EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

Stanovisko Evropského inspektora ochrany údajů k návrhu nařízení Evropského parlamentu a Rady o vízovém informačním systému (VIS) a výměně údajů o krátkodobých vízech mezi členskými státy (KOM(2004)835 v konečném znění)

(2005/C 181/06)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na článek 286 této smlouvy,

s ohledem na Listinu základních práv Evropské unie, a zejména na článek 8 této listiny,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů,

s ohledem na nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, a zejména na článek 41 tohoto nařízení,

s ohledem na žádost o stanovisko v souladu s čl. 28 odst. 2 nařízení (ES) č. 45/2001 obdržené od Komise dne 25. ledna 2005,

ZAUJAL TOTO STANOVISKO:

1. ÚVOD

1.1 Předběžné poznámky

Zavedení vízového informačního systému (VIS) představuje významnou součást společné vízové politiky EU a je předmětem několika nástrojů, které jsou vzájemně propojené.

— V dubnu roku 2003 byla předložena studie proveditelnosti ([1]) o VIS zadaná Komisí.

— V září roku 2003 Komise navrhla změnu ([2]) dosud platného nařízení, kterým se stanoví jednotný formát víz. Hlavním cílem bylo zavést v novém vízovém formátu biometrické údaje (zobrazení obličeje a dva otisky prstů). Tyto biometrické údaje by byly uloženy na mikročipu.

([1]) Vízový informační systém, konečná zpráva zadaná EK a provedená firmou Trasys v dubnu 2003.
([2]) KOM(2003)558 v konečném znění spolu s 2003/0217 (CNS) a 2003/0218 (CNS).

— V červnu roku 2004 začal rozhodnutím Rady ([1]) proces budování vízového informačního systému poskytující právní základnu pro jeho zahrnutí do rozpočtu EU. Toto rozhodnutí navrhuje centrální databázi obsahující informace související se žádostí o vízum a předpokládá postup „projednávání ve výborech“ v zájmu zvládnutí technického vývoje VIS.

V prosinci roku 2004 Komise přijala návrh nařízení o VIS a o výměně údajů o krátkodobých vízech mezi členskými státy ([2]) (dále jen „návrh“), který je předmětem tohoto stanoviska. K návrhu je připojena studie rozšířeného posouzení dopadů ([3]) (dále jen „RPD“).

Jak je však uvedeno v odůvodnění této studie, budou pro doplnění tohoto nařízení potřebné další právní nástroje, zejména v zájmu:

— změny společných konsulárních pokynů k vízům pro diplomatické mise a konzulární místa ve smluvních stranách k Schengenské úmluvě (dále jen „společné konsulární pokyny“), související se zavedením biometrických údajů do příslušných postupů;

— vypracování nového mechanismu pro výměnu údajů s Irskem a Spojeným královstvím;

— výměnu údajů o dlouhodobých vízech.

Jak rozhodla Rada ve složení pro spravedlnost a vnitřní věci na zasedání ve dnech 5. – 6. června 2003 a jak bylo uvedeno v čl. 1 odst. 2 výše uvedeného rozhodnutí Rady z června 2004, VIS bude založen na centralizované struktuře obsahující databázi, ve které budou uloženy složky s žádostmi o víza: na centrálním vízovém informačním systému (CS-VIS) a národním rozhraní (NI-VIS) umístěném v jednotlivých členských státech. Členské státy určí ([4]) centrální národní orgán spojený s národním rozhraním, jehož prostřednictvím budou mít jejich příslušné orgány přístup k CS-VIS.

1.2 **Hlavní prvky návrhu z hlediska ochrany údajů**

Cílem návrhu je zlepšit správu společné vízové politiky tím, že zřízením centrální databáze usnadní výměnu údajů mezi členskými státy. Nařízení předpokládá zavedení biometrických údajů (fotografie a otisky prstů) v rámci postupu podávání žádosti a jejich uložení v centrální databázi.

Biometrické údaje by mohly být využity ve vízové samolepce, jak to již bylo zamýšleno v pozměňujícím nařízení navrženém Komisí o jednotném formátu víza se zavedením fotografie a otisků prstů, uložených na mikročipu (dosud se čeká na rozhodnutí Rady založené na výsledcích probíhajících analýz).

Návrh podrobně popisuje různé operace prováděné s údaji (zanášení, pozměňování, výmaz a nahlížení) a různé údaje doplňované do VIS v závislosti na stavu žádosti (přijetí, odmítnutí atd.).

Návrh umožňuje dobu uchovávání v délce pěti let pro údaje týkající se jednotlivých žádostí.

Návrh uvádí restriktivním způsobem příslušné orgány jiné než vízové, které budou mít přístup k VIS, a definuje jim udělená práva přístupu.

— příslušné orgány pro provádění vízových kontrol na vnějších hranicích a uvnitř území členských států

— příslušné imigrační orgány

([1]) 2004/512/ES, Úř. věst. L 213, 15.6.2004, s. 5.
([2]) KOM(2004) 835 v konečném znění 2004/0287 (COD)
([3]) Studie rozšířeného posouzení dopadů vízového informačního systému, konečná zpráva Evropského konsorcia pro vyhodnocování politik z prosince 2004.
([4]) Článek 24 odst. 2 návrhu.

— příslušné azylové orgány

Při popisu fungování VIS a souvisejících odpovědností návrh zdůrazňuje, že Komise zpracovává údaje z VIS jménem členských států. Popisuje potřebu využívání záznamů ze zpracování dat v zájmu zabezpečení bezpečnosti údajů, jakož i podrobnosti konkrétních odpovědností v zájmu dosažení takové úrovně bezpečnosti.

Návrh obsahuje kapitolu o ochraně údajů, v níž jsou podrobně popsány úlohy národních orgánů i evropského inspektora ochrany údajů (dále jen „EIOÚ“).

Návrh svěřuje technické provádění VIS a výběr nezbytných technologií výboru zřízenému podle čl. 5 odst. 1 nařízení (ES) č. 2424/2001 o vývoji Schengenského informačního systému druhé generace (SIS II).

Rozšířené posouzení dopadů VIS zadané Komisí a prováděné EPEC je přiloženo k návrhu. Došlo se v něm k závěru, že varianta VIS podporovaného využíváním biometrie je pro zlepšení společné vízové politiky nejlepším dostupným řešením.

2. **PODSTATNÝ RÁMEC**

Návrh bude mít závažný dopad na soukromí a jiná základní práva jednotlivců; z tohoto důvodu je předmětem kontroly z hlediska dodržování zásad ochrany údajů. Hlavní body našeho zkoumání jsou tyto:

— respektování soukromého života je v Evropě zabezpečeno od přijetí Úmluvy o ochraně lidských práv a základních svobod (dále jen „Evropská úmluva“) Radou Evropy. Článek 8 Evropské úmluvy stanoví „právo na respektování soukromého a rodinného života“.

Podle čl. 8 odst. 2 je jakékoli porušení výkonu tohoto práva veřejným orgánem povoleno pouze v případě, že je „v souladu se zákonem“ a je „v demokratické společnosti nezbytné“ pro ochranu důležitých zájmů. V judikatuře Evropského soudu pro lidská práva vedly tyto podmínky k dodatečným požadavkům týkajícím se kvality právního základu pro porušení, přiměřenosti jakéhokoli opatření a potřeby vhodných ochranných opatření proti zneužití.

Základní zásady pro ochranu fyzických osob s ohledem na zpracování osobních údajů byly uvedeny v úmluvě o ochraně údajů vypracované Radou Evropy a přijaté v roce 1981.

