EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

Stanovisko Evropského inspektora ochrany údajů

— k návrhu rozhodnutí Rady o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II) (KOM(2005)230 v konečném znění),

— k návrhu nařízení Evropského parlamentu a Rady o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II) (KOM(2005)236 v konečném znění) a

— k návrhu nařízení Evropského parlamentu a Rady o přístupu subjektů odpovědných za vydávání osvědčení o registraci vozidel v členských státech k Schengenskému informačnímu systému druhé generace (SIS II) (KOM(2005)237 v konečném znění)

(2006/C 91/11)

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 17. června 2005,

ZAUJAL TOTO STANOVISKO:

1. ÚVOD

1.1 Základní informace

Schengenský informační systém (SIS) je rozsáhlým informačním systémem Evropské unie, který byl vytvořen jako vyrovnávací opatření poté, co byly v rámci schengenského prostoru zrušeny kontroly na vnitřních hranicích. SIS umožňuje příslušným orgánům v členských státech vyměňovat si informace, jichž se využívá pro provádění kontrol osob a věcí na vnějších hranicích nebo na území příslušného státu, jakož i pro vydávání víz a povolení k pobytu.

Schengenská úmluva vstoupila v platnost v roce 1995 jako mezivládní dohoda. Jako součást Schengenské úmluvy byl SIS později začleněn do rámce EU Amsterodamskou smlouvou.

Nová „druhá generace“ Schengenského informačního systému SIS II nahradí stávající systém, což umožní rozšířit schengenský prostor do nových členských států EU. Do systému budou také zavedeny nové funkce. Schengenská ustanovení vypracovaná v rámci mezivládní spolupráce budou v plném rozsahu převedena na typické nástroje evropského práva.

Dne 1. června 2005 předložila Evropská komise tři návrhy na zřízení SIS II. Tyto návrhy tvoří:

— návrh nařízení na základě hlavy IV Smlouvy o EU (víza, azyl, přistěhovalectví a další politiky týkající se volného pohybu osob), jímž se budou řídit aspekty SIS II pro první pilíř (přistěhovalectví), dále jen „návrh nařízení“,

— návrh rozhodnutí na základě hlavy VI Smlouvy o EU (policejní a soudní spolupráce v trestních věcech), jímž se bude řídit používání SIS II pro účely třetího pilíře, dále jen „návrh rozhodnutí“,

— návrh nařízení na základě hlavy V (doprava), týkající se konkrétně přístupu k údajům v SIS pro orgány odpovědné za registraci vozidel; o tomto návrhu se bude pojednávat odděleně (viz níže uvedený bod 4.6).

V této souvislosti je třeba připomenout, že Komise vydá v nadcházejících měsících sdělení o interoperabilitě a zvýšeném synergickém působení mezi informačními systémy EU (SIS, VIS, Eurodac).

SIS II se skládá z centrální databáze nazývané „Centrální informační schengenský systém“ (CS-SIS), pro který Komise zajistí provozní řízení propojené s národními přístupovými body určenými každým členským státem (NI-SIS). Orgány SIRENE zajistí výměnu veškerých doplňujících informací (informací, které souvisejí se záznamy v SIS II, ale nejsou v SIS II uloženy).

Členské státy budou dodávat do SIS II údaje o osobách hledaných za účelem zatčení, předání nebo vydání, osobách hledaných za účelem soudního řízení, osobách, jež mají být umístěny pod policejní dohled nebo mají být předmětem zvláštních kontrol, osobách, jimž má být odepřen vstup na vnějších hranicích, a o odcizených nebo pohřešovaných věcech. „Záznamy“, tj. soubor údajů, které byly zadány do SIS II, umožňují příslušnému orgánu identifikovat osobu nebo věc.

SIS II představuje tyto nové charakteristiky: rozšířený přístup k SIS (ze strany Europolu, Eurojustu, státních zástupců jednotlivých států, orgánů odpovědných za registraci vozidel), propojení záznamů, doplnění nových kategorií údajů, včetně biometrických údajů (otisků prstů a fotografií), jakož i technickou platformu, která bude společná s Vízovým informačním systémem. Tato doplnění jsou již léta předmětem diskuse o posunu v účelu SIS, a to od nástroje kontroly k systému pro informování a vyšetřování.

1.2 **Obecné zhodnocení návrhů**

1. Evropský inspektor ochrany údajů (EIOÚ) vítá, že je konzultován na základě čl. 28 odst. 2 nařízení (ES) č. 45/2001. S ohledem na závazný charakter čl. 28 odst. 2 by však toto stanovisko mělo být uvedeno v preambuli znění návrhů.

2. EIOÚ vítá návrhy z několika důvodů. Převod mezivládní dohody na nástroje evropského práva má několik kladných důsledků: vyjasní se právní síla pravidel platných pro SIS II, Soudní dvůr bude příslušný k výkladu právního nástroje pro první pilíř a Evropský parlament bude alespoň částečně (i když trochu pozdě) zapojen do tohoto procesu.

3. Navíc je značná část návrhů v podstatě věnována ochraně údajů, přičemž některé z nich představují ve srovnání se současnou situací vítané zlepšení. Zejména se jedná o opatření ve prospěch obětí krádeže totožnosti, rozšíření nařízení 45/2001 na činnost Komise při zpracování údajů v rámci činnosti podle hlavy VI a lepší definování důvodů pro zřízení záznamu o osobách pro účely odepření vstupu.

4. Je rovněž zřejmé, že formulování návrhů byla věnována velká péče; jsou složité, ale to odráží vnitřní složitost systému, který je jimi upravován. Cílem většiny připomínek uvedených v tomto stanovisku je vyjasnit a doplnit ustanovení, což si však nebude vyžadovat kompletního přepracování.

I přes celkové kladné hodnocení lze vyjádřit některé výhrady, které se zvláště týkají tohoto:

1. V mnoha ohledech je obtížné poznat úmysl, který vedl k určitému znění; je velká škoda, že chybí vysvětlení důvodů. Vzhledem ke složitému charakteru těchto dokumentů mělo být vysvětlení důvodů základním požadavkem. Jeho neexistence nedává v některých případech čtenáři jinou možnost než se dohadovat.

2. Je také politováníhodné, že nebyla vypracována žádná studie posouzení dopadu. Na tom nic nemění skutečnost, že první verze systému je již v provozu, protože mezi oběma verzemi jsou značné rozdíly. Mezi jinými se měl lépe domyslet dopad zavedení biometrických údajů.

3. Právní rámec pro ochranu osobních údajů je velmi složitý; vychází z kombinace obecného práva a zvláštního práva. Mělo by být zaručeno, že i v případě vytvoření konkrétních právních předpisů zůstane v plném rozsahu v platnosti stávající rámec pro ochranu údajů uvedený ve směrnici 95/46/ES a v nařízení 45/2001. Kombinované používání různých právních nástrojů by nemělo vést k nesouladu mezi vnitrostátními legislativními režimy v základních aspektech, ani ke snížení stávající úrovně ochrany údajů.

4. Přístup k systému ze strany mnoha nových orgánů, které neodpovídají původnímu „účelu kontrol osob a věcí“, by měl být spojen s přísnějšími ochrannými opatřeními.

5. Návrhy ze značné části vycházejí z jiných právních nástrojů, které se teprve vytvářejí (někdy ještě nebyly ani navrženy). EIOÚ chápe potíže s vytvářením právních aktů ve složitém a neustále se vyvíjejícím prostředí; avšak vzhledem k důsledkům pro dotčené osoby a vzhledem k právní nejistotě, kterou to vytváří, to považuje za nepřijatelné.

6. Rozdělení pravomocí mezi členskými státy a Komisí je poněkud nejasné. Jasnost je nanejvýš důležitá nejen pro hladké fungování systému, ale i pro základní požadavek zajistit soustavnou kontrolu nad systémem.

