, je stanje bolj zapleteno. Obdelavo osebnih podatkov ob uporabi predlagane uredbe ureja predlagana uredba sama, kot tudi Direktiva 95/46/ES. Iz uvodne izjave 14 predlagane uredbe je mogoče zelo jasno razbrati, da je treba direktivo šteti kot *lex generalis*, uredbo SIS II pa *lex specialis*. To ima številne posledice, ki so podrobneje opisane v nadaljevanju.

Za predlagani sklep je referenčni pravni instrument (*lex generalis*) za varstvo podatkov Konvencija 108, to pa lahko v nekaterih točkah pomeni pomembno razliko med sistemi varstva podatkov za prvi in tretji steber.

2.2.4. *Vpliv na raven varstva podatkov*

Kot splošni komentar na to zgradbo varstva podatkov ENVP poudarja naslednje:

— Uporaba predlagane uredbe kot *lex specialis* Direktive 95/46/ES (in podobno predlaganega sklepa kot *lex specialis* Konvencije 108) ne bi smela povzročiti slabitve ravni varstva podatkov, ki jo zagotavljata Direktiva ali Konvencija. ENVP bo v zvezi s tem oblikoval priporočila (glej na primer pravico do pravnih sredstev).

([1]) (KOM(2005)475 konč.).

— Prav tako kombinirana uporaba pravnih sredstev ne sme povzročiti, da bi se raven varstva podatkov, zagotovljena s sedanjo Schengensko konvencijo, znižala (glej na primer opombe v zvezi s členom 13 Direktive 95/46/ES v nadaljevanju).

— Čeprav je uporaba dveh različnih instrumentov zaradi okvira prava EU nujna, ne sme povzročiti neutemeljenih neskladij med varstvom podatkov zadevnih posameznikov glede na vrsto obdelovanih podatkov o njih. Temu se je treba čim bolj izogibati. Priporočila v nadaljevanju poleg tega skušajo čim bolj izboljšati doslednost (glej na primer pooblastila nacionalnih nadzornih organov).

— Pravni okvir je tako zapleten, da bo pri njegovi praktični uporabi zelo verjetno prišlo do zmede. V nekaterih primerih je težko razumeti, kako *lex generalis* in *lex specialis* medsebojno učinkujeta, zato bi bilo to koristno pojasniti v predlogih. Poleg tega je v tem zapletenem pravnem okolju zelo koristen predlog SNO za Schengen v njegovem „mnenju o predlagani pravni podlagi za SIS II“ (27. septembra 2005) o razvoju „priročnika“ s seznamom vseh pravic, ki obstajajo v zvezi s SIS II in določajo jasno hierarhijo.

To mnenje v zaključku skuša zagotoviti visoko raven varstva podatkov, doslednosti in jasnosti, da se posamezniku, na katerega se nanašajo podatki, omogoči ustrezno pravno varnost.

2.2.5. *Vpliv osnutka okvirnega sklepa na varstvo podatkov v tretjem stebru*

Konvencija 108 kot referenčni pravni instrument za varstvo podatkov za osnutek sklepa SIS II bo zamenjal okvirni sklep o varstvu podatkov v tretjem stebru [1]. To v predlogu ni omenjeno, vendar sledi iz predlaganega okvirnega sklepa. Njegov člen 34(2) določa, da „se vsi sklici na Konvencijo št. 108 Sveta Evrope z dne 28. januarja 1981 za zaščito posameznikov v zvezi z avtomatsko obdelavo osebnih podatkov štejejo kot sklic na ta okvirni sklep“. ENVP bo v prihodnjih tednih izdal mnenje o osnutku okvirnega sklepa, v njem pa ne bo podrobno analiziral njegove vsebine. Vendar pa bo to omenjeno, kjer koli ima lahko uporaba okvirnega sklepa pomemben vpliv na sistem varstva podatkov SIS II.

2.2.6. *Uporaba člena 13 Direktive 95/46/ES in člena 9 Konvencije 108*

Člen 13 Direktive 95/46/ES in člen 9 Konvencije 108 predvidevata možnost, da države članice sprejmejo zakonodajne ukrepe za omejitev obsega obveznosti in pravic, ki jih ta dokumenta določata, ko takšna omejitev predstavlja nujen ukrep za zaščito drugih pomembnih interesov (npr. nacionalne varnosti, obrambe, javne varnosti) [2].

Uvodne izjave predlagane uredbe in predlaganega sklepa omenjajo, da lahko države članice uporabijo to možnost pri izvajanju predlogov na nacionalni ravni. V tem primeru bi moral biti uporabljen dvojni preskus: uporaba člena 13 Direktive 95/46/ES mora biti v skladu s členom 8 ECHR in ne zmanjševati sedanjega sistema varstva podatkov.

V primeru SIS II je še celo pomembnejša, saj mora imeti sistem predvidljiv značaj. Ker si države članice izmenjujejo podatke, se mora omogočiti, da se z razumno gotovostjo ugotovi, kako se bodo ti obdelovali na nacionalni ravni.

V zvezi s tem obstaja zlasti en zaskrbljujoč element, zaradi katerega bi ti predlogi lahko povzročili zmanjšanje sedanje ravni varstva podatkov. Člen 102 Schengenske konvencije predvideva sistem, v katerem je uporaba podatkov strogo urejena in omejena, celo v nacionalni zakonodaji („Vsaka uporaba podatkov, ki ni v skladu z odstavki 1 do 4, se šteje za zlorabo po nacionalni zakonodaji pogodbenice“). Direktiva 94/46/ES in Konvencija 108 pa določata, da se lahko v nacionalno zakonodajo vnese izjeme, med drugim tudi načela omejitve namena. To bi predstavljalo neskladje s sedanjim sistemom v Schengenski konvenciji, glede na katero nacionalna zakonodaja ne sme odstopati od osnovnega načela omejitve namena in uporabe.

Sprejem okvirnega sklepa ne bi spremenil te ugotovitve: težava je bolj v tem, kako vzdrževati strogo načelo omejitve namena za obdelovanje podatkov SIS II, kot pa zagotavljati, da se podatki obdelujejo v skladu z okvirnim sklepom.

[1] Zamenjal bo tudi splošni sistem varstva podatkov Schengenske konvencije (členi 126 do 130 Schengenske konvencije). Ta sistem se ne uporablja za SIS.

[2] Država članica, ki uporablja to možnost za omejitev pravic, lahko to stori le v skladu s členom 8 ECHR, kot je bilo že prej omenjeno.

ENVP predlaga, da se v predloge SIS II (in sicer člen 21 predlagane uredbe in člen 40 predlaganega sklepa) vstavi določba, ki ima isti namen kot sedanji člen 102(4) Schengenske konvencije in omejuje možnost držav članic, da določajo uporabo podatkov, ki niso predvideni v besedilih SIS II. Druga možnost je, da se v predlaganem sklepu in predlagani uredbi izrecno omeji obseg izjem, ki se lahko dopuščajo po členu 13 Direktive ali členu 9 Konvencije, z določitvijo, na primer, da lahko države članice omejijo le pravice dostopa do informacij, ne pa tudi načela kakovosti podatkov.

3. NAMEN

Glede na člen 1 obeh dokumentov („vzpostavitev in splošni cilj SIS II“) je SIS II vzpostavljen, da „ustreznim organom v državah članicah omogoči, da izmenjujejo informacije za namen kontrol oseb in predmetov“ in „vzdržuje visoko stopnjo varnosti na območju brez kontrol na notranjih mejah med državami članicami“.

Namen SIS II je opisan precej na splošno; same zgoraj omenjene določbe ne nakazujejo, kaj točno je s tem ciljem zajeto (mišljeno).

Cilj SIS II se zdi veliko širši od cilja sedanjega SIS, kot je določeno v členu 92 Schengenske konvencije, ki se je posebej sklicevala na „(…) ukrepe za osebe in premoženje za namene mejnih kontrol in drugih policijskih in carinskih kontrol (…) in (v zvezi z razpisi ukrepov iz člena 96) za namen izdaje vizumov, dovoljenj za prebivanje in izvajanja zakonodaje o tujcih (…)“.

Širši namen izhaja tudi iz dodatka k SIS II o novih funkcionalnostih in dostopih, ki ne sodijo v prvotni namen kontrol oseb in predmetov, temveč bolj med preiskovalna orodja. Dostop je zlasti predviden za organe, ki bodo uporabljali podatke SIS II za svoje lastne namene in ne za uresničitev namenov SIS II (glej spodaj); medsebojna povezanost razpisov ukrepov bo posplošena, to pa predstavlja tipično značilnost policijskega preiskovalnega orodja.