— Právo na respektování soukromého života a ochranu osobních údajů bylo stanoveno nedávno v článcích 7 a 8 Listiny základních práv Evropské unie, která byla začleněna do části II nové Ústavy EU.

Podle článku 52 Listiny se uznává, že tato práva mohou být předmětem omezení za předpokladu, že jsou splněny podobné podmínky, jako podle článku 8 Evropské úmluvy. Tyto podmínky je nutno zvážit vždy, když je vyhodnocován nějaký návrh na případný zásah do těchto práv.

V rámci současných právních předpisech EU jsou základní pravidla o ochraně údajů vymezena těmito předpisy:

— Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. L 281, s. 31). Tato směrnice bude dále uváděna jako „směrnice 95/46/ES“. Směrnice stanovuje podrobné zásady, podle kterých se návrh kontroluje v takovém rozsahu, v jakém je uplatňován na členské státy. Toto je tím podstatnější, že návrh bude platit současně s vnitrostátními právními předpisy, které směrnici budou provádět. Účinnost navrhovaných ustanovení a ochranných opatření bude tedy v každém jednotlivém případě záležet na účinnosti uvedené kombinace.

— Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (Úř. věst. L 8, s. 1). Toto nařízení bude dále uváděno jako „nařízení 45/2001". Uvádí podobné zásady jako směrnice 95/46/ES a je v tomto ohledu podstatná do té míry, do jaké se návrh uplatní na činnost Komise, spolu s ustanoveními tohoto nařízení. I tato kombinace proto zaslouhuje určitou pozornost.

Směrnice 95/46/ES a nařízení 45/2001 musí být vykládány společně s jinými nástroji. Jinými slovy musí být uvedená směrnice a uvedené nařízení – do té míry, do jaké se týkají zpracování osobních údajů, jež by mohly porušit základní svobody, zejména práva na soukromí – vykládány s ohledem na základní práva. Toto rovněž vyplývá z judikatury Evropského soudního dvora ([1]).

— EIOÚ nakonec zahrne rovněž svou analýzu stanoviska č. 7/2004 ze dne 11. srpna 2004 pracovní skupiny pro ochranu údajů zřízené podle článku 29 ([2])„o zahrnutí biometrických prvků v povoleních k pobytu a vízech, zohledňujícím zavedení Evropského informačního vízového systému (VIS)". Ve svém stanovisku vyjádřila pracovní skupina obavy ohledně několika prvků návrhu. EIOÚ má v úmyslu ověřit, zda a jakým způsobem návrh tyto obavy zohlednil.

3. ANALÝZA NÁVRHU

3.1 Obecně

EIOÚ uznává, že další vývoj společné vízové politiky vyžaduje efektivní výměnu podstatných údajů. Jedním z mechanismů, který by mohl zajistit plynulý tok informací, je VIS. Takový nový nástroj by však měl být omezen na shromažďování a výměnu údajů, pokud jsou takové shromažďování nebo výměna nutné pro rozvoj společné vízové politiky a přiměřené tomuto cíli.

Zřízení VIS může mít pozitivní důsledky pro jiné oprávněné veřejné zájmy, avšak to nic nemění na smyslu VIS. Omezený účel systému hraje důležitou úlohu při určování oprávněné náplně obsahu a využití systému, a tedy i hlavní úlohu při udělování práva přístupu k VIS (nebo k některým z informací v něm obsažených) orgánům členských států v případech oprávněných veřejných zájmů.

Návrh navíc zavádí používání biometrických údajů ve VIS. EIOÚ uznává výhody používání biometrie, avšak zdůrazňuje velmi významný dopad používání takových údajů a navrhuje vložení přísných ochranných opatření pro využití biometrických údajů.

Toto stanovisko je třeba vykládat s ohledem na uvedené hlavní důvody. Je zřejmé, že toto stanovisko by mělo být zmíněno v preambuli nařízení před body odůvodnění („s ohledem na stanovisko…").

([1]) V této souvislosti je užitečné odkázat na rozhodnutí Soudního dvora v případě Österreichischer Rundfunk a ostatní (Společné případy C-465/00, C-138/01 a C-139/01, rozsudek ze dne 20. května 2003 soudu zasedajícího v plénu, (2003) Sb. rozh. I-4989). Dvůr rozhodoval o rakouském zákonu umožňujícím předávání podrobných informací o mzdách zaměstnanců ve veřejném sektoru rakouskému účetnímu dvoru a jejich následné zveřejnění. Ve svém rozhodnutí Dvůr stanovuje řadu kritérií čerpaných z článku 8 Evropské úmluvy o lidských právech, která by měla být používána při provádění směrnice 95/46/ES, pokud tato směrnice umožňuje určitá omezení práva na soukromí.

([2]) Jde o nezávislou poradní skupinu složenou ze zástupců orgánů členských států v oblasti ochrany údajů, EIOÚ a Komise, která byla zřízena směrnicí 95/46/ES.

3.2 **Účel**

Účel VIS je nanejvýš důležitý, jak ve světle článku 8 Evropské úmluvy, tak obecného rámce ochrany údajů. Podle článku 6 směrnice 95/46/ES musí být osobní údaje „shromažďovány pro stanovené účely, výslovně vyjádřené a legitimní, a nesmějí být dále zpracovávány způsobem neslučitelným s těmito účely." Pouze jasná definice účelů umožní správné vyhodnocení přiměřenosti a dostatečnosti zpracování osobních údajů, což je kritické vzhledem k povaze údajů (včetně biometrie) a rozsahu zamýšleného zpracovávání.

Účel VIS je jasně uveden v čl. 1 odst. 2 návrhu:

„VIS zlepší správu společné vízové politiky, konzulární spolupráci a konzultaci mezi ústředními konzulárními úřady tím, že usnadní výměnu údajů mezi členskými státy o žádostech a o rozhodnutích o těchto žádostech".

Všechny složky VIS musí být proto nezbytně nutnými a přiměřenými nástroji pro dosažení tohoto politického cíle v zájmu společné vízové politiky.

Článek 1 odst. 2 návrhu rovněž uvádí další přínosy zlepšení vízové politiky, jako jsou:

a) předcházení ohrožení pro vnitřní bezpečnost,

b) usnadnění boje proti podvodům,

c) usnadnění kontrol na kontrolních stanovištích na vnějších hranicích.

EIOÚ považuje tyto prvky za příklady pozitivních dopadů zřízení VIS a zlepšení společné vízové politiky, avšak nepovažuje je za samúčelné.

V této fázi to přináší dva důležité dopady:

— EIOÚ si je vědom že donucovací orgány mají zájem na tom, aby jim byl udělen přístup k VIS; v tomto smyslu byly přijaty závěry Rady dne 7. března 2005. Jelikož účelem VIS je zlepšení společné vízové politiky, je třeba poznamenat, že běžný přístup ze strany donucovacích orgánů by nebyl v souladu s tímto účelem. I když podle článku 13 směrnice 95/46/ES by mohl být takový přístup umožněn *ad hoc* za zvláštních okolností a při použití vhodných ochranných opatření, systematický přístup není možné povolit.

  V obecnější rovině je nezbytně nutné provést hodnocení přiměřenosti a nutnosti, mají-li se v budoucnosti přijmout rozhodnutí o tom, zda umožnit některým jiným orgánům přístup k VIS. Účely, pro které se přístup povolí, musí být v souladu s účely VIS.