1.3 **Struktura stanoviska**

Toto stanovisko je uspořádáno takto: nejprve objasňuje právní rámec pro SIS II. Dále se zabývá definicí účelu SIS II a prvků, které se výrazně liší od stávajícího systému. Bod 5 obsahuje připomínky k úloze Komise a členských států, pokud jde o fungování SIS II. Bod 6 se týká práv subjektů údajů a bod 7 pojednává o dozoru prováděném na úrovni členského státu a na úrovni EIOÚ a o spolupráci mezi inspektory. V bodě 8 jsou navrženy některé připomínky a případné změny týkající se bezpečnosti; body 9 a 10 pojednávají o postupu projednávání ve výborech a interoperabilitě. V souhrnu závěrů se nakonec zdůrazňují hlavní závěry pro každý bod.

2. PRÁVNÍ RÁMEC

2.1 **Právní rámec ochrany údajů v SIS II**

V návrzích se uvádí, že jejich právním rámcem ochrany údajů je směrnice 95/46/ES, Úmluva 108 a nařízení 45/2001. Relevantní jsou i další nástroje.

K objasnění tohoto rámce a hlavních bodů, z nichž vychází naše stanovisko, je užitečné připomenout toto:

— Respektování soukromého života je v Evropě zabezpečeno od přijetí Úmluvy o ochraně lidských práv a základních svobod v roce 1950 (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.

— Právo na respektování soukromého života a ochrana osobních údajů byly později zakotveny i do článků 7 a 8 Listiny základních práv Evropské unie. 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.

— Odst. 2 čl. 6 Smlouvy o EU stanoví, že Unie ctí základní práva zaručená Evropskou úmluvou.

Návrhů o SIS II se výslovně týkají tyto tři dokumenty:

— Úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat (dále jen „úmluva 108“) stanoví základní zásady ochrany osob se zřetelem na zpracování osobních údajů. Úmluvu 108 ratifikovaly všechny členské státy. Platí i pro činnost prováděnou v policejní a soudní oblasti. Režimem na ochranu údajů, který se v současné době vztahuje na úmluvu o SIS, je úmluva 108 společně s doporučením Výboru ministrů Rady Evropy č. R (87) 15 ze dne 17. září 1987, upravujícím používání údajů v policejní oblasti.

— 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“*. Je třeba poznamenat, že u většiny členských států se vnitrostátní právní předpisy, jimiž se tato směrnice provádí, vztahují také na činnost zpracování údajů v policejní a soudní oblasti.

— 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“*.

Výklad směrnice 95/46/ES a nařízení 45/2001 se musí zčásti řídit podle příslušné judikatury Evropského soudu pro lidská práva v souladu s Evropskou úmluvou o lidských právech a základních svobodách (EÚLP) z roku 1950. Jinými slovy musí být uvedená směrnice a uvedené nařízení – týkají-li se zpracování osobních údajů, jímž by mohly být porušeny základní svobody, zejména právo na soukromí – vykládány ve světle základních práv. Toto rovněž vyplývá z judikatury Evropského soudního dvora ([1]).

([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.

Dne 4. října 2005 vydala Komise „Návrh rámcového rozhodnutí Rady o ochraně osobních údajů zpracovávaných v rámci policejní a soudní spolupráce v trestních věcech“ ([1]) (dále jen „návrh rámcového rozhodnutí“). Tímto rámcovým rozhodnutím má být nahrazena úmluva 108 jako právní předpis, na který odkazuje návrh rozhodnutí o SIS II, což bude mít v této souvislosti pravděpodobně vliv na režim ochrany údajů (viz níže uvedený bod 2.2.5).

2.2 **Právní režim ochrany údajů v SIS II**

2.2.1 *Všeobecné poznámky*

Legislativní základ, jímž se musí SIS II řídit, sestává ze samostatných nástrojů; jak je však uvedeno v bodech odůvodnění, toto „nemá vliv na zásadu, že SIS II představuje jediný informační systém, který by měl jako takový fungovat. Proto by určitá ustanovení těchto nástrojů měla být totožná“.

Struktura obou dokumentů je v zásadě stejná, přičemž v obou zněních jsou kapitoly I až III téměř totožné. Skutečnost, že na SIS II je nutno pohlížet jako na jediný informační systém se dvěma rozdílnými právními základy, se rovněž odráží v poměrně složitém režimu ochrany údajů.

Režim ochrany údajů je částečně určen v samotných návrzích. Jedná se o „*zvláštní právo*“, doplněné o jiné právní předpisy („*obecné právo*“), na které se odkazuje pro každou z oblastí (Komisi, členské státy v prvním pilíři, členské státy ve třetím pilíři).

U této struktury vzniká problém, jak řešit otázku zvláštních souborů pravidel ve vztahu k obecnému právu. V tomto případě EIOÚ považuje zvláštní pravidlo za aplikaci obecného pravidla. *Zvláštní právo* tudíž musí být vždy v souladu s *obecným právem*; rozvíjí (upřesňuje nebo doplňuje) *obecné právo*, ale není pojato jako výjimka z tohoto práva.

Pokud jde o otázku, kterého pravidlo by mělo se v konkrétních případech použít, zásadou je, že *zvláštní právo* se použije přednostně; kde však není vysloveno nebo je nejasné, mělo by se odkázat na *obecné právo*.

V souladu s touto strukturou existují tři různé kombinace *obecného práva* a *zvláštního práva*. Lze je shrnout následovně.

2.2.2 *Režim platný pro Komisi*

Pokud se věc týká Komise, použije se nařízení 45/2001 včetně úlohy EIOÚ, bez ohledu na to, zda je činnost prováděna v rámci prvního pilíře (navrhované nařízení) nebo třetího pilíře (navrhované rozhodnutí). V bodu odůvodnění 21 navrhovaného rozhodnutí se uvádí, že: „Nařízení (ES) č. 45/2001 (…) platí pro zpracování osobních údajů Komisí, pokud k němu dochází při výkonu činnosti, která částečně nebo zcela spadá do oblasti působnosti práva Společenství. Část zpracování osobních údajů v SIS II spadá do oblasti působnosti práva Společenství.“

Jsou k tomu tyto praktické důvody: pokud se týká Komise, bylo by krajně obtížné určit, zda se údaje zpracovávají při výkonu činnosti, která spadá do právních předpisů prvního nebo třetího pilíře.

Používání jednoho právního nástroje pro veškerou činnost Komise související s SIS II nejenže dává z praktického hlediska větší smysl, ale rovněž zlepšuje důslednost (podle bodu odůvodnění 21 navrhovaného nařízení zajišťuje „důsledné a jednotné uplatňování pravidel o ochraně základních práv a svobod osob v souvislosti se zpracováním osobních údajů“). EIOÚ proto vítá souhlas Komise s tím, že nařízení 45/2001 se vztahuje na veškerou činnost Komise při zpracování údajů v SIS II.

2.2.3 *Režim platný pro členské státy*

Situace členských států je složitější. Zpracování osobních údajů za použití navrhovaného nařízení se řídí samotným navrhovaným nařízením a rovněž směrnicí 95/46/ES. Z bodu odůvodnění 14 navrhovaného nařízení jasně vyplývá, že tato směrnice musí být považována za obecné právo, kdežto nařízení o SIS II bude představovat zvláštní právo. To sebou nese celou řadu důsledků, které budou v dalším textu podrobně rozebrány.

Pokud jde o navrhované rozhodnutí, je právním nástrojem ochrany údajů, na který se odkazuje (obecné právo), úmluva 108, což může v některých bodech znamenat velký rozdíl mezi režimy ochrany údajů v prvním a ve třetím pilíři.

2.2.4 *Dopad na úroveň ochrany údajů*

Ve své obecné připomínce k této architektuře ochrany údajů EIOÚ zdůrazňuje toto:

— Použití navrhovaného nařízení jako zvláštního práva pro směrnici 95/46/ES (a obdobně použití navrhovaného rozhodnutí jako zvláštního práva pro úmluvu 108) by v žádném případě nemělo vést ke snížení úrovně ochrany údajů, zaručené směrnicí nebo úmluvou. EIOÚ předloží v tomto směru doporučení (viz například právo na opravné prostředky).

([1]) (KOM(2005) 475 v konečném znění).

— Obdobně nesmí být výsledkem kombinovaného uplatňování právních nástrojů to, že se sníží úroveň ochrany údajů zaručená podle aktuální Schengenské úmluvy (viz například níže uvedené připomínky ke článku 13 směrnice 95/46/ES).