Obstajajo tudi vprašanja v zvezi z biometričnim iskalnikom, ki naj bi ga razvili v prihodnjih letih in bo znotraj sistema omogočal iskanje, ki presega potrebe kontrolnega sistema.

Predlogi imajo torej veliko širši obseg kot obstoječi okvir. To zahteva dodatne nadzorne ukrepe. V tem oziru bo ENVP svojo analizo usmeril manj na širšo opredelitev člena 1 kot takega in bolj na funkcionalnosti in druge sestavne elemente SIS II.

4. POMEMBNE SPREMEMBE V SIS II

To poglavje se najprej osredotoča na nove elemente, ki jih vpeljuje SIS II, in sicer na uvedbo biometrije, novo zasnovo dostopa, s posebno pozornostjo na dostopu Europola in Eurojusta, organih za registracijo vozil, medsebojni povezanosti razpisov ukrepov in dostopu različnih organov do podatkov o priseljevanju.

4.1. Biometrija

Predlogi SIS II uvajajo možnost za obdelavo nove kategorije podatkov, ki si zasluži posebno pozornost: biometričnih podatkov. Kot je že poudarjeno v mnenju ENVP o vizumskem informacijskem sistemu ([1]), občutljiva narava biometričnih podatkov zahteva posebne nadzorne ukrepe, ki niso bili vključeni v predloge SIS II.

Na splošno je težnja, da se v informacijskih sistemih v celotni EU (VIS, EURODAC, informacijski sistem o vozniških dovoljenjih itd.) uporabljajo biometrični podatki, vedno večja, vendar pa je ne spremljajo pomisleki glede tveganj, ki so s tem povezana, in zahtevanih nadzornih ukrepov.

Ta potreba po globljem razmisleku je bila poudarjena tudi v nedavni resoluciji o biometriji, ki jo je izdala mednarodna konferenca komisarjev za varstvo podatkov v Montreuxu ([2]). Doslej je bila dodana vrednost za razvoj standardov osredotočena le na vedno večjo interoperabilnost med sistemi in ne na izboljšanje kakovosti biometričnih postopkov.

([1]) Mnenje ENVP o Predlogu uredbe Evropskega parlamenta in Sveta o vizumskem informacijskem sistemu in izmenjavi podatkov o vizumih za kratkoročno prebivanje med državami članicami, z dne 23. marca 2005, točka 3.4.2.

([2]) 27. mednarodna konferenca komisarjev za varstvo podatkov in zasebnost, Montreux, 16. septembra 2005, Resolucija o uporabi biometrije v potnih listih, na osebnih izkaznicah in v potnih listinah.

Koristno bi bilo oblikovati niz skupnih obvez ali zahtev, povezanih s posebnostjo teh podatkov, kot tudi skupno metodologijo za njihovo izvajanje. Te skupne zahteve bi lahko vsebovale zlasti naslednje elemente (katerih potreba je nakazana s predlogi SIS II):

— **Ciljna presoja vplivov:** Poudariti je treba, da predlogi niso bili predmet presoje vplivov glede uporabe biometrije ([1]).

— **Poudarek na postopku vpisa:** Vir biometričnih podatkov in način, kako se ti zberejo, nista podrobno navedena. Vpis je pomemben korak v celotnem postopku biometrične identifikacije in ne sme biti opredeljen le s prilogami ali nadaljnimi razpravami v podskupinah, saj neposredno pogojuje končni rezultat postopka, tj. ravni napačne zavrnitve ali napačne odobritve.

— **Poudarek na stopnji točnosti:** Uporaba biometrije za identifikacijo (primerjava ene z več osebami), predstavljena v predlogu kot prihodnje izvajanje „biometričnega iskalnika“ je bolj občutljiva, saj so rezultati tega postopka manj natančni kot pri uporabi avtentifikacije ali kontrole (primerjava ene osebe z drugo). Biometrična identifikacija zato ne sme predstavljati enotnega načina identifikacije ali enotnega ključa za dostop do nadaljnjih informacij.

— **Nadomestni postopek:** Zlahka dostopni nadomestni postopki se izvajajo z namenom spoštovanja dostojanstva oseb, ki so bile morda po pomoti identificirane, in da nanje ne bi prenesli bremena nepopolnosti sistema.

Uporaba biometričnih podatkov brez primerne predhodne ocene prav tako odraža precenjevanje zanesljivosti biometrije. Biometrični podatki so „živi“ podatki, ki se s časom spreminjajo; vzorci, ki so shranjeni v podatkovni bazi, so le trenutni posnetek dinamičnega elementa. Njihova trajnost ni absolutna in mora biti nadzorovana. Točnost biometrije se mora vedno upoštevati ob drugih elementih, saj nikoli ni absolutna.

([1]) Presoja bi lahko temeljila na t.i. sedmih stebrih biometrične modrosti iz publikacije „Biometrics at the frontiers: Assessing the impact on Society“ IPTS, DG-JRC, EUR 21585 EN, del 1.2, stran 32.

Možna uporaba podatkov SIS II za preiskovalne namene pomeni resna tveganja za posameznika, na katerega se nanašajo podatki, če se daje povečano in precenjeno vlogo biometričnim dokazom, kot je bilo prikazano v prejšnjih primerih ([2]).

Zato bi morali predlogi potrditi in povečati ozaveščenost o dejanski zmogljivosti biometrije v identifikacijske namene.

4.2. **Dostop do podatkov SIS II**

4.2.1 *Nova vizija dostopa*

Organi, ki imajo dostop do podatkov SIS, so opredeljeni za vsak razpis ukrepov. Načeloma se za odobritev dostopa do podatkov SIS uporablja dvojni preskus: organom mora biti odobren dostop ob popolnem spoštovanju splošnega namena SIS in posebnega namena za vsak razpis ukrepov.

To sledi iz opredelitve razpisov ukrepov, ki jo najdemo tako v predlagani uredbi kot v predlaganem sklepu (člen 3(1)(a) obeh instrumentov: *„razpis ukrepa“ pomeni skupino podatkov v SIS II, ki pristojnim organom omogoča identifikacijo osebe ali stvari, glede na poseben ukrep, ki ga je treba izvesti)*. Člen 39(3) predlaganega sklepa ta vidik poudari z določbo, da se *„podatki iz odstavka 1 uporabljajo samo v namen identifikacije oseb glede na posebni ukrep, ki ga je treba izvesti v skladu s tem sklepom“*. V tem oziru ima SIS II še vedno značilnosti sistema „zadetek – ni zadetkov“, pri katerih je vsak razpis ukrepov vstavljen s posebnim namenom (predaja, prepoved vstopa, …).

Organi, ki imajo dostop do podatkov SIS, imajo dejansko omejitev uporabe teh podatke, saj imajo načelno dostop do njih le zaradi izvedbe določenega ukrepa.

Vendar pa nekateri primeri dostopa, določeni v novih predlogih, niso v skladu s to logiko: njihov namen je, da organu zagotovijo informacije, ne pa, da mu omogočijo identifikacijo osebe in izvedbo ukrepa, ki je predviden v razpisu ukrepov.

([2]) Junija 2004 je bil odvetnik iz Portlanda (ZDA) obsojen na dva tedna zaporne kazni, ker je FBI ugotovil, da se njegov prstni odtis ujema z odtisom, ki je bil najden na plastični vrečki, v kateri je bil detonator, uporabljen v terorističnem napadu v Madridu. Na koncu se je izkazalo, da je bil postopek primerjave pomanjkljiv in je povzročil napačno razlago.

Natančneje, to zadeva:

— dostop organov za azil do podatkov o priseljevanju;

— dostop organov, odgovornih za dodelitev statusa begunca, do podatkov o priseljevanju;

— dostop Europola do razpisov ukrepov o izročitvi, prikritim evidentiranem in ukradenih dokumentih zaradi zasega;

— dostop Eurojusta do podatkov o izročitvi in lokalizaciji.

Vsi ti organi imajo enake lastnosti glede na podatke SIS II.

ne morejo izvajati posebnih ukrepov, omenjenih v opredelitvah razpisov ukrepov. Dostop do njih se jim odobri, da lahko pridobijo informacij za njihove lastne namene.

Tudi med temi organi je treba razlikovati, in sicer med tistimi, ki imajo dostop za svoje lastne namene, ampak s posebnimi cilji, in tistimi, za katere namen dostopa sploh ni podrobno opredeljen (Europol in Eurojust). Organi za azil, na primer, imajo dostop za poseben namen, tudi če to ni namen, omenjen v razpisu ukrepov. Lahko imajo dostop do podatkov o priseljevanju „da se določi, ali je prosilec za azil nezakonito prebival v drugi državi članici“. Europol in Eurojust imata dostop do podatkov iz določenih kategorij razpisov ukrepov, „ki so potrebne za izvedbo njihovih nalog“.

