EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

Stanovisko Evropského inspektora ochrany údajů k návrhu rozhodnutí Rady o konzultačním přístupu do VIS pro orgány členských států odpovědné za vnitřní bezpečnost a pro Europol za účelem prevence, odhalování a vyšetřování teroristických trestných činů a dalších závažných trestných činů (KOM (2005) 600 v konečném znění)

(2006/C 97/03)

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 obdrženou od Komise dne 29. listopadu 2005,

ZAUJAL TOTO STANOVISKO:

1. ÚVOD

1.1 Poznámka na úvod

Návrh rozhodnutí Rady o konzultačním přístupu do VIS pro orgány členských států odpovědné za vnitřní bezpečnost a pro Europol za účelem prevence, odhalování a vyšetřování teroristických trestných činů a dalších závažných trestných činů (dále jen: „návrh") odeslala Komise evropskému inspektorovi ochrany údajů (EIOÚ) v dopise ze dne 24. listopadu 2005. EIOÚ chápe tento dopis jako žádost o radu pro orgány a subjekty Společenství, jak je uvedena v čl. 28 odst. 2 nařízení (ES) č. 45/2001. Podle Evropského inspektora ochrany údajů by toto stanovisko mělo být uvedeno v preambuli rozhodnutí.

EIOÚ považuje za důležité zaujmout k tomuto citlivému tématu stanovisko, neboť tento návrh přímo vyplývá ze zavedení vízového informačního systému (VIS), který bude podléhat jeho kontrole a k němuž vydal stanovisko dne 23. března 2005 ([1]). V uvedeném stanovisku se již předpokládala možnost přístupu donucovacích orgánů (viz níže); vytvoření nových přístupových práv do VIS má na tento systém rozhodující vliv z hlediska ochrany údajů. Vydání stanoviska k tomuto návrhu tedy nutně navazuje na první stanovisko.

1.2 Význam návrhu

a) *Souvislosti*

Předkládaný návrh je důležitý nejen sám o sobě, ale i proto, že je součástí obecné tendence umožnit donucovacím orgánům přístup do několika rozsáhlých informačních a identifikačních systémů. O tom se hovoří mimo jiné ve sdělení Komise ze dne 24. listopadu 2005 o zvýšené účinnosti, zvýšené interoperabilitě a synergiích evropských databází v oblasti spravedlnosti a vnitřních věcí ([2]), zejména v bodě 4.6 tohoto sdělení: „*V souvislosti s cílem boje proti terorismu a trestné činnosti je podle aktuálního názoru Rady nevyhovující, že orgány odpovědné za vnitřní bezpečnost nemají přístup k údajům VIS. Totéž lze konstatovat rovněž o údajích SIS II týkajících se přistěhovalectví a o údajích systému EURODAC.*"

Předložený návrh by tedy mohl být považován za výchozí návrh pro podobné právní nástroj vypracované v souvislosti s jinými databázemi a je velmi důležité stanovit ihned od počátku případy, kdy by tento přístup bylo možné povolit.

([1]) 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).

([2]) KOM(2005) 597 v konečném znění.

b) *Dopad nových přístupových práv do VIS*

EIOÚ bezpochyby uznává, že je zapotřebí, aby donucovací orgány mohly využívat co nejlepších nástrojů pro identifikaci pachatelů teroristických činů nebo dalších závažných trestných činů. Je si rovněž vědom toho, že údaje VIS mohou být pro tyto orgány za jistých okolností zásadním zdrojem informací.

Avšak umožnění přístupu do databází prvního pilíře donucovacím orgánům, třebaže je lze odůvodnit bojem proti terorismu, zdaleka nelze považovat za nepodstatnou záležitost. Je třeba mít na paměti, že VIS je informační systém, který byl vyvinut s ohledem na uplatňování evropské vízové politiky, a nikoli jako nástroj pro vynucování práva. Běžný přístup by představoval vážné porušení zásady omezení účelu. Přinesl by s sebou neúměrné narušení soukromí cestujících, kteří dali souhlas se zpracováváním svých osobních údajů, aby získali vízum, a kteří očekávají, že jejich údaje budou shromažďovány, že se do nich bude nahlížet a že budou předávány pouze za tímto účelem.

