Európsky dozorný úradník pre ochranu údajov

Stanovisko Európskeho dozorného úradníka pre ochranu údajov

— k návrhu rozhodnutia Rady o zriadení, prevádzke a využívaní Schengenského informačného systému druhej generácie (SIS II) (KOM(2005)230, konečné znenie),

— k návrhu nariadenia Európskeho parlamentu a Rady o zriadení, prevádzke a využívaní Schengenského informačného systému druhej generácie (SIS II) (KOM(2005)236, konečné znenie) a

— k návrhu nariadenia Európskeho parlamentu a Rady, ktoré sa týka prístupu útvarov zodpovedných za vydávanie osvedčení o evidencii vozidiel v členských štátoch do Schengenského informačného systému druhej generácie (SIS II) (KOM(2005)237, konečné znenie)

(2006/C 91/11)

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV,

so zreteľom na Zmluvu o založení Európskeho spoločenstva, a najmä na jej článok 286,

so zreteľom na Chartu základných práv Európskej únie, a najmä na jej článok 8,

so zreteľom na smernicu Európskeho parlamentu a Rady č. 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov,

so zreteľom na nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov, a najmä na jeho článok 41,

so zreteľom na žiadosť o stanovisko v súlade s článkom 28 ods. 2 nariadenia (ES) č. 45/2001, ktorá bola 17. júna 2005 prijatá od Komisie,

PRIJAL TOTO STANOVISKO:

1. ÚVOD

1.1. Súvislosti

Schengenský informačný systém (SIS) je rozsiahlym IT systémom EÚ, ktorý bol vytvorený ako kompenzačné opatrenie po zrušení kontrol na vnútorných hraniciach v rámci schengenského priestoru. SIS umožňuje príslušným orgánom členských štátov výmenu informácií, ktoré sa používajú pri výkone kontrol osôb a predmetov na vonkajších hraniciach alebo na území, ako aj pri vydávaní víz a povolení na pobyt.

Schengenský dohovor nadobudol platnosť v roku 1995 ako medzivládna dohoda. SIS, ktorý je súčasťou Schengenského dohovoru, neskôr začlenila do rámca EÚ Amsterdamská zmluva.

Nový Schengenský informačný systém II („druhej generácie“) nahradí súčasný systém, čím sa umožní rozšírenie schengenského priestoru o nové členské štáty EÚ. Taktiež do tohto systému prinesie nové funkcie. Ustanovenia Schengenského dohovoru vypracované na medzivládnej úrovni sa plne transformujú na klasické európske právne nástroje.

Európska komisia predložila 1. júna 2005 tri návrhy na zriadenie SIS II. Tieto návrhy obsahujú:

— nariadenie navrhované na základe hlavy IV Zmluvy o ES (víza, azylová a prisťahovalecká politika a iné politiky týkajúce sa voľného pohybu osôb), ktorým sa v rámci SIS II budú riadiť aspekty prvého piliera (prisťahovalectvo), ďalej len „navrhované nariadenie“;

— rozhodnutie navrhované na základe hlavy VI Zmluvy o EÚ (policajná a justičná spolupráca v trestných veciach), ktorým sa bude riadiť používanie SIS II na účely tretieho piliera, ďalej len „navrhované rozhodnutie“;

— nariadenie navrhované na základe hlavy V (doprava), ktoré sa špecificky týka prístupu orgánov zodpovedných za evidenciu vozidiel k údajom z SIS; tento návrh sa bude rozoberať osobitne (pozri bod 4.6 nižšie).

V tomto kontexte sa žiada spomenúť, že Komisia v priebehu niekoľkých mesiacov vydá oznámenie o interoperabilite a zvýšených synergických účinkoch informačných systémov EÚ (SIS, VIS, Eurodac).

SIS II sa skladá z centrálnej databázy, ktorá sa nazýva „Centrálny schengenský informačný systém“ (CS-SIS), pre ktorý Komisia zabezpečí operačné riadenie pripojené k vnútroštátnym prístupovým bodom, ktoré si vymedzí každý členský štát (NI-SIS). Orgány SIRENE zabezpečia výmenu všetkých doplnkových informácií (informácie súvisiace so záznamami v SIS II, ktoré v ňom ale nie sú uložené).

Členské štáty budú do SIS II poskytovať údaje o osobách hľadaných na účely zatknutia, odovzdania alebo vydania, osobách, ktoré sa majú zúčastniť súdneho konania, osobách, ktoré majú byť pod dohľadom alebo sa majú podrobovať osobitnej kontrole, osobách, ktorým sa má odoprieť vstup na vonkajších hraniciach, a o stratených alebo odcudzených predmetoch. Súbory údajov nazývané „záznamy“, ktoré sú vložené v SIS, umožňujú príslušnému orgánu identifikovať osobu alebo predmet.

SIS II obsahuje nové funkcie: rozšírený prístup do SIS (Europol, Eurojust, štátni prokurátori, orgány zodpovedné za schvaľovanie vozidiel), prepojenie záznamov, pridávanie nových kategórií údajov vrátane biometrických údajov (odtlačky prstov a fotografie), ako aj technickú platformu, ktorú bude využívať aj Vízový informačný systém. Tieto dodatočné funkcie sú už roky predmetom diskusie o zmene účelu SIS z kontrolného nástroja na spravodajský a vyšetrovací systém.

1.2. **Všeobecné hodnotenie návrhov**

1. Európsky dozorný úradník pre ochranu údajov (EDPS) víta, že bol požiadaný o konzultáciu na základe článku 28 ods. 2 nariadenia (ES) č. 45/2001. So zreteľom na záväznú povahu článku 28 ods. 2 by sa však toto stanovisko malo spomenúť v preambule uvedených textov.

2. EDPS víta návrhy z niekoľkých dôvodov. Transformácia medzivládnej štruktúry na európske právne nástroje prináša niekoľko pozitívnych dôsledkov: objasní sa právna hodnota pravidiel, ktorými sa SIS II riadi, Súdny dvor získa právomoc interpretovať právny nástroj prvého piliera, aspoň čiastočne sa zapojí Európsky parlament (aj keď až v trochu neskorej etape procesu).

3. Okrem toho, pokiaľ ide o vecnú stránku, významná časť návrhov sa venuje ochrane údajov, pričom v porovnaní so súčasnou situáciou miestami ide o vítané zlepšenia. Konkrétne možno spomenúť opatrenia v prospech obetí krádeže identity, rozšírenie nariadenia 45/2001 na činnosti Komisie spojené so spracovaním údajov v rámci činností v hlave VI a lepšie vymedzenie dôvodov na vydávanie záznamov na účely odoprenia vstupu pre jednotlivcov.

4. Tiež je zrejmé, že príprave návrhov sa venovala veľká pozornosť; sú síce zložité, čo však len odráža samotnú komplexnosť systému, ktorý riadia. Väčšina pripomienok v tomto stanovisku sa zameriava na vysvetlenie alebo doplnenie ustanovení, ktoré však nebude potrebné úplne preformulovať.

Napriek tomuto celkove pozitívnemu hodnoteniu však možno vyjadriť určité výhrady, a to najmä:

1. V mnohých ohľadoch je ťažké zistiť, aký zámer sa za textom skrýva; poľutovaniahodná je najmä skutočnosť, že chýba dôvodová správa. Táto správa by bola základnou požiadavkou z hľadiska veľmi zložitého charakteru týchto dokumentov. Jej absencia v niektorých prípadoch nedáva čitateľovi inú možnosť, než sa spoľahnúť na domnienky.

2. Okrem toho je tiež poľutovaniahodné, že sa neuskutočnila žiadna štúdia o posúdení vplyvu. Neospravedlňuje to ani skutočnosť, že prvá verzia systému sa už používa, keďže medzi verziami sú významné rozdiely. Okrem iného sa mal lepšie premyslieť vplyv zavedenia biometrických údajov.

3. Právny rámec ochrany údajov je tiež veľmi komplexný; zakladá sa na spoločnom uplatňovaní *lex generalis* a *lex specialis*. Malo by sa zabezpečiť zachovanie plnej uplatniteľnosti existujúceho rámca ochrany údajov v smernici 95/46/ES a nariadení 45/2001 aj v prípade, že sa vytvoria osobitné právne predpisy. Kombinované uplatňovanie rôznych právnych nástrojov by nemalo viesť ani k rozdielom v zásadných aspektoch medzi vnútroštátnymi mechanizmami, ani k zníženiu súčasnej úrovne ochrany údajov.

4. Prístup mnohých nových orgánov, ktoré nezapadajú do pôvodného „účelu kontroly osôb a predmetov“ by mali sprevádzať prísnejšie ochranné opatrenia.

5. Návrhy sú zo značnej časti založené na iných právnych nástrojoch, ktoré sú stále v procese prípravy (niekedy ešte pred samotnou etapou navrhnutia). EDPS chápe problémy legislatívnej práce v komplexnom a stále sa vyvíjajúcom prostredí; z hľadiska dôsledkov pre dotknuté osoby a právnej neistoty, ktorú takýto stav spôsobuje, to však považuje za neprijateľné.

6. Pri rozdeľovaní právomocí medzi členské štáty a Komisiu existujú nejasnosti. Jasnosť je prioritou, keďže nie je dôležitá len pre hladký chod systému, ale je aj základnou požiadavkou na zabezpečenie komplexného dohľadu nad systémom.

1.3. **Štruktúra stanoviska**

Štruktúra stanoviska bude takáto: najprv objasní právny rámec uplatniteľný na SIS II. Potom sa bude zaoberať vymedzením účelu SIS II a prvkov, ktoré sa významne odlišujú od súčasného systému. Bod 5 obsahuje poznámky k úlohám Komisie a členských štátov vzhľadom na prevádzku SIS II. Bod 6 sa týka práv dotknutých osôb, zatiaľ čo bod 7 rieši dohľad na vnútroštátnej úrovni a na úrovni EDPS, ako aj spoluprácu medzi dozornými úradníkmi. V bode 8 sa navrhujú niektoré pripomienky a možné zmeny a doplnenia týkajúce sa bezpečnosti; body 9 a 10 sa zaoberajú komitológiou a interoperabilitou. Napokon, hlavné závery každého bodu sa nachádzajú v zhrnutí záverov.

2. PRÍSLUŠNÝ PRÁVNY RÁMEC

2.1. **Príslušný právny rámec ochrany údajov SIS II**

Návrhy sa odvolávajú na smernicu 95/46/ES, dohovor 108 a nariadenie 45/2001 ako na svoj právny rámec ochrany údajov. Dôležité sú aj ďalšie nástroje.

Z hľadiska objasnenia tohto kontextu a kvôli pripomenutiu hlavných referenčných bodov nášho skúmania je užitočné spomenúť aspoň tieto:

— Rešpektovanie súkromného života je v Európe zaistené od schválenia Dohovoru o ochrane ľudských práv a základných slobôd v roku 1950 (ďalej len: „EDĽP") Radou Európy. Článok 8 EDĽP stanovuje „právo na súkromný a rodinný život".

  Podľa článku 8 ods. 2 je akékoľvek zasahovanie verejného orgánu do výkonu tohto práva dovolené, len ak je „v súlade so zákonom" a je „v demokratickej spoločnosti nevyhnutné" na ochranu dôležitých záujmov. V judikatúre Európskeho súdu pre ľudské práva tieto podmienky viedli k dodatočným požiadavkám, pokiaľ ide o kvalitu právnych základov pre zasahovanie, proporcionalitu akéhokoľvek opatrenia a potrebu vhodných ochranných opatrení voči zneužitiu.

