EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV

Stanovisko Európskeho dozorného úradníka pre ochranu údajov k návrhu nariadenia Európskeho parlamentu a Rady o vízovom informačnom systéme (VIS) a výmene údajov o krátkodobých vízach medzi členskými štátmi (KOM(2004)835 v konečnom znení)

(2005/C 181/06)

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 fyzických osôb 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 25. januára 2005 prijatá od Komisie,

PRIJAL TOTO STANOVISKO:

1. **ÚVOD**

1.1. **Úvodné poznámky**

Vytvorenie vízového informačného systému (VIS) tvorí dôležitú súčasť spoločnej vízovej politiky EÚ a je predmetom niekoľkých nástrojov, ktoré sú prepojené.

— V apríli 2003 bola na podnet Komisie vypracovaná realizačná štúdia ([1]) k VIS.

— V septembri 2003 navrhla Komisia zmenu a doplnenie ([2]) predchádzajúceho nariadenia, ktoré stanovuje jednotný vzor víz. Hlavný cieľ bolo zaviesť biometrické údaje (fotografiu tváre a odtlačky prstov) do tohto nového vzoru víz. Tieto biometrické údaje by boli uložené na mikročipe.

([1]) Vízový informačný systém, záverečná správa, na podnet ES a vykonaná Trasys-om, apríl 2003.
([2]) KOM(2003)558 v konečnom znení s 2003/0217 (CNS) a 2003/0218 (CNS)

— V júni 2004 rozhodnutím Rady, ([1]) ktoré poskytuje právny základ pre zahrnutie VIS-u do rozpočtu EÚ, začal proces budovania vízového informačného systému. Toto rozhodnutie navrhlo centrálnu databázu, ktorá obsahuje informácie súvisiace s uplatňovaním víz a predpokladá proces „komitológie“ na riadenie technického rozvoja systému VIS.

V decembri 2004 prijala Komisia návrh nariadenia o vízovom informačnom systéme (VIS) a o výmene údajov o krátkodobých vízach medzi členskými štátmi ([2]): (ďalej len: „návrh“), ktorý je predmetom tohto stanoviska. K návrhu je pripojené štúdia rozšíreného posúdenia vplyvu ([3]) (ďalej: „EIA“).

Ako sa však uvádza vo vysvetľujúcom memorande, na doplnenie tohto nariadenia budú potrebné ďalšie právne nástroje, najmä na:

— zmenu a doplnenie Spoločných konzulárnych pokynov o vízach pre diplomatické misie a konzulárne úrady zmluvných strán Schengenského dohovoru (ďalej len „Spoločné konzulárne pokyny“), ktoré súvisia so zavedením biometrických údajov do postupov;

— rozvoj nového mechanizmu na výmenu údajov s Írskom a Spojeným kráľovstvom;

— výmenu údajov o dlhodobých vízach.

Podľa rozhodnutia Rady pre spravodlivosť a vnútorné veci z 5. a 6. júna 2003 a ako sa uvádza v článku 1 ods. 2 uvedeného rozhodnutia Rady z júna 2004, vízový informačný systém (VIS) bude založený na centralizovanej architektúre obsahujúcej databázu, v ktorej budú uložené súbory žiadostí o víza: centrálny vízový informačný systém (CS-VIS) a národný styčný bod (NI-CIS) umiestnené v členských štátoch. Členské štáty určia ([4]) ústredný vnútroštátny orgán, ktorý bude napojený na národný styčný bod a cez ktorý budú mať príslušné orgány prístup k CS-VIS.

1.2. **Hlavné body návrhu z hľadiska ochrany údajov**

Cieľom návrhu je zlepšiť správu spoločnej vízovej politiky uľahčením výmeny údajov medzi členskými štátmi vytvorením ústrednej databázy. Nariadenie predpokladá v priebehu postupu uplatňovania zaviesť biometrické údaje (fotografiu a odtlačok prsta) a uložiť ich do ústrednej databázy.

Biometrické údaje by sa tiež mohli použiť vo vízovej nálepke, ako je ustanovené v pozmeňujúcom a doplňujúcom nariadení o jednotnom vzore víz so zavedením fotografie a odtlačkov prstov uložených na mikročipe, ktoré navrhla Komisia, (ešte pred rozhodnutím Rady založenom na výsledkoch prebiehajúcej analýzy).

Návrh podrobne opisuje rôzne operácie, ktoré sa uskutočňujú s údajmi (vkladanie, úprava, vymazávanie a prezeranie údajov) a rôzne údaje, ktoré sa majú doplniť do systému VIS v závislosti od situácie uplatňovania (prijatie, odmietnutie. atď.).

Návrh ustanovuje dobu päť rokov na zachovávanie údajov o každej žiadosti.

Návrh uvádza v obmedzenej miere iné príslušné orgány okrem orgánov udeľujúcich víza, ktoré budú mať prístup k systému VIS a vymedzuje práva prístupu, ktoré sa im majú udeliť:

— orgány zodpovedné za vykonávanie kontrol na vonkajších hraniciach a na území členských štátov,

— príslušné imigračné orgány,

([1]) 2004/512/ES, Ú. v. EÚ L 213, 15.6.2004, s. 5.
([2]) KOM(2004) 835 v konečnom znení 2004/0287 (COD)
([3]) Štúdia pre rozšírené posúdenie vplyvu vízového informačného systému, záverečná správa EPEC, december 2004
([4]) článok 24 ods. 2 návrhu

— zodpovedné azylové orgány.

Návrh v opise činnosti systému VIS a súvisiacich zodpovedností zdôrazňuje, že Komisia spracováva údaje systému VIS v mene členských štátov. Opisuje potrebu používania záznamov o spracovaní údajov na zaistenie bezpečnosti údajov a podrobne uvádza príslušné zodpovednosti na zaistenie tejto úrovne bezpečnosti.

Návrh obsahuje kapitolu o ochrane údajov, v ktorej sú podrobne uvedené úlohy vnútroštátnych orgánov, ako aj úloha Európskeho dozorného úradníka pre ochranu údajov (ďalej len: „EDPS“).

Návrh poveruje technickým vykonávaním systému VIS a výberom požadovanej technológie výbor ustanovený podľa článku 5 ods. 1 nariadenia (ES) č. 2424/2001 o rozvoji druhej generácie Schengenského informačného systému (SIS II).

K návrhu je pripojené rozšírené posúdenie vplyvu systému VIS, na ktoré dala podnet Komisia a ktoré vykonal EPEC. Posúdenie dospelo k záveru, že najlepším dostupným riešením na zlepšenie spoločnej vízovej politiky je alternatíva systému VIS podporovaného použitím biometrie.

2. **PRÍSLUŠNÝ RÁMEC**

Návrh bude mať výrazný vplyv na súkromie a na ostatné základné práva fyzických osôb; podlieha preto kontrole na základe zásad ochrany údajov. Hlavné referenčné body nášho posúdenia sú:

— Rešpektovanie súkromného života je v Európe zaistené od schválenia v roku 1950 Dohovoru o ochrane ľudských práv a základných slobôd (ďalej len: „ECHR“) Radou Európy. Článok 8 dohovoru 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 ktoréhokoľvek opatrenia a potrebu vhodných ochranných opatrení voči zneužitiu.

V dohovore o ochrane údajov, ktorý pripravila a v roku 1981 schválila Rada Európy, boli vypracované základné zásady ochrany jednotlivcov s ohľadom na spracovanie osobných údajov.

— Právo na rešpektovanie súkromného života a na ochranu súkromných údajov bolo neskôr stanovené v článkoch 7 a 8 Charty základných ľudských práv Európskej únie, ktorá bola začlenená do časti II novej Ústavy EÚ.

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 ECHR. Tieto podmienky sa musia brať do úvahy vždy, keď sa hodnotí návrh na možné zasahovanie.