Vzhledem k tomu, že informační systémy se budují za zvláštním účelem, který je určující pro ochranná opatření, bezpečnost a podmínky přístupu, porušovalo by umožnění systematického přístupu za jiným než původním účelem nejen zásadu omezení účelu, ale mohlo by rovněž způsobit, že výše uvedené prvky budou nepřiměřené nebo nedostatečné.

Dále by takto významná změna systému mohla rovněž narušit platnost výsledků studie posouzení dopadů (která se zabývala pouze využitím sytému pro původní účel). Totéž platí pro stanoviska orgánů zabývajících se ochranou údajů. Dalo by se říci, že nový návrh mění výchozí předpoklady pro jejich ověřovací šetření.

c) *Přísné omezení tohoto přístupu*

S ohledem na výše uvedené připomínky by EIOÚ rád zdůraznil, že přístup do vízového informačního systému může být donucovacím orgánům umožněn pouze za zvláštních okolností, v jednotlivých případech, a musí být provázen přísnými ochrannými opatřeními. Jinými slovy, nahlédnutí ze strany donucovacích orgánů musí být vhodnými technickými a právními prostředky omezeno na zvláštní případy.

EIOÚ již ve svém stanovisku k VIS zdůraznil toto: *„EIOÚ si uvědomuje, že donucovací orgány mají zájem na tom, aby jim byl umožněn přístup do 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“.*

Zásadní požadavky by se daly shrnout takto:

— Neměl by se umožnit systematický přístup: rozhodnutí musí po celou dobu zajišťovat, aby případ od případu byla přezkoumána potřebnost a přiměřenost přístupu orgánů třetího pilíře. V tomto ohledu je rozhodující přesné znění právního nástroje, aby nezůstal prostor pro rozšířený výklad, který by dále vedl k běžnému přístupu.

— V případech, kdy je přístup umožněn, musí být s ohledem na to, že se jedná o citlivou záležitost, přijata příslušná ochranná opatření a podmínky, včetně komplexního režimu ochrany údajů pro jejich vnitrostátní využití.

1.3 **Úvodní připomínky**

EIOÚ uznává, že v tomto navrhovaném nástroji byla značná pozornost věnována ochraně údajů, a zejména omezením přístupu na zvláštní případy a výhradně v rámci boje proti závažné trestné činnosti ([1]).

Z dalších kladných prvků by EIOÚ rovněž rád výslovně zmínil tyto:

— omezení na některé formy trestné činnosti, které jsou uvedeny v Úmluvě o Europolu;

— povinnost členských států sestavit seznam orgánů majících přístup a zveřejnění těchto seznamů;

— existenci ústředního přístupového bodu pro každý členský stát (a specializované jednotky v rámci Europolu), umožňující lepší třídění žádostí o přístup, jakož i lepší kontrolu;

— přísná pravidla pro další předávání údajů, podle čl. 8 odst. 5 návrhu;

— povinnost členských států a Europolu vést záznamy o osobách odpovědných za nahlížení do údajů.

2. **ANALÝZA NÁVRHU**

2.1 **Poznámka na úvod**

Aby byl orgánům umožněn přístup podle třetího pilíře, měl by hlavní návrh týkající se VIS, jehož základem je první pilíř, obsahovat překlenovací ustanovení, které by v zásadě určovalo možný obsah takového právního nástroje v rámci třetího pilíře, jakým je tento návrh. V době, kdy EIOÚ vydal své stanovisko k VIS, nebylo toto překlenovací ustanovení ještě zavedeno a EDPS se k němu nemohl vyjádřit. Všechny zde uvedené připomínky jsou proto míněny s výhradou obsahu překlenovacího ustanovení.

([1]) To je rovněž v souladu se závěry Rady z března a července roku 2005, kde se vyžaduje udělení přístupu do vízového informačního systému orgánům pověřeným vnitřní bezpečností *„za podmínky přísného souladu s pravidly upravujícími ochranu osobních údajů“*.

2.2 **Účel přístupu**

Pro zajištění řádného omezení přístupu je nutné pečlivě stanovit podmínky přístupu do VIS. EIOÚ vítá skutečnost, že kromě samotného návrhu rozhodnutí je záměr poskytovat přístup pouze v jednotlivých případech velmi jasně stanoven též v důvodové zprávě a v bodech odůvodnění (viz zejména 7. bod odůvodnění).

K článku 5 návrhu lze učinit jednu poznámku zaměřenou na jeho výklad.