Kot povzetek, dostop do podatkov SIS II se odobri v treh primerih:

— dostop za uresničitev razpisa ukrepov;

— dostop za namen, ki ni namen SIS II, ampak je dobro opredeljen v predlogih;

— dostop za namen, ki ni namen SIS II, ampak ni natančno opredeljen.

ENVP meni, da bolj splošen ko je namen dostopa, bolj strogi morajo biti nadzorni ukrepi, ki jih je treba izvesti. Splošni nadzorni ukrepi so podrobno opredeljeni spodaj; nato se bo obravnaval poseben položaj Europola in Eurojusta.

4.2.2 *Pogoji za odobritev dostopa*

1. Dostop se lahko v vsakem primeru odobri le, ko je združljiv s splošnim namenom SIS II in je v skladu z njegovo pravno osnovo.

To v praksi pomeni, da mora dostop do podatkov o priseljevanju v skladu s predlagano uredbo podpirati izvajanje politik, povezanih z gibanjem oseb, ki so del Schengenskega pravnega reda.

Podobno dostop do razpisov ukrepov, določen s sklepom, skuša podpirati operativno sodelovanje med policijskimi in pravosodnimi organi pri kriminalnih zadevah.

V tem oziru ENVP opozarja na poglavje, povezano z dostopom služb, pristojnih za izdajo potrdil o registraciji, do podatkov SIS II (glej točko 4.6 spodaj).

2. Potreba po dostopu do podatkov SIS II mora biti nazorno prikazana, kot tudi dejstvo, da je podatke zelo težko ali nemogoče pridobiti z drugimi, manj vsiljivimi sredstvi. To bi moral vsebovati obrazložitveni memorandum, in, kot je bilo že povedano, je velika škoda, da ga ni.

3. Treba je jasno in restriktivno določiti, kako se podatki uporabljajo.

Organi za azil imajo lahko dostop do podatkov o priseljevanju „da se določi, ali je prosilec za azil nezakonito prebival v drugi državi članici“. Europol in Eurojust imata dostop do podatkov iz določenih kategorij razpisov ukrepov, „ki so potrebne za izvedbo njunih nalog“: to ni dovolj podrobno določeno (glej spodaj).

4. Treba je jasno in restriktivno določiti pogoje dostopa. Zlasti lahko dostop do podatkov SIS II dobijo samo službe znotraj teh organizacij, ki te podatke uporabljajo. Ta obveznost, ki jo določa člen 40 predlaganega sklepa in člen 21.2 predlagane uredbe, se mora dopolniti z obveznostjo, da morajo nacionalni organi voditi in sproti dopolnjevati seznam oseb, ki jim je dovoljen dostop do SIS II. Enako velja za Europol in Eurojust.

5. Dejstvo, da je tem organom omogočen dostop do podatkov iz SIS II, ne more biti nikoli razlog za vnos ali vzdrževanje podatkov v sistemu, če ti podatki niso izrecno uporabni za razpis ukrepov, katerega del so. Nove kategorije podatkov ne smejo biti dodane, saj bi koristile drugim informacijskim sistemom. Na primer, člen 39 predlaganega sklepa določa, da se uvedejo razpisi ukrepov za podatke, ki zadevajo organ izdaje. Ti podatki niso potrebni za izvedbo ukrepa (prijetje, nadzor, …), edini razlog za njihovo uvedbo je najbrž to, da koristijo Europolu in Eurojustu. Potrebna bi bila jasna utemeljitev za obdelavo teh podatkov.

6. Obdobja hrambe podatkov se ne morejo podaljšati, če to ni potrebno za doseg namena, ki je bil podlaga za vnos podatkov v sistem. To pomeni, da tudi če imata Europol in Eurojust dostop do teh podatkov, to ni zadostna podlaga za to, da bi jih zadrževali v sistemu (na primer, ko je iskana oseba izročena, se morajo podatki zbrisati, tudi če bi bili koristni za Europol). Tudi tukaj bo potreben strog nadzor za zagotovitev uporabe tega ukrepa s strani nacionalnih organov.

4.2.3 *Dostop Europola in Eurojusta*

a. *Razlogi za dostop*

O dostopu Europola in Eurojusta do nekaterih podatkov SIS je že potekala razprava, preden je bil ta uveden s Sklepom Sveta z dne 24. februarja 2005 ([1]). Glede na vse druge organe, ki imajo dostop za svoje lastne namene, jima je dostop omogočen zelo na splošno. Čeprav je uporaba teh podatkov opisana v poglavju XII Sklepa, je podlaga za prvotno odobritev dostopa premalo razdelana. Še toliko bolj, ker se bodo naloge Europola in Eurojusta s časom verjetno povečevale.

ENVP za posebna primera Europola in Eurojusta poziva Komisijo, naj restriktivno določi naloge, za izvedbo katerih bi bil dostop do podatkov upravičen.

b. *Omejitev podatkov*

Da bi se izognili „ribiškim odpravam“ Europola in Eurojusta in da bi zagotovili, da imata dostop samo do podatkov, ki so „potrebni za opravljanje njunih nalog“, je SNO za Schengen v mnenju z dne 27. septembra 2005 o predlogih SIS II predlagal, da se dostop Europola in Eurojusta do podatkov o posameznikih, katerih ime se že pojavlja v njihovih datotekah, omeji. To bi zagotovilo, da bi imela vpogled le v razpise ukrepov, ki so pomembni za njiju. ENVP to priporočilo pozdravlja.

c. *Varnostni vidiki*

ENVP pozdravlja potrebo po evidentiranju vseh postopkov Europola in Eurojusta, opravljenih s tem v zvezi, ter prepoved kopiranja ali prenašanja delov sistema.

Člen 56 predlaganega sklepa predvideva „eno ali dve“ dostopni točki za Europol in Eurojust. Četudi bi bila zaradi decentraliziranosti pristojnih organov v kateri od držav članic morda razumljiva potreba po več kot eni dostopni točki, status in dejavnosti Europola in Eurojusta te zahteve ne upravičujejo. Treba je poudariti, da bi več dostopnih točk z vidika varnosti pomenilo tudi večjo nevarnost zlorabe in jih je zato treba natančno upravičiti z doslednejšimi dejavniki. Zaradi neprepričljive utemeljitve ENVP tako predlaga, naj se za Europol in Eurojust zagotovi samo ena dostopna točka.

4.3. **Povezovanje razpisov ukrepov**

Člen 26 uredbe in člen 46 sklepa predvidevata možnost za države članice, da zaradi določanja razmerij med dvema ali več ukrepi v skladu s svojimi nacionalnimi zakonodajami med razpisi ukrepov vzpostavijo povezavo.

Povezave med razpisi ukrepov so vsekakor lahko uporabne pri kontroli (nalog za prijetje avtomobilskega tatu se lahko npr. poveže z ukradenim vozilom), a vzpostavitev povezav med razpisi ukrepov je zelo značilna lastnost policijskih preiskovalnih tehnik. Povezovanje razpisov ukrepov ima lahko velike posledice za pravice zadevne osebe, saj se je ne „obravnava“ več na podlagi podatkov, ki se nanašajo samo nanjo, ampak na podlagi možnih povezav te osebe z drugimi.

Posamezniki, katerih podatki so povezani s podatki o storilcih kaznivega dejanja ali iskanih oseb, bodo verjetno obravnavani z več suma kot ostali. Povezovanje razpisov ukrepov predstavlja tudi podaljšanje preiskovalnih pooblastil SIS, saj omogoča registracijo domnevnih skupin ali mrež (če se npr. podatki o nezakonitih priseljencih povežejo s podatki o trgovcih z ljudmi). Nazadnje lahko dejstvo, da je povezovanje razpisov ukrepov urejeno z nacionalnimi zakonodajami, vodi tudi do tega, da bi lahko bile povezave, nezakonite v eni državi članici, zakonito vzpostavljene v drugi državi članici, in bi tako v sistem vnesle „nezakonite“ podatke.

([1]) Sklep Sveta št. 2005/211/PNZ z dne 24. februarja 2005 o uvedbi nekaterih novih funkcij schengenskega informacijskega sistema, vključno z bojem proti terorizmu, UL L 68/44, 15.3.2005.