— Výslovná zmínka o „předcházení ohrožení vnitřní bezpečnosti členských států" v písmenu a) není formulována šťastně. Hlavními přínosy VIS budou zabraňování podvodů a současného podávání žádostí o víza do více členských států (boj proti podvodům je rovněž hlavním důvodem pro zahrnutí biometrie do systému) ([1]). Předcházení ohrožení bezpečnosti by proto mělo být bráno v úvahu jako „druhotný", i když velmi vítaný, přínos.

  EIOÚ doporučuje, aby rozlišení mezi účelem a přínosem bylo v textu čl. 1 odst. 2 uvedeno výslovněji, např. takto:

  „Účelem VIS je zlepšení správy společné vízové politiky, konzulární spolupráce a konzultací mezi ústředními konzulárními úřady prostřednictvím usnadnění výměny údajů o žádostech a o rozhodnutích o těchto žádostech mezi členskými státy. To rovněž přispěje…"

([1]) Ve studii EIA je toto uvedeno velmi jasně (s. 6 § 2.7): „výsledkem nedostatků v boji proti současnému podávání žádostí o vízum do více členských států a podvodům a při provádění kontrol rovněž vedou k nedostatkům pokud jde o vnitřní bezpečnost členských států". Z toho plyne, že ohrožení bezpečnosti je zčásti způsobováno neefektivní vízovou politikou. První věcí, kterou je v tomto ohledu třeba udělat, je zlepšit vízovou politiku, především bojem proti podvodům a prováděním lepších kontrol. Zlepšení v oblasti bezpečnosti bude výsledkem zlepšení vízové politiky.

Je rovněž namístě v tomto ohledu zmínit, že předcházení ohrožení vnitřní bezpečnosti bylo uvedeno na posledním místě „Hlavních zásad pro zavedení společného systému pro výměnu vízových údajů" přijatých Radou ve složení pro spravedlnost a vnitřní věci dne 13. června 2002. ([1]) Bylo by to rovněž možné a mnohem více v souladu s účelem VIS.

3.3 **Kvalita údajů**

Podle článku 6 směrnice 95/46/ES musí být osobní údaje „dostatečné, podstatné a nepřesahující míru ve vztahu k účelům, pro které jsou shromažďovány a/nebo dále zpracovávány." Toto se týká přiměřenosti VIS jako takového, avšak i údajů, které mají být shromažďovány a uchovávány ve VIS, a jejich dalšího využívání, jakož i dodatečných ochranných opatření, které se v tomto směru použijí. Tyto prvky jsou stejně důležité pro vyhodnocení návrhu ve světle článku 8 Evropské úmluvy.

Zřízení VIS představuje nepochybně významné narušení výkonu práva na soukromí, už jen s ohledem na rozsah tohoto systému a na kategorie zpracovávaných osobních údajů. Pracovní skupina zřízená podle článku 29 se ve svém stanovisku č. 7/2004 dotázala, zda „existují studie rozsahu a závažnosti těchto faktorů uvádějící přesvědčivé důvody veřejné bezpečnosti nebo veřejného pořádku, které by odůvodňovaly takový přístup".

EIOÚpečlivě zaznamenal podkladový materiál předložený v RPD. I když podkladové materiály nedovolují učinit zcela jednoznačné závěry, zřejmě existují dostatečné důvody pro zřízení VIS za účelem zlepšení společné vízové politiky.

V tomto směru by se mohlo zdát, že je na legislativních orgánech, aby se rozhodly o zřízení VIS jako nástroje pro zlepšení podmínek při vydávání víz členskými státy. Takový systém by sám o sobě příznivě doplňoval a podporoval postupné vytváření prostoru svobody, bezpečnosti a práva předpokládané Smlouvou o ES.

Avšak výsledkem zřízení a používání VIS by nikdy nemělo být to, že by v této oblasti již nebylo možné zajišťovat vysokou úroveň ochrany osobních údajů. Patří k poradním úkolům EIOÚS vyhodnotit, do jaké míry VIS ovlivní současnou úroveň ochrany údajů dotyčných osob.

Berouce toto v úvahu, EIOÚse ve svém stanovisku zaměří na tyto otázky:

— přiměřenost a vhodnost údajů a jejich použití (např. kategorie údajů, přístup k údajům jednotlivými příslušnými orgány a období uchovávání údajů);

— fungování systému (např. povinnosti a bezpečnost);

— práva dotyčných osob (např. informování, možnost opravy nebo výmazu nepřesných nebo nepodstatných údajů);

— monitorování systému a dohled nad ním.

Kromě dále uvedených odstavců z návrhu nevyplývá nutnost důležitých poznámek, pokud jde o kategorie údajů, které mají být zahrnuty do VIS, a jejich používání. Podstatná ustanovení byla vypracována s náležitou péčí a jako celek se zdají být důsledná a přiměřená.

([1]) Rámcové rozhodnutí rady ze dne 13. června 2002 o boji proti terorismu (2002/475/SVV), Úř. věst. L 164, 22.6.2002, s. 3.

3.4 **Biometrie**

3.4.1 *Dopad použití biometrie*

Použití biometrie v informačních systémech nepředstavuje v žádném případě bezvýznamnou volbu, zejména pokud se daný systém týká tak obrovského množství osob. Biometrie nepředstavuje jen další informační technologii. Biometrické údaje nezvratně mění vztah mezi tělem jedince a jeho totožností tím, že některé vlastnosti lidského těla se díky nim stávají „strojově čitelnými" a předmětem dalšího využití. I když biometrické charakteristiky nebudou čitelné lidským okem, je možné je číst a využívat vhodnými nástroji, a to navždy, kdekoli se daná osoba octne.

Bez ohledu na to, jak může být biometrie pro určité účely užitečná, její široké využívání bude mít velmi významný dopad na společnost a mělo by být předmětem široké a otevřené diskuse. EIOÚ je nucen konstatovat, že se taková diskuse do vypracování návrhu fakticky nekonala. Toto ještě více podtrhuje nutnost přísných ochranných opatření pro používání biometrických údajů a pro pečlivé zvažování a diskusi v rámci legislativního procesu.

3.4.2 *Zvláštní povaha biometrie*

Jak již bylo zdůrazněno v několika stanoviscích pracovní skupiny zřízené podle článku 29 ([1]), zavedení a zpracovávání biometrických údajů pro dokumenty související se zjišťováním totožnosti je nutno zabezpečit zvláště důslednými a vážnými ochrannými opatřeními. Biometrické údaje jsou skutečně vysoce citlivé s ohledem na několik zvláštních vlastností.

Je skutečností, že u dané osoby je ztráta biometrických údajů téměř nemožná, na rozdíl od hesla nebo klíče. Biometrické údaje umožňují téměř *absolutní rozlišitelnost*, tj. každá osoba má ojedinělou biometrii. Ty se v průběhu života osoby téměř nikdy nezmění, což poskytuje těmto charakteristikám *stálost*. Každý má stejné fyzické „prvky", což rovněž dává biometrii rozměr *univerzálnosti*.

Změna biometrického údaje je přitom téměř nemožná: prst nebo tvář je obtížné změnit. Tato z mnoha ohledů pozitivní charakteristika vede k významnému problému v případě *krádeže totožnosti*: uchovávání otisků prstů a fotografií v databázi odkazujících na odcizený průkaz totožnosti by mohlo vést k závažným a trvalým problémům pro skutečného nositele takové totožnosti. Biometrické údaje navíc ve své podstatě *nejsou tajné* a mohou dokonce *zanechávat stopy* (otisky prstů, DNA), což umožňuje shromažďování takových údajů, *aniž by si toho jejich nositel byl vědom*.