Dnes sú v právnych predpisoch EÚ základné pravidlá na ochranu údajov stanovené v:

— smernici Rady 95/46/ES Európskeho parlamentu a Rady 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“. Smernica stanovuje podrobné zásady, na základe ktorých sa bude návrh kontrolovať v rozsahu, v akom sa má uplatňovať na členské štáty. Toto má väčší význam, pretože návrh sa bude uplatňovať spolu s vnútroštátnymi právnymi predpismi, ktoré uvádzajú smernicu do účinnosti. Účinnosť navrhovaných opatrení a ochranných opatrení tak bude závisieť od účinnosti tejto kombinácie v každom jednotlivom prípade.

— 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/". Stanovuje podobné zásady, ako smernica 95/46/ES a v tejto súvislosti sa v rozsahu, v akom sa má návrh uplatňovať, vzťahuje na činnosti Komisie spolu s ustanoveniami nariadenia. Táto kombinácia si preto tiež zaslúži určitú pozornosť.

Smernica 96/46/ES a nariadenie 45/2001 sa musia vykladať spolu s ostatnými nástrojmi. Inými slovami, smernica a 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]) .

— Nakoniec, EDPS zahrnie do svojej analýzy tiež stanovisko č. 7/2004 z 11. augusta 2004 pracovnej skupiny podľa článku 29 o ochrane údajov ([2])„o zahrnutí biometrických prvkov do povolení na pobyt a víz, pričom zohľadní zriadenie Európskeho informačného systému o vízach (VIS)". Pracovná skupina vyjadrila v tomto stanovisku znepokojenie nad niekoľkými prvkami návrhu. EDPS má v úmysle overiť, či a ako návrh zohľadnil toto znepokojenie.

3. ANALÝZA NÁVRHU

3.1. Všeobecne

EDPS uznáva, že ďalší vývoj spoločnej vízovej politiky si vyžaduje efektívnu výmenu príslušných údajov. Jeden z mechanizmov, ktorý môže zabezpečiť hladký tok informácií v systéme VIS. Tento nový nástroj by sa však mal obmedziť na výber a výmenu údajov, pokiaľ je zber alebo výmena údajov potrebná na vývoj spoločnej vízovej politiky a primeraná k tomuto cieľu.

Zriadenie systému VIS môže mať priaznivé dôsledky na iné oprávnené verejné záujmy, ale to nemení účel systému VIS. Obmedzený účel systému zohráva hlavnú úlohu pri stanovení oprávneného obsahu a použitia systému, a preto tiež pri udeľovaní práva prístupu do systému VIS (alebo k časti jeho údajov) orgánom členských štátov pre oprávnené verejné záujmy.

Okrem toho návrh zavádza použitie biometrických údajov v systéme VIS. EDPS uznáva výhody použitia biometrických údajov, ale zdôrazňuje veľký vplyv používania týchto údajov a navrhuje zavedenie prísnejších bezpečnostných opatrení na používanie biometrických údajov.

Toto stanovisko sa musí vykladať na základe týchto hlavných hľadísk. Uvádza sa, že súčasné názory by sa mali uviesť v preambule nariadenia pred odôvodneniami („so zreteľom na stanovisko Komisie ...").

([1]) V tejto súvislosti je účelné odvolať sa na rozsudok Súdneho dvora vo veci Österreichischer Rundfunk a ostatní (spojené prípady C-465/00, C-138/01 a C-138/01, rozsudok z 20. mája 2003,), Súdny dvor (2003) HZb. I-4989). Dvor sa zaoberal rakúskym zákonom upravujúcom prenos údajov o platoch zamestnancov vo verejnom sektore na rakúsky Dvor 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.

([2]) Je to nezávislá poradenská skupina zložená zo zástupcov orgánov na ochranu údajov členských štátov, EDPS a Komisie, ktorá bola zriadená smernicou 95/46/ES.

3.2. **Účel**

Účel systému VIS má rozhodujúci význam so zreteľom na článok 8 ECHR aj na všeobecný rámec ochrany údajov. Podľa článku 6 smernice 95/46/ES musia byť osobné údaje „zhromaždené na špecifikované, explicitné a zákonné účely a nebudú sa ďalej spracovávať spôsobmi, ktoré nie sú zlučiteľné s týmito účelmi". Len zreteľné stanovenie účelu umožní správne hodnotenie proporcionality a primeranosti spracovania osobných údajov, ktoré je rozhodujúce z dôvodu charakteru údajov (vrátane biometrických údajov) a rozsahu predpokladanej operácie spracovania.

Účel systému VIS je jasne uvedený v článku 1 ods. 2 návrhu:

„Systém VIS zlepšuje riadenie spoločnej vízovej politiky, konzulárnu spoluprácu a konzultácie medzi ústrednými konzulárnymi orgánmi uľahčením výmeny údajov o žiadostiach a súvisiacich rozhodnutiach".

Všetky prvky systému VIS preto musia byť nevyhnutné a primerané nástroje na dosiahnutie tohto politického cieľa v záujme spoločnej vízovej politiky.

Článok 1 ods. 2 návrhu uvádza tiež dodatočné výhody zlepšenia vízovej politiky ako je:

a) predchádzať ohrozeniu vnútornej bezpečnosti,

b) uľahčiť boj proti podvodom,

c) uľahčiť kontroly na vonkajších hraničných priechodoch.

EDPS považuje tieto prvky za príklady priaznivých dôsledkov zriadenia systému VIS a zlepšenia spoločnej vízovej politiky, ale nie ako nezávislé ciele v nich obsiahnuté.

V tejto etape to prináša dva hlavné dôsledky:

— EDPS si je vedomý, že orgány činné v trestnom konaní majú záujem na udelení prístupu k systému VIS; Závery Rady boli v tomto zmysle schválené 7. marca 2005. Keďže účelom systému VIS je zlepšenie spoločnej vízovej politiky, malo by sa brať do úvahy, že rutinný prístup orgánov činných v trestnom konaní by nebol v súlade s týmto účelom. Pokiaľ v súlade s článkom 13 smernice 95/46/ES by tento prístup mohol byť udelený na *ad hoc* základe, systematický prístup nemôže byť udelený za špecifických okolností a ak primerané bezpečnostné opatrenia neustanovujú inak.

  Vo všeobecnosti je nevyhnutné hodnotenie proporcionality a potreby, ak sa prijímajú rozhodnutia do budúcnosti o tom, či umožniť niektorým iným orgánom prístup k systému VIS. Úlohy, na ktoré sa udelí prístup, musia byť v súlade s účelmi systému VIS.

— Vyslovene uviesť „predchádzanie ohrozenia vnútornej bezpečnosti ktoréhokoľvek z členských štátov" v písmene a) nie je šťastné riešenie. Hlavná výhoda systému VIS bude predchádzanie podvodom a tzv. visa-shoppingu (boj proti podvodom je tiež hlavný dôvod pre zahrnutie biometrických údajov do systému) ([1]). Predchádzanie ohrozenia bezpečnosti by sa preto malo považovať za „druhotnú", hoci veľmi vítanú výhodu.

  EDPS odporúča, aby sa rozlišovanie medzi „účelom" a „výhodami" v súvislosti s článkom 1 ods. 2, robilo jasnejšie, napríklad takto:

  „Účelom systému VIS je zlepšiť riadenie spoločnej vízovej politiky, konzulárna spolupráca a konzultácie medzi ústrednými konzulárnymi orgánmi uľahčením výmeny údajov o žiadostiach a súvisiacich rozhodnutiach medzi členskými štátmi. Týmto sa tiež prispeje k...."

