EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV

Stanovisko Európskeho dozorného úradníka pre ochranu údajov k návrhu rozhodnutia Rady o prístupe orgánov členských štátov zodpovedných za vnútornú bezpečnosť a Europolu do vízového informačného systému (VIS) na účely predchádzania, odhaľovania a vyšetrovania trestných činov terorizmu a iných závažných trestných činov (KOM(2005) 600, konečné znenie)

(2006/C 97/03)

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 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov,

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

so zreteľom na žiadosť o stanovisko v súlade s článkom 28 ods. 2 nariadenia (ES) č. 45/2001, ktorá bola 29. novembra 2005 prijatá od Komisie,

PRIJAL TOTO STANOVISKO:

1. ÚVOD

1.1. Predbežná poznámka

Návrh rozhodnutia Rady o prístupe orgánov členských štátov zodpovedných za vnútornú bezpečnosť a Europolu do vízového informačného systému (VIS) na účely predchádzania, odhaľovania a vyšetrovania trestných činov terorizmu a iných závažných trestných činov (ďalej len „návrh“) zaslala Komisia Európskemu dozornému úradníkovi pre ochranu údajov (EDPS) listom z 24. novembra 2005. EDPS považuje tento list za žiadosť o radu pre inštitúcie a orgány Spoločenstva v zmysle článku 28 ods. 2 nariadenia (ES) č. 45/2001. Podľa EDPS by sa toto stanovisko malo uviesť v preambule rozhodnutia.

EDPS považuje za dôležité zaujať stanovisko k tejto citlivej otázke, pretože tento návrh vychádza priamo zo zavedenia VIS, na ktorý bude dozerať a ku ktorému vydal stanovisko 23. marca 2005 [1]. V tomto stanovisku sa už predpokladala hypotéza prístupu orgánov činných v trestnom konaní (pozri ďalej); vytvorenie nových prístupových práv do VIS má určujúci vplyv na systém v zmysle ochrany údajov. Stanovisko k tomuto návrhu musí preto nadväzovať na prvé stanovisko.

1.2. Dôležitosť návrhu

a) *Kontext*

Dôležitosť tohto návrhu nespočíva len v samotnom návrhu, ale aj v tom, že návrh sa stáva súčasťou všeobecného trendu udeľovať orgánom činným v trestnom konaní prístup k viacerým rozsiahlym informačným a identifikačným systémom. To sa okrem iného spomína v oznámení Komisie z 24. novembra 2005 o zlepšení efektívnosti, posilňovaní interoperability a synergií medzi európskymi databázami v oblasti spravodlivosti a vnútorných vecí [2], najmä v jeho bode 4.6: *„V súčasnosti označila Rada neprístupnosť údajov systému VIS pre orgány vnútornej bezpečnosti za nedostatok v súvislosti s cieľom boja proti terorizmu a zločinu. To isté by sa dalo povedať o všetkých imigračných údajoch v SIS II a o údajoch v systéme EURODAC.“*

Tento návrh by sa dal preto vnímať ako predchodca podobných právnych nástrojov, ktoré sa vypracujú v súvislosti s inými databázami, a je kľúčové na začiatku definovať prípady, v ktorých by mohol byť tento prístup prípustný.

---

[1] Stanovisko Európskeho dozorného úradníka pre ochranu osobných 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, konečné znenie).

[2] KOM(2005) 597, konečné znenie.

b) *Vplyv nového prístupu do VIS*

EDPS samozrejme uznáva potrebu orgánov činných v trestnom konaní využívať najlepšie možné nástroje na určenie páchateľov teroristických činov alebo inej závažnej trestnej činnosti. Uvedomuje si tiež, že údaje VIS môžu za určitých okolností predstavovať základný zdroj informácií pre tieto orgány.