S ohledem na uvedená rizika, jež vyplývají z povahy biometrie, bude nutno zavést důležitá ochranná opatření (zejména pokud jde o respektování zásady omezeného účelu, o omezení přístupu a o bezpečnostní opatření).

3.4.3. *Technická nedokonalost otisků prstů*

Hlavní výhody biometrie popsané výše (univerzálnost údajů a jejich rozlišitelnost, stálost a použitelnost atd.) nejsou nikdy absolutní. To má přímý dopad na efektivitu postupů plánovaných v nařízení, týkajících se zanášení biometrických údajů a jejich ověřování.

Odhaduje se ([2]), že až 5 % lidí se nebude moci zúčastnit (protože nemají čitelné otisky prstů nebo je nemají vůbec). V RDP v příloze k návrhu počítá s okolo 20 milióny žadatelů o vízum v r. 2007, což znamená, že až 1 milión osob se nebude moci zúčastnit „normálního" postupu zanášení údajů se zřejmými následky pro žádost o vízum a při hraničních kontrolách.

([1]) Stanovisko 7/2004 o zahrnutí biometrických prvků v povoleních k pobytu a vízech zohledňující zavedení Evropského informačního vízového systému (VIS) (Markt/11487/04/EN - WP 96) a pracovní dokument o biometrických údajích (MARKT/10595/03/EN - WP 80).

([2]) A. Sasse, *Cybertrust and CrimePrevention:Usability and Trust in Information Systems*, v „Foresight cybertrust and crime prevention project") 04/1151, 10. června 2004, s. 7, a Technology Assessment, „Using Biometrics for Border Security", United States General Accounting Office, GAO-03-174, listopad 2002.

Biometrické zjišťování totožnosti je rovněž svou podstatou statistický proces. Běžně se vyskytuje chybovost 0,5 až 1 % ([1]), což znamená, že kontrolní systém na vnějších hranicích bude mít míru chybného odmítnutí (False Rejection Rate, FRR) ve výši 0,5 až 1 %. Tato míra závisí na prahu založeném na politice rizik prováděné příslušnými orgány (odpovídající vyváženosti dosažené mezi počtem osob neprávem odmítnutých a osob neprávem přijatých). Prohlášení uvedené v 9. bodu odůvodnění navrhovaného nařízení o tom, že tyto technologie nabízejí „přesné zjištění totožnosti" dotyčné osoby je proto přehnané.

Podle nedávné výhledové studie ([2]) zadané Výborem pro občanské svobody, spravedlnost a vnitřní věci (LIBE) Evropského parlamentu by měly být k dispozici *záložní postupy* představující významná ochranná opatření pro zavádění biometrie, která není ani přístupná pro všechny, ani úplně přesná. Takové postupy by měly být zavedeny a používány v zájmu respektování důstojnosti osob, která nejsou schopny účastnit se úspěšně procesu zanášení údajů, a taktéž aby se na ně nepřenášela odpovědnost za nedokonalost systému. ([3]).

EIOÚ proto doporučuje, aby byly vypracovány a do návrhu zahrnuty záložní postupy. Tyto postupy by neměly snižovat úroveň bezpečnosti vízové politiky, ani stigmatizovat osobu s nečitelnými otisky prstů.

3.5 **Zvláštní kategorie údajů**

Některé kategorie údajů (mimo biometrické údaje) je třeba zvlášť zohlednit: údaje týkající se důvodů odmítnutí víza (3.5.1) a údaje související s ostatními členy skupiny žadatelů (3.5.2).

3.5.1 *Důvody odmítnutí víza*

Článek 10 odst. 2 obsahuje ustanovení pro zpracování údajů týkajících se důvodů odmítnutí, pokud bylo přijato rozhodnutí o odmítnutí víza. Důvody odmítnutí jsou plně standardizované.

— První dva důvody uvedené v písmenech a) a b) jsou spíše administrativní povahy: nepředložení platného cestovního dokumentu nebo platných dokumentů uvádějících účel a podmínky zamýšleného pobytu.

— písmeno c) uvádí „žadatel je veden jako osoba, které má být odepřen vstup", z čehož vyplývá, že bylo nahlédnuto do databáze SIS.

— písmeno d) pak uvádí jako důvod pro odmítnutí víza skutečnost, že žadatel „představuje hrozbu pro veřejný pořádek, vnitřní bezpečnost, veřejné zdraví nebo mezinárodní vztahy kteréhokoli z členských států".

([1])

Biometrie	tvář	prst	duhovka
FTE % neúspěch při zanášení údajů	údaje nedostupné	4	7
FNMR % míra odmítnutí	4	2,5	6
FMR1 % chybovost ověřování shody	10	< 0,01	< 0,001
FMR2 % chybovost v stanovení totožnostipro dB o velikosti > 1 m	40	0,1	údaje nedostupné
FMR3 % chybovost shody při hromadných kontrolách pro dB o velikosti = 500	12	< 1	údaje nedostupné

A. K. Jain a jiní, *Biometrie: Velká výzva*, Rozpravy mezinárodní konference o rozpoznávání obrazců, Cambridge, UK., srpen 2004

([2]) *Biometrie na hranicích: hodnocení dopadu na společnost*, únor 2005, Institute for Prospective Technological Studies, DG Společné výzkumné středisko, ES.

([3]) *Zpráva o pokroku v používání zásad Úmluvy 108 o shromažďování a zpracovávání biometrických údajů, Rada Evropy*, 2005, s. 11.

Všechny důvody pro odmítnutí musí být použity s velkou obezřetností s ohledem na následky, jaké to může pro osobu mít. Některé z nich, konkrétně důvody uvedené v písmenech c) a d), navíc povedou ke zpracování „citlivých údajů" ve smyslu článku 8 směrnice 95/46/ES.

EIOÚ by rád upozornil konkrétněji na podmínku související s veřejným zdravím, která se zdá být neurčitá a zahrnuje zpracování velmi citlivých údajů. Podle komentáře k článkům připojeným k návrhu se odkaz na ohrožení veřejného zdraví zakládá na „návrhu nařízení Rady, kterým se zřizuje zákoník Společenství o pravidlech pro řízení pohybu osob přes hranice" (KOM (2004)391 v konečném znění).

EIOÚ si je vědom, že „veřejné zdraví" je kritérium široce používané v právu Společenství týkajícím se volného pohybu osob a je uplatňováno velmi přísně, jak ukazuje směrnice Evropského parlamentu a Rady 2004/38/ES ze dne 29. dubna 2004 o právu občanů Unie a jejich rodinných příslušníků svobodně se pohybovat a pobývat uvnitř území členských států. Článek 29 uvedené směrnice stanoví podmínky pro zohlednění ohrožení veřejného zdraví: „Jedinými nemocemi, které odůvodňují opatření omezující svobodu pohybu, jsou výhradně nemoci s epidemickým potenciálem definované příslušnými předpisy Světové zdravotnické organizace a ostatní nakažlivé nemoci a nakažlivé parazitické nemoci, pokud se na ně vztahují ochranná opatření používaná na státní příslušníky hostitelského členského státu."

— Je však třeba poznamenat, že výše uvedený návrh dosud zůstává pouhým návrhem a zahrnutí podmínky nepředstavovat ohrožení veřejného zdraví do nařízení o VIS je podmíněno přijetím zákoníku Společenství.