Sklepi Sveta z dne 14. junija 2004 glede zahtev delovanja SIS II določajo, da mora imeti vsaka povezava jasno operativno zahtevo, temeljiti na jasno določenem razmerju in upoštevati načelo sorazmernosti. Poleg tega ne sme vplivati na pravico do dostopa. V vsakem primeru je povezovanje razpisov za ukrepe del postopka obdelave podatkov, zato mora spoštovati določbe nacionalnih zakonodaj o izvajanju Direktive 95/46/ES in/ali Konvencije 108.

V predlogih je ponovljeno, da vzpostavitev povezav ne sme vplivati na pravice do dostopa (v nasprotnem primeru bi se omogočil dostop do podatkov, katerih obdelava bi bila pod nacionalnimi zakonodajami nezakonita, saj bi kršila člen 6 Direktive).

ENVP poudarja, da je zelo pomembno strogo interpretirati člen 26 predlagane uredbe in člen 46 predlagane direktive. To se lahko zagotovi tudi z jasno določbo, da organi brez pravice do dostopa do določenih kategorij podatkov nimajo dostopa do povezav do teh kategorij, pa tudi, da ne smejo niti vedeti za obstoj teh povezav. Če ni pravice do dostopa do podatkov o povezavah, se povezav ne sme vizualizirati.

Poleg tega bi si ENVP želel, da se z njim posvetuje glede tehničnih ukrepov za zagotavljanje zgoraj navedenega.

4.4. **Razpisi za ukrepe za namen zavrnitve vstopa**

4.4.1. *Razlogi za vključitev*

Uporaba „razpisov ukrepov glede državljanov tretjih držav za namen zavrnitve vstopa“ (člen 15 Uredbe) pomembno vpliva na svoboščine posameznika. Posameznik, o katerem se poroča pod to določbo, več let nima vstopa na schengensko območje. Doslej je to najpogosteje uporabljani razpis ukrepov glede na število sporočenih oseb. Glede na posledice takega razpisa ukrepov in število zadevnih oseb ga je treba zelo pazljivo načrtovati in izvajati. To drži tudi za ostale ukrepe, a ENVP bo temu razpisu za ukrepe posvetil posebno poglavje, saj sproža določene pomisleke glede razlogov za vključitev.

Nov razpis za ukrep za zavrnitev vstopa pomeni izboljšanje glede na sedanji položaj, a prav tako ni popolnoma zadovoljujoč, saj v veliki meri temelji na instrumentih, ki še niso sprejeti ali predlagani.

Izboljšave so vidne predvsem v jasnejših opisih razlogov za vključitev podatkov. Sedanje besedilo Schengenske konvencije je pripeljalo do velikih razlik med državami članicami, kar se tiče števila oseb, sporočenih v okviru člena 96 Konvencije. Skupni nadzorni organ za Schengen je o tej zadevi izvedel izčrpno raziskavo ([1]) in predlagal, naj „oblikovalci politik preučijo uskladitev razlogov za razpis ukrepov v različnih schengenskih državah“.

Predlagani člen 15 je podrobneje oblikovan, kar je treba pozdraviti.

Člen 15 (2) vsebuje tudi seznam primerov uporabe različnih statusov, ko za osebe ni moč razpisati ukrepov, ker zakonito prebivajo na ozemlju katere od držav članic. Čeprav je to moč sklepati že iz sedanje Schengenske konvencije, je dejanska uporaba pokazala, da se tudi ta mehanizem v državah članicah različno uporablja. Zaradi tega je pojasnitev dobrodošla,

vendar se ta ukrep tudi resno kritizira, saj v velikem delu temelji na besedilu, ki še ni bilo sprejeto, tj. direktivi „o vrnitvi“.

Od sprejetja predlogov za SIS II je Komisija (1. septembra 2005) predlagala „Direktivo o skupnih standardih in postopkih v državah članicah za vračanje državljanov tretjih držav, ki nezakonito prebivajo v EU“, a dokler to ni dokončna različica besedila, se je ne sme upoštevati kot veljavno podlago za vnašanje podatkov v sistem. Še posebej pomeni kršitev 8. člena Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin (ENCH), saj mora biti poseganje v zasebnost posameznika utemeljeno z – med drugim – jasno in dostopno zakonodajo.

Zato ENVP poziva Komisijo, naj to določbo umakne ali jo ponovno oblikuje tako, da bo temeljila na sedanji zakonodaji in bo posamezniku omogočala, da lahko predvidi, katere ukrepe lahko organi sprejmejo v zvezi z njim.

4.4.2. *Dostop do razpisov ukrepov iz člena 15*

Člen 18 določa, kateri organi imajo dostop do teh razpisov ukrepov in za kakšne namene. Člen 18(1) in (2) določa, kateri organi imajo dostop do razpisov ukrepov, vnešenih na podlagi direktive o vrnitvi. Velja enaka opomba kot zgoraj.

([1]) Poročilo skupnega nadzornega organa za Schengen (SNO) o pregledu uporabe razpisov ukrepov iz člena 96 v schengenskem informacijskem sistemu, Bruselj, 20. junija 2005.

Člen 18 (3) predlagane uredbe odobri dostop organom, zadolženim za dodelitev statusa begunca skladno z direktivo, ki ni bila še niti predlagana. Ker besedilo ni na voljo, mora ENVP na tem mestu ponoviti zgornje opombe.

Morebitne posledice za osebe, na katere se nanašajo sporočeni podatki v SIS II, lahko pomembno vplivajo na življenja zadevnih oseb. To je zlasti zaskrbljujoče glede razpisov ukrepov prikritega evidentiranja za osebe ali namenskih kontrol, saj se ti ukrepi lahko razpišejo na podlagi suma.

4.4.3. *Obdobja hrambe razpisov ukrepov iz člena 15*

ENVP bi si želel resno utemeljitev za to podaljšanje obdobij hrambe podatkov. Če prepričljive utemeljitve ni, ENVP predlaga, naj se obdobja skrajšajo na sedanje trajanje, pri čemer vztraja predvsem glede razpisov ukrepov prikritega evidentiranja ali namenskih kontrol.

Razpis ukrepov se skladno s členom 20 ne sme hraniti dlje kot za obdobje zavrnitve vstopa, določeno v sklepu (o odstranitvi ali vrnitvi). To je v skladu s pravili glede varstva podatkov. Po petih letih je treba razpis avtomatično izbrisati, razen če država članica, ki je podatke vnesla v SIS II, ne odloči drugače.

Ustrezen nadzor na nacionalni ravni mora zagotavljati, da ne prihaja do avtomatičnega neupravičenega podaljšanja obdobja hrambe, in da države članice podatke izbrišejo pred pretekom petih let, kadar je obdobje zavrnitve vstopa krajše.

4.5. **Obdobja hrambe**

Četudi načelo hrambe ostaja nespremenjeno (v splošnem velja pravilo, da je treba razpis ukrepov iz SIS II izbrisati takoj, ko se ukrepa, kot zahteva razpis), iz predlogov izhaja posledica na splošno daljšega obdobja hrambe.

Schengenska konvencija je predvidela pregled potrebe po nadaljnjem hranjenju podatkov za največ tri leta po njihovem vnosu (ali za eno leto v primeru podatkov, vnesenih zaradi prikritega evidentiranja). Nov predlog predvideva avtomatični izbris (z možnostjo ugovora države članice izdajateljice) po petih letih za podatke o priseljevanju, desetih letih za podatke o prijetju, pogrešanih osebah in osebah, iskanih zaradi sodnih postopkov, ter treh letih za osebe, ki so predmet prikritega evidentiranja.

Čeprav morajo načeloma vse države članice po izpolnjenem namenu razpisa ukrepa podatke izbrisati, to predstavlja pomembno podaljšanje najdaljšega roka hrambe (največkrat kar trikratno), za kar Komisija ne poda utemeljitve. Glede podatkov o priseljevanju se lahko samo ugiba, ali ni obdobje petih let povezano s trajanjem prepovedi vstopa iz predlagane direktive o vrnitvi. V vseh drugih primerih pa ENVP ne vidi nobene logične osnove.

4.6. **Dostop organov, pristojnih za izdajo potrdil o registraciji vozil**

Glavna opomba se nanaša na izbiro več spornih pravnih podlag. Komisija ni prepričljiva glede uporabe pravne podlage „promet“ iz prvega stebra za ukrep, ki bi upravnim organom dovoljeval dostop do SIS za namene preprečevanja in boja proti kriminalu (trgovina z ukradenimi vozili). Potreba po trdni utemeljitvi in jasni pravni podlagi za odobritev dostopa do SIS II je podrobno razložena v točki 4.2.2 tega mnenja.