Udelenie prístupu k databázam prvého piliera orgánom činným v trestnom konaní, akokoľvek to môže byť opodstatnené z hľadiska boja proti terorizmu, sa však nemôže označiť za zanedbateľné. Musí sa totiž pamätať na to, že VIS je informačný systém, ktorý sa vytvoril so zreteľom na uplatňovanie európskej vízovej politiky a nie ako nástroj na vynucovanie práva. Rutinný prístup by naozaj predstavoval vážne porušenie zásady obmedzenia účelu. Malo by to za následok neprimerané zasahovanie do súkromia cestujúcich, ktorí súhlasili so spracovaním ich údajov na účely získania víza a ktorí očakávajú, že ich údaje sa zhromažďujú, konzultujú a prenášajú len na tento účel.

Keďže informačné systémy sa vybudovali na osobitný účel s ochrannými a bezpečnostnými opatreniami a s podmienkami prístupu určenými týmto účelom, udelením systematického prístupu na iný ako pôvodný účel by sa nielen porušila zásada obmedzenia účelu, ale uvedené prvky by mohli tiež stratiť svoju adekvátnosť a dostatočnosť.

Takáto významná zmena systému by okrem toho mohla zbaviť platnosti výsledky posúdenia vplyvu (, ktoré sa zaoberalo využitím systému len na pôvodný účel). To isté platí o stanoviskách orgánov na ochranu údajov. Mohlo by sa tvrdiť, že nový návrh mení predpoklady analýzy súladu, ktorú tieto orgány uskutočnili.

c) *Striktné obmedzenie tohto prístupu*

S ohľadom na uvedené poznámky by EDPS rád zdôraznil, že prístup k VIS sa môže orgánom činným v trestnom konaní udeľovať len za osobitných okolností, pre jednotlivé prípady a musia ho sprevádzať prísne ochranné opatrenia. Inými slovami, nahliadanie orgánov činných v trestnom konaní musí byť vhodnými technickými a právnymi prostriedkami obmedzené na konkrétne prípady.

EDPS to už zdôraznil vo svojom stanovisku k VIS: *„EDPS si je vedomý, že orgány činné v trestnom konaní majú záujem na udelení prístupu k systému VIS; Závery Rady boli v tomto zmysle prijaté 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, za osobitných okolností a ak primerané bezpečnostné opatrenia neustanovujú inak, systematický prístup nemôže byť udelený.“*

Základné požiadavky by sa na záver dali zhrnúť takto:

— Nemal by sa udeľovať systematický prístup: rozhodnutie musí zabezpečiť, že nevyhnutnosť a proporcionalita prístupu orgánov tretieho piliera sa budú skúmať vždy pre každý jednotlivý prípad. Z tohto hľadiska je presné znenie právneho nástroja prvoradé, aby sa nenechal priestor širokému výkladu, ktorý by následne viedol k rutinnému prístupu.

— V prípadoch, keď sa prístup udeľuje, sa musia prijať vhodné bezpečnostné opatrenia a podmienky vrátane komplexného mechanizmu ochrany údajov pre použitie údajov na vnútroštátnej úrovni, pričom sa zohľadní citlivá povaha tohto prístupu.

1.3. **Úvodné poznámky**

EDPS uznáva, že v tomto navrhovanom nástroji sa venovala značná pozornosť ochrane údajov, a to najmä v obmedzení prístupu na konkrétne prípady a výlučne v rámci boja proti závažnej trestnej činnosti ([1]).

Spomedzi ďalších pozitívnych prvkov by EDPS rád tiež spomenul konkrétne:

— obmedzenie na určité formy trestnej činnosti, ako sa uvádza v dohovore o Europole;

— povinnosť členských štátov vytvoriť zoznam orgánov, ktoré majú prístup, a zverejniť tieto zoznamy;

— existencia centrálneho prístupového bodu v každom členskom štáte (a osobitnej jednotky v rámci Europolu), čo umožňuje lepšiu kontrolu žiadostí o prístup, ako aj lepší dozor;

— prísne pravidlá o ďalšom prenose údajov podľa článku 8 ods. 5 návrhu;

— povinnosť členských štátov a Europolu viesť záznamy o osobách zodpovedných za prístup k údajom.