Článek 5 omezuje rozsah přístupu věcnými podmínkami:

b) přístup za účelem nahlédnutí musí být nutný z důvodu prevence, odhalování nebo vyšetřování teroristických trestných činů nebo dalších závažných trestných činů;

c) přístup za účelem nahlédnutí musí být nutný ve zvláštním případě (...), a

d) pro rozhodnutí, že nahlédnutí do VIS přispěje k prevenci, odhalování nebo vyšetřování jakýchkoli uvedených trestných činů, musí existovat přiměřené důvody, založené na konkrétních skutečnostech.

Tyto podmínky jsou kumulativní, přičemž podmínka uvedená v písmeni b) je spíše vymezením oblasti působnosti *ratione materie*. Z praktického hlediska to znamená, že orgán žádající o přístup musí být v situaci, kdy čelí závažnému trestnému činu, jak je uvedeno v písmeni b) návrhu; musí se jednat o zvláštní případ, jak je uvedeno v písmeni c). Orgán navíc musí být schopen prokázat, že nahlédnutí do údajů VIS přispěje v uvedeném zvláštním případě k prevenci, odhalování nebo vyšetřování uvedeného trestného činu, jak je stanoveno v písmeni d).

Rovněž v případě tohoto výkladu článku 5 má EIOÚ obavy v souvislosti s pružným zněním písmene d): formulace „přispěje k“ je velmi široká. Existuje mnoho případů, kdy by údaje z VIS mohly „přispět k“ prevenci nebo vyšetřování závažného trestného činu. EIOÚ je toho názoru, že aby bylo možné odůvodnit přístup k údajům VIS, který se odchyluje od zásady omezení účelu, mělo by toto nahlédnutí „podstatně přispět k“ prevenci, odhalování nebo vyšetřování dotyčného závažného trestného činu, a navrhuje tedy změnit odpovídajícím způsobem článek 5.

V článku 10 se stanoví, že ze záznamů by měl být zřejmý přesný účel přístupu. „Přesný účel“ by měl obsahovat prvky, na základě kterých je nahlédnutí do VIS nutné ve smyslu článku 5 písmene d). To by pomohlo zajistit ověření nezbytnosti veškerých případů nahlédnutí do VIS a současně snížit riziko běžného přístupu.

2.3 **Kritéria pro vyhledávání v databázi VIS**

V čl. 5 odst. 2 a 3 se stanoví dvoustupňový přístup k údajům VIS, přičemž soubor údajů je zpřístupněn pouze tehdy, pokud nahlédnutí do prvního souboru údajů přinese výsledky. Tento přístup je sám o sobě správný. Avšak první soubor údajů se zdá být velmi široký. Zejména lze zpochybnit přiměřenost prvního souboru údajů, uvedeného v čl. 5 odst. 2 písm. e) a i).

— „Účel cesty“ se zdá být příliš obecným kritériem pro účinné vyhledávání v systému. Navíc s sebou přináší riziko profilování cestujících na základě tohoto prvku.

— Co se týče „fotografií“, možnost vyhledávat v takto rozsáhlé databázi podle fotografií je omezená; výsledky získané na základě tohoto vyhledávání obsahují za současného stavu rozvoje technologií nepřijatelnou míru klamné shody nálezů. Nesprávná identifikace má pro dotčeného jednotlivce velmi vážné důsledky.

EIOÚ proto požaduje, aby údaje uvedené v čl. 5 odst. 2 písm. e) a i) byly považovány za doplňující informace přístupné v případě, že první nahlédnutí ukáže, že systém již obsahuje údaje, a aby byly přesunuty do čl. 5 odst. 3.

Možnost vyhledávat v databázi podle fotografií by jinak mohla být podmíněna posouzením této technologie poradním výborem a vyhledávání by bylo možno provádět pouze v případě, že technologie bude vyspělá a že ji bude možné považovat za dostatečně spolehlivou.

2.4 **Použití v případě členských států, na něž se nevztahuje nařízení o VIS**

Přístup do VIS za účelem nahlédnutí lze udělit rovněž orgánům členských států, které nejsou součástí VIS, odpovědným za vnitřní bezpečnost. Tyto útvary musí nahlédnutí uskutečnit prostřednictvím zúčastněného členského státu a náležitě dodržet podmínky uvedené v čl. 5 odst. 1 písm. b) až d) (tj. postupovat případ od případu) a předložit řádně zdůvodněnou písemnou žádost.