— Právo na rešpektovanie súkromného života a ochranu osobných údajov sa nedávno ustanovilo v článkoch 7 a 8 Charty základných práv Európskej únie. Podľa článku 52 Charty sa uznáva, že tieto práva môžu podliehať obmedzeniam za predpokladu, že sú splnené podobné podmienky, ako sa uplatňujú v článku 8 EDĽP.

— Článok 6 ods. 2 Zmluvy o EÚ ustanovuje, že Únia dodržiava základné práva zaručené EDĽP.

Nasledujú tri texty, ktoré sú explicitne uplatniteľné na návrhy o SIS II:

— Dohovorom Rady Európy č. 108 z 28. januára 1981 o ochrane osôb pri automatizovanom spracovaní osobných údajov (ďalej len „*Dohovor 108*") sa vytvorili základné zásady ochrany jednotlivcov v súvislosti so spracovaním osobných údajov. Dohovor 108 ratifikovali všetky členské štáty. Uplatňuje sa aj na činnosti vykonávané v rámci policajnej a justičnej oblasti. Dohovor 108 je v súčasnosti mechanizmom ochrany údajov, ktorý je uplatniteľný na Dohovor o SIS, spolu s odporúčaním Výboru ministrov Rady Európy č. R (87) 15 zo 17. septembra 1987 upravujúcim používanie osobných údajov v oblasti polície.

— Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov (Ú. v. ES L 281, s. 31). Táto smernica sa bude uvádzať ako „*smernica 95/46/ES*". Treba pripomenúť, že vo väčšine členských štátov zahŕňajú vnútroštátne právne predpisy, ktorými sa smernica vykonáva, aj činnosti spracovania údajov uskutočňované v oblasti polície a súdnictva.

— Nariadenie Európskeho parlamentu a Rady (ES) 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi spoločenstva a o voľnom pohybe takýchto údajov (Ú. v. ES L 8, s. 1). Toto nariadenie sa bude uvádzať ako „*nariadenie 45/2001*".

Interpretácia smernice 95/46/ES a nariadenia 45/2001 musí sčasti závisieť od príslušnej judikatúry Európskeho súdu pre ľudské práva podľa Európskeho dohovoru o ľudských právach a základných slobodách z roku 1950 (EDĽP). Inými slovami, uvedená smernica a uvedené nariadenie, pokiaľ sa zaoberajú spracovaním osobných údajov, ktoré môžu porušovať základné slobody, najmä právo na súkromie, sa musia vykladať so zreteľom na ľudské práva. Vyplýva to tiež z jurisdikcie Európskeho súdneho dvora ([1]).

([1]) V tejto súvislosti je účelné odvolať sa na rozsudok Súdneho dvora vo veci Österreichischer Rundfunk a ostatní (spojené veci C-465/00, C-138/01 a C-139/01, rozsudok z 20. mája 2003, Súdny dvor (2003) Zb. I-4989). Dvor sa zaoberal rakúskym zákonom upravujúcom prenos údajov o platoch zamestnancov vo verejnom sektore rakúskemu Dvoru audítorov a ich následné uverejnenie. Súd vo svojom rozsudku stanovuje niekoľko kritérií na základe článku 8 Európskeho dohovoru o ľudských právach, ktoré by sa mali použiť pri uplatňovaní smernice 95/46/ES, pokiaľ táto smernica umožňuje určité obmedzenia práva na súkromie.

Komisia vydala 4. októbra 2005 Návrh rámcového rozhodnutia Rady o ochrane osobných údajov spracovávaných v rámci policajnej a justičnej spolupráce v trestných veciach ([1]) (ďalej len „návrh rámcového rozhodnutia“). Zámerom tohto rámcového rozhodnutia je nahradiť Dohovor 108 ako referenčný právny predpis pre návrh rozhodnutia o SIS II, čo bude mať v tomto kontexte pravdepodobne vplyv na mechanizmus ochrany údajov (pozri bod 2.2.5 nižšie).

2.2. **Právny mechanizmus ochrany údajov SIS II**

2.2.1. *Všeobecná poznámka*

Legislatívny základ potrebný na riadenie SIS II pozostáva zo samostatných nástrojov; ako sa však uvádza aj v odôvodneniach, táto skutočnosť „nemá vplyv na zásadu, že SIS II je jednotným informačným systémom a ako taký by aj mal fungovať. Určité ustanovenia týchto nástrojov by preto mali byť totožné.“

Štruktúra príslušných dvoch dokumentov je v podstate totožná, pričom kapitoly I – III sú v oboch zneniach skutočne skoro identické. Skutočnosť, že SIS II treba chápať ako jednotný informačný systém s dvomi rozdielnymi právnymi základmi sa tiež odráža v – dosť zložitom – mechanizme ochrany údajov.

Mechanizmus ochrany údajov je sčasti určený v samotných návrhoch ako „*lex specialis*“, pričom je doplnený rozličnými referenčnými právnymi predpismi („*lex generalis*“) pre každý sektor (Komisia, členské štáty v prvom pilieri, členské štáty v treťom pilieri).

Táto štruktúra nastoľuje otázku spôsobu, akým sa zaoberať so špecializovanými súbormi pravidiel vo vzťahu k všeobecnému právu. V takomto prípade považuje EDPS konkrétne pravidlo za spôsob uplatnenia všeobecného pravidla. V dôsledku toho musí byť *lex specialis* vždy v súlade s *lex generalis*; je nadstavbou (upresňuje alebo dopĺňa) *lex generalis* ale nechápe sa ako výnimka z neho.

Čo sa týka otázky, aké pravidlo by sa malo uplatniť v konkrétnom prípade, zásadou je, že prioritne sa uplatňuje *lex specialis*; ale kedykoľvek je neuplatniteľný alebo nejasný, mal by sa použiť *lex generalis*.

Podľa tejto štruktúry existujú tri rôzne kombinácie *lex generalis* a *lex specialis*. Zhrnúť by sa dali takto.

2.2.2. *Uplatniteľný mechanizmus pre Komisiu*

Ak sa zúčastňuje Komisia, uplatňuje sa nariadenie 45/2001 vrátane úlohy EDPS, či už sa činnosti vykonávajú v rámci prvého (navrhované nariadenie) alebo tretieho piliera (navrhované rozhodnutie). V odôvodnení 21 navrhovaného rozhodnutia sa uvádza, že: „Nariadenie (...) (ES) č. 45/2001 (...) sa uplatňuje na spracovávanie osobných údajov Komisiou, ak sa také spracovávanie uskutočňuje pri výkone činností, z ktorých všetky alebo časť z nich patria do rozsahu pôsobnosti práva Spoločenstva. Časť spracovávania osobných údajov v SIS II patrí do rozsahu pôsobnosti práva Spoločenstva.“

Na takýto postup existujú praktické dôvody: z hľadiska Komisie by bolo skutočne nesmierne zložité určiť, či sa údaje spracovávajú v rámci činností, ktoré spadajú pod právne predpisy prvého alebo tretieho piliera.

Okrem toho dáva uplatňovanie jedného právneho nástroja na všetky činnosti Komisie v kontexte SIS II väčší zmysel z praktického hľadiska, ale aj zvyšuje jednotnosť (čiže zabezpečuje podľa odôvodnenia 21 navrhovaného nariadenia „jednotné a homogénne uplatňovanie pravidiel týkajúcich sa ochrany základných práv a slobôd jednotlivca so zreteľom na spracovávanie osobných údajov“). Preto EDPS víta, že Komisia uznala skutočnosť, že nariadenie 45/2001 sa uplatňuje na všetky činnosti spracovania údajov zo strany Komisie v rámci SIS II.

2.2.3. *Uplatniteľný mechanizmus pre členské štáty*

Situácia týkajúca sa členských štátov je zložitejšia. Spracovanie osobných údajov pri uplatňovaní navrhovaného nariadenia sa riadi samotným navrhovaným nariadením, ako aj smernicou 95/46/ES. Znenie odôvodnenia 14 navrhovaného nariadenia uvádza veľmi jasne, že smernica sa musí považovať za *lex generalis*, zatiaľ čo nariadenie o SIS II bude *lex specialis*. Z tohto vyplýva niekoľko dôsledkov, ktorými sa budeme podrobnejšie zaoberať nižšie.

Čo sa týka navrhovaného rozhodnutia, referenčným právnym nástrojom z hľadiska ochrany údajov (*lex generalis*) je Dohovor 108, čo môže v niektorých otázkach znamenať dôležitý rozdiel medzi mechanizmami ochrany údajov v prvom a treťom pilieri.

2.2.4. *Vplyv na úroveň ochrany údajov*

Ako všeobecnú poznámku k tejto architektúre ochrany údajov EDPS zdôrazňuje toto:

— Uplatňovanie navrhovaného nariadenia ako *lex specialis* smernice 95/46/ES (a podobne uplatňovanie navrhovaného rozhodnutia ako *lex specialis* Dohovoru 108) by z žiadnom prípade nemalo viesť k zníženiu úrovne ochrany údajov, ktorú zaručuje smernica alebo dohovor. EDPS z tohto hľadiska poskytne odporúčania (pozri napríklad právo na opravné prostriedky).

([1]) 2 (KOM(2005) 475, konečné znenie).

— Podobne ani výsledkom spoločného uplatňovania právnych nástrojov nemôže byť zníženie úrovne ochrany údajov, ktoré zaručuje súčasný Schengenský dohovor (pozri napríklad pripomienky k článku 13 smernice 95/46/ES v tomto texte).

— Uplatňovanie dvoch rozličných nástrojov, akokoľvek potrebné z hľadiska rámca európskeho práva, by nemalo viesť k bezdôvodným rozporom medzi ochranou dotknutých osôb podľa typu údajov, ktoré sa v súvislosti s nimi spracovávajú. Tomuto sa treba v čo najväčšej miere vyhnúť. Odporúčania v tomto texte sa budú snažiť aj o čo najväčšie zvýšenie jednotnosti (pozri napríklad právomoci vnútroštátnych dozorných orgánov).

— Právny rámec je tak komplexný, že pri praktickom uplatňovaní môže veľmi ľahko spôsobiť zmätok. V niektorých prípadoch je ťažké určiť, ako spolupôsobia *lex generalis* a *lex specialis*, a bolo by vhodné to v návrhoch vysvetliť. Okrem toho je v tomto komplexnom právnom prostredí veľmi užitočný aj návrh spoločného dozorného orgánu (JSA) pre Schengen v „stanovisku o navrhovanom právnom základe pre SIS II“ (27. september 2005) na vytvorenie „príručky“, ktorá by obsahovala všetky existujúce práva v súvislosti s SIS II a určovala jasnú hierarchiu uplatniteľných právnych predpisov.

Záverom skonštatujeme, že toto stanovisko sa bude snažiť zabezpečiť vysokú úroveň ochrany údajov, jednotnosti a zrozumiteľnosti, aby sa dotknutej osobe poskytla potrebná právna istota.

2.2.5. *Vplyv rámcového rozhodnutia na ochranu údajov v rámci tretieho piliera*

Dohovor 108 sa ako referenčný nástroj ochrany údajov pre návrh rozhodnutia o SIS II nahradí rámcovým rozhodnutím o ochrane údajov v treťom pilieri ([1]). Táto skutočnosť sa v návrhu nespomína, ale vyplýva z navrhovaného rámcového rozhodnutia. V jeho článku 34 ods. 2 sa uvádza, že „akýkoľvek odkaz na Dohovor Rady Európy č. 108 z 28. januára 1981 o ochrane osôb pri automatizovanom spracovaní osobných údajov sa považuje za odkaz na toto rámcové rozhodnutie“. EDPS v nadchádzajúcich týždňoch vydá stanovisko k návrhu rámcového rozhodnutia a nebude teda jeho obsah podrobne analyzovať v tomto stanovisku. Kdekoľvek by však mohlo mať uplatňovanie tohto rámcového rozhodnutia podstatný vplyv na mechanizmus ochrany údajov v rámci SIS II, táto skutočnosť sa spomenie.