([1]) EIA to uvádza veľmi jasne (s. 6, čl. 2.7).: „*neefektívnosť v boji proti visa-shoppingu* (t.j. podávaniu si žiadostí o vízum vo viacerých štátoch súčasne), podvodom a vo vykonávaní kontrol spôsobuje tiež neefektívnosť vnútornej bezpečnosti členských štátov". To znamená, že ohrozenie bezpečnosti je čiastočne spôsobené neúčinnou vízovou politikou. Prvú vec, ktorú treba v tomto smere urobiť, je zlepšiť vízovú politiku, najmä bojom proti podvodom, a vykonávať lepšie kontroly. Zvýšenie bezpečnosti vyplynie zo zlepšenia vízovej politiky.

V tejto súvislosti treba tiež vziať na vedomie, že „Usmernenia pre zavedenie spoločného systému na výmenu údajov o vízach“, ktoré 13. júna 2002 ([1]) prijala Rada SVV, zaradili predchádzanie ohrozenia vnútornej bezpečnosti na koniec zoznamu. Bolo by to tiež možné a omnoho viac v súlade s účelom systému VIS.

3.3. **Kvalita údajov**

Podľa článku 6 smernice 95/46/ES osobné údaje musia byť „primerané, relevantné a nie nadbytočné z hľadiska účelu, na ktorý sa zbierajú a/alebo ďalej spracúvajú“. Súvisí to s proporcionalitou samotného systému VIS, ale aj s údajmi, ktoré sa majú zbierať a ukladať v systéme VIS, a s ich ďalším použitím, ako aj dodatočnými bezpečnostnými opatreniami, ktoré sa v tejto súvislosti uplatňujú. Tieto prvky sú rovnako podstatné pre hodnotenie návrhu so zreteľom na článok 8 EDĽP.

Zriadenie systému VIS nepochybne predstavuje významné zasahovanie pri výkone práva do súkromia, pokiaľ ide o jeho rozsah a kategórie spracovaných osobných údajov. Preto pracovná skupina článku 29 vo svojom stanovisku č. 7/2004 chcela vedieť „aké presvedčivé dôvody odhalili štúdie rozsahu a závažnosti týchto javov pre verejnú bezpečnosť alebo verejný poriadok, ktoré by odôvodňovali tento prístup“.

EDPS pozorne zobral na vedomie dôkaz uvedený v štúdii EIA. Hoci tento dôkaz nie je úplne dostačujúci, zdá sa, že existujú dostačujúce dôvody na odôvodnenie zriadenia systému VIS na účely zlepšenia spoločnej vízovej politiky.

V tejto súvislosti sa zdá, že hodnotenie zriadenia systému VIS, ako nástroja na zlepšenie podmienok vydávania víz v členských štátoch, patrí do rámca zákonodarnej moci. Takýto systém by sám o sebe mohol dobre vyhovovať pokrokovému vytváraniu a podpore priestoru pre slobodu, bezpečnosť a spravodlivosť, ako sa uvádza v Zmluve o ES.

Vytvorenie a využívanie systému VIS by však nikdy nemohlo mať taký účinok, aby sa v tejto oblasti naďalej nemohol zaistiť vysoký stupeň ochrany osobných údajov. Preskúmanie rozsahu, v akom ovplyvní systém VIS existujúcu úroveň ochrany údajov dotknutých osôb, patrí do poradnej úlohy EDPS.

EDPS sa v tejto súvislosti zameria v uvedenom stanovisku na tieto otázky:

— proporcionalita a primeranosť údajov a ich použitia (napr. kategórie údajov, prístup k údajom každého dotknutého orgánu a doba uchovávania);

— prevádzka systému (napr. zodpovednosti a bezpečnosť);

— práva dotknutých osôb (napr. informovanie, možnosť opraviť alebo vymazať nesprávne alebo neopodstatnené údaje);

— sledovanie a dohľad nad systémom.

Okrem týchto odsekov návrh nevedie k dôležitým pripomienkam, čo sa týka kategórií údajov, ktoré sa majú zahrnúť do systému VIS, a ich využívania. Príslušné ustanovenia boli uvážlivo navrhnuté a zdá sa, že sú zosúladené a primerané ako celok.

([1]) „Rámcové rozhodnutie Rady z 13. júna 2002 o boji proti terorizmu (2002/475/SVV)“ (Ú. v. EÚ L 164, 22.6.2002, s. 3.)

3.4. **Biometria**

3.4.1. *Vplyv použitia biometrie*

Použitie biometrických údajov v informačnom systéme nikdy nie je bezvýznamná voľba, najmä ak sa príslušný systém týka takého veľkého počtu jednotlivcov. Biometria nie je len iná forma technológie. Neodvolatene mení vzah medzi telom a totožnosou tým, že robí prístrojovo snímateľné charakteristiky ľudského tela, ktoré sa dajú ďialej použi. Aj keď biometrické charakteristiky sa nedajú číta ľudským okom, stále ich môžu čítať a využívať príslušné nástroje, kamkoľvek osoba ide.

Biometria však môže byť užitočná na niektoré účely; ich široké využitie má silný vplyv na spoločnosť a mali by sa o nich viesť rozsiahle a otvorené diskusie. EDPS musí konštatovať, že v skutočnosti takáto diskusia sa pred prípravou návrhu neuskutočnila. Toto podčiarkuje ešte viac potrebu prísnejších bezpečnostných opatrení na použitie biometrických údajov a na starostlivé zváženie a diskusiu počas legislatívneho procesu.

3.4.2. *Osobitný charakter biometrie*

Ako už bolo zdôraznené v niekoľkých stanoviskách pracovnej skupiny podľa článku 29, ([1]) je potrebné podporiť zavedenie a spracovávanie biometrických údajov pre dokumenty týkajúce sa totožnosti obzvlášť dôslednými a závažnými bezpečnostnými opatreniami. V skutočnosti sú biometrické údaje vysoko citlivé, čo spôsobujú niektoré osobitné charakteristiky.

Je pravda, že strata biometrických údajov dotknutej osoby je na rozdiel od hesla alebo kľúča takmer nemožná. Poskytujú *kvázi-absolútnu charakteristickú* zvláštnosť, t. j. každá fyzická osoba má jedinečnú biometriu. Takmer nikdy sa v priebehu života človeka nemenia, čo týmto charakteristikám zabezpečuje *trvalosť*. Každý má rovnaké fyzické „prvky", čo tiež dáva biometrii rozmer *univerzálnosti*.

Zrušenie biometrických údajov je však takmer nemožné: prst alebo tvár je ťažké zmeniť. Táto pozitívna charakteristika vedie z mnohých výhľadov k závažnému poklesu v prípade *krádeže totožnosti*; uchovávanie odtlačkov a fotografií v databáze v spojení s ukradnutým preukazom totožnosti by mohlo viesť k veľkým a trvalým problémom skutočného vlastníka tejto totožnosti. Okrem toho biometrické údaje *nie sú* svojim charakterom *tajné* a môžu dokonca *zanechávať stopy* (odtlačky prstov, DNA), čo umožňuje zbieranie týchto údajov *bez toho, aby si toho bol ich vlastník vedomý*.

Z dôvodu týchto rizík, ktoré sú súčasťou charakteru biometrie, sa budú musieť vykonávať dôležité bezpečnostné opatrenia (najmä z hľadiska dodržiavania zásady obmedzenia účelu, obmedzenia prístupu a bezpečnostných opatrení).

3.4.3. *Technická nedokonalosť odtlačkov prstov*

Hlavné výhody biometrie uvedené vyššie (údaje o univerzálnosti, rozlíšenie, stálosť, použiteľnosť, atď.), nikdy nie sú absolútne. Má to priamy vplyv na účinnosť biometrickej registrácie a overovacích postupov plánovaných v nariadení.