2. **ANALÝZA NÁVRHU**

2.1. **Predbežná poznámka**

S cieľom udeľovať prístup orgánom v rámci tretieho piliera by mal hlavný návrh o VIS v rámci prvého piliera ustanoviť preklenujúce ustanovenie, ktoré by hlavne určilo možný obsah právneho nástroja v rámci tretieho piliera, ako napríklad tento návrh. Vo chvíli, keď EDPS vydal svoje stanovisko k VIS, preklenujúce ustanovenie ešte nebolo predložené a EDPS sa nemohol k nemu vyjadriť. Všetky ďalšie poznámky sú preto vypracované s výhradou obsahu preklenujúceho ustanovenia.

([1]) Je to tiež v súlade so závermi Rady z marca a júla 2005, v ktorých sa požaduje udelenie prístupu k VIS orgánom zodpovedných za vnútornú bezpečnosť *„pod podmienkou prísneho dodržiavania predpisov upravujúcich ochranu osobných údajov“*.

2.2. **Účel prístupu**

S cieľom zabezpečiť náležité obmedzenie prístupu je dôležité opatrne vymedziť podmienky prístupu do VIS. Je dobré, že okrem samotného navrhovaného rozhodnutia aj dôvodová správa a odôvodnenia (pozri najmä odôvodnenie 7) za zámer jasne označujú poskytovanie prístupu len v jednotlivých prípadoch.

Je možné uviesť jednu poznámku k článku 5 návrhu, aby sa usmernil jeho výklad.

Článok 5 obmedzuje rozsah prístupu hmotnoprávnymi podmienkami:

b) prístup na nahliadnutie musí byť nevyhnutný na účely predchádzania, odhaľovania alebo vyšetrovania trestných činov terorizmu alebo iných závažných trestných činov;

c) prístup na nahliadnutie musí byť nevyhnutný v konkrétnom prípade (...) a

d) musia existovať opodstatnené dôvody založené na skutkových zisteniach, na základe ktorých by bolo možné domnievať sa, že nahliadnutie do údajov VIS prispeje k zabráneniu, odhaleniu alebo vyšetreniu ktoréhokoľvek z predmetných trestných činov.

Tieto podmienky sú kumulatívne, pričom podmienka v písmene b) predstavuje skôr vymedzenie rozsahu *ratione materiae*. Z praktického hľadiska to znamená, že orgán, ktorý žiada o prístup, sa musí zaoberať závažným trestným činom, ako sa uvádza v písmene b) návrhu; musí existovať konkrétny prípad, ako sa uvádza v písmene c). Daný orgán musí byť okrem toho schopný preukázať, že nahliadnutie do údajov VIS prispeje v tomto konkrétnom prípade k zabráneniu, odhaleniu alebo vyšetreniu tohto trestného činu, ako sa predpokladá v písmene d).

Napriek tomuto výkladu článku 5 vyjadruje EDPS znepokojenie nad pružným znením v písmene d): „prispeje k" je dosť nejednoznačné. Existuje veľa prípadov, v ktorých by údaje VIS mohli prispieť k zabráneniu alebo vyšetreniu závažného trestného činu. S cieľom opodstatniť prístup k údajom VIS ako výnimku zo zásady obmedzenia účelu, je EDPS názoru, že toto nahliadnutie by malo „zásadne prispieť" k zabráneniu, odhaleniu alebo vyšetreniu danej závažnej trestnej činnosti a navrhuje v tomto zmysle zmeniť a doplniť článok 5.