2.2.6. *Uplatňovanie článku 13 smernice 95/46/ES a článku 9 dohovoru 108*

Článok 13 smernice 95/46/ES a článok 9 smernice 108 ustanovujú pre členské štáty možnosť prijať legislatívne opatrenia na obmedzenie rozsahu povinností a práv, ktoré stanovujú, a to v prípade, že takéto obmedzenie predstavuje nevyhnutné opatrenie na ochranu ďalších dôležitých záujmov (napr. národná bezpečnosť, obrana, verejná bezpečnosť) ([2]).

V odôvodneniach navrhovaného nariadenia aj navrhovaného rozhodnutia sa spomína, že túto možnosť by mali členské štáty využívať pri vykonávaní návrhov na vnútroštátnej úrovni. V tomto prípade by sa malo použiť dvojité overenie: uplatňovanie článku 13 smernice 95/46/ES musí byť v súlade s článkom 8 EDĽP a nemalo by viesť k oslabeniu súčasného mechanizmu ochrany údajov.

Toto je ešte dôležitejšie v prípade SIS II, keďže uvedený systém musí byť predvídateľný. V prípade, že si členské štáty vymieňajú údaje a spoločne ich používajú, musí existovať možnosť s primeranou určitosťou vedieť, akým spôsobom sa tieto údaje budú spracovávať na vnútroštátnej úrovni.

Z hľadiska uvedeného existuje jeden konkrétny znepokojujúci prvok, pri ktorom by návrhy viedli k zníženiu súčasnej úrovne ochrany údajov. Článok 102 Schengenského dohovoru ustanovuje systém, v ktorom sa použitie údajov prísne upravuje a obmedzuje dokonca i vo vnútroštátnych právnych predpisoch („Akékoľvek použitie údajov, ktoré nie je v súlade s odsekmi 1 až 4 sa podľa vnútroštátneho práva zmluvnej strany považuje za zneužitie.“). Aj smernica 95/46/ES, aj dohovor 108 však stanovujú, že vo vnútroštátnych právnych predpisoch je možné zaviesť výnimky, okrem iného, zo zásady obmedzenia účelu. Ak sa tak stane, predstavovalo by to rozpor so súčasným systémom v Schengenskom dohovore, podľa ktorého sa vnútroštátne právne predpisy nesmú odchyľovať od kľúčovej zásady obmedzenia účelu a použitia,

Prijatím rámcového rozhodnutia by sa tento postreh nezmenil: väčším problémom ako zabezpečenie, aby sa údaje spracovávali v súlade s rámcovým rozhodnutím, je zachovanie zásady prísneho obmedzenia účelu pri spracovaní údajov v SIS II.

([1]) Taktiež nahradí všeobecný mechanizmus ochrany údajov Schengenského dohovoru (články 126 až 130 Schengenského dohovoru). Tento mechanizmus sa na SIS neuplatňuje.

([2]) Členský štát, ktorý využije túto možnosť na obmedzenie práv, tak môže urobiť len v súlade s článkom 8 EDĽP, ako už bolo spomenuté.

EDPS navrhuje, aby sa do návrhov o SIS II (najmä článku 21 navrhovaného nariadenia a článku 40 navrhovaného rozhodnutia) zaviedlo ustanovenie s rovnakým účinkom ako súčasný článok 102 ods. 4 Schengenského dohovoru, ktorým sa obmedzuje možnosť členských štátov ustanoviť použitie údajov, ktoré sa nepredpokladá v textoch o SIS II. Ďalšou možnosťou je v navrhovanom nariadení a navrhovanom rozhodnutí explicitne obmedziť rozsah výnimiek, ktoré sa môžu využiť podľa článku 13 smernice a článku 9 dohovoru, napríklad ustanovením, že členské štáty môžu obmedziť len právo na prístup a informácie, ale nie zásady týkajúce sa kvality údajov.

3. ÚČEL

Podľa článku 1 oboch dokumentov („zriadenie a všeobecný cieľ SIS II“) sa SIS II zriaďuje, aby sa „príslušným orgánom členských štátov umožnila výmena informácií na účely kontrol osôb a predmetov“, a „prispeje k zachovaniu vysokej úrovne bezpečnosti v rámci priestoru bez kontroly na vnútorných hraniciach medzi členskými štátmi“.

Účel SIS II je vymedzený z dosť širokého hľadiska; uvedené ustanovenia samy osebe presne neurčujú, čo tento cieľ zahŕňa (čo sa ním myslí).

Cieľ SIS II sa zdá byť omnoho širší než cieľ súčasného SIS, ako sa uvádza v článku 92 Schengenského dohovoru, ktorý konkrétne odkazoval na „(...) záznamy týkajúce sa vstupu osôb a majetku na účely hraničných kontrol a iných policajných a colných kontrol (...) a (z hľadiska záznamov v článku 96) na účely vydávania víz, povolení na pobyt a správy právnych predpisov o cudzincoch (...)“.

Tento širší cieľ sa tiež odvodzuje z vloženia nových funkcií a prístupov do SIS II, ktoré nezapadajú do pôvodného účelu kontrol osôb a predmetov, ale skôr do rámca vyšetrovacieho nástroja.

Konkrétne sa predpokladá prístup pre orgány, ktoré budú používať údaje z SIS II na svoje vlastné účely a nie na realizáciu účelov SIS II (pozri nižšie); prepojenie záznamov sa zvyčajne všeobecní, čo predstavuje typickú črtu policajného vyšetrovacieho nástroja. Otázne je aj zavedenie biometrického vyhľadávacieho nástroja, ktorý by sa mal vyvinúť v priebehu najbližších rokov a umožniť vyhľadávanie v systéme, čo presahuje potreby kontrolného systému.

Záverom, návrhy majú omnoho širší rozsah než súčasný rámec, čo vyžaduje dodatočné ochranné opatrenia. Z tohto hľadiska EDPS zameria svoju analýzu ani nie tak na širšie vymedzenie článku 1 ako takého, ale na funkcie a iné základné časti SIS II.

4. ZÁSADNÉ ZMENY V SIS II

V tejto kapitole sa najprv zameriame na nové prvky, ktoré SIS II prináša, a to najmä zavedenie biometrie, novú koncepciu prístupu s osobitnou pozornosťou venovanou prístupu Europolu a Eurojustu, prístup pre orgány zodpovedné za evidenciu vozidiel, prepojenie záznamov a na prístup rozličných orgánov k údajom o prisťahovalectve.

4.1. Biometria

Návrhy o SIS II zavádzajú možnosť spracovávania novej kategórie údajov, ktoré si zaslúžia osobitnú pozornosť: biometrických údajov. Ako sa už zdôraznilo v stanovisku EDPS o Vízovom informačnom systéme ([1]), prirodzene citlivá povaha biometrických údajov si vyžaduje osobitné ochranné opatrenia, ktoré návrhy o SIS II neobsahujú.

Všeobecným postrehom je, že tendencia používania biometrických údajov v informačných systémoch EÚ (VIS, EURODAC, informačný systém pre vodičské preukazy atď.) vytrvalo rastie, ale nesprevádza ju pozorné zváženie súvisiacich rizík a vyžadovaných ochranných opatrení.

Túto potrebu hlbších úvah zdôraznilo aj nedávne uznesenie o biometrii, ktoré vypracovali delegáti medzinárodnej konferencie komisárov pre údaje v Montreux ([2]). Až doteraz sa pridaná hodnota na vytváranie noriem zameriavala len na rastúcu interoperabilitu medzi systémami a nie na zvýšenie kvality biometrických procesov.

([1]) Stanovisko EDPS k návrhu nariadenia Európskeho parlamentu a Rady o vízovom informačnom systéme (VIS) a výmene údajov o krátkodobých vízach medzi členskými štátmi, 23. marec 2005, časť 3.4.2.

([2]) 27. medzinárodná konferencia komisárov pre ochranu údajov a súkromia, Montreux, 16. september 2005, uznesenie o biometrii v pasoch, preukazoch totožnosti a cestovných dokladoch.

Bolo by užitočné vytvoriť súbor spoločných povinností alebo požiadaviek, ktoré sa týkajú osobitosti takýchto údajov, ako aj spoločnú metodiku ich vykonávania. Tieto spoločné požiadavky by mohli konkrétne obsahovať tieto prvky (ktorých potrebu znázorňujú návrhy o SIS II):

— **Posudzovanie cieleného vplyvu:** Je potrebné zdôrazniť, že návrhy sa nepodrobili posudzovaniu vplyvu použitia biometrie ([1]).

— **Dôraz na proces registrácie:** Zdroje biometrických údajov a spôsob, akým sa uskutoční ich zber, nie sú podrobne opísané. Registrácia je kľúčovým krokom v celkovom procese biometrickej identifikácie a nemôžu ju vymedzovať len prílohy alebo ďalšie rokovania na úrovni podskupín, keďže priamo podmieni konečný výsledok procesu, t. j. úroveň miery chybných odmietnutí alebo miery chybných prijatí.

— **Zdôraznenie úrovne presnosti:** Použitie biometrie na identifikáciu (porovnanie jedného z viacerými) prezentované v návrhu ako budúce uplatnenie „biometrického vyhľadávacieho nástroja“ je dôležitejšie, pretože výsledky tohto procesu nie sú také presné, ako použitie na overenie alebo kontrolu (porovnávanie jedného s jedným). Biometrická identifikácia by preto nemala predstavovať jediný spôsob identifikácie alebo jediný prístupový kľúč k ďalším informáciám.

— **Postup v prípade chyby:** Zavedú sa okamžite dostupné postupy v prípade chyby, aby sa rešpektovala dôstojnosť osôb, ktoré boli nesprávne identifikované a aby sa vyhlo tomu, aby museli znášať bremeno nedostatkov systému.

Používanie biometrických údajov bez riadneho predchádzajúceho posúdenia odhaľuje aj nadhodnotenie spoľahlivosti biometrie. Biometrické údaje sú „živými“ údajmi, ktoré sa časom vyvíjajú; vzorky uložené v databáze predstavujú len momentku dynamického prvku. Ich trvácnosť nie je absolútna a musí sa kontrolovať. Presnosť biometrie sa vždy podporiť inými prvkami, keďže nikdy nebude absolútna.

([1]) Posudzovanie by sa mohlo zakladať na takzvaných siedmich pilieroch biometrických vedomostí v *Biometrika na hraniciach: Posudzovanie vplyvu na spoločnosť*, IPTS, DG-JRC, EUR 21585 EN, časť 1.2, strana 32.

Možné použitie údajov o SIS II na vyšetrovacie účely znamená pre dotknutú osobu vážne riziko v prípade, že sa biometrickým údajom pripisuje zvýšená alebo nadhodnotená úloha, ako sa ukázalo v predchádzajúcich prípadoch ([2]).

Preto by sa v návrhoch mali určiť skutočné možnosti biometrie na účely identifikácie a mala by sa zvýšiť informovanosť o týchto možnostiach.

4.2. **Prístup k údajom v SIS II**

4.2.1 *Nová vízia prístupu*

Orgány s prístupom k údajom v SIS II sú určené pri každom zázname. V zásade sa na poskytnutie prístupu k údajom v SIS uplatňuje zásada dvojitého overenia: prístup sa musí udeliť orgánom v plnom súlade so všeobecným účelom SIS a s konkrétnym účelom každého záznamu.