Odhaduje sa ([2]), že až do 5 % ľudí nie je možné zaregistrovať (pretože nemajú snímateľné odtlačky prstov alebo vôbec žiadne odtlačky). Štúdia EIA pripojená k návrhu predpovedá v roku 2007 20 miliónov žiadateľov o víza, čo znamená, že až do 1 milióna osôb nebude schopných dodržať „bežný" registračný postup bez zrejmých následkov pre žiadosť o víza a pri hraničných kontrolách.

([1]) Stanovisko 7/2004 a zahrnutí biometrických prvkov do povolení na pobyt a víz, pričom zohľadní zriadenie Európskeho informačného systému o vízach (VIS) (Markt/11487/04/EN PS - 96) a pracovný dokument o biometrii (MARKT/10595/03/EN - PS 80).

([2]) A *Sasse, Cybertrust a predchádzanie zločinom*: *použiteľnosť a dôvera informačných systémov v*„Prognostickom projekte Cybertrust a predchádzanie zločinom". 04/1151, 10. jún 2004, s. 7, a posúdenie technológie, „Využívanie biometrie pre bezpečnosť hraníc", Úrad všeobecného finančného účtovníctva Spojených štátov, GAO-03-174, november 2002.

Biometrická identifikácia je aj podľa definície štatistický proces. Chybovosť od 0,5 do 1 % je bežná ([1]), čo znamená, že kontrola systému na vonkajších hraniciach bude mať FRR (pravdepodobnosť, že biometrické skúmanie neidentifikuje autorizovanú osobu) od 0,5 do 1 %. Táto miera chybovosti sa ladí po prahovú úroveň založenú na politike rizika príslušných orgánov (zodpovedá rozdielu stanovenému medzi počtom osôb, ktoré boli nesprávne zamietnuté a tými, ktoré boli nesprávne prijaté). Preto je nadsadená domnienka, že tieto technológie budú poskytovať „presnú identifikáciu" dotknutej osoby uvedenú v 9. odôvodnení navrhovaného nariadenia.

Podľa poslednej prieskumnej štúdie ([2]) ktorú zadal výbor LIBE Európskeho parlamentu, by mali byť k dispozícii *záložné postupy* na vytvorenie dôležitých bezpečnostných opatrení na zavedenie biometrie, keďže nie sú všetkým dostupné, ani úplne presné. Tieto postupy by sa mali vykonať a použiť, aby sa rešpektovala dôstojnosť osôb, ktoré sa nemohli úspešne zúčastniť na registračnom procese, a aby sa zabránilo preneseniu záťaže nedokonalosti systému na nich ([3]).

EDPS preto odporúča, aby sa vypracovali zálohové postupy a aby sa zahrnuli do návrhu. Tieto postupy by nemali znižovať úroveň bezpečnosti vízovej politiky ani trvalo označiť jednotlivca ako s nečitateľnými odtlačkami prstov.

3.5. **Osobitné kategórie údajov**

Niektoré kategórie údajov (okrem biometrických údajov) si vyžadujú osobitné posúdenie: údaje týkajúce sa dôvodov neudelenia víza (3.5.1) a údaje týkajúce sa ostatných členov skupiny (3.5.2).

3.5.1. *Dôvody neudelenia víza*

Článok 10 ods. 2 návrhu určuje spracovanie údajov o dôvodoch neudelenia, ak sa prijalo rozhodnutie o neudelení víza. Tieto dôvody neudelenia sú plne normalizované.

— Prvé dva dôvody v pododsekoch a) a b) majú skôr administratívny charakter: nepredloženie platného cestovného dokladu dokazujúceho účel a podmienky plánovaného pobytu.

— Pododsek c) uvádza „upozornenie na žiadateľa na účely odmietnutia vstupu", ktorý znamená prezeranie databázy systému SIS

— Nakoniec pododsek d) uvádza ako dôvod neudelenia víza skutočnosť, že žiadateľ „predstavuje hrozbu pre verejný poriadok, vnútornú bezpečnosť, verejné zdravie alebo medzinárodné vzťahy niektorého z členských štátov".

([1])

Biometria	Tvár	Prst	Dúhovka
FTE % nezaregistrovanie	N/A	4	7
FNMR % častosť zamietnutia	4	2,5	6
FMR1 % chybovosť overenia zhody	10	< 0,01	< 0,001
FMR2 % chybovosť identifikácie pre veľkosť dB > 1 m	40	0,1	N/A
FMR3 % chybovosť zhody screeningu pre veľkosti dB = 500	12	< 1	N/A

A. K. Jain et al., *Biometria: Veľká výzva,* Výsledky Medzinárodnej konferencie o rozpoznávaní vzorov, Cambridge UK., august 2004.

([2]) *Biometria na hraniciach: posúdenie vplyvu na spoločnosť,* február 2005, Inštitút pre perspektívne technologické štúdie, DG stredisko spoločného výskumu, ES.

([3]) Správa o pokroku o uplatňovaní zásady dohovoru 108 na zber a spracovávanie biometrických údajov, Rada Európy 2005, strana 11

Všetky dôvody neudelenia z dôvodu následkov, ktoré znamenajú pre jednotlivca, sa musia uplatňovať veľmi opatrne. Okrem toho niektoré z údajov, ktoré sú uvedené v pododsekoch c) a d), budú viesť k spracovaniu „citlivých údajov“ v zmysle článku 8 smernice 95/46/ES.

EDPS by rád upriamil pozornosť najmä na podmienku súvisiacu s verejným zdravím, ktorá sa zdá byť neurčitá a vyžaduje si spracovanie citlivých údajov. Podľa komentára k článkom pripojeného k návrhu sa odkaz na ohrozenie verejného zdravia zakladá na „návrhu nariadenia Rady, ktorým sa zriaďuje kódex Spoločenstva o pravidlách upravujúcich pohyb osôb cez hranice“ (KOM (2004)391 v záverečnom znení).

EDPS si je vedomý toho, že kritérium „verejného zdravia“ sa v širokej miere používa v právnych predpisoch Spoločenstva o voľnom pohybe osôb a uplatňuje sa veľmi prísne, ako je uvedené v smernici Európskeho parlamentu a Rady 2004/38/ES z 29. apríla 2004 o práve občanov Únie a ich rodinných príslušníkov voľne sa pohybovať a zdržiavať sa v rámci územia členských štátov. Článok 29 smernice stanovuje podmienky zohľadnenia ohrozenia verejného zdravia: „Jediné choroby, ktoré opodstatňujú opatrenia obmedzujúce slobodu pohybu, sú choroby s epidemickým potenciálom, ako je definované v príslušných nástrojoch Svetovej zdravotníckej organizácie a iné infekčné choroby alebo nákazlivé parazitické ochorenia, ak podliehajú ochranným opatreniam, ktoré sa uplatňujú na štátnych príslušníkov hostiteľského členského štátu“

— Napriek tomu je potrebné poznamenať, že predtým uvedený návrh je zatiaľ iba návrh a že zahrnutie podmienky neohrozenia verejného zdravia do nariadenia o systéme VIS podlieha schváleniu kódexu Spoločenstva.

— Okrem toho, ak sa táto podmienka odmietnutia vstupu schváli, mala by sa chápať reštriktívne. V skutočnosti sa návrh kódexu Spoločenstva zakladá práve na uvedenej smernici 2004/58/ES.

EDPS preto odporúča, aby sa odkaz na článok 29 smernice 2004/58/ES zahrnul do znenia návrhu s cieľom zaistiť, aby sa „ohrozenie verejného zdravia“ chápalo so zreteľom na toto ustanovenie. V každom prípade a s ohľadom na ich citlivosť, sa údaje môžu spracovať len vtedy, ak predstavujú reálnu, podloženú a dostatočne závažnú hrozbu pre verejné zdravie.