— Používání dvou různých nástrojů, i když je jich vzhledem k rámci evropského práva zapotřebí, by nemělo vést k neoprávněným rozdílům mezi ochranou údajů o dotčených osobách v závislosti na druhu údajů, které se o nich zpracovávají. Tomuto je třeba bránit v co nejvyšší možné míře. Doporučení uvedená v dalším textu budou také zaměřena na zlepšení důslednosti a jednotnosti (viz například pravomoc vnitrostátních kontrolních orgánů).

— Právní rámec je tak složitý, že je velmi pravděpodobné, že se při praktickém provádění objeví nejasnosti. V některých případech je obtížné rozeznat, jak na sebe obecné a zvláštní právo vzájemně působí, a bylo by tedy užitečné toto v návrzích objasnit. V tomto složitém právním prostředí se navíc jeví jako velmi užitečný návrh, který předložil Společný kontrolní orgán pro Schengen (JSA Schengen) ve svém „stanovisku k navrhovanému právnímu základu pro SIS II“ (ze dne 27. září 2005), že vypracuje „uživatelskou příručku“ s přehledem o všech právech existujících v souvislosti s SIS II a s jasnou hierarchií platných právních předpisů.

A konečně bude toto stanovisko usilovat o to, aby byla zaručena vysoká úroveň ochrany údajů, důslednost a jasnost a aby se subjektu údajů dostalo nezbytné právní jistoty.

2.2.5 *Dopad návrhu rámcového rozhodnutí na ochranu údajů ve třetím pilíři*

Pro návrh rozhodnutí o SIS II bude úmluva 108 nahrazena jako nástroj ochrany údajů, na který se odkazuje, rámcovým rozhodnutím o ochraně údajů ve třetím pilíři ([1]). Toto není v návrhu uvedeno, ale vyplývá to z navrhovaného rámcového rozhodnutí. V jeho čl. 34 odst. 2 se uvádí, že „jakýkoli odkaz na Úmluvu Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat se považuje za odkaz na toto rámcové rozhodnutí“. EIOÚ vydá v průběhu příštích týdnů stanovisko k návrhu rámcového rozhodnutí a v tomto stanovisku nebude jeho obsah podrobně rozebírat. Avšak v případech, kdy je pravděpodobné, že použití rámcového rozhodnutí bude mít značný dopad na režim ochrany údajů v SIS II, toto bude uvedeno.

([1]) Toto rámcové rozhodnutí rovněž nahradí obecný režim ochrany údajů v Schengenské úmluvě (články 126 a 130 Schengenské úmluvy). Tento režim se nevztahuje na SIS.

2.2.6 *Použití článku 13 směrnice 95/46/ES a článku 9 úmluvy 108*

Článek 13 směrnice 95/46/ES a článek 9 úmluvy 108 dávají členským státům možnost přijmout legislativní opatření, jimiž omezí rozsah povinností a práv podle těchto nástrojů, pokud takové omezení představuje opatření nezbytné pro ochranu důležitých zájmů (např. bezpečnosti státu, obrany, veřejné bezpečnosti) ([2]).

V bodech odůvodnění navrhovaného nařízení i navrhovaného rozhodnutí se uvádí, že této možnosti by mohly členské státy využít při provádění návrhů na vnitrostátní úrovni. V tom případě by se mělo vyžadovat splnění těchto dvou podmínek: použití článku 13 směrnice 95/46/ES musí být v souladu s článkem 8 EÚLP a nemělo by vést ke zmírnění stávajícího režimu ochrany údajů.

V případě SIS II je to ještě důležitější, protože tento systém musí mít předvídatelný charakter. Vzhledem k tomu, že členské státy své údaje sdílejí, musí existovat možnost, aby s dostatečnou jistotou věděly, jak budou na vnitrostátní úrovni zpracovány.

V tomto ohledu existuje jeden zvláště znepokojivý prvek, kdyby totiž návrhy vedly ke snížení stávající úrovně ochrany údajů. Článek 102 Schengenské úmluvy počítá se systémem, v němž je využití údajů přísně regulováno a omezeno, a to i ve vnitrostátních právních předpisech („Každé využití údajů, které není v souladu s odstavci 1 a 4, je podle vnitrostátních právních předpisů dané smluvní strany považováno za zneužití“). Jak směrnice 95/46/ES, tak úmluva 108 však stanoví, že ve vnitrostátních právních předpisech lze učinit výjimky, zejména výjimku ze zásady omezení účelu zpracování údajů. Pokud se tak učiní, představovalo by to rozpor se stávajícím systémem v Schengenské úmluvě, podle níž se vnitrostátní právní předpisy nesmí odchýlit od základní zásady omezení účelu zpracování údajů a jejich využití.

Přijetím rámcového rozhodnutí by se nezměnilo toto zjištění: je mnohem větším problémem přísně dodržet zásadu omezení účelu zpracování údajů v SIS II než zajistit, aby údaje byly zpracovávány v souladu s rámcovým rozhodnutím.

([2]) Členský stát, který využije možnosti omezit práva, tak smí učinit jen v souladu s článkem 8 EÚLP, jak bylo zmíněno dříve.

EIOÚ navrhuje zařadit do návrhů o SIS II (zejména do článku 21 navrhovaného nařízení a článku 40 navrhovaného rozhodnutí) ustanovení, které bude mít stejný účinek jako stávající čl. 102 odst. 4 Schengenské úmluvy, omezující možnost členských států stanovit takové využití údajů, které není předpokládáno ve zněních o SIS II. Další možností je v navrhovaném rozhodnutí a navrhovaném nařízení výslovně omezit rozsah výjimek, jichž lze podle článku 13 směrnice nebo článku 8 úmluvy použít, například tím, že se stanoví, že členské státy mohou omezit pouze právo přístupu a právo být informován, ale nikoli zásady týkající se kvality údajů.

3. ÚČEL

Podle článku 1 obou dokumentů („zřízení a obecný cíl SIS II“) se SIS II zřizuje, aby „umožnil příslušným orgánům v členským státech vyměňovat si informace, jichž se využívá pro provádění kontrol osob a věcí“ a „přispěje k zachování vysoké úrovně bezpečnosti v rámci prostoru bez kontrol na vnitřních hranicích mezi členskými státy“.

Účel SIS II je formulován dosti široce; výše uvedená ustanovení nejsou sama o sobě přesným vyjádřením, čeho se tento cíl týká (co se jím míní).

Jak se zdá, cíl SIS II je mnohem širší, než cíl stávajícího SIS tak, jak je stanoven v článku 92 Schengenské úmluvy, kde se konkrétně hovoří o „(…) přístupu k záznamům o osobách a věcech při provádění hraničních kontrol a jiných policejních a celních kontrol (…) a (pro kategorie záznamů podle článku 96) zajistí přístup k těmto záznamům pro účely řízení o udělování víz, vydávání povolení k pobytu a řízení s cizinci (…)“.

Tento širší cíl rovněž vyplývá z toho, že do SIS II byly doplněny nové funkce a přístupy, které neodpovídají původnímu cíli kontrol osob a věcí, ale jsou spíše nástrojem pro vyšetřování. Zejména se předpokládá přístup pro orgány, které budou využívat údajů ze SIS II pro své vlastní účely a nikoli pro uskutečňování účelů SIS II (viz níže); všeobecně bude zavedeno propojení záznamů, což je typickým rysem nástroje policejního vyšetřování.

Jsou zde i otázky týkající se vyhledávače na základě biometrických údajů, který má být vyvinut v příštích létech a který má umožnit vyhledávání v systému, což přesahuje jeho potřeby jako kontrolního systému.

Na závěr je nutno říci, že oblast působnosti návrhů je mnohem širší než u stávajícího rámce. To si vyžaduje dodatečných ochranných opatření. Se zřetelem na to se EIOÚ ve své analýze tolik nezaměří na širokou definici v článku 1 jako takovou, ale spíše na funkce a další části, ze kterých se skládá SIS II.

4. VÝZNAMNÉ ZMĚNY V SIS II

Tato kapitola se nejprve zaměří na nové prvky SIS II, jako je zavedení biometrie, nová koncepce přístupu se zvláštním zřetelem na přístup Europolu, Eurojustu a orgánů odpovědných za registraci vozidel, propojení záznamů a přístup různých orgánů k údajům o přistěhovalectví.