Uvedené vyplýva z vymedzenia záznamov v navrhovanom nariadení a navrhovanom rozhodnutí (článok 3 ods. 1 písm. a) oboch nástrojov: *„Záznam“ je súbor údajov vložených do SIS II, ktorý umožňuje príslušným orgánom identifikovať osobu alebo vec na účely osobitného opatrenia, ktoré sa má prijať*; článok 39 ods. 3. navrhovaného rozhodnutia posilňuje tento pohľad ustanovením, že *„údaje uvedené v odseku 1 sa môžu použiť iba na účely určenia totožnosti osoby so zreteľom na konkrétne opatrenie, ktoré sa má uskutočniť v súlade s týmto rozhodnutím“*.

Z tohto hľadiska má SIS stále črty systému „hit-no hit“, v ktorom sa každý záznam vkladá na konkrétny účel (odovzdanie, odoprenie vstupu, ...). Orgány s prístupom k údajom v SIS majú de facto obmedzené použitie týchto údajov, keďže ich v zásade môžu používať len na výkon konkrétnej činnosti.

Niektoré prístupy v nových návrhoch však nie sú v súlade s touto logikou: v skutočnosti sa zameriavajú na poskytnutie informácií príslušnému orgánu, ale nie na to, aby sa jej umožnilo určiť totožnosť osoby a prijať opatrenie predpokladané v zázname.

([2]) V júni 2004 strávil právnik z Portlandu (USA) dva týždne vo väzení, pretože FBI úspešne porovnala jeho odtlačky prstov s odtlačkami, ktoré sa našli na mieste bombových teroristických útokov v Madride (na plastovej taške, v ktorej sa nachádzala rozbuška). Nakoniec sa preukázalo, že proces porovnávania bol chybný a jeho výsledkom bol nesprávny záver.

Konkrétnejšie sa to týka:

— prístupu azylových orgánov k údajom o prisťahovalectve;

— prístupu orgánov zodpovedných za udelenie štatútu utečenca k údajom o prisťahovalectve;

— prístupu k záznamom o vydávaní, diskrétnom dohľade a odcudzených dokladoch na zaistenie pre Europol;

— prístupe k údajom o vydávaní a lokalizácii pre Eurojust.

Všetky tieto orgány majú z hľadiska údajov v SIS II rovnaké možnosti:

nemôžu uskutočniť konkrétnu činnosť uvedenú v definícii záznamu. Prístup sa im poskytne ako zdroj informácií na ich vlastné účely.

Dokonca aj medzi týmito orgánmi sa musí rozlišovať, a to medzi tými, ktoré majú prístup na vlastné účely, ale s dosť konkrétnym cieľom, a medzi tými (konkrétne Europolom a Eurojustom), pre ktoré z hľadiska účelu prístupu neexistuje žiadna špecifikácia. Azylové orgány majú napríklad prístup na konkrétny účel, dokonca aj ak to nie je účel uvedený v zázname. Môže sa im poskytnúť prístup k údajom o prisťahovalectve „na účely určenia, či sa žiadateľ o azyl nelegálne zdržiaval v inom členskom štáte“. Europol a Eurojust však majú v určitých kategóriách záznamov zahrnutý prístup, „ktorý je potrebný na výkon ich úloh“.

V súhrne, prístup k údajom v SIS II sa poskytuje v troch prípadoch:

— prístup na realizáciu záznamu;

— prístup na iný účel ako SIS II, ale riadne opísaný v návrhoch;

— prístup na iný účel ako SIS II, ale presne neopísaný.

EDPS sa domnieva, že čím všeobecnejší je účel prístupu, tým prísnejšie by mali byť ochranné opatrenia, ktoré sa musia prijať. Všeobecné ochranné opatrenia sú podrobnejšie opísané nižšie; potom sa budeme zaoberať konkrétnou situáciou Europolu a Eurojustu.

4.2.2 *Podmienky poskytnutia prístupu*

1. Prístup sa v každom prípade môže poskytnúť len vtedy, keď je v súlade so všeobecným účelom SIS II a jeho právnym základom.

V praxi to znamená, že prístup k údajom o prisťahovalectve podľa navrhovaného nariadenia musí podporovať vykonávanie politík spojených s časťou schengenského acquis o pohybe osôb.

Podobne sa aj prístup k záznamom ustanoveným v rozhodnutí musí zamerať na podporu operačnej spolupráce medzi policajnými a justičnými orgánmi v trestných veciach.

Z tohto hľadiska upriamuje EDPS pozornosť na kapitolu týkajúcu sa prístupu útvarov zodpovedných za vydávanie registračných osvedčení do SIS II (pozri časť 4.6 nižšie).

2. Musí sa preukázať potreba prístupu k údajom v SIS II, ako aj nemožnosť alebo veľké ťažkosti pri získavaní údajov inými, menej rušivými prostriedkami. Toto sa malo urobiť v dôvodovej správe, ktorej neexistencia je, ako sa už uviedlo, veľmi poľutovaniahodná.

3. Použitie údajov sa musí vymedziť explicitne a reštriktívne.

Napríklad, azylové orgány majú prístup k údajom o prisťahovalectve „na účely určenia, či sa žiadateľ o azyl nelegálne zdržiaval v inom členskom štáte“. Europol a Eurojust však majú v určitých kategóriách záznamov zahrnutý prístup, „ktorý je potrebný na výkon ich úloh“: toto však nie je vymedzené podrobne (pozri nižšie).

4. podmienky prístupu musia byť riadne vymedzené a obmedzené. Konkrétne by mali dostať prístup k údajom v SIS II len tie útvary v rámci uvedených organizácii, ktoré s týmito údajmi musia pracovať. Táto povinnosť, ustanovená v článku 40 navrhovaného rozhodnutia a v článku 21 ods. 2 navrhovaného nariadenia, by sa mala doplniť povinnosťou vnútroštátnych orgánov viesť aktualizovaný zoznam osôb, ktoré sú oprávnené na prístup do SIS II. To isté by malo platiť pre Eurojust a Europol.

5. skutočnosť, že sa týmto orgánom umožní prístup k údajom v SIS II, nemôže byť v žiadnom prípade dôvodom na vloženie alebo uchovávanie údajov v systéme, ak nie sú potrebné pre konkrétny záznam, ktorého sú súčasťou. Nesmú sa vkladať nové kategórie údajov, pretože by z nich mali prospech iné informačné systémy. Napríklad, článok 39 navrhovaného rozhodnutia ustanovuje zavedenie údajov o vydávajúcom orgáne do záznamov. Tieto údaje nie sú potrebné na výkon opatrenia (zatknutie, dohľad, ...) a jediným dôvodom, prečo by sa mohli zaviesť, je asi prospech pre Europol a Eurojust. Malo by sa poskytnúť jasné odôvodnenie spracovania takýchto údajov.

6. ak to nie je nevyhnutné na účely, kvôli ktorým sa údaje vložili, doba uchovávania údajov sa nesmie predlžiť. To znamená, že aj keď má Europol a Eurojust prístup k týmto údajom, nie je to dostatočným dôvodom na ich zachovávanie v systéme (napríklad, ak bola hľadaná osoba vydaná, údaje by sa mali vymazať aj napriek tomu, že by mohli byť pre Europol užitočné). Tu bude znovu potrebný pozorný dohľad, aby sa zabezpečilo, že vnútroštátne orgány tieto ustanovenia uplatňujú.

4.2.3 *Prístup Europolu a Eurojustu*

a) *Dôvody na prístup*

O prístupe Europolu a Eurojustu k niektorým údajom v SIS sa diskutovalo už pred jeho zavedením v rozhodnutí Rady z 24. februára 2005 [1]. Spomedzi všetkých orgánov, ktoré majú prístup na svoje vlastné účely, majú prospech z poskytnutého prístupu pri najotvorenejších podmienkach. Hoci sa používanie týchto údajov opisuje v kapitole XII rozhodnutia, dôvody na poskytnutie prístupu nie sú rozvinuté dostatočne. Je to ešte závažnejšie, keď si uvedomíme, že úlohy Europolu a Eurojustu sa budú časom vyvíjať.

EDPS naliehavo vyzýva Komisiu, aby reštriktívne vymedzila úlohy, na výkon ktorých by bol oprávnený prístup Europolu a Eurojustu.

b) *Obmedzenie údajov*

S cieľom vyhnúť sa „výlovu“ zo strany Europolu a Eurojustu a zaistiť, aby sa dostali len k údajom „potrebným na výkon svojich úloh“, navrhol SDO Schengen vo svojom stanovisku o návrhoch o SIS II z 27. septembra 2005, aby sa obmedzil prístup Europolu a Eurojustu k údajom o osobách, ktorých mená sa už nachádzajú v ich súboroch. Tým by sa zaručilo, že konzultujú len údaje, ktoré sú pre nich dôležité. EDPS toto odporúčanie podporuje.

c) *Bezpečnostné aspekty*

EDPS víta povinnosť logovania všetkých operácií, ktoré pri pripojení vykoná Europol a Eurojust, ako aj zákaz reprodukcie alebo sťahovania častí systému.

Článok 56 navrhovaného rozhodnutia predpokladá pre Europol a Eurojust „jeden alebo dva“ prístupové body. Akokoľvek odôvodniteľná by pre členský štát bola potreba viac než jedného prístupového bodu, pre decentralizovaný stav jeho príslušných orgánov štatút a činnosti Europolu a Eurojustu takúto požiadavku neoprávňujú. Treba tiež zdôrazniť, že z hľadiska bezpečnosti zvyšuje znásobovanie prístupových bodov riziko zneužitia a preto by sa malo presne odôvodniť s použitím súdržnejších prvkov. Preto, a pri absencii presvedčivejších argumentov, EDPS navrhuje v prípade Europolu a Eurojustu poskytnúť len jeden prístupový bod.

4.3. **Prepojenie záznamov**

Článok 26 nariadenia a článok 46 rozhodnutia ustanovujú, že členské štáty môžu vytvoriť prepojenia medzi záznamami v súlade so svojimi vnútroštátnymi právnymi predpismi s cieľom vytvoriť vzťah medzi dvomi alebo viacerými záznamami.

Hoci môžu byť takéto prepojenia určite užitočné pri kontrolách (napríklad zatykač na zlodeja automobilov sa môže spojiť s odcudzeným vozidlom), zavedenie prepojení medzi záznamami je veľmi typickou črtou policajného vyšetrovacieho nástroja.

Prepojenie záznamov môže mať zásadný vplyv na práva dotknutej osoby, keďže táto osoba sa už „neposudzuje“ na základe údajov, ktoré sa týkajú iba jej, ale aj na základe jej možného spojenia s inými osobami. S osobami, ktorých údaje sú spojené s údajmi zločincov alebo hľadaných osôb, sa bude zaobchádzať s väčším podozrením ako s inými. Prepojenie záznamov okrem toho predstavuje aj rozšírenie vyšetrovacích právomocí SIS, pretože umožní evidenciu údajných skupín alebo sietí (ak sa napríklad údaje o nelegálnych prisťahovalcoch prepoja s údajmi o prevádzačoch). Napokon, keďže sa zriadenie prepojení ponecháva na vnútroštátnych právnych predpisoch, možným dôsledkom je, že prepojenia, ktoré sú v niektorom členskom štáte nezákonné, iný štát zriadi, čím do systému vloží „nezákonné údaje“.

[1] Rozhodnutie Rady 2005/211/SVV z 24. februára 2005 o zavedení niektorých nových funkcií pre Schengenský informačný systém vrátane boja proti terorizmu, Ú. v. EÚ L 68/44, 15.3.2005.