3.5.2. *Údaje o ostatných členoch skupiny*

Článok 2 ods. 7 vymedzuje pojem „členov skupiny“ ako „ďalších žiadateľov, s ktorými žiadateľ cestuje vrátane manžela/manželky a detí sprevádzajúcich žiadateľa“. Komentár k článkom uvádza, že vymedzenia pojmov v článku 2 návrhu odkazujú na Zmluvu alebo na Schengenské acquis o vízovej politike, okrem niektorých pojmov vrátane „členov skupiny“, ktoré sa vymedzujú osobitne na účely tohto nariadenia. Možno preto predpokladať, že toto vymedzenie pojmov neodkazuje na vymedzenie pojmu „skupinového víza“ uvedeného v článku 2.1.4 Spoločných konzulárnych pokynov. Komentár k článkom odkazuje na „žiadateľov cestujúcich v skupine s inými žiadateľmi, t.j. v rámci dohody ADS alebo spolu s ostatnými rodinnými príslušníkmi“.

EDPS zdôrazňuje, že presné a súhrnné vymedzenie pojmu „členov skupiny“ by sa malo uviesť v nariadení. V súčasnom návrhu musí EDPS konštatovať, že pre nedostatok presných odkazov na Zmluvu alebo Schengenské acquis je vymedzenie pojmov príliš všeobecné. Podľa tohto znenia by „členovia skupiny“ mohli zahŕňať kolegov, iných zákazníkov z tej istej cestovnej kancelárie, ktorí sa zúčastnili na organizovanom zájazde, atď. Dôsledky sú skutočne veľmi významné:

podľa článku 5 návrhu nariadenia súbor žiadosti žiadateľa bude pripojený k súborom žiadostí ostatných členov skupiny.

3.6. **Uchovávanie údajov**

Článok 20 návrhu nariadenia ustanovuje dobu 5 rokov na uchovávania údajov pre každý súbor žiadosti. Ustanovenie primeranej lehoty je politická voľba zákonodarnej moci Spoločenstva.

Neexistuje dôkaz – najmä nie so zreteľom na dôvody uvedené v komentári k článkom – ktorý by naznačoval, že politická voľba v tomto návrhu je neodôvodnená alebo že by mohla mať neprijateľné dôsledky, ak sa zavedú všetky vhodné opravné mechanizmy. To znamená, že sa musí zaistiť oprava alebo vymazanie údajov, ak údaje už nie sú presné alebo najmä ak osoba získala štátnu príslušnosť členského štátu alebo získala status, ktorý nevyžaduje jeho začlenenie do systému.

Okrem toho, ak sa údaje ešte nachádzajú v systéme, nemôžu sa žiadnym spôsobom dotknúť nového rozhodnutia. Niektoré dôvody odmietnutia (upozornenie na žiadateľa na účely odmietnutia vstupu najmä z dôvodu ohrozenia verejného zdravia) majú obmedzenú časovú platnosť. Skutočnosť, že v určitom okamžiku platia dôvody odmietnutia vstupu, by nemala ovplyvniť nové rozhodnutie. Pri každej novej žiadosti o víza sa celá situácia musí prehodnotiť a malo by sa to podľa potreby jasne uviesť v nariadení.

3.7. **Prístup k údajom a ich využívanie**

3.7.1. *Predbežné zistenia*

EDPS v úvodnej poznámke uznáva pozornosť, ktorá sa zjavne venovala regulačnému systému prístupu k údajom systému VIS a ich využívaniu. Každý orgán má prístup k rôznym údajom na rôzne účely. Je to primeraný prístup, ktorý môže EDPS len podporiť. Cieľom týchto zistení je uplatňovať tento prístup v najvyššej miere.

3.7.2. *Kontroly víz na vonkajších hraničných priechodoch a na území členských štátov*

V prípade kontrol víz na vonkajších hraniciach článok 16 navrhovaného nariadenia jasne stanovuje dva presné účely:

— „overenie totožnosti osoby“, čo podľa uvedenej definície znamená porovnanie „dvoch údajov“

— „overenie pravosti víza“. Ako sa navrhuje v normách ICAO, mikročip víz by na vykonanie tohto procesu overenia mohol využívať súkromný/verejný kľúčový systém (PKI).

Tieto dva účely sa môžu riadne dosiahnuť s výhradným prístupom príslušných orgánov k chránenému mikročipu na vykonanie kontroly víz. Prístup k centrálnej databáze systému VIS by bol preto v tomto konkrétnom prípade neprimeraný. Táto posledne uvedená možnosť by si vyžadovala zapojenie viacerých orgánov do systému VIS, čo by mohlo zvýšiť riziko zneužitia. Mohla by to byť tiež drahšia možnosť, pretože výrazne stúpne počet chránených a kontrolovaných prístupov do systému VIS, ako aj potreba špeciálnej odbornej prípravy súvisiacej s týmto prístupom.

Okrem toho existujú pochybnosti o primeranosti prístupu k údajom predpokladaného v druhom bode článku 16. V skutočnosti odsek 2 písmeno a) uvádza, že ak po prvej požiadavke sú údaje o žiadateľovi zaznamenané v systéme VIS (čo by v zásade mali byť), príslušný orgán ešte môže na účely overenia totožnosti prezerať iné údaje. Tieto údaje sa týkajú všetkých informácií súvisiacich s používaním, fotografiami, odtlačkami, prstov, ako aj s vízami, ktoré boli predtým vydané, zrušené, odobraté alebo predĺžené.

Ak overenie totožnosti bolo úspešné, vôbec nie je jasné, z akého dôvodu je ešte potrebný zvyšok týchto údajov. V skutočnosti by sa mali sprístupniť za obmedzujúcich podmienok, iba ak overovací proces zlyhal. V takomto prípade by údaje uvedené v článku 16 ods. 2 primerane prispeli k záložnému postupu, ktorý napomáha zistiť totožnosť osoby. Nemali by byť potom prístupné zamestnancom na každom hraničnom priechode, ale iba v obmedzujúcejšom rozsahu úradníkom zodpovedným za problematické prípady.

Nakoniec by malo byť presnejšie definovanie orgánov, ktoré majú prístup. Najmä nie je jasné, ktoré sú „orgány zodpovedné za vykonávania kontrol na území členského štátu“. EDPS predpokladá, že sa to týka orgánov zodpovedných za vykonávanie kontrol *víz* a článok 16 by sa mal v tomto zmysle zmeniť a doplniť.

3.7.3. *Využívanie údajov pri identifikácii a navracaní nelegálnych migrantov a pri azylových konaniach*

V prípadoch opísaných v článkoch 17, 18 a 19 (navracanie nelegálnych migrantov a azylové konanie) sa systém VIS využíva na účely identifikácie. Fotografie patria medzi údaje, ktoré sa môžu použiť na účely identifikácie. Pri súčasnom stave technológie súvisiacej s automatickým rozoznávaním tváre sa však fotografie nemôžu používať na identifikáciu (porovnanie jednej s mnohými) v takýchto rozsiahlych systémoch IT; nemôžu zabezpečiť spoľahlivý výsledok. Nemajú sa preto považovať za údaje primerané na účely identifikácie.

V dôsledku toho EDPS dôrazne navrhuje, aby sa „fotografie“ odstránili z prvej časti týchto článkov a zostali v druhej časti (fotografie sa môžu použiť ako nástroj na overenie totožnosti niekoho, ale nie na identifikáciu v rozsiahlej databáze).

Druhou možnosťou by bolo zmeniť a doplniť článok 36 v tom zmysle, že funkcie na spracovanie fotografií na účely identifikácie sa budú uplatňovať iba ak sa táto technológia bude považovať za spoľahlivú (prípadne na podnet technického výboru).