— Pokud bude tento důvod pro odmítnutí vstupu přijat, měl by však být vykládán restriktivně. Návrh zákoníku Společenství je samotný založen na právě zmíněné směrnici 2004/38/ES.

EIOÚ proto doporučuje, aby znění návrhu obsahovalo odkaz na článek 29 směrnice 2004/38/ES v zájmu jistoty, že pojem „ohrožení veřejného zdraví" je chápán s ohledem na toto ustanovení. V každém případě, vezmeme-li v úvahu citlivost údajů, tyto by měly být zpracovány pouze je-li ohrožení veřejného zdraví opravdové, aktuální a dostatečně závažné.

3.5.2 *Údaje o jiných členech skupiny*

V článku 2 odst. 7 jsou „členové skupiny" definováni jako „ostatní žadatelé, se kterými žadatel cestuje společně, včetně manžela (manželky) a dětí doprovázejících žadatele". Komentář k článkům uvádí, že definice v článku 2 návrhu odkazují na Smlouvu nebo Schengenské acquis o vízové politice, kromě některých výrazů, jako „členové skupiny" – definovaných konkrétně pro účely tohoto nařízení. Proto je možné předpokládat, že tato definice neodkazuje na definici „skupinového víza" uvedenou v článku 2.1.4 Společných konzulárních instrukcí. Komentář k článkům odkazuje na „žadatele cestující ve skupině s ostatními žadateli, např. v rámci dohody o statusu schváleného místa určení, nebo spolu s členy rodiny".

EIOÚ zdůrazňuje, že v nařízení by mělo být uvedeno přesné a úplné vymezení pojmu „členové skupiny". Pokud jde o současný návrh, EIOÚ je nucen s ohledem na chybějící přesný odkaz na Smlouvu nebo schengenské acquis konstatovat, že definice je příliš neurčitá. Podle uvedeného znění by výraz „členové skupiny" mohl zahrnovat spolupracovníky, jiné zákazníky stejné cestovní kanceláře účastnící se organizovaného výletu atd. Důsledky jsou opravdu velmi závažné:

podle článku 5 návrhu nařízení bude dokumentace k žádosti žadatele spojena s dokumentací žádostí ostatních členů skupiny.

3.6 **Uchovávání údajů**

Článek 20 návrhu nařízení stanovuje, že dokumentace ke každé žádosti má být uchovávána pro dobu pěti let. Stanovení rozumné časové lhůty je věcí politického rozhodnutí zákonodárných orgánů Společenství.

Nic nenasvědčuje tomu – zejména s ohledem na důvody uvedené v komentáři k článkům – že by politické rozhodnutí přijaté v tomto návrhu bylo nepřiměřené nebo by mělo nepřijatelné následky, pokud budou uplatněny veškeré vhodné opravné mechanismy. To znamená, že bude muset být zajištěna oprava nebo výmaz údajů, pokud již údaje nejsou přesné a zejména pokud osoba získala státní příslušnost členského státu nebo získala postavení, které nevyžaduje její zahrnutí do systému.

Pokud jsou navíc údaje stále obsaženy v systému, nemohou žádným způsobem ovlivnit nové rozhodnutí. Některé důvody odmítnutí (žadatel je osoba, které má být odepřen vstup a zejména ohrožení veřejného zdraví) mají omezenou časovou platnost. Skutečnost, že v jednom časovém bodu představovaly závažné důvody odmítnutí vstupu, by neměla ovlivnit nové rozhodnutí. Je třeba znovu důkladně posoudit situaci každé nové žádosti o vízum, což by případně mělo být v nařízení výslovně uvedeno.

3.7 **Přístup k údajům a jejich využití**

3.7.1 *Předběžné poznámky*

Jako předběžnou poznámku EIOÚ uznává péči, která byla očividně věnována regulačnímu systému přístupu k údajům VIS a jejich používání. Každý orgán má přístup k odlišným údajům pro různé účely. Jde o vhodný přístup, který EIOÚ může pouze podpořit. Následující poznámky mají za cíl uplatnit tento přístup v co největší míře.

3.7.2 *Kontroly víz v kontrolních stanovištích na vnějších hranicích a uvnitř území členských států*

V případě kontrol víz na vnějších hranicích článek 16 navrhovaného nařízení jasně uvádí dva přesné účely:

— „ověření totožnosti osoby“, kterým se rozumí v souladu s příslušnou definicí porovnání dvou údajů („one to one comparison“);

— „ověření pravosti víza“. Jak je navrhováno v normách Mezinárodní organizace pro civilní letectví (ICAO), vízový mikročip by mohl za účelem provedení uvedeného procesu ověření pravosti použít veřejno-soukromý systém Public Key Infrastructure.

Těchto dvou účelů lze náležitě dosáhnout pouhým zpřístupněním chráněného mikročipu příslušným orgánům za účelem provádění vízových kontrol. Přístup k centrální databázi VIS by proto byl v tomto konkrétním případě nepřiměřený. Tato možnost by znamenala spojení více orgánů s VIS, což by mohlo zvýšit riziko zneužití. Tato varianta by rovněž mohla být nákladnější, protože počet zabezpečených a kontrolovaných přístupů k VIS a potřeba zvláštního výcviku souvisejícího s tímto přístupem se také podstatně zvýší.

Navíc existují pochybnosti ohledně přiměřenosti přístupu k údajům, který se předpokládá v druhém bodu článku 16. Odstavec 2 písm. a) skutečně uvádí, že pokud se po prvním dotazu bude zdát, že VIS obsahuje údaje o žadateli (což by mělo být zásadní), příslušný orgán může nahlédnout do jiných údajů, stále za účelem ověření totožnosti. Tyto údaje se týkají všech informací souvisejících se žádostí, fotografií, otisků prstů, jakož i všech v minulosti vydaných víz a víz, jejichž platnost byla zrušena, pozastavena či prodloužena.

Pokud je ověření totožnosti úspěšné, není vůbec jasné, z jakých důvodů jsou ještě potřebné zbývající údaje. Tyto by ve skutečnosti měly být zpřístupněny za omezujících podmínek, pouze pokud ověřovací postup nevedl k úspěchu. V tomto případě by údaje uvedené v čl. 16 odst. 2 vhodně přispěly k záložnímu postupu napomáhajícímu zjistit totožnost osoby. Neměly by tedy být přístupné veškerému personálu pohraničních kontrolních stanovišť, avšak přístup k nim by měl být omezen pouze na úředníky pověřené obtížnými případy.

Konečně, vymezení orgánů majících přístup by mělo být přesnější. Zejména není zřejmé, co to jsou „příslušné orgány pro provádění kontrol uvnitř území členského státu". EIOÚ předpokládá, že jde o orgány příslušné pro provádění kontrol *víz*, a článek 16 by mel být v tomto smyslu pozměněn.

3.7.3 *Použití údajů pro zjišťování totožnosti a vracení nelegálních přistěhovalců a pro azylové řízení*

V případech popsaných v článcích 17, 18 a 19 (vracení nelegálních přistěhovalců a azylové řízení) je VIS využíván pro účely zjišťování totožnosti. Mezi údaji, které je možné využít pro účely zjišťování totožnosti, jsou fotografie. Za současného stavu technologie související s automatickým rozpoznáváním tváří pro tak rozsáhlé systémy IT však fotografie ke zjištění totožnosti nelze použít (porovnávat jeden údaj s mnoha – „one-to-many"); nemohou zabezpečit spolehlivý výsledek. Proto je není možné považovat za údaje vhodné pro účely zjišťování totožnosti.