V záveroch Rady zo 14. júna 2004 o funkčných požiadavkách na SIS II sa uvádza, že každé prepojenie musí mať jasnú operačnú požiadavku, musí sa zakladať na jasne vymedzenom vzťahu a musí byť v súlade so zásadou proporcionality. Okrem toho nesmie mať negatívny vplyv na prístupové práva. V každom prípade, keďže prepojenie záznamov predstavuje operáciu spracovania, musí byť v súlade s ustanoveniami vnútroštátnych právnych predpisov, ktorými sa vykonáva smernica 95/46/ES a/alebo dohovor 108.

V návrhoch sa opätovne zdôrazňuje, že existencia prepojení nemôže zmeniť prístupové práva (v skutočnosti by inak v rozpore s článkom 6 smernice poskytla prístup údajom, ktorých spracovanie by podľa vnútroštátnych právnych predpisov nebolo zákonné).

EDPS zdôrazňuje dôležitosť dôslednej interpretácie článku 26 navrhovaného nariadenia a článku 46 navrhovaného rozhodnutia: jedným spôsobom na jej zabezpečenie je vysvetlenie, že orgány bez prístupového práva k určitým kategóriám údajov nielenže nemôžu mať prístup k prepojeniam na tieto kategórie, ale nemali by vôbec vedieť o existencii takýchto prepojení. V prípadoch, keď neexistuje prístupové právo na prepojené údaje by sa mala znemožniť vizualizácia prepojení.

Okrem toho si EDPS želá, aby sa s ním konzultovali technické opatrenia, ktorými sa to zabezpečí.

4.4. **Záznamy na účely odoprenia vstupu**

4.4.1. *Dôvody na zaradenie*

Použitie „záznamov vydaných v súvislosti so štátnymi príslušníkmi tretích krajín na účely odoprenia vstupu“ (článok 15 nariadenia) má podstatný vplyv na slobody jednotlivca: osobe, ktorá sa podľa tohto ustanovenia oznámi, sa počas niekoľkých rokov neumožní prístup do schengenského priestoru. Uvedený záznam bol doteraz najčastejšie používaným záznamom, čo sa týka počtu oznámených osôb. Vzhľadom na dôsledky takéhoto záznamu, ako aj počet dotknutých osôb, sa musí pri jeho koncipovaní a vykonávaní postupovať veľmi opatrne. Aj keď sa uvedené skutočnosti týkajú aj iných záznamov, EDPS sa tomuto záznamu bude venovať v osobitnej kapitole, pretože spôsobuje špecifické problémy z hľadiska dôvodov na zaradenie.

Nový záznam na odoprenie vstupu predstavuje v porovnaní so súčasným stavom zlepšenie, ale nie je ani úplne uspokojivý, keďže sa zo značnej časti zakladá na nástrojoch, ktoré ešte neboli prijaté alebo ani navrhnuté.

Zlepšenie spočíva v presnejšom opise dôvodov na zaradenie údajov. Súčasné znenie Schengenského dohovoru viedlo k významným rozdielom medzi členskými štátmi z hľadiska počtu osôb oznámených podľa článku 96 dohovoru. JSA pre Schengen uskutočnil komplexnú štúdiu ([1]) tejto otázky a vydal odporúčania v tom zmysle, že „tvorcovia politík by mali zvážiť zosúladenie dôvodov na vytvorenie záznamu v rôznych štátoch schengenského priestoru“.

Navrhované znenie článku 15 je podrobnejšie, čo bude vítané.

Okrem toho sa v článku 15 ods. 2 uvádza zoznam prípadov, v ktorých sa na základe rôznych štatútov na osoby nemôže vydať záznam, pretože majú riadny pobyt na území členského štátu. Aj keď sa uplatňovanie tohto mechanizmu môže odvodiť z platného Schengenského dohovoru, v praxi sa ukázalo, že sa pri ňom medzi členskými štátmi vyskytli rozdiely. Preto je objasnenie pozitívnym prvkom.

Toto ustanovenie je však aj predmetom vážnej kritiky, keďže jeho dôležitá časť sa zakladá na ešte neprijatom znení, konkrétne na smernici o „vrátení osôb“.

Po prijatí návrhov o SIS II navrhla Komisia (1. septembra 2005) „smernicu o spoločných normách a postupoch navracania štátnych príslušníkov tretích krajín, ktorí sa nelegálne sa zdržiavajú v členských štátoch“, ale keďže jej znenie nie je konečné, nemôže sa považovať za platný dôvod na vkladanie údajov do systému. Predstavuje najmä porušenie článku 8 EDĽP, keďže narušenie súkromia osôb by mali odôvodňovať – okrem iného – jasné a prístupné právne predpisy.

Preto EDPS naliehavo vyzýva Komisiu, aby buď stiahla tento predpis, alebo aby ho na základe platných právnych predpisov preformulovala spôsobom, ktorý umožní, aby osoby presne vedeli, aké opatrenia voči nim môžu použiť príslušné orgány.

4.4.2. *Prístup k záznamom podľa článku 15*

V článku 18 sa ustanovuje, ktoré orgány majú k týmto záznamom prístup a na aké účely. V článku 18 ods. 1 a 2 sa určuje, ktoré orgány majú prístup k záznamom vloženým na základe smernice o vrátení. Platia rovnaké pripomienky, ako sú uvedené vyššie.

([1]) Správa schengenského spoločného dozorného orgánu o kontrole používania záznamov podľa článku 96 v Schengenskom informačnom systéme, 20. júna 2005 v Bruseli.

Článok 18 ods. 3 navrhovaného nariadenia umožňuje prístup orgánom zodpovedným za udelenie štatútu utečenca podľa smernice, ktorá ešte nebola ani navrhnutá. Pri neexistencii dostupného znenia musí EDPS opätovne zdôrazniť pripomienky uvedené vyššie.

4.4.3. *Obdobie uchovávania záznamov podľa článku 15*

Záznam sa podľa článku 20 nesmie uchovávať dlhšie, ako je obdobie odoprenia vstupu ustanovené v rozhodnutí (o vyhostení alebo vrátení). Toto je v súlade s pravidlami ochrany údajov. Okrem toho sa po piatich rokoch vymazáva automaticky, pokiaľ členský štát, ktorý údaje do SIS II vložil, nerozhodne inak.

Primeraný dohľad na vnútroštátnej úrovni by mal zabezpečiť, že sa obdobie uchovávania údajov automaticky neodôvodnene nepredĺži a že členské štáty vymažú údaje ešte pred lehotou piatich rokov v prípade, že je doba odoprenia vstupu kratšia.

4.5. **Doby uchovávania údajov**

Hoci sa zásada uchovávania nemení (všeobecným pravidlom je, že záznam by sa mal z SIS II vymazať, akonáhle sa vykoná činnosť vyžadovaná v zázname), výsledkom návrhov je všeobecné predĺženie doby uchovávania pre záznamy.

Schengenský dohovor ustanovil preskúmanie potreby priebežného uchovávania údajov nie dlhšie než tri roky po ich vložení (alebo jeden rok v prípade údajov vložených na účely diskrétneho dohľadu). Nové návrhy predpokladajú automatické vymazanie (s možnosťou výhrad pre vydávajúci členský štát) po piatich rokoch pri údajoch o prisťahovalectve, 10 rokoch pri údajoch o zatknutí, nezvestných osobách a osobách, ktoré sú hľadané na účely súdneho konania, a troch rokoch pri osobách, ktoré sa majú podrobiť diskrétnemu dohľadu.

Hoci v zásade budú členské štáty musieť vymazať údaje po splnení účelu záznamu, znamená to významné predĺženie maximálneho obdobia uchovávania údajov (vo väčšine prípadov až na trojnásobok) bez akéhokoľvek odôvodnenia zo strany Komisie. V prípade údajov o prisťahovalectve sa dá iba tušiť, že päťročné trvanie sa spája s trvaním zákazu vstupu uvedeným v návrhu smernice o vrátení. Vo všetkých ostatných prípadoch neexistuje dôvod, o ktorom by EDPS vedel.

Potenciálny vplyv predmetov údajov oznámených v SIS môže mať závažné následky na život dotknutých osôb. Zvlášť znepokojivé je to v prípade záznamov o osobách na účely diskrétneho dohľadu alebo osobitných kontrol, keďže takéto záznamy sa môžu vytvárať na základe podozrenia.

EDPS by chcel poznať vážny dôvod na takéto predĺženie obdobia uchovávania údajov. Ak neexistuje presvedčivé odôvodnenie, navrhuje skrátenie týchto období na ich súčasnú dĺžku, pričom trvá najmä na prípadoch záznamov na účely diskrétneho dohľadu alebo osobitných kontrol.

4.6. **Prístup orgánov zodpovedných za vydávanie osvedčení o evidencii vozidla**

Hlavný problém spočíva vo výbere viac než otázneho právneho základu. Komisia nedokázala presvedčivo odôvodniť použitie „dopravného“ právneho základu pre prvý pilier pri opatreniach, ktorými by sa umožnil prístup správnych orgánov do SIS na účely predchádzania trestnej činnosti a boja proti nej (obchod s odcudzenými vozidlami). Potreba dôkladného odôvodnenia a pevného právneho základu na poskytnutie prístupu do SIS II sa podrobne rozobrala v bode 4.2.2 tohto stanoviska.

EDPS sa odvoláva na poznámky k tejto téme, ktoré vypracoval JSA pre Schengen vo svojom stanovisku k navrhovanému právnemu základu pre SIS II. Konkrétne by sa malo postupovať podľa návrhu JSA pre Schengen, aby sa navrhované rozhodnutie zmenilo a doplnilo s cieľom zaradiť doň takýto prístup.

5. ÚLOHA KOMISIE A ČLENSKÝCH ŠTÁTOV

Kľúčovou otázkou nielen pre hladké fungovanie systému, ale i z hľadiska dohľadu, je jasný opis a rozdelenie povinností v kontexte SIS II. Rozdelenie dozorných právomocí bude vyplývať z opisu povinností, a preto je potrebná absolútna zrozumiteľnosť.

5.1. **Úloha Komisie**

EDPS víta kapitolu III oboch návrhov, ktorá opisuje úlohu a povinnosti Komisie vo vzťahu k SIS II (ako úlohu „operačného riadenia“). Takéto vysvetlenie sa v návrhu o VIS nenachádzalo. Táto kapitola sama osebe však nevymedzuje úlohu Komisie vyčerpávajúco. V skutočnosti, ako sa uvádza v kapitole 9 tohto stanoviska, sa Komisia zúčastňuje na vykonávaní a riadení systému prostredníctvom komitologického postupu.

Z hľadiska ochrany údajov zohráva Komisia úlohu, ktorá je známa aj v systémoch VIS a Eurodac, čiže inštitúcie zodpovednej za operačné riadenie. V kombinácii s jej hlavnou úlohou pri rozvoji a údržbe systému by sa to malo vnímať ako úloha kontrolóra sui generis. Táto úloha je, ako sa už spomenulo v stanovisku EDPS k VIS, omnoho viac než úloha spracovateľa, ale tiež obmedzenejšia než úloha obyčajného kontrolóra, keďže Komisia nemá vôbec prístup k údajom spracovávaným v SIS II.

Keďže sa SIS II vybuduje na komplexných systémoch, z ktorých niektoré sa spoliehajú na úplne nové technológie, EDPS trvá na posilnení zodpovednosti Komisie pri aktualizácii systémov prostredníctvom zavádzania najlepších dostupných technológií týkajúcich sa bezpečnosti a ochrany údajov.

Preto by sa do článku 12 návrhov malo vložiť, že Komisia by mala pravidelne navrhovať zavádzanie nových technológií, ktoré predstavujú v tejto oblasti to najmodernejšie a prostredníctvom ktorých sa zvýši úroveň ochrany údajov a bezpečnosti, ako aj uľahčia úlohy vnútroštátnych orgánov, ktoré majú k týmto údajom prístup.