Článok 10 ustanovuje, že záznamy by mali dokladovať presný účel prístupu. „Presný účel" by mal obsahovať údaje, na základe ktorých bolo nahliadnutie do VIS nevyhnutné v zmysle článku 5 písm. d). To by pomohlo pri zabezpečovaní toho, aby sa test nevyhnutnosti uplatnil na všetky prípady nahliadnutia do VIS, ako aj znížiť riziko rutinného prístupu.

2.3. **Kľúče na vyhľadávanie v databáze VIS**

Článok 5 ods. 2 a 3 ustanovuje dvojkrokový prístup k údajom VIS, pričom je súbor údajov prístupný len ak bolo vyhľadávanie úspešné na základe prvého súboru údajov. Tento prístup je sám osebe korektný. Prvý súbor údajov sa však zdá byť veľmi široký. Je možné najmä spochybniť relevantnosť údajov, ktoré sa uvádzajú v článku 5 ods. 2 v písmenách e) a i), pre prvý súbor údajov.

— „Účel cesty" sa javí ako veľmi všeobecný kľúč na umožnenie efektívneho nahliadania do systému. Okrem toho so sebou prináša riziko profilovania cestujúcich na základe tejto informácie.

— Pokiaľ ide o „fotografie", možnosť vyhľadávať v takej veľkej databáze na základe fotografií je obmedzená; výsledky takéhoto vyhľadávania predstavujú vzhľadom na súčasné technické možnosti neprijateľný pomer nesprávnych výsledkov vyhľadávania. Dôsledky nesprávnej identifikácie sú pre dotknuté fyzické osoby veľmi vážne.

EDPS preto požaduje, aby sa údaje v článku 5 ods. 2 písm. e) a i) považovali za doplňujúce informácie, ktoré sú prístupné, ak prvé nahliadnutie ukáže, že údaje sa už v systéme nachádzajú, a aby sa presunuli do článku 5 ods. 3.

Možnosť vyhľadávania v databáze na základe fotografií by na druhej strane mohlo byť predmetom posúdenia tejto techniky poradným výborom a vykonávala by sa až keď bude táto technika natoľko vyspelá, že sa bude môcť považovať za dostatočne spoľahlivú.

2.4. **Uplatnenie na členské štáty, na ktoré sa nevzťahuje nariadenie o VIS**

Orgány zodpovedné za vnútornú bezpečnosť členských štátov, ktoré sa nepodieľajú na VIS, môžu nahliadať do VIS. Tieto orgány musia nahliadať prostredníctvom zúčastneného členského štátu a zároveň dôsledne spĺňať podmienky, ktoré stanovuje článok 5 ods. 1 písm. b) až d) (t.j. pre jednotlivé prípady), a predložiť riadne odôvodnenú písomnú žiadosť.

EDPS by chcel zvýrazniť potrebu uloženia nejakých podmienok na spracúvanie, ktoré presahuje rámec nahliadania. Podľa pravidla, ktoré sa vzťahuje na členské štáty zúčastnené na VIS, sa údaje získané z VIS musia spracúvať v súlade s rámcovým rozhodnutím o ochrane údajov v treťom pilieri (pozri ďalej). Rovnaká podmienka by sa mala uplatniť na členské štáty, na ktoré sa nariadenie o VIS nevzťahuje ale ktoré do údajov nahliadajú. Takto by sa malo uvažovať aj o uchovávaní záznamov pre potreby dozoru v budúcnosti. EDPS preto odporúča, aby sa do článku 6 návrhu doplnil odsek, na základe ktorého by sa články 8 a 10 rozhodnutia vzťahovali aj na členské štáty, na ktoré sa nariadenie o VIS nevzťahuje.

2.5. **Mechanizmus ochrany údajov**

a) *Uplatňovanie rámcového rozhodnutia o ochrane údajov v treťom pilieri*

Keďže prístup orgánov zodpovedných za vnútornú bezpečnosť predstavuje výnimku z účelu VIS, mal by podliehať jednotnému mechanizmu ochrany údajov, ktorý by zabezpečoval vysokú úroveň ochrany údajov získaných z VIS a spracúvaných vnútroštátnymi orgánmi alebo Europolom.