3.7.4. *Uverejnenie orgánov, ktoré majú prístup*

Článok 4 návrhu nariadenia stanovuje uverejnenie zodpovedných orgánov, ktoré sú v každom členskom štáte určené na prístup k systému VIS v Úradnom vestníku Európskej únie. Toto uverejnenie by sa malo uskutočňovať pravidelne (ročne), aby informovalo o zmenách vo vnútroštátnych situáciách. EDPS zdôrazňuje dôležitosť tohto uverejnenia, ako nevyhnutného nástroja kontroly na európskej, ako aj národnej alebo miestnej úrovni.

3.8. **Zodpovednosti**

Pripomína sa tu, že systém VIS je založený na centralizovanej architektúre s centrálnou databázou, v ktorej budú uložené všetky informácie o systéme VIS a národných styčných bodoch umiestnených v členských štátoch, ktoré umožňujú ich zodpovedným orgánom prístup k centrálnemu systému. Podľa odôvodnení (14) a (15) návrhu nariadenia sa smernica 95/46/ES bude uplatňovať na spracovanie osobných údajov členskými štátmi pri uplatňovaní nariadenia a nariadenie 45/2001 sa bude uplatňovať na činnosti Komisie súvisiace s ochranou osobných údajov. Ako sa v tejto súvislosti uvádza v odôvodneniach, cieľom návrhov je vyjasniť niektoré body týkajúce sa okrem iného zodpovednosti za použitie údajov a dohľadu nad ochranou údajov.

V skutočnosti by sa zdalo, že tieto body súvisia s veľmi dôležitými podrobnosťami, bez ktorých by sa neuplatňoval systém bezpečnostných opatrení v smernici 95/46/ES a nariadení 45/2001 alebo by nebol plne v súlade s návrhom. Uplatniteľnosť vnútroštátneho práva podľa smernice bežne predpokladá kontrolóra, ktorý je ustanovený v členskom štáte (článok 4), keďže uplatniteľnosť nariadenia závisí od spracovávania osobných údajov inštitúciami a orgánmi Spoločenstva, pokiaľ sa takéto spracovávanie realizuje pri výkone činností, z ktorých všetky alebo časť spadajú do pôsobnosti práva Spoločenstva (článok 3).

Podľa článku 23 ods. 2 návrhu nariadenia údaje „v mene členských štátov spracúva systém VIS“. Podľa článku 23 ods. 3 členský štát vymenuje orgán, ktorý má kontrolnú funkciu v súlade s článkom 2 písm. d) smernice 95/46/ES. Z toho sa zdá, že vyplýva, že podľa systému smernice by sa Komisia mala považovať za spracovateľa. Je to potvrdené vo vysvetleniach článkov ([1]).

Tento výklad má sklon podceňovať veľmi dôležitú a v podstate rozhodujúcu úlohu Komisie v rozvojovej etape systému aj v priebehu jeho normálnej prevádzky. Je ťažké naviazať úlohu Komisie presne na koncepciu kontrolóra a spracovateľa; je buď spracovateľ s nezvyčajnými právomocami (medziiným pri navrhovaní systému) alebo kontrolór s obmedzeniami (pretože údaje zapisujú a používajú členské štáty). Komisia skutočne má to, čo sa musí uznať ako úloha *sui generis* ([2]) v systéme VIS.

Významná úloha Komisie by sa mala uznať skôr prostredníctvom celkového opisu úloh Komisie než formou znenia, ktoré sa nie celkom zhoduje s realitou, lebo je príliš obmedzujúce, nič nemení v prevádzke systému VIS a iba vedie k nejasnostiam. Je to tiež dôležité na účely a dôsledného a účinného dohľadu nad systémom VIS (pozri tiež odsek 3.11). EDPS preto odporúča vypustiť článok 23 ods. 2.

EDPS by chcel zdôrazniť, že úplný opis úloh Komisie ohľadne systému VIS je o to dôležitejší, ak Komisia predpokladá poveriť riadiacimi úlohami iný orgán. „Opis – Fiche Financière“ pripojený k návrhu uvádza možnosť prenosu úloh na orgán na vonkajších hraniciach. V tejto súvislosti je veľmi dôležité, aby Komisia nenechávala žiadne pochybnosti, čo sa týka rozsahu svojich právomocí, aby jej nástupca poznal hranice, v rámci ktorých môže konať.

3.9. **Bezpečnosť**

Riadenie a dodržiavanie optimálneho stupňa bezpečnosti systému VIS predstavuje predpoklad na zaistenie požadovanej ochrany osobných údajov uložených v jeho databáze. Musia sa vykonávať správne bezpečnostné opatrenia, aby sa získala uspokojujúca úroveň ochrany na zvládnutie možného rizika súvisiaceho s infraštruktúrou systému a so zúčastnenými osobami. O tejto téme sa teraz diskutuje v rôznych častiach návrhu a zaslúži si určité zlepšenie.

Články 25 a 26 návrhu obsahujú rôzne opatrenia v oblasti bezpečnosti údajov a uvádzajú druhy zneužití, ktorým treba predchádzať. Tieto ustanovenia by však mohli byť efektívne doplnené o opatrenia na systematické sledovanie a podávanie správ o účinnosti bezpečnostných opatrení, ktorá už boli uvedené. EDPS odporúča najmä, aby sa do týchto článkov vkladali ustanovenia o systematickej (samo)kontrole bezpečnostných opatrení.

Súvisí to s článkom 40 návrhu, ktorý ustanovuje sledovanie a hodnotenie. Toto by sa nemalo týkať stavu, len pokiaľ ide o výsledky, efektívnosť nákladov a kvalitu služieb, ale aj súladu s právnymi požiadavkami najmä v oblasti ochrany údajov. EDPS preto odporúča, aby sa rozšíril rozsah pôsobnosti článku 40 na sledovanie a podávanie správ o zákonnosti spracovania.

Okrem toho na doplnenie článku 24 ods. 4 písm. c) alebo článku 24 ods. 2 písm. e) o plne oprávnených pracovníkoch, ktorí majú prístup k údajom, by sa malo doplniť, že členské štáty by mali zaistiť, aby boli k dispozícii presné profily užívateľov (ktoré by boli k dispozícii národným dozorným orgánom na kontroly). Okrem profilov užívateľa musia členské štáty vypracovať úplný zoznam údajov o totožností užívateľa a stále ho aktualizovať. To isté platí pre Komisiu. Článok 25 ods. 2 písm. b) by sa mal v tomto zmysle preto doplniť.

([1]) Pozri stranu 37 návrhu.

([2]) Hoci definícia kontrolóra v smernici 95/46/ES a nariadení 45/2001 ustanovuje tiež možnosť viacerých kontrolórov s rôznymi zodpovednosťami.

Tieto bezpečnostné opatrenia sú doplnené o sledovanie a organizačné bezpečnostné opatrenia. Článok 28 návrhu opisuje podmienky a účely, na ktoré sa musia uchovávať záznamy všetkých operácií pri spracovaní údajov. Tieto záznamy sa nebudú uchovávať len na účely sledovania ochrany údajov a zaistenia bezpečnosti údajov, ale tiež na vykonávanie samokontroly systému VIS. Správy o samokontrole budú prispievať k účinnému vykonávaniu úloh dozorných orgánov, ktoré budú počas samotného kontrolného postupu schopné zistiť najslabšie miesta a zamerať sa na ne.

3.10. **Práva dotknutých osôb**

3.10.1. *Informácie o dotknutých osobách*

Poskytnutie informácií dotknutej osobe je najdôležitejšie na zabezpečenie spravodlivého spracovania údajov. Predstavuje to nevyhnutnú bezpečnostnú ochranu práv fyzickej osoby. Článok 30 návrhu na tento účel v zásade dodržiava článok 10 smernice 95/46/ES.