5.2. **Úloha členských štátov**

Situácia členských štátov nie je úplne jasná, keďže je dosť zložité zistiť, ktoré orgány sa stanú kontrolórom údajov.

Návrhy opisujú úlohu Národného úradu pre SIS II (zabezpečiť prístup príslušných orgánov k SIS II), ako aj orgánov SIRENE (zabezpečiť výmenu všetkých dodatočných informácií). Členské štáty musia zabezpečiť aj fungovanie a bezpečnosť svojich NS (národných systémov). Nie je jasné, či táto posledná povinnosť pripadne niektorému z uvedených orgánov. V každom prípade sa v tejto súvislosti vyžaduje vysvetlenie.

Z hľadiska ochrany údajov by sa Komisia a členské štáty mali považovať za spoločných kontrolórov, pričom každý z nich má osobitné povinnosti. Uznanie tohto doplnkového poslania je jediným spôsobom, akým sa zabezpečí, že žiadna z oblastí činností SIS II neostane bez dohľadu.

6. **PRÁVA DOTKNUTÝCH OSÔB**

6.1. **Informácie**

6.1.1. *Navrhované nariadenie*

Článok 28 navrhovaného nariadenia predpokladá právo na informovanie dotknutej osoby, pričom sa drží najmä článku 10 smernice 95/46. Toto je v porovnaní so súčasnou situáciou vítanou zmenou, nakoľko v dohovore sa explicitne nepredpokladá právo na informácie. V nasledujúcich bodoch však ešte stále existuje priestor na určité zlepšenie.

Na zoznam by sa mali pridať niektoré informácie, pretože by to prispelo k spravodlivému zaobchádzaniu s dotknutou osobou ([1]). Tieto informácie by sa mali týkať doby uchovávania údajov, existencie práva požadovať preskúmanie rozhodnutia o vytvorení záznamu alebo práva odvolať sa voči nemu (v niektorých prípadoch, pozri článok 15 ods. 3 navrhovaného nariadenia), možnosti pomoci od orgánu pre ochranu údajov a existencie opravných prostriedkov.

V navrhovanom nariadení nie je ani náznak týkajúci sa momentu, kedy by sa informácie mali poskytnúť. Týmto by sa mohol znemožniť výkon práv dotknutej osoby. Aby boli tieto práva účinné, nariadenie by malo ustanoviť presný moment, v ktorom by sa mali informácie poskytnúť, pričom by to záviselo od orgánu, ktorý vytvoril záznam.

Praktickým riešením by bolo vloženie informácií o zázname do rozhodnutia, ktoré je primárnym dôvodom na záznam: buď súdne alebo správne rozhodnutie založené na ohrození verejného poriadku (...) alebo rozhodnutie o vrátení alebo príkaz na vyhostenie spojený so zákazom ďalšieho vstupu. Tieto ustanovenia by sa mali vložiť do článku 28 nariadenia.

6.1.2. *Navrhované rozhodnutie*

Článok 50 rozhodnutia ustanovuje, že informácie sa poskytujú na žiadosť dotknutej osoby a uvádza možné dôvody na odmietnutie poskytnutia takýchto informácií. Pri povahe údajov a kontexte, v ktorom sa spracovávajú, sú obmedzenia tohto práva zjavne pochopiteľné.

Právo na informácie by však nemalo podliehať žiadosti dotknutej osoby (to by bolo skutočne skôr vymedzením žiadosti o prístup). Je možné sa domnievať, že potreba „žiadať“ o informácie bola odôvodnená v prípadoch, kedy nebolo možné informovať dotknutú osobu, pretože nebolo známe miesto jej pobytu.

Táto skutočnosť by sa lepšie riešila vložením výnimky z práva na informácie v prípadoch, ak je poskytnutie informácií nemožné alebo ak si vyžaduje neprimerané úsilie. Článok 50 rozhodnutia by sa mal zodpovedajúcim spôsobom zmeniť a doplniť.

([1]) V rovnakom zmysle pozri stanovisko EDPS k zriadeniu vízového informačného systému, časť 3.10.1.

Toto riešenie by tiež bolo v súlade s uplatňovaním návrhu rámcového rozhodnutia o ochrane údajov v treťom pilieri.

6.2. **Prístup**

Navrhované nariadenie aj rozhodnutie zavádzajú lehoty na odpoveď na žiadosti o prístup, čo je pozitívny vývoj. Keďže je však postup vykonávania práva na prístup vymedzený na vnútroštátnej úrovni, možno sa zaujímať, ako môžu lehoty v návrhoch vzájomne fungovať s platnými postupmi, najmä ak majú členské štáty kratšie lehoty na odpoveď na žiadosť o prístup. Malo by sa vysvetliť, že by sa mali uplatňovať lehoty, ktoré sú najvýhodnejšie pre dotknuté osoby.

6.2.1. *Navrhované nariadenie*

Treba pripomenúť, že obmedzenia práva na prístup („sa odmietne, ak to môže škodiť vykonaniu zákonnej úlohy v súvislosti so záznamom alebo pre ochranu práv a slobôd tretích osôb"), ktoré v súčasnosti existuje v Schengenskom dohovore, sa v navrhovanom nariadení nenachádza.

Dôvodom je však zrejme uplatniteľnosť smernice 95/46/ES, ktorá predpokladá (vo svojom článku 13) možnosť zaviesť vo vnútroštátnych právnych predpisoch výnimky. V každom prípade by sa však malo zdôrazniť, že použitie článku 13 vo vnútroštátnych právnych predpisoch na obmedzenie práva na prístup by malo byť vždy v súlade s článkom 8 EDĽP a len obmedzené.

6.2.2. *Navrhované rozhodnutie*

Navrhované rozhodnutie pristupuje k obmedzeniam ako Schengenský dohovor. Navrhované rámcové rozhodnutie obsahuje v zásade rovnaké obmedzenia práva na prístup; takže prijatie tohto nástroja nebude z tohto hľadiska znamenať žiadny rozdiel.

Keďže v niekoľkých členských štátoch je prístup k údajom z oblasti vynútiteľnosti práva „nepriamy" (čo znamená, že sa vykonáva prostredníctvom vnútroštátneho orgánu pre ochranu údajov), mohlo by byť užitočné ustanoviť povinnosť orgánov pre ochranu údajov aktívne spolupracovať pri výkone práva na prístup.

6.3. **Právo na preskúmanie rozhodnutia o vytvorení záznamu alebo na odvolanie sa proti nemu**

Článok 15 ods. 3 zriaďuje právo na preskúmanie rozhodnutia o vytvorení záznamu alebo na odvolanie sa proti nemu pred súdnym orgánom v prípade, že toto rozhodnutie prijme správny orgán. V porovnaní s platným znením Schengenského dohovoru je to vítaným doplnením.

Zdôrazňuje potrebu úplných a včasných informácií o dotknutej osobe, ako sa spomína v bode 6.1 vyššie: bez týchto informácií by toto nové právo ostalo len v teoretickej rovine.

6.4. **Opravné prostriedky**

Článok 30 navrhovaného nariadenia a článok 52 navrhovaného rozhodnutia ustanovujú právo na žalobu alebo sťažnosť o získanie informácií alebo nápravu na súde ktoréhokoľvek členského štátu v prípade, že sa dotknutej osobe odoprie právo na prístup, opravu alebo vymazanie údajov.

Znenie („každá osoba na území ktoréhokoľvek členského štátu") naznačuje, že nato, aby mohol navrhovateľ podať žalobu na súd, sa musí fyzicky nachádzať na takomto území. Toto územné obmedzenie nie je odôvodnené a mohlo by spôsobiť stratu účinnosti opravných prostriedkov, keďže navrhovateľ veľmi často žaluje práve preto, že sa mu odoprie vstup na schengenské územie. Okrem toho sa z hľadiska navrhovaného nariadenia musí zohľadniť článok 22 smernice, keďže smernica je *lex generalis;* ustanovuje, že „každá osoba" má právo na súdny opravný prostriedok bez ohľadu na miesto jej pobytu. Ani navrhované rámcové rozhodnutie neobsahuje územné obmedzenie. EDPS navrhuje územné obmedzenie z článku 30 a článku 52 vypustiť.

7. **DOZOR**

7.1. **Úvodná poznámka: rozdelenie povinností**

Návrhy rozdeľujú dozorné úlohy medzi vnútroštátne dozorné orgány ([1]) a EDPS, každému v rámci vlastného rozsahu pôsobnosti. Je to v súlade s prístupom návrhov k platnému právu a k zodpovednosti za prevádzku a používanie systému SIS II, ako aj s potrebou účinného dozoru.

EDPS preto víta tento prístup v článku 31 navrhovaného nariadenia a v článku 53 navrhovaného rozhodnutia. Pre lepšie pochopenie a objasnenie príslušných úloh však EDPS navrhuje rozdelenie každého článku na niekoľko ustanovení, pričom každé z nich sa bude venovať úrovni dozoru tak, ako tomu bolo v návrhu o VIS.

([1]) V menšom rozsahu sa zúčastňujú aj dozorné orgány Europolu a Eurojustu.

7.2. **Dozor zo strany vnútroštátnych orgánov pre kontrolu údajov**

Podľa článku 31 navrhovaného nariadenia a článku 53 navrhovaného rozhodnutia musí každý členský štát zabezpečiť, aby zákonnosť spracovania osobných údajov v SIS II monitoroval nezávislý orgán.

Článok 53 navrhovaného rozhodnutia pridáva právo jednotlivca, aby požiadal dozorný orgán o kontrolu zákonnosti spracovania údajov, ktoré sa ho týkajú. Do navrhovaného nariadenia sa podobné ustanovenie nezahrnulo, keďže smernica sa uplatňuje ako *lex generalis*. Preto sa musí konštatovať, že vnútroštátne orgány pre ochranu údajov môžu v súvislosti s SIS II vykonávať všetky právomoci, ktoré im prislúchajú z článku 28 smernice 95/46/ES, vrátane kontroly zákonnosti spracovania údajov. Článok 31 ods. 1 nariadenia vysvetľuje ich poslanie ale nemôže ustanovovať obmedzenie týchto právomocí. Uznanie týchto právomocí by sa malo vysvetliť v znení navrhovaného nariadenia.

Čo sa týka navrhovaného rozhodnutia, priznáva vnútroštátnym dozorným orgánom rozsiahlejšie právomoci, keďže jeho *lex generalis* je iný. Situácia, v ktorej by dozorné orgány mali rôzne poslanie a právomoci podľa kategórie spracovávaných údajov, však nie je rozumná a je veľmi zložitá na praktické uplatňovanie. Preto by sa jej malo predísť, buď pridelením rovnakých právomocí týmto orgánom v znení samotného navrhovaného rozhodnutia, alebo pridelením ďalších právomocí orgánom pre ochranu údajov prostredníctvom odkazu na iný *lex generalis* (konkrétne rámcové rozhodnutie o ochrane údajov v treťom pilieri).

7.3. **Dozor zo strany EDPS**

EDPS sleduje, aby sa činnosti Komisie spojené so spracovaním údajov vykonávali v súlade s návrhmi. Podobne by mal byť EDPS schopný vykonávať všetky svoje právomoci podľa nariadenia 45/2001, pričom by sa však mali zohľadniť obmedzené právomoci Komisie v súvislosti so samotnými údajmi.

Je užitočné dodať, že podľa článku 46 písm. f) nariadenia 45/2001 EDPS „spolupracuje s národnými dozornými orgánmi v rozsahu nevyhnutnom pre výkon ich príslušných služobných povinností“. Spolupráca s členskými štátmi pri dozore SIS II nevychádza len z návrhov, ale aj z nariadenia 45/2001.