4.1 Biometrie

Návrhy o SIS II zavádějí možnost zpracovávat novou kategorii údajů – biometrické údaje -, které si zaslouží zvláštní pozornosti. Jak již bylo zdůrazněno ve stanovisku EIOÚ o vízovém informačním systému ([1]), citlivá povaha biometrických údajů si vyžaduje zvláštních ochranných opatření, která nebyla do návrhů o SIS II zařazena.

Všeobecně lze říci, že tendence využívat ve velkých informačních systémech EU (ve VIS, EURODAC, Informačním systému o řidičských průkazech a jiných) biometrických údajů se vytrvale šíří, ale nedoprovází ji pečlivé posouzení s tím souvisejících rizik a nezbytných ochranných opatření.

Tato potřeba hlubšího zamyšlení byla rovněž zdůrazněna v nedávném usnesení o biometrii, které bylo přijato na Mezinárodní konferenci inspektorů ochrany údajů a soukromého života konané v Montreux ([2]) Až dosud se výhody zavedení norem zaměřovaly pouze na zvýšení interoperability mezi systémy a nikoli na zlepšení kvality biometrických postupů.

([1]) Stanovisko EIOÚ k návrhu nařízení Evropského parlamentu a Rady o vízovém informačním systému a výměně údajů o krátkodobých vízech mezi členskými státy ze dne 23. března 2005, bod 3.4.2.

([2]) 27. Mezinárodní konference inspektorů ochrany údajů a soukromého života, Montreux, 16. září 2005, usneseni o využívání biometrie v pasech, průkazech totožnosti a cestovních dokladech.

Bylo by užitečné vytvořit soubor společných povinností nebo požadavků odpovídajících zvláštnostem těchto údajů a rovněž společnou metodiku jejich uplatňování v praxi. Tyto společné požadavky by mohly obsahovat zejména prvky, jejichž potřeba je dokreslena v návrzích o SIS II. Jsou to zejména tyto prvky:

— **Cílená studie posouzení dopadu:** Je nutno podtrhnout, že návrhy nebyly předmětem studie posouzení dopadu, vyplývajícího z používání biometrie ([1]).

— **Důraz na postup registrování:** Není podrobně popsán ani zdroj biometrických údajů, ani způsob, jak mají být shromažďovány. V celkovém procesu biometrické identifikace je registrování kritickým krokem a nelze je definovat v přílohách ani v dalších jednáních v podskupinách, protože přímo podmiňuje konečný výsledek procesu, tj. stupeň chybných odmítnutí nebo chybných přijetí.

— **Důraz na stupeň přesnosti:** Používání biometrie pro identifikaci (porovnání jednoho prvku s mnoha dalšími), předkládané v návrhu jako budoucí realizace „biometrického vyhledávače", je ještě kritičtějším krokem, protože výsledky tohoto procesu jsou méně přesné než výsledky, kterých by se dosáhlo při použití údajů za účelem ověřování nebo kontroly (porovnání jednoho prvku s jedním). Biometrická identifikace by tedy neměla představovat jediný způsob identifikace nebo jediný klíč pro přístup k dalším informacím.

— **Záložní postup:** Budou vypracovány snadno dostupné záložní postupy, aby byla respektována důstojnost osob, které mohly být chybně identifikovány, a aby se zamezilo tomu, že ponesou tíhu nedokonalosti systému.

Používání biometrických údajů bez řádného předchozího zhodnocení rovněž ukazuje, že spolehlivost biometriky je přeceňována. Biometrické údaje jsou „živými" údaji, které se v průběhu času vyvíjejí; vzorky, které jsou uloženy v databázi, představují jen malý výsek z dynamického prvku. Jejich trvání není absolutní a je nutno je prověřovat. Přesnost biometrie se musí vždy dávat do perspektivy s jinými prvky, protože nikdy nebude absolutní.

Pokud se bude biometrickým důkazům připisovat zvýšená úloha nebo budou přeceňovány, jak ukázaly předchozí případy ([2]), bude případné využívání údajů v SIS II pro účely vyšetřování představovat pro subjekt údajů vážné riziko.

V návrzích by se tedy měly vzít v úvahu reálné možnosti biometrie pro účely identifikace a měla by se zvýšit informovanost o této věci.

4.2 **Přístup k údajům v SIS II**

4.2.1 *Nová koncepce přístupu*

Orgány, které mají přístup k údajům v SIS, jsou definovány pro každý jednotlivý záznam. Pro udělení přístupu k údajům v SIS je nutno v zásadě splnit tyto dvě podmínky: přístup musí být udělen orgánům splňujícím v plném rozsahu obecný účel SIS a splňujícím zvláštní účel daného záznamu.

Toto vyplývá z následující definice záznamů, která se vyskytuje jak v navrhovaném nařízení, tak v navrhovaném rozhodnutí (čl. 3 odst. 1 písm. a) v obou těchto nástrojích: *„Záznamem" se rozumí soubor údajů zadaných do SIS II, umožňující příslušným orgánům identifikovat osobu nebo věc s ohledem na konkrétní opatření, které je třeba učinit).* Čl. 39 odst. 3 navrhovaného rozhodnutí tento názor dále rozvádí s tím, že *„údaje uvedené v odstavci 1 se použijí pouze za účelem zjištění totožnosti osoby se zřetelem ke konkrétnímu opatření, které je třeba učinit v souladu s tímto rozhodnutím"*. V tomto ohledu má SIS II stále ještě rysy systému „hit – no hit", kdy se každý záznam vkládá pro určitý účel (předání, odepření vstupu, ...).

Orgány, které mají přístup k údajům v SIS, mají využívání těchto údajů de facto omezeno, protože v zásadě k nim mají přístup jen k provedení určitého opatření.

Některé z přístupů stanovených v nových návrzích však nejsou s touto logikou v souladu: jejich cílem je poskytovat orgánu informace, a nikoli mu umožňovat, aby identifikoval osobu a činil opatření předpokládané v záznamu.

([1]) Toto posouzení by mohlo vycházet z tzv. sedmi pilířů moudrosti v otázkách biometrie uvedených v „Biometrii na hranicích": hodnocení dopadu na společnost IPTS, DG-JRC, EUR 21585 EN, část 1.2, s. 32.

([2]) V červnu 2004 byl jeden advokát z Portlandu (USA) po dobu dvou týdnů ve vězení, protože FBI zjistil, že jeho otisky prstů odpovídají otiskům nalezeným po bombových atentátech v Madridu (na umělohmotném pytli, který obsahoval rozbušku). Nakonec se prokázalo, že způsob porovnání byl nespolehlivý a způsobil chybu v interpretaci.

To se konkrétně týká:

— přístupu k údajům o přistěhovalectví ze strany azylových orgánů;

— přístupu k údajům o přistěhovalectví ze strany orgánů odpovědných za udělování právního postavení uprchlíka;

— přístupu Europolu k záznamům o vydání, utajeném sledování a odcizených dokumentech pro účely zabavení;

— přístupu Eurojustu k údajům o vydání a místu, kde se osoba nebo věc nachází.

Pro všechny tyto orgány platí ve vztahu k údajům v SIS II tytéž charakteristiky:

nemohou učinit konkrétní opatření předpokládané podle definice záznamu. Přístup je jim udělen jako zdroj informací pro vlastní účely.

I mezi těmito orgány je třeba rozlišovat mezi orgány, které mají přístup pro vlastní účely, ale za určitým konkrétním cílem, a mezi orgány (jmenovitě Europolem a Eurojustem), pro něž neexistuje žádné upřesnění účelu jejich přístupu. Azylové orgány mají například přístup pro konkrétní účel, i když se nejedná o účel uvedený v záznamu. Mohou mít přístup k údajům o přistěhovalectví „za účelem zjištění, zda žadatel o azyl nedovoleně nepobýval v jiném členském státě". Europol a Eurojust mají zase přístup k údajům, obsažených v některých kategoriích záznamů, „které jsou nezbytné k plnění jejich úkolů".