V důsledku výše uvedeného EIOÚ důrazně navrhuje, aby „fotografie" byly z první části uvedených článků vypuštěny a ponechány ve druhé části (fotografie je možné používat jako nástroj pro ověřování něčí totožnosti, avšak ne pro zjišťování totožnosti v rozsáhlé databázi).

Jinou možností by bylo pozměnit článek 36 v tom smyslu, že funkce zpracování fotografií pro účely zjišťování totožnosti budou zavedeny pouze až poté, co bude tato technologie shledána věrohodnou (případně po poradě s technickým výborem).

3.7.4 *Zveřejnění orgánů majících přístup*

Článek 4 navrhovaného nařízení stanoví, že příslušné orgány, pro něž členské státy určí, že mají přístup k VIS, mají být zveřejněny v *Úředním věstníku Evropské unie*. Takové zveřejnění by mělo být prováděno pravidelně (každoročně) s cílem informovat o změnách v situaci v jednotlivých členských státech. EIOÚ zdůrazňuje důležitost takového zveřejnění jako nepostradatelného nástroje kontroly na evropské, celostátní i místní úrovni.

3.8 **Odpovědnost**

Připomíná se zde, že VIS bude založen na centralizované architektuře s centrální databází, kam budou ukládány všechny informace o vízech, a národních rozhraních umístěných v členských státech, která příslušných orgánům umožní přístup k centrálnímu systému. Podle 14. a 15. bodu odůvodnění navrhovaného nařízení se na zpracování osobních údajů členskými státy v rámci provádění tohoto nařízení bude vztahovat směrnice 95/46/ES, a na činnosti Komise v souvislosti s ochranou osobních údajů se použije nařízení 45/2001. Jak je v této souvislosti zmiňují uvedené body odůvodnění, cílem návrhu je objasnit určité body, které se mj. týkají odpovědnosti za využívání údajů a dohledu nad ochranou údajů.

Dokonce by se zdálo, že tyto body souvisí s některými důležitými podrobnostmi, bez nichž by systém ochranných opatření uvedený ve směrnici 95/46/ES a nařízení 45/2001 neplatil nebo by nebyl plně v souladu s návrhem. Použitelnost vnitrostátních právních předpisů podle dané směrnice běžně předpokládá správce ustaveného v daném členském státě (článek 4), přičemž použitelnost nařízení závisí na zpracování osobních údajů orgánem nebo útvarem Společenství v rámci výkonu činností, jež cele nebo zčásti spadají do oblasti působnosti právních předpisů Společenství (článek 3).

Podle čl. 23 odst. 2 navrhovaného nařízení se údaje „zpracovávají v systému VIS jménem členských států". Podle čl. 23 odst. 3 každý členský stát určí orgán považovaný za správce v souladu s čl. 2 písm. d) směrnice 95/46/ES. Na základě toho by se mohlo zdát, že v souladu se systémem dané směrnice by Komise měla být považována za zpracovatele. Toto je potvrzeno ve vysvětlení článků ([1]).

Taková formulace poněkud nedoceňuje velmi důležitou a dokonce rozhodující úlohu Komise, a sice ve fázi vývoje systému, i během jeho normálního fungování. Právě úlohu Komise lze obtížně spojit s pojmem správce nebo zpracovatele; buď jde o zpracovatele s neobvyklými pravomocemi (mj. v oblasti navržení systému), nebo o správce s určitými omezeními (jelikož údaje vkládají a používají členské státy). Je třeba uznat, že Komisi v rámci systému VIS skutečně náleží úloha *sui generis* ([2]).

Tato významná úloha by měla být uznána úplným popisem úkolů Komise, a ne formulací, která zcela neodpovídá skutečnosti, protože je příliš omezující, nemění nic na fungování VIS a pouze vede k nejasnostem. To je rovněž důležité s ohledem na důsledný a účinný dohled nad VIS (viz rovněž odstavec 3.11). Z tohoto důvodu EIOÚ doporučuje vypustit čl. 23 odst. 2.

EIOÚ by chtěl zdůraznit, že pokud Komise zamýšlí svěřit řídící úkoly jinému subjektu, bude úplný popis úkolů Komise ohledně VIS o to důležitější. V části „Fiche Financičre" připojené k návrhu je uvedena možnost převodu těchto úkolů na Agenturu pro vnější hranice. V této souvislosti je klíčové zamezit veškerým nejistotám ohledně rozsahu pravomocí Komise, tak aby její nástupce znal hranice, v jejichž rámci může jednat.

3.9 **Bezpečnost**

Řízení a zachování optimální úrovně bezpečnosti VIS představuje nutnou podmínku pro zajištění požadované ochrany osobních údajů uložených v databázi. V zájmu dosažení této uspokojivé úrovně ochrany bude třeba provést vhodná ochranná opatření pro zvládnutí možných rizik souvisejících s infrastrukturou systému a se zúčastněnými osobami. Tímto problémem se nyní zabývají různé části návrhu a je třeba provést jistá zlepšení.

Články 25 a 26 návrhu obsahují různá opatření pro bezpečnost údajů a upřesňují možné způsoby zneužití, jimž je třeba předcházet. Tato ustanovení by však mohla být užitečně doplněna opatřeními pro systematické monitorování a podávání zpráv o účinnosti již zmíněných bezpečnostních opatření. EIOÚ konkrétněji doporučuje, aby k těmto článkům byla doplněna ustanovení o systematické (interních) kontrolách bezpečnostních opatření.

To souvisí s článkem 40 návrhu, který obsahuje ustanovení o monitorování a vyhodnocování. To by se mělo týkat nejen aspektů výstupů, efektivnosti nákladů a kvality služeb, ale i souladu se zákonnými požadavky, zejména v oblasti ochrany údajů. EIOÚ proto doporučuje, aby oblast působnosti článku 40 byla rozšířena o monitorování zákonnosti zpracování a předkládání zpráv o tomto problému.

V souladu s čl. 24 odst. 4 písm. c) nebo čl. 26 odst. 2 písm. e) týkajících se řádně pověřených zaměstnanců majících přístup k údajům by se mělo dále doplnit, že členské státy by měly zabezpečit dostupnost přesných uživatelských profilů (které by měly být za účelem kontroly k dispozici dohlížecím orgánům členských států). Vedle těchto uživatelských profilů musí být navíc vypracován úplný seznam totožností uživatelů, který musí členské státy neustále aktualizovat. Totéž platí pro Komisi. Článek 25 odst. 2 písm. b) by proto měl být doplněn v témže smyslu.

([1]) Viz stranu 37 návrhu.

([2]) Ačkoli vymezení pojmu správce ve směrnici 95/46/ES a nařízení 45/2001 uvádí rovněž možnost více správců s odlišnými odpovědnostmi.

Výčet těchto bezpečnostních opatření doplňují ochranná opatření monitorovacího a organizačního rázu. Článek 28 návrhu popisuje podmínky a účely vedení záznamů o veškerém zpracování dat. Tyto záznamy nebudou uchovávány pouze za účelem monitorování ochrany údajů a zajištění bezpečnosti údajů, ale i za účelem provádění pravidelných interních kontrol systému VIS. Zprávy na základě interních kontrol přispějí k účinnému plnění úkolů dohlížecích orgánů, které budou schopny určit největší slabiny a soustředit se na ně během provádění jejich vlastních kontrolních postupů.