Článok 8 návrhu ustanovuje, že rámcové rozhodnutie Rady o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach (ďalej len: „rámcové rozhodnutie") sa vzťahuje na spracúvanie údajov podľa navrhovaného rozhodnutia. Pokiaľ ide o ochranu údajov, tento návrh by sa mal preto vnímať ako *lex specialis*, ktorý dopĺňa alebo špecifikuje *lex generalis* (t.j. rámcové rozhodnutie). Tak napríklad pravidlá o ďalšom prenose údajov sú prísnejšie v tomto návrhu a mali by sa dodržiavať. To isté platí pre dôvody prístupu k údajom.

b) *Rozsah pôsobnosti*

EDPS víta skutočnosť, že mechanizmus ochrany údajov rámcového rozhodnutia je uplatniteľný na všetky prípady spracúvania osobných údajov podľa navrhovaného rozhodnutia. To znamená, že úroveň ochrany údajov je rovnaká bez ohľadu na to, ktorý orgán nahliada do údajov VIS.

Keďže v článku 2 sa používa funkčné kritérium na definovanie týchto orgánov („tie orgány členských štátov, ktoré sú zodpovedné za predchádzanie, odhaľovanie alebo vyšetrovanie trestných činov terorizmu alebo iných závažných trestných činov"), táto definícia by sa mohla vzťahovať na spravodajské služby, ako aj na orgány činné v trestnom konaní. Spravodajské služby, ktoré nahliadajú do VIS, majú preto z hľadiska ochrany údajov v zásade rovnaké povinnosti, čo je očividne pozitívny prvok.

Avšak vzhľadom na to, že by sa mohli objaviť pochybnosti o tomto výklade, ktorý sa týka uplatniteľnosti rámcového rozhodnutia na spravodajské služby, keď nahliadajú do údajov VIS, EDPS navrhuje takéto alternatívne znenie:

„V prípadoch, kedy sa rámcové rozhodnutie (...) nedá uplatniť, členské štáty zabezpečia aspoň takú úroveň ochrany údajov, ktorá by sa rovnala úrovni zabezpečenej podľa rámcového rozhodnutia."

c) *Dozor*

Pokiaľ ide o znenie článku 8, malo by sa objasniť, že odsek 1 sa týka spracúvania údajov v rámci územia členských štátov. Odseky 2 a 3 objasňujú ich rozsah pôsobnosti (spracúvanie údajov Europolom a Komisiou) a malo by sa explicitne uviesť, že odsek 1 sa týka iného predpokladu.

Rozdelenie dozorných právomocí podľa príslušných činností predstavuje korektný prístup. Jeden prvok však chýba: potreba koordinovaného prístupu pri dozore. Ako to už EDPS uviedol vo svojom stanovisku k VIS: *„Pokiaľ ide o dozor nad systémom VIS je dôležité tiež zdôrazniť, že dozor nad činnosťami národných dozorných orgánov a EDPS by sa do určitej miery mal koordinovať. Skutočne je potrebné zosúladiť vykonávanie nariadenia a ďalej pracovať na spoločnom prístupe k spoločným problémom.*

Článok 35 [návrhu o VIS] by mal teda obsahovať ustanovenie, ktoré by stanovilo, že EDPS zvolá aspoň raz ročne zasadnutie všetkých národných dozorných orgánov."

To isté sa vzťahuje na osobitné využitie systému VIS (aj so zapojením spoločného dozorného orgánu Europolu v tomto prípade). Dozor by mal byť úplne jednotný s dozorom „VIS prvého piliera", keďže ide o ten istý systém. Koordinačné stretnutia všetkých strán zúčastnených na dozore, ktoré zvoláva EDPS, sa okrem toho zvolili ako vzor aj v súvislosti s dozorom nad inými rozsiahlymi systémami, ako napríklad Eurodac.