Souhrnně řečeno, přístup k údajům v SIS II se uděluje v těchto třech případech:

— přístup za účelem přijetí opatření podle záznamu,

— přístup za jiným účelem, než který odpovídá SIS II, ale který je dostatečně vymezen v návrzích,

— přístup za jiným účelem, než který odpovídá SIS II, ale který není přesně popsán.

EIOÚ je toho názoru, že ochranná opatření, která je nutno přijmout, by měla být tím přísnější, čím je účel přístupu obecnější. V dalším textu jsou podrobně popsána obecná ochranná opatření a poté se pojednává o situaci Europolu a Eurojustu.

4.2.2 *Podmínky pro udělení přístupu*

1. Přístup lze každopádně udělit jen tehdy, je-li slučitelný s obecným účelem SIS II a je-li v souladu s jeho právním základem.

To v praxi znamená, že přístup k údajům o přistěhovalectví musí podle navrhovaného nařízení podporovat provádění politik, které odpovídají části schengenského acquis týkající se volného pohybu osob.

Obdobně má být cílem přístupu k záznamům, který se předpokládá v rozhodnutí, podporovat operativní spolupráci mezi policejními a soudními orgány v trestních věcech.

V této souvislosti EIOÚ upozorňuje na kapitolu o přístupu k SIS II ze strany subjektů odpovědných za vydávání osvědčení o registraci vozidel (viz níže uvedený bod 4.6).

2. Potřebu přístupu k údajům v SIS II je nutno prokázat, což platí i pro nemožnost získat údaje za použití jiných, méně nešetrných prostředků anebo s velkými obtížemi. Toto mělo být uvedeno v odůvodnění. Jak již bylo řečeno dříve, je velká škoda, že odůvodnění chybí.

3. Využití údajů musí být definováno výslovně a omezujícím způsobem.

Například orgány příslušné v otázkách azylu mají přístup k údajům o přistěhovalectví „za účelem zjištění, zda žadatel o azyl nedovoleně nepobýval v jiném členském státě". Naproti tomu Europol a Eurojust mají přístup k údajům, obsaženým v některých kategoriích záznamů, „které jsou nezbytné k plnění jejich úkolů": tato formulace není dostatečně přesná (viz níže).

4. Podmínky přístupu musí být dostatečně definovány a vymezeny. V rámci určité organizace by se mělo dostat přístupu do SIS II pouze subjektům, které musejí zacházet s údaji ze SIS II. Tato povinnost, která je stanovena v článku 40 navrhovaného rozhodnutí a v čl. 21 odst. 2 navrhovaného nařízení, by se měla doplnit o povinnost vnitrostátních orgánů vést aktuálně platný seznam osob, kterým je povolen přístup do SIS II. Totéž by mělo platit pro Europol a Eurojust.

5. Skutečnost, že těmto orgánům je udělen přístup k údajům v SIS II, není v žádném případě důvodem, aby do systému zadávaly nebo v něm aktualizovaly údaje, které nejsou užitečné pro konkrétní záznam, na němž se podílejí. Nesmějí se doplňovat nové kategorie údajů z toho důvodu, že by byly užitečné pro jiné informační systémy. Tak například, v článku 39 navrhovaného rozhodnutí se počítá s tím, že do záznamů budou zařazovány údaje týkající se vydávajícího orgánu. Těchto údajů není zapotřebí k provedení opatření (zatčení, sledování,…) a jediným důvodem, proč by se mohly zařazovat, je pravděpodobně to, že by zajímaly Europol nebo Eurojust. Pro zpracování těchto údajů by měly být stanoveny jasné důvody.

6. Dobu uchovávání údajů nelze prodlužovat, pokud to není nutné vzhledem k účelu, pro který byly údaje zadány. Znamená to, že i když má Europol nebo Eurojust přístup k těmto údajům, není to dostatečným důvodem pro jejich udržování v systému (byla-li například hledaná osoba jednou vydána, údaje o tom by měly být vymazány, i když by mohly být užitečné pro Europol). Zde bude opět zapotřebí pečlivé kontroly, aby bylo zaručeno dodržování tohoto pravidla vnitrostátními orgány.

4.2.3 *Přístup Europolu a Eurojustu*

a) *Důvody pro přístup*

O přístupu Europolu a Eurojustu k některým údajům v SIS II se již jednalo před tím, než byl rozhodnutím Rady ze dne 24. února 2005 zahájen ([1]). Ve srovnání se všemi ostatními orgány, které mají přístup pro vlastní účely, jim byl přístup udělen za zvláště výhodných podmínek. I když je využití těchto údajů popsáno v kapitole XII rozhodnutí, důvody k udělení přístupu nejsou dostatečně specifikovány. To je tím významnější, vezmeme-li v úvahu, že úkoly Europolu a Eurojustu se v průběhu času budou pravděpodobně rozvíjet.

EIOÚ vybízí Komisi, aby omezujícím způsobem definovala úkoly, jejichž plnění by ospravedlňovalo přístup Europolu a Eurojustu k systému.

b) *Omezení týkající se údajů*

Aby se zabránilo „lovení údajů“ ze strany Europolu a Eurojustu a aby bylo zajištěno, že budou mít přístup jen k údajům „nezbytným pro jejich úkoly“, Společný kontrolní orgán pro Schengen navrhl ve svém stanovisku k návrhům o SIS II ze dne 27. září 2005, aby se přístup Europolu a Eurojustu omezil na údaje o osobách, jejichž jméno se již objevuje v jejich souborech. To by zaručilo, že Europol a Eurojust budou nahlížet jen do záznamů, které se jich týkají. EIOÚ toto doporučení podporuje.

c) *Bezpečnostní aspekty*

EIOÚ vítá povinnost vést protokoly o všech transakcích uskutečněných Europolem a Eurojustem v rámci spojení a rovněž vítá zákaz kopírovat nebo stahovat části systému.

V článku 56 navrhovaného rozhodnutí se předpokládá, že jak Europol, tak Eurojust určí „jeden až dva“ přístupové body. I když lze pochopit, že vzhledem k decentralizaci svých příslušných orgánů by členský stát mohl potřebovat více než jeden přístupový bod, statut a činnost Europolu a Eurojustu takový požadavek neospravedlňují. Je také nutno zdůraznit, že z bezpečnostního hlediska se zvýšením počtu přístupových bodů zvyšuje riziko zneužití, a proto by se takové zvýšení mělo přesně odůvodnit přesvědčivějšími důkazy. Proto EIOÚ navrhuje, aby vzhledem k neexistenci přesvědčivých argumentů byl v případě Europolu a Eurojustu schválen jen jeden přístupový bod.

4.3 **Propojování záznamů**

V článku 26 nařízení a článku 46 rozhodnutí se stanoví, že členské státy mohou vytvářet odkazy mezi záznamy v souladu s vnitrostátními právními předpisy, aby zavedly spojení mezi dvěma nebo více záznamy.

I když odkazy mezi záznamy mohou být pro účely kontrol užitečné (například zatýkací rozkaz na zloděje automobilu může být propojen s ukradeným vozidlem), zavádění odkazů mezi záznamy je typickým rysem nástroje pro policejní vyšetřování.

Propojení záznamů může mít velký dopad na práva dotčených osob, protože osoba se již „nehodnotí“ na základě údajů, které se týkají jen této osoby, ale na základě jejího případného spojení s jinými osobami. Osoby, jejichž údaje jsou propojeny s údaji o pachatelích trestných činů nebo o hledaných osobách, budou pravděpodobně již předem podezřelejší než jiné osoby. Propojování záznamů kromě toho představuje rozšíření vyšetřovacích funkcí SIS, protože umožní registrovat údajné bandy nebo sítě (například propojí-li se údaje o nelegálních přistěhovalcích s údaji o převaděčích). A nakonec, vzhledem k tomu, že zřizování odkazů je ponecháno na vnitrostátních právních předpisech, může to mít za následek, že odkazy, které jsou nepovolené v jednom státě, budou moci být zřízeny jiným státem, čímž budou do systému vstupovat „nepovolené“ údaje.