ENVP opozarja na opombe k tej zadevi, ki jih je v svojem mnenju o predlagani pravni podlagi za SIS II podal SNO za Schengen. Zlasti je treba upoštevati predlog SNO za Schengen, naj se predlagani sklep spremeni za namen vključitve v ta dostop.

5. NALOGE KOMISIJE IN DRŽAV ČLANIC

Za gladko delovanje sistema SIS II in z vidika nadzora je najpomembneje podati jasen opis in razporeditev odgovornosti v okviru SIS II. Razporeditev nadzornih pristojnosti sledi opisu odgovornosti, zato je potrebna popolna jasnost.

5.1. **Vloga Komisije**

ENVP pozdravlja Poglavje III obeh predlogov, kjer so opisane naloge in odgovornosti Komisije v SIS II (naloga „operativnega vodenja“). V predlogu o VIS te jasnosti ni bilo. Kljub temu samo to poglavje nalog Komisije ne določa dovolj izčrpno. V resnici je Komisija, kot je omenjeno v poglavju 9 tega mnenja, prek komitologije vključena tudi v izvajanje in upravljanje sistema.

Glede varstva podatkov je Komisija odgovorna za operativno vodenje, kar je bilo določeno že v sistemih VIS in Eurodac. Poleg njene pomembne vloge pri razvoju in vzdrževanju sistema je to naloga upravljalca *sui generis*. Komisija je, kot je bilo že omenjeno v mnenju ENVP o VIS, mnogo več od obdelovalca, a tudi manj od običajnega nadzornika, saj nima dostopa do podatkov v obdelavi v SIS II.

Zaradi gradnje SIS II na zapletenih sistemih, med katerimi se nekateri zanašajo na nastajajoče tehnologije, ENVP vztraja na poudarjanju odgovornosti Komisije za vzdrževanje posodobljenosti sistemov z izvajanjem najboljše razpoložljive tehnologije s področja varnosti in varstva podatkov.

Zato je treba v členu 12 predlogov dodati, naj Komisija redno predlaga izvajanje novih tehnologij, ki predstavljajo največji dosežek s tega področja, zvišujejo raven varstva in varnosti podatkov ter pospešujejo delo nacionalnih organov z dostopom do teh podatkov.

5.2. **Vloga držav članic**

Položaj držav članic je nejasen, ker je dokaj težko vzpostaviti, kateri organ(i) bo(do) nadzoroval(i) podatke.

Predloga opisujeta nalogo nacionalnega urada SIS II (ki pristojnim organom zagotavlja dostop do SIS II) in organov SIRENE (ki zagotavljajo izmenjavo vseh dopolnilnih podatkov). Države članice morajo zagotoviti tudi delovanje in varnost njihovih NS (nacionalnih sistemov). Ni jasno, ali je za slednje odgovoren kateri od zgoraj navedenih organov. V vsakem primeru so s tem v zvezi potrebna pojasnila.

Glede varstva podatkov je treba Komisijo in države članice upoštevati kot skupne nadzornike, od katerih ima vsak svoje odgovornosti. Priznavanje teh dopolnjujočih se nalog je edini način, da nobeno področje dejavnosti SIS II ne ostane brez nadzora.

6. **PRAVICE OSEB, NA KATERE SE PODATKI NANAŠAJO**

6.1. **Obveščanje**

6.1.1. *Predlog uredbe*

Člen 28 predlagane uredbe predvideva obveščanje osebe, na katero se podatki nanašajo, skladno predvsem s členom 10 Direktive 95/46. To je dobrodošla sprememba glede na sedanji položaj, ko v konvenciji ni izrecno vsebovana pravica do informacij. Še vedno pa je moč nekoliko izboljšati sledeče.

Na seznam je treba dodati nekaj informacij, ki bi pripomogle k zagotavljanju poštenega obravnavanja osebe, na katero se podatki nanašajo. Dodatne informacije bi se morale nanašati na obdobje hrambe podatkov, morebitno pravico do prošnje za pregled ali pritožbo na sklep za izdajo razpisa ukrepov (v nekaterih primerih, glej člen 15 (3) predlagane uredbe), možnost pridobitve pomoči pri organu za varstvo podatkov in razpoložljiva pravna sredstva.

V predlogu uredbe ni nobene omembe časa, ko je treba informacije podati. To bi lahko pomenilo onemogočeno izvrševanje pravic osebe, na katero se podatki nanašajo. Za učinkovito izvrševanje teh pravic mora uredba vzpostaviti natančen čas, ko je treba podati informacije, odvisno od organa, ki izda razpis za ukrep.

Pripravna rešitev bi lahko bila dodati informacije o razpisu v sklep, ki je vseskozi podlaga za razpis ukrepov: tj. v sklep pravosodnega ali upravnega organa, ki temelji na ogrožanju javnega reda (…) oz. sklep o vrnitvi ali nalog za odstranitev, skupaj s prepovedjo ponovnega vstopa. To je treba dodati v člen 28 uredbe.

6.1.2. *Predlog sklepa*

Člen 50 sklepa določa, da se posameznika, na katerega se podatki nanašajo, na njegovo prošnjo obvesti; navaja tudi možne razloge za zavrnitev dostopa do teh informacij. Omejitve te pravice so vsekakor razumljive glede na naravo podatkov in širši okvir njihove obdelave.

Vendar pa mora biti pravica do informacij neodvisna od prošnje osebe, na katero se podatki nanašajo (to bi bila prej definicija prošnje za dostop). Lahko se predpostavlja, da je za informacije potrebno upravičeno „zaprositi“ v primerih, če oseba, na katero se podatki nanašajo, ne more biti obveščena, ker se ne ve, kje je nameščena.

To bi lahko bilo bolje obravnavano z vnosom izjeme pri pravici do informacij v primerih, ko obveščanje ni mogoče ali bi zahtevalo nesorazmerne napore. Člen 50 predlaganega sklepa je treba ustrezno spremeniti.

Ta rešitev bi bila tudi v skladu z uporabo predloga okvirnega sklepa o varstvu osebnih podatkov v tretjem stebru.

6.2. **Dostop**

Predlagana uredba in sklep določata roke za odgovore na prošnje za dostop, kar je pozitivna sprememba glede na prej. Ker je postopek za izvajanje pravice do dostopa določen na nacionalni ravni, ni jasno, kako v predlogih določeni roki vplivajo na obstoječe postopke, še posebej v državah članicah, kjer so določeni krajši roki za odgovor na prošnje za dostop. Treba je jasno navesti, da je treba uporabljati roke, ki so najbolj ugodni za osebo, na katero se podatki nanašajo.

6.2.1. *Predlog uredbe*

Pomembno je, da omejevanje pravice do dostopa iz sedanje Schengenske konvencije („se zavrne, če je to nujno za izvedbo zakonite naloge v zvezi z razpisom ukrepov ali za zaščito pravic in svoboščin tretjih strank“) v predlagani uredbi ni zajeto.

Najbrž je temu vzrok uporaba Direktive 95/46/ES, ki v členu 13 predvideva možnost izjem v nacionalnih zakonodajah. Vsekakor je treba poudariti, da mora biti uporaba člena 13 v nacionalnih zakonodajah za omejevanje pravice do dostopa vedno skladna z 8. členom ECHR in le v izjemnih primerih.

6.2.2. *Predlog sklepa*

Predlog sklepa vzpostavlja omejevanje pravice do dostopa podobno kot Schengenska konvencija. Predlagani okvirni sklep v bistvu vsebuje iste omejitve pravice do dostopa, zato sprejetje tega instrumenta s tem v zvezi ne bi prineslo pomembne spremembe.

Ker je v več državah članicah dostop do podatkov o kazenskem pregonu „posreden“ (to pomeni, da se izvaja prek nacionalnega organa za varstvo osebnih podatkov), bi bilo priporočljivo, naj organi za varstvo osebnih podatkov obvezno dejavno sodelujejo pri izvajanju pravice do dostopa.

6.3. **Pravica do pregleda sklepa za razpis ukrepa ali pritožbe na sklep za razpis ukrepa**

Člen 15 (3) vzpostavlja pravico do pregleda ali pritožbe pred pravosodnim organom, kar se tiče sklepa o razpisu ukrepov, če je ta sklep sprejel upravni organ. V primerjavi s sedanjo Schengensko konvencijo je ta dodatek dobrodošla sprememba.

To poudarja potrebo po popolni in pravočasni obveščenosti osebe, na katero se podatki nanašajo, kot je bilo že omenjeno v zgornji točki 6.1, saj bi brez obveščanja ta nova pravica ostala samo teoretična.