3.10 **Práva dotyčné osoby**

3.10.1 *Informování dotyčné osoby*

Informování dotyčné osoby, aby bylo zajištěno nediskriminační zpracování, má zásadní význam. Představuje nezbytnou ochranu práv jedince. Článek 30 návrhu z tohoto důvodu nyní v podstatě čerpá z článku 10 směrnice 95/46/ES.

Tomuto ustanovení by však z hlediska jeho lepšího přizpůsobení rámci VIS prospěly některé změny. Směrnice skutečně stanoví, že mají být poskytovány některé informace, avšak umožňuje případné poskytování dalších informací ([1]). V důsledku toho by se článek 30 měl změnit tak, aby obsahoval tyto body:

— Dotyčné osoby by rovněž měly být informovány o době, po kterou jsou jejich údaje uchovávány.

— Článek 30 odst. 1 písm. e) se týká „práva přístupu a práva na opravu údajů“. Přesnější by bylo uvádět „právo přístupu a právo *požádat o* opravu *nebo vypuštění* údajů“. V tomto směru by dotyčné osoby měly být informovány o možnosti požádat o radu nebo pomoc příslušné dohlížecí orgány.

— Konečně, článek 30 odst. 1 písm. a) uvádí informaci o totožnosti správce a jeho případného zástupce. Správce je vždy jmenován pro území Evropské unie, a proto není nutné předpokládat uvedenou možnost případného zástupce.

3.10.2 *Práva přístupu, práva na opravy a vymazání*

Poslední věta čl. 31 odst. 1 stanoví, že „takový přístup k údajům může povolit pouze členský stát“. Lze předpokládat, že se tím rozumí, že přístup k údajům (nebo jejich poskytnutí) nemůže povolit centrální jednotka, ale kterýkoli členský stát. EIOÚ doporučuje výslovně stanovit, že o takové poskytnutí informací je možné požádat v kterémkoli členském státě.

Navíc se rovněž zdá, že z návrhu tohoto ustanovení vyplývá, že není možné odmítnout přístup a že tento přístup bude umožněn bez schválení odpovědného členského státu. To by vysvětlovalo nutnost spolupráce mezi orgány členských států při prosazování práv stanovených v čl. 31 odst. 2, 3 a 4, avšak ne v čl. 31 odst. 1 ([2]).

3.10.3 *Pomoc ze strany dohlížecích orgánů*

Článek 33.2 stanoví, že povinnost dohlížecích orgánů členských států pomáhat a poskytnout poradenství dotčené osobě trvá během celého řízení (před soudem). Smysl tohoto odstavce je nejasný. Dohlížecí orgány členských států zastávají různá stanoviska, pokud jde o jejich úlohu během soudního řízení. Vypadá to, jako by členské státy musely u soudu zastávat roli obhájce stěžovatele, což v mnoha zemích není možné.

([1]) *Zmiňuje „jakékoli další informace (…), pokud jsou takové další informace nutné s ohledem na zvláštní okolnosti shromažďování údajů, aby bylo zaručeno nediskriminační zpracování s ohledem na osobu, jíž se údaje týkají“.*

([2]) V zájmu větší jasnosti v tomto smyslu mohl být rovněž pozměněn čl. 31 odst. 3 týkající se spolupráce mezi orgány členských států při výkonu práv na opravu nebo vymazání údajů: „v případě žádosti *uvedené v čl. 31 odst. 2*“. Žádosti uvedené v čl. 31 odst. 1 (přístup) nezahrnují spolupráci mezi orgány.

3.11 **Dohled**

Návrh rozděluje úlohu dohledu mezi dohlížecí orgány členských států a EIOÚ. Toto je v souladu s přístupem návrhu k platným právním předpisům a odpovědnosti za fungování a využívání VIS i s potřebou účinného dohledu. Z tohoto důvodu EIOÚ vítá tento přístup obsažený v článcích 34 a 35.

Dohlížecí orgány členských států monitorují zákonnost zpracování osobních údajů členskými státy, *včetně jejich přenosu do VIS a z něj*. EIOÚ monitoruje činnosti Komise *(…) včetně toho, že osobní údaje jsou předávány v zákonným způsobem mezi národními rozhraními a centrálním vízovým informačním systémem*. To by mohlo vést ke zdvojování činnosti, protože jak dohlížecí orgány členských států, tak EIOÚ jsou současně odpovědné za monitorování zákonnosti přenosu údajů mezi národními rozhraními a centrálním vízovým informačním systémem.

EIOÚ proto navrhuje změnu článku 34, aby se vyjasnilo, že dohlížecí orgány členských států monitorují zákonnost zpracování osobních údajů členskými státy, včetně jejich přenosu do národního rozhraní VIS a z něj.

Pokud jde o dohled VIS, je rovněž důležité zdůraznit, že dohlížecí činnosti dohlížecích orgánů členských států a EIOÚ by měly být do jisté míry koordinovány, a to v zájmu zabezpečení dostatečné úrovně součinnosti a celkové účinnosti. Je skutečně zapotřebí, aby při provádění nařízení panoval soulad a aby se pracovalo na společném přístupu ke společným problémům. Navíc, pokud jde o bezpečnost, je možné doplnit, že bezpečnostní úroveň VIS bude – nakonec – určena bezpečnostní úrovní jeho nejslabšího článku. V tomto směru je rovněž třeba uspořádat a posílit spolupráci mezi EIOÚ a orgány členských států. Článek 35 by tedy měl obsahovat ustanovení v tom smyslu, že EIOÚ pořádá alespoň jednou ročně jednání se všemi dohlížecími orgány členských států.

3.12 **Provádění**

Článek 36 odst. 2 návrhu stanoví: *„Opatření nezbytná pro technické zavedení funkcí uvedených v odstavci 1 se přijmou postupem podle čl. 39 odst. 2“*. Článek 39 odkazuje na výbor, který je nápomocný Komisi a který byl zřízen v prosinci roku 2001 ([1]) a který byl využit v několika nástrojích.

Technické zavádění funkcí systému VIS (interakce s příslušnými orgány a jednotný formát víz) představuje celou řadu možných závažných dopadů na ochranu údajů. Například rozhodnutí, za do víz vkládat mikročip či nikoli,, které bude mít dopad na způsob využívání centrální databáze, podobně jako standard formátu použitého pro výměnu biometrických údajů bude určovat směr nebo obsah politiky související s ochranou údajů ([2]).

Volba technologií bude mít rozhodující vliv na náležité provádění zásad účelu a proporcionality a měla by v důsledku toho být předmětem dohledu. Volby ohledně technologií, které mají významný dopad na ochranu údajů by proto měly přednostně probíhat formou nařízení, v souladu se spolurozhodovacím postupem. Pouze v takovém případě může být vykonávána nezbytná politická kontrola. Ve všech ostatních případech dopadu na ochranu údajů by EIOÚ měl dostat možnost vyjádřit se k volbám provedeným tímto výborem.

3.13 **Interoperabilita**

Interoperabilita představuje rozhodující a zásadní podmínku efektivity rozsáhlých systémů informačních technologií, jako je VIS. Nabízí možnost soustavně snižovat celkové náklady a vyhýbat se překrývání různorodých opatření, k němuž přirozeně dochází. Interoperabilita může rovněž přispět k cíli společné vízové politiky tím, že do všech prvků, které tvoří tuto politiku, zavede stejné procedurální standardy. Je však zásadní rozlišovat mezi dvěma úrovněmi interoperability.

— Interoperabilita mezi členskými státy EU je vysoce žádoucí; žádosti o víza zaslané orgány jednoho členského státu musejí být interoperabilní s těmi, které zašlou orgány jiného členského státu.