7.4. **Spoločný dozor**

V návrhoch sa tiež stanovuje potreba koordinácie dozorných činností rôznych zúčastnených orgánov. Článok 31 navrhovaného nariadenia a článok 53 navrhovaného rozhodnutia ustanovujú, že „vnútroštátne dozorné orgány a Európsky dozorný úradník pre ochranu údajov navzájom aktívne spolupracujú. Európsky dozorný úradník pre ochranu údajov na tento účel zvoláva zasadnutie najmenej raz do roka.“

EDPS víta tento návrh, ktorý v podstate obsahuje potrebné prvky na nadviazanie spolupráce – ktorá je skutočne kľúčovou – medzi orgánmi zodpovednými za dozor na vnútroštátnej a Európskej úrovni. Malo by sa zdôrazniť, že hoci návrhy ustanovujú zasadnutie najmenej raz do roka, malo by sa to považovať za minimum.

Tieto ustanovenia (článok 31 navrhovaného nariadenia a článok 53 navrhovaného rozhodnutia) by mohli mať prospech z určitých objasnení obsahu uvedenej spolupráce. Existujúci JSA má právomoc preskúmať ťažkosti týkajúce sa interpretácie alebo uplatňovania dohovoru, preštudovať problémy, ktoré sa môžu vyskytnúť pri výkone nezávislého dozoru alebo práva na prístup, a vypracovávať zosúladené návrhy na spoločné riešenie existujúcich problémov.

Nové návrhy nemôžu viesť k zúženiu existujúceho rozsahu spoločného dozoru. Ak je jasné, že orgány pre ochranu údajov môžu v súvislosti s SIS II vykonávať všetky dozorné právomoci, ktoré im prideľuje smernica, spolupráca týchto orgánov môže zahŕňať množstvo aspektov dozoru nad SIS II vrátane úloh existujúceho JSA podľa článku 115 Schengenského dohovoru.

Aby to však bolo absolútne jasné, bolo by užitočné to explicitne opätovne potvrdiť v návrhoch.

8. **BEZPEČNOSŤ**

Riadenie a dodržiavanie optimálneho stupňa bezpečnosti SIS II predstavuje základnú požiadavku na zaistenie požadovanej ochrany osobných údajov uložených v databáze. Aby sa získala uspokojujúca úroveň ochrany na zvládnutie možného rizika súvisiaceho s infraštruktúrou systému a so zúčastnenými osobami, musia sa zaviesť riadne bezpečnostné opatrenia. Táto téma sa teraz rieši v rôznych častiach návrhu, pričom bude potrebné určité zlepšenie.

Články 10 a 13 návrhu obsahujú rôzne opatrenia v oblasti bezpečnosti údajov a vymedzujú druhy zneužitia, ktorým treba predchádzať. EDPS víta skutočnosť, že sa do týchto článkov vložili ustanovenia o systematickej (samo)kontrole bezpečnostných opatrení.

Článok 59 navrhovaného rozhodnutia a článok 34 navrhovaného nariadenia, ktoré upravujú monitorovanie a hodnotenie, by sa nemali týkať len aspektov výkonu, hospodárnosti a kvality služieb, ale aj súladu s právnymi požiadavkami, a to najmä v oblasti ochrany údajov. EDPS preto odporúča, aby sa rozsah pôsobnosti týchto článkov rozšíril na monitorovanie a podávanie správ o zákonnosti spracovania.

Okrem toho, na doplnenie článku 10 ods. 1 písm. f) alebo článku 18 navrhovaného rozhodnutia a článku 17 navrhovaného nariadenia o riadne oprávnených pracovníkoch, ktorí majú prístup k údajom, by sa malo doplniť, že členské štáty (ako aj Europol a Eurojust) by mali zaistiť, aby boli k dispozícii presné profily užívateľov (ktoré by boli k dispozícii vnútroštátnym dozorným orgánom na účely kontroly). Okrem užívateľských profilov musia členské štáty vypracovať úplný zoznam údajov o totožnosti užívateľov a stále ho aktualizovať. To isté platí obdobne pre Komisiu.

Tieto bezpečnostné opatrenia sú doplnené o monitorovanie a organizačné ochranné opatrenia. Článok 14 návrhov opisuje podmienky a účely, na ktoré sa musia uchovávať záznamy všetkých operácií spracovania údajov. Tieto záznamy sa neuchovávajú len na účely monitorovania ochrany údajov a zaistenia ich bezpečnosti, ale tiež na vykonávanie pravidelnej samokontroly SIS II, ktorá sa vyžaduje podľa článku 10. Správy o samokontrole prispejú k účinnému vykonávaniu úloh dozorných orgánov, ktoré budú počas vlastného kontrolného postupu schopné zistiť najslabšie miesta a zamerať sa na ne.

Ako sa už v tomto stanovisku uviedlo, znásobenie prístupových bodov systému sa musí náležite odôvodniť, keďže automaticky zvyšuje riziko zneužitia. V článku 4 ods. 1 písm. b) by sa preto malo požadovať konkrétne preukázanie potreby druhého prístupového bodu.

Návrhy jasne nevysvetľujú potrebu vnútroštátnych kópií centrálneho systému a spôsobujú vážne obavy, pokiaľ ide o celkový stupeň rizika a bezpečnosť systému, ako napríklad:

— znásobenie kópií zvyšuje riziko zneužitia (najmä pri zohľadnení prítomnosti nových údajov, ako sú biometrické údaje),

— údaje, ktorých sa tieto kópie týkajú, nie sú riadne vymedzené,

— požiadavky článku 9 na presnosť, kvalitu a dostupnosť predstavujú veľkú technickú výzvu a preto zvyšujú náklady podľa stavu dostupnej techniky,

— dozor nad týmito kópiami zo strany vnútroštátnych orgánov si bude vyžadovať dodatočné ľudské a finančné zdroje, ktoré nemusia byť vždy dostupné.

Vzhľadom na tieto riziká nie je EDPS presvedčený ani o potrebe (z hľadiska dostupných technológií), ani o pridanej hodnote používania vnútroštátnych kópií. Odporúča vypustiť možnosť členských štátov využívať vnútroštátne kópie.

Ak sa však majú vytvoriť vnútroštátne kópie, EDPS pripomína, že na ich vnútroštátne použitie sa musí uplatňovať prísna zásada obmedzenia účelu. Taktiež sa v národnej kópii nesmie vyhľadávať iným spôsobom, ako v centrálnej databáze.

Zákonnosť operácie, ktorou sa spracovávajú osobné údaje, je založená na prísnom dodržiavaní bezpečnosti a integrity údajov. EDPS bude tieto procesy efektívne monitorovať v prípade, že dokáže prostredníctvom analýzy dostupných protokolov monitorovať nielen bezpečnosť údajov, ale aj ich integritu. Preto je potrebné doplniť do článku 14 ods. 6. „integritu údajov“.

9. **KOMITOLÓGIA**

Komitologické postupy sa v návrhoch predpokladajú v niekoľkých prípadoch, keď sa na realizáciu alebo riadenie SIS II vyžadujú technické rozhodnutia. Ako sa už z podobných dôvodov uviedlo v stanovisku k VIS, tieto rozhodnutia budú mať podstatný vplyv na riadne vykonávanie zásady účelu a proporcionality.

EDPS navrhuje, aby sa rozhodnutia so zásadným vplyvom na ochranu údajov, ako napríklad prístup k údajom a ich vkladanie, výmena dodatočných informácií, kvalita údajov a kompatibilita záznamov, technický súlad vnútroštátnych kópií atď. by sa mali prijímať formou nariadenia alebo rozhodnutia, a najlepšie s použitím spolurozhodovacieho postupu ([1]).

([1]) V rovnakom zmysle pozri stanovisko EDPS k vízovému informačnému systému, ods. 3.12, a stanovisko EDPS k návrhu smernice o uchovávaní údajov spracovaných v súvislosti s poskytovaním verejných elektronických komunikačných služieb vydané 26. septembra 2005, časť 60.

Vo všetkých ostatných prípadoch s vplyvom na ochranu údajov by EDPS mal mať možnosť poskytovať poradenstvo pri výbere alternatív, ktoré si zvolia tieto výbory.

Poradná úloha EDPS by sa mala nachádzať v článkoch 60 a 61 rozhodnutia a v článku 35 nariadenia.

V osobitnom prípade technických pravidiel pre prepájanie záznamov (článok 26 nariadenia a článok 46 rozhodnutia) sa musí vysvetliť potreba rozdielnej komitologickej metódy (poradná metóda pri rozhodnutí a regulačná metóda pri nariadení).

10. **INTEROPERABILITA**

Keďže stále chýba oznámenie Komisie o interoperabilite nových systémov EÚ, je zložité riadne zhodnotiť pridanú hodnotu predpokladaných, ale ešte nevymedzených synergických účinkov.

EDPS by chcel v tejto súvislosti poukázať na vyhlásenie Rady o boji proti terorizmu z 25. marca 2004, v ktorej sa od Komisie žiada, aby predložila návrhy s cieľom posilniť interoperabilitu a synergické účinky medzi informačnými systémami (SIS, VIS a Eurodac). Tiež by chcel poukázať na prebiehajúce diskusie vzhľadom na to, ktorý orgán by mohol byť v budúcnosti poverený riadením rôznych rozsiahlych systémov (pozri tiež bod 3.8 tohto stanoviska).

EDPS už vo svojom stanovisku k vízovému informačnému systému uviedol, že interoperabilita je dôležitým a rozhodujúcim predpokladom účinnosti rozsiahlych systémov IT, ako je SIS II. Poskytuje možnosť znížiť celkové náklady konzistentným spôsobom a zabrániť prirodzenej nadbytočnosti nerovnorodých prvkov.

— Interoperabilita môže prispieť aj k cieľu zachovania vysokej úrovne bezpečnosti v priestore bez kontrol na vnútorných hraniciach členských štátov, a to prostredníctvom zavádzania rovnakých procesných noriem pre všetky základné prvky tejto politiky. Je však dôležité rozlišovať medzi dvoma stupňami interoperability:

  — Veľmi potrebná je interoperabilita medzi členskými štátmi EÚ; záznam zaslaný orgánmi jedného členského štátu musí byť skutočne interoperabilný so záznamami, ktoré zaslali orgány ktoréhokoľvek iného členského štátu.

  — Interoperabilita medzi systémami vytvorenými na rôzne účely alebo interoperabilita so systémami tretích krajín je podstatne otáznejšia.

Spomedzi dostupných ochranných opatrení používaných na obmedzenie účelu systému a na predchádzanie neplánovaného využívania funkčnosti („function creep“) môže k tomuto obmedzeniu prispieť použitie rôznych technických noriem. Okrem toho by sa malo dôkladne podložiť dokumentmi akékoľvek vzájomné pôsobenie dvoch rozličných systémov. Interoperabilita by nikdy nemala viesť k takej situácii, aby orgán, ktorý nie je oprávnený na prístup k určitým údajom alebo na ich používanie, mohol získať takýto prístup cez iný informačný systém. Zo znenia návrhov sa napríklad zdá, že automatický systém na identifikáciu odtlačkov prstov (AFIS) sa v prvých rokoch trvania SIS II nebude používať; odkazuje sa v nich len na budúci biometrický vyhľadávací nástroj. Ak sa uvažuje o scenári použitia AFIS z iných systémov EÚ, malo by sa to jasne zdokumentovať spolu s potrebnými ochrannými opatreniami vyžadovanými na takéto synergické účinky.

EDPS chce opäť zdôrazniť, že interoperabilita systémov sa nemôže zavádzať v rozpore so zásadou obmedzenia účelu a že by sa mu mal predložiť akýkoľvek návrh v tejto veci.