([1]) Rozhodnutí Rady 2005/211/SVV ze dne 24. února 2005 o zavedení některých nových funkcí Schengenského informačního systému, také se zřetelem k boji proti terorismu (Úř. věst. L 68/44, 15.3.2005)

V závěrech Rady o funkčních požadavcích na SIS II ze dne 14. června 2004 se uvádí, že každý odkaz musí mít jasné funkční požadavky, zakládat se na přesně definovaném vztahu a splňovat zásadu proporcionality. Odkaz navíc nesmí poškozovat práva přístupu. Vzhledem k tomu, že propojování záznamů představuje operaci zpracování, musí každopádně splňovat ustanovení vnitrostátních právních předpisů, kterými se provádí směrnice 95/46/ES nebo úmluva 108.

V návrzích se zdůrazňuje, že existence odkazů nesmí mít vliv na práva přístupu (jinak by se de facto uděloval přístup k údajům, jejichž zpracování by nebylo podle vnitrostátních právních předpisů dovolené a bylo by v rozporu s článkem 6 směrnice).

EIOÚ zdůrazňuje důležitost striktního výkladu článku 26 navrhovaného nařízení a článku 46 navrhovaného rozhodnutí. Toto lze zajistit zejména tak, že se upřesní, že orgány, které nemají právo přístupu k určitým kategoriím údajů, nejenže nemohou mít přístup k odkazům na tyto kategorie, ale ani by neměly o existence těchto odkazů vědět. Kde neexistuje právo přístupu k údajům, na které se odkazuje, musí být vizualizace těchto odkazů znemožněna.

S dotazy na technická opatření, jimiž to bude zaručeno, se prosím obracejte na EIOÚ.

4.4 **Záznamy pro účel odepření vstupu**

4.4.1 *Důvody pro zavedení*

Využívání „záznamů vydaných o státních příslušnících třetích zemí pro účel odepření vstupu“ (článek 15 nařízení) má velký vliv na svobody dané osoby: osoba, která má podle tohoto ustanovení záznam, nemá po dobu několika let přístup do schengenského prostoru. Z hlediska počtu osob, o nichž byl pořízen záznam, toto byl až dosud nejčastěji používaný záznam. Vzhledem k důsledkům tohoto záznamu a počtu osob, jichž se týká, je zapotřebí velké opatrnosti při jeho formulování a rovněž provádění. I když toto platí i pro jiné záznamy, věnuje EIOÚ tomuto záznamu zvláštní kapitolu, protože představuje zvláštní problémy, které souvisejí s důvody pro jeho zavedení.

Nový záznam o odepření vstupu představuje vzhledem k současné situaci zlepšení, ale není zcela uspokojivý, protože se převážně zakládá na nástrojích, které nebyly ještě přijaty a dokonce ani navrženy.

Zlepšení spočívá v přesnějším popisu důvodů pro zařazení údajů. Současné znění Schengenské úmluvy vedlo k situaci, kdy mezi členskými státy vznikaly velké rozdíly, pokud jde o počet osob, o nichž byl pořízen záznam podle článku 96 úmluvy. Společný kontrolní orgán pro Schengen vypracoval souhrnnou studii ([1]) o této otázce a doporučil, aby „tvůrci politik posoudili harmonizaci důvodů pro vytvoření záznamu v různých státech Schengenu“.

Navrhovaný článek 15 je formulován s většími podrobnostmi, což lze uvítat.

Čl. 15 odst. 2 navíc uvádí seznam případů, kdy o osobách nelze pořídit záznam, protože legálně pobývají na území členského státu na základě jiných právních postavení. I když by bylo možno tento mechanismus odvodit ze stávající Schengenské úmluvy, praxe ukázala, že jeho používání se v jednotlivých členských státech liší. Toto objasnění je tedy kladným prvkem.

Toto ustanovení je však také předmětem ostré kritiky, protože vychází z velké části z textu, který nebyl dosud přijat, jmenovitě ze směrnice „o vracení“.

Od té doby, co byly schváleny návrhy o SIS II, Komise navrhla (dne 1. září 2005) „Směrnici o společných normách a postupech v členských státech při vracení nelegálně pobývajících státních příslušníků třetích zemí“, ale vzhledem k tomu, že se nejedná o konečné znění, nelze je považovat za základ platný pro zadávání údajů do systému. Představuje to zejména porušení článku 8 EÚLP, protože narušení soukromého života by se mělo zakládat mezi jinými na jasném a dostupném právním předpisu.

EIOÚ proto vybízí Komisi, aby toto ustanovení buď stáhla nebo přeformulovala je na základě stávajících právních předpisů tak, aby osoby přesně věděly, která opatření mohou vůči nim orgány přijmout.

4.4.2 *Přístup k záznamům zaváděným podle článku 15*

V článku 18 se stanoví, které orgány mají k těmto záznamům přístup a za jakými účely. V čl. 18 odst. 1 a 2 se určuje, které orgány mají přístup k záznamům zavedeným na základě směrnice o vracení. Ohledně této situace platí tytéž připomínky jako připomínky uvedené výše.

([1]) Zpráva Společného kontrolního orgánu pro Schengen o kontrole využití záznamů podle článku 96 v Schengenském informačním systému, Brusel, 20. června 2005.

V čl. 18 odst. 3 navrhovaného nařízení se povoluje přístup orgánům odpovědným za udělování právního postavení uprchlíka v souladu se směrnicí, která ještě nebyla ani navržena. Vzhledem k neexistenci dostupného znění musí EIOÚ zopakovat tytéž připomínky jako připomínky uvedené výše.

4.4.3 *Doba uchovávání záznamů zavedených podle článku 15*

Podle článku 20 se nesmí záznam uchovávat déle, než je doba odepření vstupu stanovená v rozhodnutí (o odjezdu nebo vrácení). To je v souladu s pravidly o ochraně údajů. Záznam bude navíc po pěti letech automaticky vymazán, pokud členský stát, který údaje do SIS II zadal, nerozhodne jinak.

Na vnitrostátní úrovni by se mělo pomocí odpovídající kontroly zajistit, že nedojde k automatickému neoprávněnému prodloužení doby uchování záznamu a že členské státy provedou výmaz údajů před skončením lhůty pěti let, pokud se stane, že doba odepření vstupu bude kratší.

4.5 **Doba uchovávání**

I když zásada, jíž se řídí uchovávání údajů, se nemění (obecně platí, že záznamy by se měly ze SIS II vymazat, jakmile je vykonáno opatření požadované v záznamu), budou mít návrhy za následek všeobecné prodloužení doby uchovávání záznamů.

V Schengenské úmluvě se stanoví, že potřeba nadále uchovávat údaje se přezkoumá ve lhůtě nejpozději tří let od jejich zavedení (nebo jednoho roku u údajů zavedených pro utajené sledování). Nové návrhy předpokládají automatický výmaz (proti němuž může vydávající stát protestovat) ve lhůtě 5 let u údajů o přistěhovalectví, 10 let u údajů o zatčení, pohřešovaných osobách a osobách hledaných pro soudní řízení a 3 let u osob, které mají být předmětem utajeného sledování.

I když členské státy musejí v zásadě vymazat údaje poté, co byl účelu záznamu splněn, jedná se o významné prodloužení maximální doby uchovávání (ve většině případů ztrojnásobení), které Komise nijak neodůvodnila. V případě údajů o přistěhovalectví se lze pouze dohadovat, že lhůta 5 let souvisí s délkou zákazu vstupu navrhovanou v návrhu směrnice o vracení. Pokud je EIOÚ známo, ve všech ostatních případech žádné odůvodnění neexistuje.

Potenciální dopad záznamů v SIS na život dotčených osob může být značný, což je zvláště znepokojivé u záznamů o osobách pro účely utajeného sledování nebo zvláštních kontrol, protože tyto záznamy mohou být pořízeny na základě podezření.

EIOÚ by si přál, aby toto prodloužení doby uchovávání údajů bylo řádně zdůvodněno. Nebude-li předloženo přesvědčivé zdůvodnění, navrhuje snížit dobu uchovávání na současnou délku, přičemž na tomto trvá zejména v případě záznamů pro účely utajeného sledování nebo zvláštních kontrol.

4.6 **Přístup orgánů odpovědných za vydávání osvědčení o registraci vozidel**

Hlavní problém spočívá v tom, že byl zvolen více než sporný právní základ. U opatření, které by umožnilo přístup správních orgánů do SIS pro účely předcházení trestné činnosti a boje proti ní (obchod s kradenými vozidly), Komise přesvědčivě nezdůvodňuje, proč se má použít právního základu „doprava“ odpovídajícího prvnímu pilíři. Nutnost řádného zdůvodnění a solidního právního základu pro udělení přístupu k SIS II je podrobně popsána v bodu 4.2.2 tohoto stanoviska.