EDPS si je vedomý toho, že návrh do istej miery predpokladá koordináciu, pričom uvádza úlohu budúcej pracovnej skupiny pre ochranu fyzických osôb pokiaľ ide o ochranu osobných údajov, ktorú ustanovuje článok 31 navrhovaného rámcového rozhodnutia. Malo by sa však zopakovať, že poslaním tohto poradného orgánu nie je dozor vykonávať.

EDPS navrhuje doplniť ustanovenie o tom, že koordinačné stretnutia, ktoré zvoláva EDPS v rámci dozoru „VIS prvého piliera", by mali tiež právomoc pokiaľ ide o údaje spracúvané podľa tohto návrhu a že na tento účel by mať zastúpený spoločný dozorný orgán Europolu.

2.6. **Vnútorný audit**

Článok 12 návrhu ustanovuje pre VIS monitorovacie systémy. EDPS je názoru, že toto monitorovanie by sa nemalo týkať len výsledku, nákladovej efektívnosti a kvality služieb, ale aj súladu s právnymi požiadavkami, najmä v oblasti ochrany údajov. Článok 12 by sa mal zmeniť a doplniť v tomto zmysle.

S cieľom vykonávať tento vnútorný audit právoplatnosti spracúvania by Komisia mala mať možnosť využiť záznamy, ktoré sa uchovávajú v súlade s článkom 10 návrhu. Článok 10 by mal preto ustanoviť, že tieto záznamy sa nebudú uchovávať len na účely monitorovania ochrany údajov a zaistenia bezpečnosti údajov, ale tiež na vykonávanie pravidelného vnútorného auditu VIS. Správy o vnútornom audite budú prispievať k vykonávaniu dozornej úlohy EDPS a ostatných dozorcov, ktorí budú lepšie vedieť zvoliť svoje prioritné oblasti na vykonávanie dozoru.

3. ZÁVER

S ohľadom na uvedené EDPS zdôrazňuje, že je veľmi dôležité, aby sa orgánom zodpovedným za vnútornú bezpečnosť a Europolu udeľoval prístup len pre jednotlivé prípady a pod podmienkou dodržania prísnych bezpečnostných opatrení. Z celkového hľadiska sa tento cieľ v návrhu dosahuje uspokojivo, avšak niektoré veci by sa dali vylepšiť, ako sa navrhuje v tomto stanovisku:

— Na prístup k VIS podľa článku 5 by sa mala vzťahovať podmienka, že nahliadnutie musí „zásadne“ prispieť k zabráneniu, odhaleniu alebo vyšetreniu závažnej trestnej činnosti a že záznamy, ktoré sa vyžadujú v článku 10, by mali umožniť vyhodnotenie splnenia tejto podmienky v každom jednotlivom prípade.

— Dva kľúče na vyhľadávanie pre prístup do VIS uvedené v článku 5 ods. 2, konkrétne „účel cesty“ a „fotografie“, by sa mali považovať za doplňujúce informácie v prípade úspešného vyhľadávania a ako také aj sprístupniť.

— Úroveň ochrany údajov, ktorá sa uplatňuje nad rámec nahliadania, by mala byť rovnaká bez ohľadu na to, ktorý orgán nahliada do údajov VIS. Články 8 a 10 by sa mali vzťahovať aj na tie členské štáty, na ktoré sa nariadenie o VIS nevzťahuje.

— Mal by sa zabezpečiť koordinovaný prístup k vykonávaniu dozoru, a to aj s ohľadom na prístup do VIS, ako sa predpokladá v tomto návrhu.

— Ustanovenia o monitorovacích systémoch by mali takisto zabezpečiť vnútorný audit spĺňania požiadaviek ochrany údajov.

V Bruseli 20. januára 2006

Peter HUSTINX

Európsky dozorný úradník pre ochranu údajov