11. **ZHRNUTIE ZÁVEROV**

11.1. **Všeobecné body**

1. EDPS víta niekoľko pozitívnych aspektov týchto návrhov, ktoré v určitých bodoch predstavujú zlepšenie oproti súčasnému stavu. Uznáva, že ustanovenia o ochrane údajov sa, všeobecne povedané, navrhovali veľmi starostlivo.

2. EDPS zdôrazňuje, že nový právny režim by aj pri svojej komplexnosti mal

   — zabezpečiť vysokú úroveň ochrany údajov,

   — byť predvídateľný pre občanov, ako aj orgány, ktoré údaje spoločne používajú,

   — byť konzistentne uplatňovaný v rôznych súvislostiach (prvý a tretí pilier).

3. Okrem toho by malo byť doplnenie nových prvkov do SIS II, ktoré zvýši jeho možný vplyv na život jednotlivca, sprevádzané prísnejšími ochrannými opatreniami, ktoré sa opisujú v stanovisku. Konkrétne:

— Prístup do SIS II sa nemôže udeliť novým orgánom bez zásadného odôvodnenia. Tiež by sa mal obmedziť v čo najväčšom rozsahu, pokiaľ ide o dostupné údaje i o oprávnené osoby.

— Prepojenie záznamov nesmie nikdy, a ani nepriamo, viesť k zmene prístupových práv.

— Neprijaté právne predpisy sa nesmú považovať za platný dôvod na vloženie údajov do SIS II (záznamy na účely odoprenia vstupu).

— Právny základ na prístup orgánov zodpovedných za vydávanie osvedčení o evidencii vozidla by sa mal znovu zvážiť, keďže sa zameriava hlavne na boj proti trestnej činnosti.

— EDPS uznáva, že použitie biometrických údajov môže zlepšiť výkonnosť systému a pomôcť obetiam krádeže identity. Zdá sa však, že vplyv tejto novinky nie je dostatočne premyslený a spoľahlivosť príslušných údajov je nadhodnotená.

11.2. **Konkrétne pripomienky**

1. EDPS víta skutočnosť, že Komisia uznala, že nariadenie 45/2001 sa vzťahuje na všetky činnosti Komisie súvisiace so spracovaním údajov v SIS II, keďže sa tým pomôže zabezpečiť jednotné a homogénne uplatňovanie pravidiel týkajúcich sa ochrany základných práv a slobôd jednotlivca so zreteľom na spracovávanie osobných údajov.

2. S cieľom zabezpečiť prísne obmedzenie účelu na vnútroštátnej úrovni odporúča EDPS, aby sa do návrhov o SIS II (menovite článku 21 navrhovaného nariadenia a článku 40 navrhovaného rozhodnutia) zaviedlo ustanovenie s rovnakým účinkom ako súčasný článok 102.4 Schengenského dohovoru, ktorým sa obmedzuje možnosť členských štátov ustanoviť použitie údajov, ktoré sa nepredpokladá v zneniach o SIS II.

3. Pri poskytovaní prístupu do SIS II akémukoľvek orgánu by sa mali uplatňovať prísne podmienky:

— prístup musí byť v súlade so všeobecným účelom SIS II a s jeho právnym základom,

— musí sa preukázať potreba prístupu k údajom v SIS II,

— použitie údajov sa musí vymedziť explicitne a reštriktívne,

— podmienky prístupu musia byť riadne vymedzené a obmedzené. Konkrétne by mal aj pre Europol a Eurojust existovať aktualizovaný zoznam osôb oprávnených na prístup.

— skutočnosť, že sa týmto orgánom umožní prístup k údajom v SIS II, nemôže byť v žiadnom prípade dôvodom na vloženie alebo uchovávanie údajov v systéme, ak nie sú potrebné pre konkrétny záznam, ktorého sú súčasťou,

— ak to nie je nevyhnutné na účely, kvôli ktorým sa údaje vložili, doba uchovávania údajov sa nesmie predĺžiť.

4. V konkrétnom prípade Europolu a Eurojustu EDPS naliehavo vyzýva Komisiu, aby reštriktívne vymedzila úlohy, na výkon ktorých by bol prístup odôvodnený. Prístup Europolu a Eurojustu by sa okrem toho mal obmedziť na údaje o osobách, ktorých meno sa už v ich záznamoch objavuje. V prípade Europolu a Eurojustu sa tiež navrhuje poskytnutie len jedného prístupového bodu.

5. Čo sa týka záznamov na účely odoprenia vstupu, ustanovenia založené na ešte neprijatých právnych predpisoch by sa mali buď stiahnuť alebo preformulovať na základe platných právnych predpisov spôsobom, ktorý umožní, aby osoby presne vedeli, aké opatrenia voči nim môžu použiť príslušné orgány.

6. Doby uchovávania údajov sa predĺžili bez akéhokoľvek závažného odôvodnenia. Ak neexistuje presvedčivé odôvodnenie, mali by sa skrátiť na ich súčasné trvanie, pričom najmä v prípade záznamov na účely diskrétneho dohľadu alebo osobitných kontrol.

7. Úloha Komisie sa opisuje ako úloha inštitúcie, ktorá zodpovedá za operačné riadenie. V kombinácii s jej hlavnou úlohou pri rozvoji a údržbe systému by sa to malo vnímať ako úloha kontrolóra *sui generis*. Táto úloha je omnoho viac než úloha spracovateľa, ale tiež obmedzenejšia než úloha obyčajného kontrolóra, keďže Komisia nemá vôbec prístup k údajom spracovávaným v SIS II.

   Do článku 12 oboch návrhov by sa malo vložiť, že pri uplatňovaní tejto úlohy by mala Komisia pravidelne navrhovať zavádzanie nových technológií, ktoré predstavujú v tejto oblasti to najmodernejšie a prostredníctvom ktorých sa zvýši úroveň ochrany údajov a bezpečnosti.

8. Pokiaľ ide o úlohu členských štátov, je potrebné vysvetlenie z hľadiska orgánov, ktoré konajú v pozícii kontrolóra.

9. K informáciám o dotknutých osobách:

   — v navrhovanom nariadení by sa do zoznamu mali doplniť niektoré informácie: doba uchovávania údajov, existencia práva požadovať preskúmanie rozhodnutia o vytvorení záznamu alebo odvolať sa voči nemu, možnosť pomoci od orgánu pre ochranu údajov a existencia opravných prostriedkov.

     Čo sa týka momentu, kedy sa informácie poskytnú, mala by sa ustanoviť povinnosť najprv poskytnúť informácie o zázname v rozhodnutí, ktoré je dôvodom na záznam.

   — v navrhovanom rozhodnutí by sa mal zmeniť a doplniť článok 50, aby sa právo na informácie nezakladalo na žiadosti dotknutej osoby.

10. Čo sa týka lehôt na odpoveď na žiadosť o prístup, víta sa zavedenie týchto lehôt do návrhov. Ak lehoty stanovujú aj vnútroštátne predpisy, malo by sa vysvetliť, že by sa mali uplatňovať lehoty, ktoré sú najvýhodnejšie pre dotknuté osoby.

    Okrem toho by bolo užitočné ustanoviť povinnosť orgánov pre ochranu údajov aktívne spolupracovať pri výkone práva na prístup.

11. Pokiaľ ide o právo na opravné prostriedky, EDPS navrhuje vypustiť územné obmedzenie z článku 30 a článku 52.

12. K právomociam vnútroštátnych orgánov pre ochranu údajov:

    — v nariadení: musí sa konštatovať, že môžu v súvislosti s SIS II vykonávať všetky právomoci, ktoré im prislúchajú podľa článku 28 smernice 95/46/ES; toto by sa malo objasniť v texte navrhovaného nariadenia.

    — čo sa týka navrhovaného rozhodnutia: dozorným orgánom by sa mali priznať rovnaké právomoci, ako v nariadení/smernici.

13. Pokiaľ ide o právomoci EDPS: EDPS by mal byť schopný vykonávať všetky svoje právomoci podľa nariadenia 45/2001, pričom by sa však zohľadnili obmedzené právomoci Komisie v súvislosti so samotnými údajmi.

14. Čo sa týka koordinácie dozoru: v návrhoch sa tiež uznáva potreba koordinácie dozorných činností rôznych zúčastnených orgánov. EDPS víta skutočnosť, že návrhy v podstate obsahujú potrebné prvky na nadviazanie spolupráce medzi orgánmi zodpovednými za dozor na vnútroštátnej a európskej úrovni. Tieto ustanovenia (článok 31 navrhovaného nariadenia a článok 53 navrhovaného rozhodnutia) by mohli mať prospech z určitých objasnení obsahu uvedenej spolupráce.

15. Články 10 a 13 návrhu obsahujú rôzne opatrenia v oblasti bezpečnosti údajov; víta sa skutočnosť, že sa do týchto článkov vložili ustanovenia o systematickej (samo)kontrole bezpečnostných opatrení.

    — Článok 59 navrhovaného rozhodnutia a článok 34 navrhovaného nariadenia, ktoré upravujú monitorovanie a hodnotenie, by sa nemali týkať len aspektov výkonu, hospodárnosti a kvality služieb, ale aj súladu s právnymi požiadavkami, a to najmä v oblasti ochrany údajov. Tieto ustanovenia by sa mali náležitým spôsobom zmeniť a doplniť.

    — Okrem toho na doplnenie článku 10 ods. 1 písm. f) alebo článku 18 navrhovaného rozhodnutia a článku 17 navrhovaného nariadenia, by sa malo doplniť, že členské štáty, Europol a Eurojust by mali zaistiť, aby boli k dispozícii presné profily užívateľov (ktoré by boli k dispozícii vnútroštátnym dozorným orgánom na účely kontroly). Okrem užívateľských profilov musia členské štáty vypracovať úplný zoznam údajov o totožnosti užívateľov a stále ho aktualizovať. To isté platí pre Komisiu.

    — Zákonnosť operácie, ktorou sa spracovávajú osobné údaje, je založená na prísnom dodržiavaní bezpečnosti a integrity údajov. EDPS by mal mať možnosť prostredníctvom analýzy dostupných protokolov monitorovať nielen bezpečnosť údajov, ale aj ich integritu. Preto je potrebné doplniť do článku 14 ods. 6. „integritu údajov“.

16. S používaním vnútroštátnych kópií sa spája množstvo dodatočných rizík. EDPS nie je presvedčený ani o potrebe (z hľadiska dostupných technológií), ani o pridanej hodnote používania vnútroštátnych kópií. Odporúča vyhnúť sa možnosti členských štátov využívať vnútroštátne kópie, alebo ju aspoň podstatne obmedziť. Ak sa však majú vytvoriť vnútroštátne kópie, na ich vnútroštátne použitie sa musí vzťahovať prísna zásada obmedzenia účelu. Taktiež sa vo vnútroštátnej kópii nesmie vyhľadávať iným spôsobom, ako v centrálnej databáze.

17. Ku komitológii: rozhodnutia s významným vplyvom na ochranu údajov by sa mali uskutočňovať s použitím spolurozhodovacieho postupu prostredníctvom nariadenia alebo rozhodnutia. Ak sa skutočne použije komitologický postup, poradná úloha EDPS by sa mala nachádzať v článkoch 60 a 61 rozhodnutia a v článku 35 nariadenia.

18. Interoperabilita systémov sa nemôže vykonávať v rozpore so zásadou obmedzujúcou účel a akýkoľvek návrh v tejto veci by sa mal predložiť EDPS.

V Bruseli 19. októbra 2005

Peter HUSTINX

Európsky dozorný úradník pre ochranu údajov