EIOÚ se odvolává na připomínky k této věci, které učinil Společný kontrolní orgán Schengen ve svém stanovisku k právnímu základu navrhovanému pro SIS II. Zvláště by se měl zohlednit návrh Společného kontrolního orgánu Schengen na změnu navrhovaného rozhodnutí tak, aby obsahovalo i tento přístup.

5. ÚLOHA KOMISE A ČLENSKÝCH STÁTŮ

Popis a rozdělení odpovědností v rámci SIS II musí být naprosto přesné, a to nejen k zajištění hladkého fungování systému, ale i z hlediska kontroly. Rozdělení kontrolních pravomocí vyplyne z popisu odpovědností, je tedy zapotřebí, aby byl naprosto přesný.

5.1 **Úloha Komise**

V obou návrzích EIOÚ vítá kapitolu III, kde se popisuje úloha a odpovědnost Komise ve vztahu k SIS II (pokud jde o funkci „operativního řízení“). Takové objasnění nebylo v návrhu o VIS obsaženo. Avšak sama tato kapitola nedefinuje úlohu Komise vyčerpávajícím způsobem. Jak je uvedeno v kapitole 9 tohoto stanoviska, Komise se také de facto podílí na provádění a řízení systému prostřednictvím postupu projednávání ve výborech.

Pokud jde o ochranu údajů, sehrává Komise úlohu, kterou již má v systémech VIS a Eurodac, tj. je odpovědná za operativní řízení. Připojíme-li k tomu její velmi důležitou úlohu ve vývoji a fungování systému, měla by se úloha Komise považovat za úlohu kontrolora svého druhu. Jak již bylo řečeno ve stanovisku EIOÚ o VIS, tato úloha jde dále než je úloha zpracovatele údajů, ale zároveň je omezenější než u normálního kontrolora, protože Komise nemá přístup k údajům zpracovávaným v SIS II.

Vzhledem k tomu, že SIS II se bude zakládat na komplexních systémech a některé z nich využívají nově vznikajících technologií, trvá EOIÚ na posilování odpovědnosti Komise za neustálé zdokonalování systémů zaváděním nejlepších dostupných technologií k zajištění bezpečnosti a ochrany údajů.

Proto by se mělo do článku 12 návrhů doplnit, že Komise by měla pravidelně navrhovat zavádění nových technologií, které představují špičku ve svém oboru a jimiž se zvýší úroveň ochrany a bezpečnosti údajů, a které zároveň usnadňují plnění úkolů vnitrostátním orgánům, které mají přístup k těmto údajům.

5.2 **Úloha členských států**

Situace ohledně členských států není příliš jasná, protože je dosti těžké rozeznat, který orgán nebo orgány budou kontrolory údajů.

V návrzích se popisuje úloha Národního úřadu pro SIS II (zajišťuje přístup příslušných orgánů do SIS II) a orgánů SIRENE (zajišťují výměnu všech doplňujících informací). Členské státy rovněž musejí zajistit fungování a bezpečnost svých „NS“ („vnitrostátních systémů“). Není jasně uvedeno, zda tato poslední odpovědnost přísluší jednomu z výše zmíněných orgánů. V tomto ohledu je každopádně nezbytné další upřesnění.

Pokud jde o ochranu údajů, jak Komise, tak členské státy by měly být považovány za společné kontrolory s tím, že každý by měl vlastní odpovědnost. Uznání toho, že jejich odpovědnosti se doplňují, je jedinou cestou, jak zabránit, aby některá z oblastí činnosti SIS II zůstala bez kontroly.

6. **PRÁVA SUBJEKTŮ ÚDAJŮ**

6.1. **Informování**

6.1.1 *Navrhované nařízení*

Článek 28 navrhovaného nařízení uvádí právo subjektu údajů na informování, které vyplývá zejména z článku 10 směrnice 95/46. Ve srovnání se současnou situací, kdy právo na informování není v úmluvě výslovně uvedeno, se jedná o vítanou změnu. V následujících bodech je však ještě prostor pro vylepšení.

Na seznam by měly být doplněny některé informace, což by přispělo k zajištění spravedlivého zacházení se subjektem údajů ([1]). Tyto informace by se měly týkat doby uchovávání údajů, existence práva požadovat přezkum rozhodnutí nebo podat odvolání proti rozhodnutí o pořízení záznamu (v některých případech viz čl. 15 odst. 3 navrhovaného nařízení), možnost získat pomoc od orgánu pro ochranu údajů a existence opravných prostředků.

V navrhovaném nařízení není zmínka o tom, ve které chvíli by se měly informace poskytovat. To by mohlo subjektu údajů znemožnit výkon těchto práv. Aby bylo možno tato práva účinně uplatňovat, měla by se v nařízení přesně stanovit chvíle, kdy by měly být informace poskytnuty, a to podle orgánu, který záznam pořídil.

Praktickým řešením by bylo připojit informace o záznamu k rozhodnutí, na němž se záznam zakládá: k soudnímu nebo správnímu rozhodnutí, založenému na ohrožení veřejného pořádku (…), rozhodnutí o vrácení nebo příkazu k odjezdu spojenému se zákazem opětovného vstupu. Toto by mělo být doplněno do článku 28 nařízení.

6.1.2 *Navrhované rozhodnutí*

V článku 50 rozhodnutí se stanoví, že informace se poskytují na žádost subjektu údajů, a uvádějí se v něm důvody, na něž se lze pro odepření poskytnutí těchto informací odvolat. Omezení tohoto práva je zcela pochopitelné, vezmeme-li v úvahu povahu údajů a v jaké souvislosti se zpracovávají.

Právo na informování by však nemělo být podřízeno žádosti subjektu údajů (v tom případě by se de facto jednalo spíše o definování žádosti o přístup). Dá se předpokládat, že nutnost podat „žádost“ o informace se zdůvodňovala případy, kdy subjekt údajů nelze informovat, protože není zjištěno místo jeho pobytu.

Tato otázka by se dala lépe vyřešit tím, že se doplní výjimka z práva na informování v případech, kdy se ukáže, že poskytnutí informací není možné nebo by znamenalo nepřiměřené úsilí. V tomto smyslu by měl být článek 50 rozhodnutí změněn.

([1]) V témže smyslu viz stanovisko EIOÚ o zřízení Vízového informačního systému, bod 3.10.1.

Toto řešení by také bylo v souladu s použitím návrhu rámcového rozhodnutí o ochraně údajů v rámci třetího pilíře.

6.2 **Přístup**

Jak navrhované nařízení, tak navrhované rozhodnutí stanoví lhůty pro odpovědi na žádosti o přístup, což představuje pozitivní krok. Avšak vzhledem k tomu, že postupy, jimž se řídí výkon práva na přístup, jsou na vnitrostátní úrovni definovány, vzniká otázka, jak by se lhůty stanovené v návrzích daly těmto postupům přizpůsobit, a to zvláště v případě členských států, které mají pro odpověď na žádost o přístup kratší lhůty. Mělo by být jasně upřesněno, že by měly platit lhůty, které jsou pro subjekt údajů nejpříznivější.

6.2.1 *Navrhované nařízení*

Je třeba poznamenat, že omezení práva na přístup („bude zamítnuto, pokud je takové zamítnutí nevyhnutelné pro výkon právního úkonu souvisejícího se záznamem nebo z důvodu ochrany práv a svobod třetích stran"), které je v současné době v Schengenské úmluvě, se v navrhovaném nařízení nevyskytuje.

To je však pravděpodobně způsobeno tím, že lze použít směrnice 95/46/ES, která (v článku 13) počítá s možností provádět výjimky ve vnitrostátních právních předpisech. Každopádně je třeba poznamenat, že použití článku 13 ve vnitrostátních právních předpisech s cílem omezit právo přístupu by mělo být vždy v souladu s článkem 8 EÚLP a mělo by se k němu přikročit pouze v omezeném počtu případů.