Ustanovenie by však pre jeho lepšie začlenenie do rámca systému VIS mohlo využívať niektoré zmeny a doplnenia. Smernica v skutočnosti stanovuje určité informácie, ktoré sa majú poskytovať, ale umožňuje, aby sa v prípade potreby ([1]) poskytlo viac informácií. V dôsledku toho by sa článok 30 mohol zmeniť a doplniť s cieľom zahrnúť tieto body:

— Dotknuté osoby by mali byť tiež informované o dobe uchovávania údajov, ktorá sa uplatňuje na ich údaje.

— Článok 30 ods. 1 písm. c) sa týka „práva na prístup k údajom a práva na opravu údajov“. Bolo by výstižnejšie, keby sa uviedlo „právo na prístup a právo *požiadať* o opravu alebo *vymazanie* údajov“. Dotknuté osoby by mali byť v tejto súvislosti informované o možnosti požiadať o radu alebo pomoc príslušné dozorné orgány.

— Nakoniec v článku 30 ods. 1 písm. a) sa uvádza informácia o totožnosti kontrolóra a jeho prípadného zástupcu. Posledná uvedená možnosť sa nemusí predpokladať u kontrolóra, ktorý sa vždy nachádza na území Európskej únie.

3.10.2. *Právo na prístup, opravu a vymazanie*

V poslednej vete článku 31 ods. 1 sa uvádza, že „takýto prístup k údajom môže udeliť len členský štát“. Je možné predpokladať, že to znamená, že prístup k údajom (alebo prenos údajov) nesmie udeliť centrálna jednotka ale ktorýkoľvek členský štát. EDPS odporúča, aby sa jasne uviedlo, že o prenos údajov sa môže požiadať v ktoromkoľvek členskom štáte.

Okrem toho sa zdá, že navrhnutie tohto ustanovenia znamená tiež to, že prístup nie je možné odmietnuť a bude udelený bez povolenia zodpovedného členského štátu. To by vysvetľovalo, prečo vnútroštátne orgány musia spolupracovať pri presadzovaní práv stanovených v článku 31 ods. 2, 3 a 4 ale nie tých, ktoré sú stanovené v článku 31 ods. 1. ([2]).

3.10.3. *Pomoc dozorných orgánov*

Článok 33.2 stanovuje, že povinnosť vnútroštátnych dozorných orgánov poskytnúť dotknutej osobe pomoc a radu trvá počas celého konania (pred súdom). Význam tohto odseku nie je jasný. Národné dozorné orgány majú rozdielne postoje k svojej úlohe v priebehu súdnych konaní. To znie, ako keby museli zohrávať úlohu poradcu žalobcu na súde, čo v mnohých krajinách nie je možné.

([1]) Uvádza *„akékoľvek ďalšie informácie (...), pokiaľ sú tieto informácie nevyhnutné, so zreteľom na špecifické okolnosti, za ktorých sú údaje zhromažďované, aby sa zaručilo spravodlivé spracovanie vo vzťahu k dotknutej osobe.“*

([2]) V dôsledku toho článok 31 ods. 3 o spolupráci medzi vnútroštátnymi orgánmi pri výkone práv na opravu alebo vymazanie by sa mohol v tomto zmysle pre lepšiu zrozumiteľnosť zmeniť alebo doplniť: „ak je žiadosť, *ako sa uvádza v článku 31 ods. 2*“. Žiadosti uvedené v článku 31 ods. 1 (prístup) nezahrňujú spoluprácu medzi orgánmi.

3.11. **Dohľad**

Návrh rozdeľuje dozornú úlohu medzi národné dozorné orgány a EDPS. Je to v súlade s prístupom návrhu k platnému zákonu a k zodpovednostiam za prevádzku a používanie systému VIS a s potrebou účinného dohľadu. EDPS preto víta tento prístup v článku 34 a 35.

Národné dozorné orgány dohliadajú na zákonnosť pri spracovaní osobných údajov členskými štátmi *vrátane ich prenosu do a zo systému VIS*. EDPS sleduje činnosť Komisie *vrátane toho, či sa prenos osobných údajov medzi vnútroštátnymi používateľskými rozhraniami a centrálnym vízovým informačným systémom uskutočňuje v súlade so zákonom*. Mohli by viesť k prekrývaniu, keďže národný dozorný orgán aj EDPS súčasne zodpovedajú za dohliadanie na zákonnosť prenosu údajov medzi vnútroštátnymi používateľskými rozhraniami a centrálnym vízovým informačným systémom

EDPS preto navrhuje zmenu a doplnenie článku 34 s cieľom vyjasniť, že národné dozorné orgány dohliadajú na zákonnosť spracovania osobných údajov členským štátom vrátane ich prenosu do vnútroštátneho používateľského rozhrania systému VIS a z neho.

Pokiaľ ide o dohľad nad systémom VIS je dôležité tiež zdôrazniť, že dozor nad činnosťami národných dozorných orgánov a EDPS by sa do určitej miery mal koordinovať s cieľom zabezpečiť dostatočnú úroveň zosúladenia a celkovú účinnosť. Skutočne je potrebné zosúladiť vykonávanie nariadenia a ďalej pracovať na spoločnom prístupe k spoločným problémom. Okrem toho, čo sa týka bezpečnosti, môže sa doplniť, že úroveň bezpečnosti systému VIS bude – v konečnom dôsledku – vymedzená podľa úrovne bezpečnosti jeho najslabšieho článku. V tejto súvislosti je potrebné zorganizovať a posilniť spoluprácu medzi EDPS a vnútroštátnymi orgánmi. Článok 35 by mal teda obsahovať ustanovenie, ktoré by stanovilo, že EDPS zvolá aspoň raz ročne zasadnutie všetkých národných dozorných orgánov.

3.12. **Vykonávanie**

Článok 36 ods. 2 nariadenia ustanovuje: „*Opatrenia nevyhnutné na zavedenie funkcií uvedených v odseku 1 po technickej stránke sa prijmú v súlade s postupom uvedeným v článku 39 ods. 2.*“ Článok 39 odkazuje na výbor na pomoc Komisii, ktorý bol vytvorený v decembri 2001 ([1]) a ktorý sa použil v niekoľkých nástrojoch.

Vykonávanie funkcií systému VIS po technickej stránke (súčinnosť s príslušnými orgánmi a s jednotným vzorom víz) predstavuje celý rad možných rozhodujúcich vplyvov na ochranu údajov. Napríklad voľba či zabudovať alebo nezabudovať mikročip do víza, ktorá bude mať vplyv na to, akým spôsobom sa databáza bude používať, ako aj norma vzoru používaného na výmenu biometrických údajov, budú riadiť alebo navrhovať politiku ochrany príslušných údajov. ([2]).

Výber technológií bude mať určujúci vplyv na správne vykonávanie zásady účelu a proporcionality a mal by sa nad nimi súčasne vykonávať dozor. Voľby z technického hľadiska, ktoré majú významný vplyv na ochranu údajov, by sa preto mali prednostne uskutočňovať v súlade so spolurozhodovacím postupom prostredníctvom nariadenia. Nevyhnutné politická kontrola sa môže poskytnúť až potom. Vo všetkých ostatných prípadoch s vplyvom na ochranu údajov by EDPS mal mať možnosť radiť pri výbere alternatív, ktoré si zvolí tento výbor.

3.13. **Interoperabilita**

Interoperabilita je dôležitý a rozhodujúci predpoklad účinnosti rozsiahlych IT systémov, ako je systém VIS. Poskytuje možnosť znížiť celkové náklady vyhovujúcim spôsobom a zabrániť prirodzeným redundanciám nerovnorodých prvkov. Interoperabilita tiež môže prispieť k dosiahnutiu cieľa spoločnej vízovej politiky zavedením tej istej procedurálnej normy do všetkých základných prvkov tejto politiky. Je však dôležité rozlišovať medzi dvoma stupňami interoperability:

— Veľmi žiaduca je interoperabilita medzi členskými štátmi EÚ; žiadosti o víza zaslané orgánmi jedného členského štátu musia byť skutočne interoperabilné so žiadosťami, ktoré zaslali orgány ktoréhokoľvek iného členského štátu.