EIOÚ by rád zdůraznil, že je zapotřebí stanovit některé podmínky pro zpracování přesahující rámec nahlédnutí. Pro členské státy účastnící se VIS platí pravidlo, že poté, co byly údaje vyhledány ve VIS, musí být zpracovávány v souladu s rámcovým rozhodnutím o ochraně údajů ve třetím pilíři (viz níže). Stejná podmínka by měla platit pro členské státy, na něž se nevztahuje nařízení o VIS, ale které nahlížejí do údajů v něm uvedených. Stejná logika by se měla uplatnit rovněž na uchovávání záznamů pro budoucí kontrolu. EIOÚ z tohoto důvodu doporučuje vložit do článku 6 návrhu nový odstavec v tom smyslu, že články 8 a 10 rozhodnutí platí rovněž pro ty členské státy, na něž se nevztahuje nařízení o VIS.

2.5 **Režim ochrany údajů**

a) *Použití rámcového rozhodnutí o ochraně údajů ve třetím pilíři*

Vzhledem k tomu, že přístup orgánů odpovědných za vnitřní bezpečnost představuje výjimku, pokud jde o účel VIS, měl by podléhat důslednému režimu ochrany údajů, zajišťujícímu vysokou úroveň ochrany údajů vyhledaných ve VIS a zpracovávaných vnitrostátními orgány nebo Europolem.

V článku 8 návrhu se stanoví, že rámcové rozhodnutí Rady o ochraně osobních údajů zpracovávaných v rámci policejní a soudní spolupráce v trestních věcech (dále jen: „rámcové rozhodnutí") se vztahuje na zpracovávání údajů podle navrhovaného rozhodnutí. Z hlediska ochrany údajů by tento návrh měl být považován za *lex specialis*, jímž se doplňuje nebo upřesňuje *lex generalis* (tj. rámcové rozhodnutí). Například pravidla o dalším předávání údajů jsou v tomto návrhu přísnější a mělo by se postupovat podle nich. Totéž platí o důvodech pro přístup k údajům.

b) *Oblast působnosti*

EIOÚ vítá skutečnost, že režim ochrany údajů stanovený rámcovým rozhodnutím je použitelný na veškeré zpracování osobních údajů podle navrhovaného rozhodnutí. To znamená, že úroveň ochrany údajů musí být rovnocenná, bez ohledu na to, které orgány nahlížejí do údajů VIS.

Vzhledem k tomu, že v článku 2 se tyto orgány definují pomocí funkčního kritéria („orgány v členských státech, které jsou odpovědné za prevenci, odhalování a vyšetřování teroristických trestných činů nebo jiných závažných trestných činů"), mohla by se tato definice vztahovat jak na zpravodajské služby, tak na donucovací orgány. Proto se na zpravodajské služby nahlížející do VIS vztahují v zásadě stejné povinnosti, pokud jde o ochranu údajů, což je samozřejmě pozitivní.

Avšak vzhledem k tomu, že o tomto výkladu použitelnosti rámcového rozhodnutí na zpravodajské služby v případě jejich přístupu do VIS mohou existovat pochybnosti, navrhuje EIOÚ alternativní formulaci, například v tomto znění:

„V případech, na něž se nevztahuje rámcové rozhodnutí (…), stanoví členské státy úroveň ochrany údajů, která je přinejmenším rovnocenná s úrovní jejich ochrany podle rámcového rozhodnutí".

c) *Kontrola*

Pokud jde o znění článku 8, mělo by se ujasnit, že odstavec 1 se týká zpracovávání údajů na území členských států. V odstavcích 2 a 3 je objasněna jejich oblast působnosti (zpracovávání údajů Europolem a Komisí) a mělo by být výslovně stanoveno, že odstavec 1 se vztahuje na jiný případ.

Rozdělení kontrolních pravomocí na základě příslušných činností různých subjektů je správný přístup. Jedna věc však chybí: potřeba koordinovaného přístupu při výkonu kontroly. Jak již bylo uvedeno ve stanovisku EIOÚ k VIS: „Pokud jde o kontrolu VIS, je rovněž důležité zdůraznit, že kontrolní činnosti kontrolních orgánů členských států a EIOÚ by měly být do jisté míry koordinovány. Je skutečně zapotřebí, aby při provádění nařízení panoval soulad a aby se pracovalo na společném přístupu ke společným problémům.