6.4. **Pravna sredstva**

Člen 30 predlagane uredbe in člen 52 predlaganega sklepa določata, da ima vsaka oseba, na katero se podatki nanašajo, pravico do vložitve tožbe ali pritožbe na sodišču katere koli države članice, če se ji odreče pravica do dostopa, popravljanja ali izbrisa podatkov, pridobitve podatkov ali odškodnine.

Izbira besed („vsaka oseba na ozemlju vsake države članice“) bi lahko pomenila, da mora biti pritožnik ali tožnik fizično na ozemlju, da lahko vloži tožbo pred sodiščem. Ta omejenost z ozemljem ni upravičena in bi lahko povzročila neučinkovito uveljavljanje pravice do pravnih sredstev, saj bo verjetno veliko tožnikov ali pritožnikov tožbe oz. pritožbe vložilo prav zaradi zavrnitve vstopa na Schengensko območje. Glede predlagane uredbe je treba upoštevati tudi člen 22 direktive, ki je *lex generalis;* v njem je določeno, da ima „vsaka oseba“ pravico do pravnih sredstev, ne glede na kraj njenega prebivališča. Predlagani okvirni sklep ne vsebuje nobene od ozemeljskih omejitev. ENVP predlaga, naj se ozemeljska omejitev v členih 30 in 52 izpusti.

7. **NADZOR**

7.1. **Uvodna opomba: deljene odgovornosti**

Predlogi predvidevajo delitev nadzora med nacionalnimi nadzornimi organi ([1]) in ENVP, od katerih je vsak zadolžen za svoje področje. To je skladno s pristopom predlogov k veljavnemu pravnemu redu in odgovornostim za delovanje in uporabo SIS II ter s potrebo po učinkovitem nadzoru.

Zato ENVP pozdravlja ta pristop v členu 31 predlagane uredbe in členu 53 predlaganega sklepa. Za boljše in jasnejše razumevanje posamičnih nalog ENVP predlaga, naj se vsak člen razdeli v več določb, od katerih bo vsaka obravnavala stopnjo nadzora, kot je bilo že primerno narejeno v predlogu VIS.

([1]) Vključeni so tudi nadzorni organi za Europol in Eurojust, a v manjši meri.

7.2. **Nadzor, ki ga izvajajo nacionalni organi za varstvo podatkov**

Skladno s členom 31 predlagane uredbe in členom 53 predlaganega sklepa mora vsaka država članica zagotavljati, da neodvisen organ spremlja zakonitost obdelave osebnih podatkov v SIS II.

Člen 53 predlaganega sklepa dodaja tudi pravico posameznika, da zaprosi nadzorni organ, naj preveri zakonitost obravnave podatkov, ki se nanj nanašajo. Podobna določba ni vključena v predlagano uredbo, ker se direktiva uporablja kot *lex generalis*. Zato velja, da lahko nacionalni organi za varstvo osebnih podatkov glede na SIS II izvajajo vse pristojnosti, ki jim jih podeljuje člen 28 direktive 95/46/ES, vključno s preverjanjem zakonitosti določenega procesa obdelave podatkov. Člen 31 (1) uredbe njihove naloge pojasnjuje, a ne sme predstavljati omejitev teh pristojnosti. Priznavanje teh pristojnosti bi moralo biti v besedilu predlagane uredbe jasneje izraženo.

Predlagani sklep priznava razširjene dolžnosti nacionalnim nadzornim organom, ker je njegov *lex generalis* drugačen od tistega predlagane uredbe. A položaj, ko bi imeli nadzorni organi glede na kategorijo podatkov v obdelavi različne naloge in pristojnosti, ni smiseln in je v praksi zelo težko izvedljiv. Zato se mu je treba izogniti, bodisi s priznavanjem istih pristojnosti tem organom v samem besedilu sklepa ali s sklicevanjem na kateri drugi *lex generalis* (npr. okvirni sklep o varstvu osebnih podatkov v tretjem stebru), ki podeljuje več pristojnosti organom za varstvo osebnih podatkov.

7.3. **Nadzor, ki ga izvaja ENVP**

ENVP spremlja, da se dejavnosti obdelave podatkov Komisije izvajajo v skladu s predlogi. Podobno bi moral ENVP izvajati vse svoje pristojnosti iz Uredbe 45/2001 ob upoštevanju omejenih pooblastil Komisije v zvezi s samimi podatki.

Treba je dodati, da ENVP skladno s členom 46 (f) Uredbe 45/2001 „sodeluje z nacionalnimi nadzornimi organi iz člena v obsegu, potrebnem za opravljanje njegovih dolžnosti". Sodelovanje z državami članicami pri nadzoru SIS II ne izhaja samo iz predlogov, ampak tudi iz Uredbe 45/2001.

7.4. **Skupni nadzor**

Predlogi tudi priznavajo potrebo po usklajenih dejavnostih nadzora različnih zadevnih organov. Člen 31 predlagane uredbe in člen 53 predlaganega sklepa določata, da „nacionalni nadzorni organi in evropski varuh osebnih podatkov aktivno sodelujejo. V ta namen evropski varuh osebnih podatkov najmanj enkrat letno skliče sestanek."

ENVP toplo pozdravlja ta predlog, ki vsebuje bistvene elemente za vzpostavitev resnično ključnega sodelovanja med organi, zadolženimi za nadzor na nacionalni ravni in na ravni EU. Poudari naj se, da je treba sestanek najmanj enkrat letno, kot je predvideno v predlogih, obravnavati kot minimum.

Te določbe (člen 31 predlagane uredbe in člen 53 predlaganega sklepa) bi lahko bile jasnejše, kar se tiče vsebine tega sodelovanja. Sedanji SNO je pristojen za preučevanje težav pri interpretaciji in izvajanju konvencije, težav, ki se lahko pojavijo pri izvajanju neodvisnega nadzora ali uresničevanju pravice do dostopa, in za pripravo usklajenih predlogov skupnih rešitev obstoječih težav.

Novi predlogi ne smejo voditi k temu, da bi se sedanji okvir skupnega nadzora razrahljal. Če je jasno, da lahko organi za varstvo osebnih podatkov v zvezi s SIS II izvajajo vse pristojnosti nadzora, ki jim jih podeljuje a direktiva, lahko sodelovanje teh organov pokrije mnoge vidike nadzora SIS II, vključno z nalogami obstoječega SNO iz člena 115 Schengenske konvencije.

Za popolno jasnost navedenega bi bilo priporočljivo to v predlogih izrecno ponovno potrditi.

8. **VARNOST**

Upravljanje optimalne stopnje varnosti in njeno upoštevanje pri SIS II je osnovni pogoj za zagotavljanje ustreznega varstva osebnih podatkov, shranjenih v bazi podatkov. Da bi zagotovili to zadovoljivo stopnjo varstva, je treba vpeljati ustrezne nadzorne ukrepe za obvladovanje morebitnih tveganj, povezanih z infrastrukturo sistema in zadevnimi osebami. Trenutno se o tej zadevi razpravlja ob različnih delih predloga in jo je treba nekoliko izboljšati.

Člena 10 in 13 predloga vsebujeta različne ukrepe za varnost podatkov in izrecno navajata oblike zlorab, ki jih je treba preprečiti. ENVP pozdravlja vnos določb sistematičnih varnostnih ukrepov samonadzora v te člene.

A člen 59 predlaganega sklepa in člen 34 predlagane uredbe, ki predvidevata spremljanje in oceno, se ne bi smela nanašati le rezultate, stroškovno učinkovitost in kakovost storitev, temveč tudi na spoštovanje pravnih določb, posebej na področju varstva podatkov. Zato ENVP predlaga, naj se obseg teh členov razširi tudi na spremljanje in poročanje o zakonitosti obdelave.

Poleg tega je treba – k členoma 10 (1) (f) ali 18 predlaganega sklepa in členu 17 predlagane uredbe o pooblaščenem osebju s pravico dostopa do podatkov – dodati, da bi morale države članice (in Europol ter Eurojust) zagotavljati, da so na voljo natančni profili uporabnikov (ki jih je treba hraniti na razpolago za preglede nacionalnih nadzornih organov). Poleg teh profilov uporabnikov morajo države članice pripraviti in nenehno posodabljati popoln seznam istovetnosti uporabnikov. To smiselno velja tudi za Komisijo.