([1]) Nařízení Rady č. 2424/2001 ze dne 6. prosince 2001 o vývoji Schengenského informačního systému druhé generace (SIS II).

([2]) Návrh nařízení Rady, kterým se mění (ES)1683/95 (jednotný formát pro VISA), zahrnoval v září roku 2003 rovněž podobný článek.

— Interoperabilita mezi systémy zavedená z jiných důvodů nebo interoperabilita se systémy třetích zemí je daleko problematičtější.

Mezi dostupnými ochrannými opatřeními používanými k omezení účelu systému a k zamezení neplánované funkce („function creep“) může k tomuto omezení přispět použití odlišných technologických norem. Dále by měla být pečlivě dokumentována jakákoli forma interakce mezi dvěma odlišnými systémy. Interoperabilita by nikdy neměla vést k tomu, že by orgán, kterému není povolen přístup k určitým údajům nebo jejich použití, mohl získat přístup prostřednictvím jiného informačního systému.

V tomto směru by EIOÚ rád odkázal na usnesení Rady ze dne 25. března 2004 o boji proti terorismu, ve kterém se Komise vybízí, aby předložila návrhy pro zvýšení interoperability a synergického působení mezi informačními systémy (SIS, VIS a Eurodac).

EIOÚ by rovněž rád odkázal na probíhající diskusi o tom, kterému subjektu by v budoucnu bylo možné svěřit řízení rozdílných rozsáhlých systémů (viz rovněž odstavec 3.8 tohoto stanoviska).

EIOÚ by chtěl znovu zdůraznit, že interoperabilita systémů nemůže být zavedena v rozporu se zásadou omezení účelu, a že jakýkoli návrh v této věci by měl být předložen jemu.

4. ZÁVĚRY

4.1 Obecné body

1. EIOÚ uznává, že další vývoj společné vízové politiky vyžaduje efektivní výměnu příslušných údajů. Jedním z mechanismů, který může zajistit hladký tok informací, je VIS. EIOÚ důkladně prověřil podkladový materiál předložený v EIA. Ačkoli podkladové materiály nejsou zcela přesvědčivé, zdá se, že existují dostatečné důvody pro zřízení VIS za účelem zlepšení společné vízové politiky.

   Tento nový nástroj by však měl být omezen na shromažďování a výměnu údajů, pokud jsou takové shromažďování nebo výměna nutné pro rozvoj společné vízové politiky a přiměřené tomuto cíli.

2. Zavedení VIS může mít pozitivní dopady na jiné oprávněné veřejné zájmy, avšak to nic nemění na účelu VIS. Všechny prvky VIS proto musí být nezbytnými a přiměřenými nástroji pro dosažení výše uvedeného cíle dané politiky. Kromě toho:

   — běžný přístup donucovacích orgánů by nebyl v souladu s tímto účelem.

   — EIOÚ doporučuje, aby uvedené rozlišení mezi „účelem“ a „přínosem“ bylo v textu čl. 1 odst. 2 uvedeno výslovněji.

   — Interoperabilita s jinými systémy nesmí být zaváděna v rozporu se zásadou omezení účelu.

3. EIOÚ uznává výhody používání biometrie, avšak zdůrazňuje významný dopad používání takových údajů a navrhuje zařadit při využití biometrických údajů nejpřísnějších ochranná opatření. Technická nedokonalost otisků prstů navíc vyžaduje, aby byly vypracovány a do návrhu zahrnuty záložní postupy.

4. Současné stanovisko by mělo být zmíněno v preambuli nařízení před body odůvodnění („s ohledem na stanovisko…“).

4.2 **Jiné body**

5. Pokud jde o důvody odmítnutí víza: znění návrhu by mělo obsahovat odkaz na článek 29 směrnice 2004/58/ES, aby se zaručilo, že pojem „ohrožení veřejného zdraví“ je chápán s ohledem na toto ustanovení.

6. Údaje o členech skupiny mají v návrhu zvláštní význam: proto by mělo být uvedeno přesné a úplné vymezení pojmu „členové skupiny“.

7. Nic nenasvědčuje tomu, že by politické rozhodnutí přijaté v tomto návrhu ohledně zdržení v otázce doby uchovávání údajů bylo nepřiměřené nebo by mělo nepřijatelné následky, pokud budou uplatněny veškeré vhodné opravné mechanismy.

   V návrhu by dále mělo být výslovně uvedeno, že osobní údaje musí být opětovně posouzeny při každé nové žádosti o vízum.

8. Pokud jde o vízové kontroly na vnějších hranicích: Článek 16 návrhu by měl být změněn, protože přístup k centrální databázi VIS by byl v těchto případech nepřiměřený. Je dostačující, aby příslušné orgány měly za účelem provádění vízových kontrol přístup pouze k chráněnému mikročipu.

   Pokud bylo navíc ověření totožnosti úspěšné, není vůbec jasné, z jakých důvodů jsou ještě potřebné zbývající údaje.

9. Pokud jde o použití údajů pro zjištění totožnosti a vracení nelegálních přistěhovalců a pro azylové řízení: „fotografie“ by měly být vypuštěny z první části článků 17, 18 a 19 a ponechány v druhé části.

10. Pokud jde o odpovědnost Komise a členských států: V článku 23 by se měl vypustit odstavec 2.

11. Do návrhu by se měla doplnit ustanovení o systematické (interní) kontrole bezpečnostních opatření. Rozsah působnosti článku 40 musí být rozšířen o monitorování zákonnosti zpracování a předkládání zpráv o tomto problému. Kromě toho:

   — musí členské státy vypracovat úplný seznam totožností uživatelů a tento seznam musí neustále aktualizovát. Totéž platí pro Komisi: Článek 25 odst. 2 písm. b) by proto měl být doplněn ve stejném duchu.

   — Článek 28 návrhu popisuje podmínky a účely, pro které musí být vedeny záznamy všech operací zpracování údajů. Tyto záznamy nejsou uchovávány pouze za účelem monitorování ochrany údajů a zajištění bezpečnosti údajů, ale i za účelem provádění pravidelných interních kontrol systému VIS.

12. Pokud jde o práva dotyčných osob:

   — článek 30 by měl být změněn, aby zajistil, že dotyčné osoby budou rovněž informovány o době, po kterou jsou jejich údaje uchovávány.

   — Článek 30 odst. 1 písm. e) by měl zmínit „právo přístupu a právo na opravu nebo vymazání údajů“.

   — Článek 31 odst. 1 musí výslovně stanovit, že o poskytnutí určitých informací je možné požádat v kterémkoli členském státě.

13. Pokud jde o dohled:

— Článek 34 by měl být pozměněn v zájmu vyjasnění, že dohlížecí orgány členských států monitorují zákonnost zpracování osobních údajů členskými státy, včetně jejich přenosu do národního rozhraní VIS a z něj.

— Článek 35 by tedy měl obsahovat ustanovení v tom smyslu, že EIOÚ pořádá alespoň jednou ročně jednání se všemi dohlížecími orgány členských států.

14. Pokud jde o provádění:

— Volby ohledně technologií, které mají významný dopad na ochranu údajů, by proto měly přednostně probíhat formou nařízení, v souladu se spolurozhodovacím postupem.

— V jiných případech by EIOÚ měl dostat možnost sdělit svá doporučení výboru, který tento návrh předpokládá, ohledně jím prováděných voleb.

V Bruselu dne 23. března 2005.

Peter HUSTINX

Evropský inspektor ochrany údajů