Článek 35 [návrhu týkajícího se VIS] by tedy měl obsahovat ustanovení v tom smyslu, že EIOÚ pořádá alespoň jednou ročně schůzku, již se účastní všechny kontrolní orgány členských států."

Totéž platí pro toto konkrétní použití systému VIS (v tomto případě rovněž za účasti společného kontrolního orgánu Europolu). Kontrola by měla probíhat zcela v souladu s kontrolou „VIS prvního pilíře", neboť se jedná o stejný systém. Model koordinačních schůzek, které svolává EIOÚ a jichž se účastní všechny strany provádějící kontrolu, byl navíc zvolen rovněž pro kontrolu jiných rozsáhlých informačních systémů, jako je Eurodac.

EIOÚ si je vědom, že koordinace se do jisté míry předpokládá v návrhu, který zmiňuje úlohu budoucí Pracovní skupiny pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů, zřízené podle článku 31 navrhovaného rámcového rozhodnutí. Je však třeba opětovně zdůraznit, že kontrola jako taková není součástí poslání tohoto poradního orgánu.

EIOÚ navrhuje vložit ustanovení o tom, že koordinační schůzce svolané EIOÚ v rámci kontroly „VIS prvního pilíře" rovněž náleží pravomoc v oblasti zpracování údajů podle tohoto návrhu a že by v tomto smyslu měl být zastoupen společný kontrolní orgán Europolu.

2.6 **Interní kontroly**

V článku 12 návrhu se stanoví systém sledování VIS. EIOÚ zastává názor, že monitorování by se mělo týkat nejen aspektů výkonu, účinnosti vynaložených prostředků a kvality služeb, ale i souladu se zákonnými požadavky, zejména v oblasti ochrany údajů. Odpovídajícím způsobem by měl být změněn článek 12.

Aby mohla provádět tuto interní kontrolu zákonnosti postupů, měla by Komise mít možnost využívat záznamů vedených v souladu s článkem 10 návrhu. V souladu s tím by v článku 10 mělo být stanoveno, že tyto záznamy budou uchovávány nejen za účelem monitorování ochrany údajů a zajištění jejich bezpečnosti, ale i za účelem provádění pravidelných interních kontrol VIS. Zprávy na základě interních kontrol přispějí k plnění kontrolního úkolu EIOÚ a ostatních kontrolních subjektů, které budou lépe schopny zvolit si oblasti, na něž se při kontrole především zaměří.

3. ZÁVĚR

Vzhledem k výše uvedeným skutečnostem EIOÚ zdůrazňuje, že je zásadní, aby přístup orgánů odpovědných za vnitřní bezpečnost a Europolu byl umožňován pouze v jednotlivých případech a za přísných ochranných opatření. Tohoto cíle je v návrhu dosaženo celkově uspokojivým způsobem, třebaže lze provést některá zlepšení, jak je navrženo v tomto stanovisku:

— Podle článku 5 by přístup do VIS měl být podmíněn tím, že nahlédnutí „významně“ přispěje k prevenci, odhalování nebo vyšetřování závažného trestného činu, a záznamy vyžadované v článku 10 by měly umožnit posouzení této podmínky v každém konkrétním případě.

— Dvě kritéria pro vyhledávání ve VIS uvedená v čl. 5 odst. 2, tj. „účel cesty“ a „fotografie“, by měla být přezkoumána a zpřístupněna jakožto doplňující informace v případě získaných výsledků.

— Úroveň ochrany údajů v případě překročení rámce nahlédnutí by měla být rovnocenná bez ohledu na to, který orgán nahlíží do VIS. Články 8 a 10 by měly platit rovněž pro členské státy, na něž se nevztahuje nařízení o VIS.

— Měl by být zajištěn koordinovaný přístup v oblasti kontroly, a to rovněž pokud jde o přístup do VIS předpokládaný v tomto návrhu.

— Ustanovení týkající se systémů sledování by měla rovněž zajistit interní kontrolu jejich souladu s požadavky na ochranu údajů.

V Bruselu dne 20. ledna 2006.

Peter HUSTINX

Evropský inspektor ochrany údajů