Ti varnostni ukrepi so dopolnjeni s spremljanjem in organizacijskimi nadzornimi ukrepi. Člen 14 predlogov vsebuje opise pogojev in namenov hranjenja zapisov o vseh operacijah obdelave podatkov. Ti zapisi se ne hranijo samo zaradi spremljanja varstva podatkov in zagotavljanja njihove varnosti, temveč tudi za utrditev rednega samonadzora SIS II, predpisanega v členu 10. Poročila o samonadzoru pripomorejo k učinkovitemu uresničevanju nalog nadzornih organov, ki lahko tako prepoznajo najšibkejše točke in se med postopkom lastnega nadzora osredotočijo nanje.

Kot je bilo že omenjeno, mora biti več dostopnih točk za sistem pazljivo upravičenih, saj takoj povečujejo tveganje zlorab. Člen 4 (1) (b) naj zato zahteva konkretno ponazoritev potrebe po drugi dostopni točki.

Predlogi ne pojasnijo dovolj potrebe po nacionalnih kopijah osrednjega sistema, kar povzroča resno zaskrbljenost glede splošne stopnje tveganja in varnosti sistema, saj med drugim:

— več kopij pomeni večje tveganje zlorab (posebej ob upoštevanju prisotnosti novih podatkov, npr. biometričnih),

— ni točno določeno, na katere podatke se te kopije nanašajo,

— zahteve po točnosti, kakovosti in razpoložljivosti iz člena 9 predstavljajo velik tehnični izziv in zato večje stroške glede na najboljšo možno razpoložljivo tehnologijo,

— nadzor, ki ga nad temi kopijami izvajajo nacionalni nadzorni organi, zahteva dodatne človeške in finančne vire, ki morda niso vedno na voljo.

Glede na možna tveganja ENVP ni prepričan niti o potrebi po nacionalnih kopijah (ob upoštevanju razpoložljivih tehnologij) niti o dodatni vrednosti njihove uporabe. Predlaga opustitev možnosti uporabe nacionalnih kopij v državah članicah.

Če naj bi se nacionalne kopije vseeno zasnovale, pa ENVP ponovno opozarja, da je pri njihovi nacionalni uporabi potrebno uporabljati načelo strogih omejitev namenov. Podobno lahko nacionalno kopijo preverja samo centralna podatkovna zbirka.

Zakonitost obdelave osebnih podatkov temelji na strogem spoštovanju varnosti in neoporečnosti podatkov. Spremljanje teh procesov s strani ENVP je učinkovito, kadar lahko s pomočjo analize razpoložljivih evidenc spremlja varnost podatkov in njihovo neoporečnost. Zato je v členu 14 (6) treba dodati „neoporečnostjo podatkov“.

9. **KOMITOLOGIJA**

Predlogi predvidevajo postopke komitologije v več primerih, ko so potrebne tehnične odločitve glede izvajanja ali upravljanja SIS II. Te odločitve pomembno vplivajo na primerno izvajanje načela namena in sorazmernosti, kakor je bilo iz podobnih razlogov že navedeno v mnenju o VIS.

Po nasvetu ENVP je treba odločitve z velikim vplivom na varstvo podatkov sprejemati kot uredbo ali sklep, po možnosti s postopkom soodločanja; sem med drugim spadajo odločitve glede dostopa do podatkov in njihovega vnosa, izmenjave dopolnilnih podatkov, kakovosti podatkov in primerljivosti med razpisi ukrepov, tehnične skladnosti nacionalnih kopij itd.

V vseh drugih primerih, ki lahko vplivajo na varstvo podatkov, mora ENVP imeti možnost svetovanja pri odločitvah teh odborov.

Svetovalno vlogo ENVP je treba vključiti v člena 60 in 61 sklepa in člen 35 uredbe.

V primeru natančnejših določb za tehnična pravila glede razpisov ukrepov (člen 26 uredbe in člen 46 sklepa) je treba razložiti zahtevo po drugačni komitologiji (svetovalna za sklepe in regulativna za uredbe).

10. **INTEROPERABILNOST**

Zaradi pomanjkljivega poročanja Komisije glede interoperabilnosti nastajajočih sistemov EU je težko ustrezno oceniti dodatno vrednost predvidenih sinergij, ki še niso natančno določene.

V zvezi s tem ENVP omenja tudi deklaracijo Sveta z dne 25. marca 2004 o boju proti terorizmu, v kateri se Komisija poziva, naj predstavi predloge za povečanje interoperabilnosti ter sinergij med informacijskimi sistemi (SIS, VIS in Eurodac). ENVP bi želel omeniti tudi sedanjo razpravo o tem, kateremu organu naj bi se v prihodnje poverilo upravljanje različnih velikih sistemov (glej tudi odstavek 3.8 tega mnenja).

Že v svojem mnenju o vizumskem informacijskem sistemu je ENVP navedel, da je interoperabilnost ključna in nujna za doseganje učinkovitosti velikih sistemov, kot je SIS II. Omogoča zmanjšanje skupnih stroškov, doslednost in preprečuje naravne presežke heterogenih elementov.

— Lahko tudi pripomore k cilju vzdrževanja visoke ravni varnosti na območju brez notranjih mejnih kontrol med državam članicami, in sicer z izvajanjem enakega standarda za postopke vseh sestavnih delov te politike. Na vsak način pa je treba ločiti dve ravni interoperabilnosti:

  — interoperabilnost med državami članicami EU je zelo zaželena; razpisi ukrepov organov ene države članice morajo biti interoperabilni s tistimi, ki jih razpišejo organi druge države članice.

  — Interoperabilnost med sistemi, zgrajenimi v različne namene, ali med njimi in sistemi tretjih držav, je bistveno bolj vprašljiva.

K tej omejitvi lahko med nadzornimi ukrepi, ki so na voljo za omejevanje namena sistema in preprečevanje postopne širitve področja uporabe sistema (*„function creep“*), prispeva uporaba različnih tehnoloških standardov. Dejansko je treba vsako interakcijo med dvema različnima sistemoma natančno zabeležiti. Interoperabilnost naj ne bi nikoli pripeljala do položaja, ko lahko organ, ki ni pooblaščen za dostop ali uporabo določenih podatkov, pridobi dostop prek drugega informacijskega sistema. Na podlagi branja predlogov se zdi, da avtomatski sistem prepoznavanja prstnih odtisov (AFIS), na primer, ne bo prisoten v prvih letih SIS II, saj se omenja samo načrtovani biometrični iskalnik. Če to predvideva uporabo AFIS iz drugih sistemov EU, je treba to jasno zabeležiti s potrebnimi nadzornimi ukrepi, zahtevanimi za take sinergije.

ENVP vnovič poudarja, da interoperabilnosti med sistemi ni moč izvajati s kršenjem načela omejitve namena in da mu je treba posredovati vsak predlog v zvezi s to zadevo.

11. **POVZETEK ZAKLJUČKOV**

11.1. **Splošne točke**

1. ENVP pozdravlja številne pozitivne vidike teh predlogov, ki v mnogih točkah pomenijo napredek glede na sedanje razmere. Priznava, da so bile določbe v zvezi z varstvom podatkov na splošno zelo pazljivo zasnovane.

2. Poudarja, da mora nova pravna ureditev ne glede na stopnjo zapletenosti

   — zagotavljati visoko raven varstva podatkov,

   — omogočati zanesljivost za državljane in za organe, ki si izmenjujejo podatke,

   — biti pri uporabi v različnih kontekstih (prvega ali tretjega stebra) dosledna.

3. Dodani novi deli v SIS II zahtevajo strožje nadzorne ukrepe, ki so opisani v tem mnenju, saj povečujejo možnost vpliva sistema na življenja posameznikov. In sicer zlasti:

— Dostopa do podatkov v SIS II si novi organi ne morejo pridobiti brez kar najmočnejše utemeljitve. Treba ga je tudi kar najbolj omejiti, tako glede dostopnih podatkov kot tudi pooblaščenih oseb.

— Povezave med ukrepi ne smejo v nobenem primeru – niti neposredno – povzročiti spremembe pravic do dostopa.

— Nesprejeta zakonodaja ne more veljati za utemeljeno podlago za vnašanje podatkov v SIS II (razpisi ukrepov v namen zavrnitve vstopa).

— Da bi se upoštevalo cilj boja proti kriminalu, je treba ponovno preučiti pravno podlago za dostop organov, ki so pristojni za izdajo potrdil o registraciji.

— ENVP se strinja, da lahko uporaba biometričnih podatkov izboljša učinkovitost sistema in pomaga žrtvam kraje identitete. Zdi pa se, da posledice te uvedbe niso bile dovolj podrobno pretehtane, in da se precenjuje zanesljivost teh podatkov.

— Dostop mora biti skladen s splošnim namenom SIS II in se ujemati s pravno podlago sistema.