([1]) Nariadenie Rady č. 2424/2001 zo 6. decembra 2001 o vývoji druhej generácie Schengenského informačného systému (SIS II).

([2]) Návrh pozmeňujúceho a doplňujúceho nariadenia Rady (ES)1683/95 (jednotný vzor víz) v septembri 2003 tiež zahŕňal podobný článok.

— Interoperabilita medzi systémami budovaná na rôzne účely alebo systémami tretej krajiny je podstatne spornejšia.

Spomedzi dostupných bezpečnostných opatrení použitých na obmedzenie účelu systému a na zabránenie „funkčnému prieťahu“ môže použitie technických noriem prispieť k tomuto obmedzeniu. 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 alebo na používanie určitých údajov, mohol získať prístup cez iný informačný systém.

EDPS by chcel v tejto súvislosti poukázať na deklaráciu Rady o boji proti terorizmu z 25. marca 2004, v ktorej sa od Komisie žiada, aby predložila návrhy s cieľom posilniť interoperabilitu a synergie medzi informačnými systémami (SIS, VIS a Eurodac).

Tiež by chcel poukázať na prebiehajúce diskusie ohľadne toho, ktorý orgán by mohol byť v budúcnosti poverený riadením rôznych rozsiahlych systémov (pozri tiež odsek 3.8 tohto stanoviska).

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

4. ZÁVER

4.1. Všeobecné body

1. EPS uznáva, že ďalší vývoj spoločnej vízovej politiky si vyžaduje efektívnu výmenu príslušných údajov. Systém VIS je jeden z mechanizmov, ktorý môže zabezpečiť hladký tok informácií. EDPS vzal plne na vedomie dôkaz uvedený v štúdii EIA. Hoci tento dôkaz nie úplne dostačujúci, zdá sa, že existujú dostačujúce dôvody na odôvodnenie zriadenia systému VIS na účely zlepšenia spoločnej vízovej politiky.

   Tento nový nástroj by sa však mal obmedziť na zhromažďovanie a výmenu údajov, pokiaľ je toto zhromažďovanie alebo výmena nevyhnutná pre rozvoj spoločnej vízovej politiky a pokiaľ je úmerná tomuto cieľu.

2. Zriadenie systému VIS môže mať priaznivé následky pre iné oprávnené verejné záujmy, ale to nemení účel systému VIS. Všetky prvky systému musia preto byť nevyhnutné a úmerné nástroje na dosiahnutie uvedeného politického cieľa. Okrem toho:

   — Bežný prístup orgánov činných v trestnom konaní by nebol v súlade s týmto účelom.

   — EDPS odporúča, aby sa rozlišovanie medzi „účelom“ a „výhodami“ v znení článku 1 ods. 2, robilo jasnejšie.

   — Interoperabilita s inými systémami sa nemôže zavádzať v rozpore so zásadou obmedzujúcou účel.

3. EDPS uznáva výhody využívania biometrických údajov, ale zdôrazňuje veľký vplyv využívania týchto údajov a navrhuje zavedenie prísnejších bezpečnostných opatrení na využívanie biometrických údajov. Okrem toho technická nedokonalosť odtlačkov prstov vyžaduje, aby sa vypracovali zálohové postupy a aby sa zahrnuli do návrhu.

4. Súčasné stanovisko by sa malo uviesť v preambule nariadenia pred odôvodneniami („so zreteľom na stanovisko ...“).

4.2. **Ostatné body**

5. K dôvodom neudelenia víz: by sa mal zahrnúť odkaz na článok 29 smernice 2004/58/ES do znenia návrhu s cieľom zaistiť, aby sa „ohrozenie verejného zdravia“ chápalo so zreteľom na toto ustanovenie.

6. Údaje o členoch skupiny majú v návrhu osobitný význam: preto by sa mala uviesť presná a úplná definícia „členov skupiny“.

7. Neexistuje dôkaz o tom, že politická voľba o odklade uchovávania údajov v tomto návrhu je neodôvodnená, alebo že by mala neprijateľné dôsledky, za predpokladu, že sa zavedú všetky vhodné opravné mechanizmy.

   Okrem toho by sa v návrhu malo jasne uviesť, že pri každej novej žiadosti o víza sa musia osobné údaje úplne prehodnotiť.

8. Ku kontrole víz na vonkajších hraniciach: mal by sa zmeniť a doplniť článok 16 návrhu, pretože prístup k centrálnej databáze systému VIS by bol v týchto prípadoch neprimeraný. Výhradný prístup príslušných orgánov k chránenému mikročipu na vykonanie kontrol víz je dostatočný.

   Okrem toho, ak totožnosť bola úspešne overená, vôbec nie je jasné, z akého dôvodu je ešte potrebný zvyšok týchto údajov.

9. K použitiu údajov pri identifikácii a navracaní nelegálnych migrantov a pri azylových konaniach: „fotografie“ by sa mali odstrániť z prvej časti článkov 17, 18 a 19 a mali by sa ponechať v druhej časti.

10. K zodpovednosti Komisie a členských štátov: V článku 23 by sa mal vypustiť odsek 2.

11. Do návrhu by sa mali doplniť ustanovenia o systematickej samokontrole bezpečnostných opatrení. Rozsah článku 40 sa musí rozšíriť na sledovanie zákonnosti spracovania a podávanie správ. Okrem toho:

   — členské štáty musia vypracovať úplný zoznam údajov o totožnosti užívateľa a stále ho musia aktualizovať. To isté platí pre Komisiu: Článok 25 ods. 2 písm. b) by sa mal preto v tomto zmysle preto doplniť.

   — Článok 28 návrhu opisuje podmienky a účely, na ktoré sa musia uchovávať záznamy všetkých operácií pri spracovaní údajov. Tieto záznamy sa nebudú uchovávať len na účely sledovania ochrany údajov a zaistenia bezpečnosti údajov, ale tiež na vykonávanie pravidelnej samokontroly systému VIS.

12. K právam dotknutých osôb:

   — Článok 30 by sa mal zmeniť a doplniť s cieľom zabezpečiť, aby boli dotknuté osoby tiež informované o dobe uchovávania údajov, ktorá sa uplatňuje na ich údaje.

   — V článku 30 ods. 1 písm. e) by sa malo uviesť „právo na prístup k údajom a právo požadovať opravu alebo vymazanie údajov“.

   — V článku 31 ods. 1 sa musí jasne uviesť, že o určité prenosy sa môže požiadať v ktoromkoľvek členskom štáte.

13. K dohľadu:

— článok 34 by sa mal zmeniť a doplniť s cieľom vyjasniť, že národné dozorné orgány dohliadajú na zákonnosť spracovania osobných údajov členským štátom vrátane ich prenosu do vnútroštátneho používateľského rozhrania systému VIS a z neho.

— Článok 35 by mal teda obsahovať ustanovenie, ktoré by stanovilo, že EDPS zvolá aspoň raz ročne zasadnutie všetkých národných dozorných orgánov.

14. K vykonávaniu:

— voľby z technického hľadiska, ktoré majú významný vplyv na ochranu údajov, by sa preto mali prednostne uskutočňovať v súlade so spolurozhodovacím postupom prostredníctvom nariadenia.

— V ostatných prípadoch by mal mať EDPS možnosť radiť pri výbere alternatív, ktoré si zvolí tento výbor.

V Bruseli 23. marca 2005

Peter HUSTINX

Európsky dozorný úradník pre ochranu údajov