— Treba je nazorno prikazati potrebo po dostopu do podatkov iz SIS II.

— Treba je jasno in restriktivno določiti, kako se podatki uporabljajo.

— Treba je jasno in restriktivno določiti pogoje dostopa. Zlasti je treba sestaviti posodobljen seznam oseb, ki so pooblaščene za dostop do SIS II tudi za Europol in Eurojust.

— Dejstvo, da je zadevnim organom odobren dostop do podatkov iz SIS II, ne more biti nikoli razlog za vnos ali vzdrževanje podatkov v sistemu, če ti podatki niso izrecno uporabni za razpis ukrepov, katerega del so.

— Obdobja hrambe podatkov se ne morejo podaljšati, če to ni potrebno za doseg namena, ki je bil podlaga za vnos podatkov v sistem.

11.2. **Posebne opombe**

1. ENVP pozdravlja priznanje Komisije, da se Uredba 45/2001 uporablja za vse dejavnosti obdelave podatkov Komisije in SIS II, saj to zagotavlja dosledno in enotno uporabo pravil glede varstva posameznikovih temeljnih pravic in svoboščin pri obdelavi osebnih podatkov.

2. Za zagotavljanje stroge omejitve namena na nacionalni ravni ENVP predlaga, da se v predloge SIS II (in sicer člen 21 predlagane uredbe in člen 40 predlaganega sklepa) vstavi določba, ki ima isti namen kot sedanji člen 102(4) Schengenske konvencije in omejuje možnost držav članic, da določajo uporabo podatkov, ki niso predvideni v besedilih SIS II.

3. Pri odobravanju dostopa do podatkov v SIS II je treba uporabljati stroge pogoje:

4. ENVP za posebna primera Europola in Eurojusta poziva Komisijo, naj restriktivno določi naloge, za izvedbo katerih bi bil dostop do podatkov upravičen. Poleg tega je treba dostop Europola in Eurojusta omejiti na podatke o posameznikih, katerih ime se že pojavlja v njunih podatkovnih zbirkah. Predlaga se tudi, naj se za Europol in Eurjust določi samo ena dostopna točka.

5. Glede razpisov ukrepov v namen zavrnitve vstopa je treba določbe, temelječe na še ne sprejeti zakonodaji, umakniti ali ponovno oblikovati tako, da bodo temeljile na obstoječi zakonodaji in omogočale posameznikom natančno poznavanje ukrepov, ki jih lahko organi sprejmejo v zvezi z njimi.

6. Obdobja hrambe podatkov so bila podaljšana brez kakršne koli predlagane resne utemeljitve za to. Če prepričljive utemeljitve ni, je treba obdobja skrajšati na sedanje trajanje, predvsem glede razpisov ukrepov prikritega evidentiranja ali namenskih kontrol.

7. Komisija ima po opisu nalogo operativnega vodenja. Poleg njene pomembne vloge pri razvoju in vzdrževanju sistema je to naloga upravljalca *sui generis*. Komisija je mnogo več od obdelovalca, a tudi manj od običajnega nadzornika, saj nima dostopa do podatkov, ki so v obdelavi v SIS II.

   Za uporabo te vloge je treba v členu 12 obeh predlogov dodati, naj Komisija redno predlaga izvajanje novih tehnologij, ki predstavljajo najboljše razpoložljivo s tega področja in povečujejo stopnje varnosti in varstva podatkov.

8. Glede vloge držav članic je potrebno pojasniti, kateri so nadzorni organi.

9. Glede pravice osebe, na katero se podatki nanašajo:

   — V predlagani uredbi je treba na seznam dodati: obdobje hrambe podatkov, morebitno pravico do prošnje za pregled ali pritožbo na sklep za izdajo razpisa ukrepov, možnost pridobitve pomoči pri organu za varstvo podatkov in razpoložljiva pravna sredstva.

     Zlasti pa podatke o razpisu ukrepov v sklepu, ki je podlaga samemu razpisu, od trenutka, ko so ti podatki na voljo.

   — V predlogu sklepa je treba člen 50 spremeniti, da pravica so informacij ne bo odvisna od zahteve osebe, na katero se podatki nanašajo.

10. Glede rokov za odgovor na prošnjo za dostop se pozdravlja uvedbo rokov v predlogih. Kadar tudi nacionalni pravni predpisi določajo roke, je treba jasno navesti, da se morajo uporabljati roki, ki so najbolj ugodni za osebo, na katero se podatki nanašajo.

    Bilo bi tudi priporočljivo vpeljati obvezo, naj organi za varstvo podatkov dejavno sodelujejo pri uresničevanju pravice do dostopa.

11. Glede pravice do pravnih sredstev ENVP predlaga opustitev omejenosti z ozemljem iz člena 30 in člena 52.

12. Glede pristojnosti nacionalnih organov za varstvo podatkov:

   — v uredbi: je treba upoštevati, da lahko glede SIS II izvajajo vse pristojnosti, ki jim jih podeljuje člen 28 Direktive 95/46/ES, kar je treba v besedilu predlagane uredbe jasno navesti;

   — v sklepu: nadzornim organom je treba podeliti enake pristojnosti kot v uredbi/direktivi.

13. Glede pristojnosti ENVP: ENVP se mora omogočiti izvajanje vseh njegovih pristojnosti iz Uredbe 45/2001 ob upoštevanju omejenih pooblastil Komisije v zvezi s samimi podatki.

14. Glede usklajenega nadzora: predlogi tudi priznavajo potrebo po usklajenih dejavnostih nadzora različnih zadevnih organov. ENVP toplo pozdravlja, da vsebujejo bistvene elemente za vzpostavljanje resnično ključnega sodelovanja med organi, zadolženimi za nadzor na nacionalni ravni in na ravni EU. Te določbe (člen 31 predlagane uredbe in člen 53 predlaganega sklepa) pa bi lahko jasneje določale vsebino takega sodelovanja.

15. Člena 10 in 13 predloga navajata različne ukrepe za varnost podatkov; pozdravlja se vključenje varnostnih ukrepov sistematičnega samonadzora.

   — A člen 59 predlaganega sklepa in člen 34 predlagane uredbe, ki predvidevata spremljanje in oceno, se ne bi smela nanašati le rezultate, stroškovno učinkovitost in kakovost storitev, temveč tudi na spoštovanje pravnih določb, posebej na področju varstva podatkov. Te določbe je treba ustrezno spremeniti.

   — Poleg tega je treba – k členoma 10(1)(f) ali 18 predlaganega sklepa in členu 17 predlagane uredbe o pooblaščenem osebju s pravico dostopa do podatkov – dodati, da bi morale države članice, Europol in Eurojust zagotavljati, da so na voljo natančni profili uporabnikov (ki jih je treba hraniti na razpolago za preglede nacionalnih nadzornih organov). Poleg teh profilov uporabnikov morajo države članice pripraviti in nenehno posodabljati popoln seznam istovetnosti uporabnikov. Enako velja za Komisijo.

   — Zakonitost obdelave osebnih podatkov temelji na strogem spoštovanju varnosti in neoporečnosti podatkov. ENVP je treba s pomočjo analize razpoložljivih evidenc omogočiti spremljanje varnosti podatkov in njihove neoporečnosti. Zato je v členu 14(6) treba dodati „neoporečnostjo podatkov“.

16. Uporaba nacionalnih kopij lahko pomeni več dodatnih vrst tveganja. ENVP ni prepričan niti o potrebi po nacionalnih kopijah (ob upoštevanju razpoložljivih tehnologij), niti o dodatni vrednosti njihove uporabe. Predlaga opustitev ali vsaj strogo omejitev možnosti držav članic za uporabo nacionalnih kopij. Če naj bi se nacionalne kopije vseeno zasnovale, pa je pri njihovi nacionalni uporabi potrebno uporabljati načelo strogih omejitev namenov. Podobno lahko nacionalno kopijo preverja samo centralna podatkovna zbirka.

17. Glede komitologije: odločitve, ki lahko pomembno vplivajo na varstvo podatkov, je najbolj priporočljivo sprejeti z uredbo, po možnosti v skladu s postopkom soodločanja.Za dejansko uporabo komitologije je treba svetovalno vlogo ENVP vključiti v člena 60 in 61 sklepa in člen 35 uredbe.

18. Interoperabilnost sistemov se ne sme izvajati s kršenjem načela omejitve namena; ENVP je treba posredovati vsak predlog v zvezi s to zadevo.

V Bruslju, 19. oktobra 2005

Peter HUSTINX

Evropski nadzornik za varstvo podatkov