6.2.2 *Navrhované rozhodnutí*

V navrhovaném rozhodnutí se stanoví omezení práva přístupu stejně jako v Schengenské úmluvě. Navrhované rámcové rozhodnutí obsahuje v podstatě tatáž omezení práva přístupu; přijetí tohoto nástroje by tedy v tomto bodě neznamenalo žádný velký rozdíl.

Vzhledem k tomu, že v několika členských státech je přístup k údajům o vynucování práva „nepřímý" (což znamená, že se vykonává prostřednictvím vnitrostátního orgánu odpovědného za ochranu údajů), mělo by se pro orgány odpovědné za ochranu údajů stanovit, že při výkonu práva na přístup jsou povinny aktivně spolupracovat.

6.3 **Právo na přezkum rozhodnutí o zřízení záznamu nebo na odvolání proti němu**

V čl. 15 odst. 3 nařízení se zřizuje právo na přezkum nebo odvolání před soudním orgánem proti rozhodnutí o zřízení záznamu, pokud takové rozhodnutí přijal správní orgán. Ve srovnání se stávající Schengenskou úmluvou to představuje vítaný doplněk.

Podtrhuje to nutnost úplně a včas informovat subjekt údajů, jak je zmíněno v bodu 6.1 výše; bez takového informování by toto nové právo platilo pouze teoreticky.

6.4 **Opravné prostředky**

V článku 30 navrhovaného nařízení a v článku 52 navrhovaného rozhodnutí se stanoví právo podat žalobu nebo stížnost před soudy kteréhokoli členského státu, pokud je subjektu údajů odepřeno právo na přístup k údajům, které se ho týkají, právo na opravu nebo výmaz těchto údajů a právo na poskytnutí informací nebo náhradu škody.

Formulace („každý na území členského státu") naznačuje, že žalobce musí být fyzicky přítomen na území, aby mohl podat žalobu soudu. Toto územní omezení není zdůvodněno a mohlo by způsobit, že právo na opravné prostředky nebude účinné, protože se velmi často stává, že žalobce chce podat žalobu právě proto, že mu není povolen přístup na schengenské území. Vzhledem k tomu, že směrnice představuje obecné právo, musí se kromě toho vzít u navrhovaného nařízení v úvahu článek 22 této směrnice, v němž se stanoví, že „každý" má právo na opravný prostředek nezávisle na místě svého pobytu. Navrhované rámcové rozhodnutí již územní omezení neobsahuje. EIOÚ navrhuje vypustit územní omezení z článku 30 a z článku 52.

7. **DOZOR**

7.1 **Úvodní poznámka: rozdělení odpovědností**

V návrzích jsou úkoly dozoru rozděleny mezi vnitrostátní kontrolní orgány a EIOÚ ([1]), a to podle jejich příslušných oblastí působnosti. Toto je v souladu s přístupem k platným právním předpisům a odpovědnosti za fungování a využití SIS II, který je stanoven v návrzích, a s potřebou účinného dozoru.

Tento přístup, vyjádřený v článku 31 navrhovaného nařízení a v článku 53 navrhovaného rozhodnutí, EIOÚ vítá. K lepšímu pochopení a objasnění odpovídajících úkolů však EIOÚ navrhuje rozdělit každý článek na několik ustanovení a každé z nich věnovat určité úrovni dozoru, jak bylo správně provedeno v návrhu o VIS.

([1]) Zde se účastní i kontrolní orgány pro Europol a Eurojust, ale v menší míře.

7.2 **Dozor ze strany vnitrostátních orgánů pro ochranu údajů**

Podle článku 31 navrhovaného nařízení a článku 53 navrhovaného rozhodnutí musí každý členský stát zajistit, aby zákonnost zpracování osobních údajů v SIS II sledoval nezávislý orgán.

V článku 53 navrhovaného rozhodnutí se kromě toho stanoví, že každý má právo požádat kontrolní orgán o kontrolu zákonnosti zpracování údajů v SIS II, které se ho týkají. Podobné ustanovení nebylo do navrhovaného nařízení zařazeno, protože směrnice zde platí jako obecné právo. Proto je nutno vzít v úvahu, že vnitrostátní orgány pro ochranu údajů mohou vykonávat ve vztahu k SIS II všechny pravomoci, které jsou jim svěřeny na základě článku 28 směrnice 95/46/ES, včetně kontroly zákonnosti zpracování údajů. Čl. 31 odst. 1 nařízení objasňuje jejich úkoly, ale nemůže představovat omezení těchto pravomocí. Ve znění navrhovaného nařízení by uznání těchto pravomocí mělo být jasně vyjádřeno.

Pokud jde o navrhované rozhodnutí, ukládají se v něm vnitrostátním kontrolním orgánům rozsáhlejší povinnosti, protože pro ně platí jiné obecné právo. Nebylo by však rozumné, aby kontrolní orgány měly rozdílné úkoly a pravomoci podle kategorie zpracovávaných údajů, protože toto by se v praxi velmi obtížně zajišťovalo. Tomu by se tedy mělo zamezit buď tím, že se v samotném znění navrhovaného rozhodnutí svěří těmto orgánům stejné pravomoci anebo že se odkáže na jiné obecné právo (jmenovitě na rámcové rozhodnutí o ochraně údajů ve třetím pilíři), v němž se uděluje orgánům pro ochranu údajů více pravomocí.

7.3 **Dozor ze strany EIOÚ**

EIOÚ sleduje, zda je činnost Komise při zpracování osobních údajů v SIS II v souladu s návrhy. Zároveň by měl mít EIOÚ možnost vykonávat všechny své pravomoci podle nařízení 45/2001, přičemž by ale bral v úvahu omezené pravomoci, které má Komise ohledně samotných údajů.

Je užitečné doplnit, že podle čl. 46 písm. f) nařízení 45/2001 EIOÚ„spolupracuje s vnitrostátními kontrolními orgány uvedenými v článku 28 nařízení v míře nezbytné pro plnění jejich povinností“. Spolupráce s členskými státy při dozoru nad SIS II nevyplývá pouze z návrhů, ale rovněž z nařízení 45/2001.

7.4 **Společný dozor**

V návrzích se rovněž uznává nutnost koordinovat kontrolní činnost různých orgánů, které se na ní podílí. Článek 31 navrhovaného nařízení a článek 53 navrhovaného rozhodnutí stanoví, že „vnitrostátní orgány pro ochranu údaje a evropský inspektor ochrany údajů spolu aktivně spolupracují. Za tím účelem svolává evropský inspektor ochrany údajů nejméně jednou za rok zasedání“.

EIOÚ vítá tento návrh, který v zásadě obsahuje prvky potřebné k navázání spolupráce – která má skutečně klíčový význam – mezi orgány odpovědnými za dozor na vnitrostátní a na evropské úrovni. Je třeba podtrhnout, že svolání zasedání jednou za rok, které je předpokládáno v návrzích, je nutno považovat za minimum.

Tato ustanovení (článek 31 navrhovaného nařízení a článek 53 navrhovaného rozhodnutí) by však měla být co do obsahu koordinace jasnější. Společný kontrolní orgán (JSA) je příslušný k přezkoumávání obtíží při výkladu nebo uplatňování úmluvy, k posuzování obtíží, které mohou vzniknout při výkonu nezávislého dozoru nebo práva na přístup, a k vypracování harmonizovaných návrhů s cílem nacházet společná řešení stávajících problémů.

Nové návrhy nemohou vést ke zmenšení stávající oblasti působnosti společného dozoru. Je jasné, že orgány pro ochranu údajů mohou ve vztahu k SIS II vykonávat veškeré kontrolní pravomoci, které jim byly svěřeny směrnicí, a že spolupráce těchto orgánů se může vztahovat na široké aspekty dozoru nad SIS II, včetně úkolů stávajícího Společného kontrolního orgánu (JSA) podle článku 115 Schengenské úmluvy.

Aby však toto bylo naprosto jasné, bylo by užitečné to v návrzích výslovně potvrdit.

8. **BEZPEČNOST**

Řízení a dodržování optimální úrovně bezpečnosti pro SIS II představuje základní požadavek k zajištění dostatečné ochrany osobních údajů uložených v databázi. V zájmu dosažení této uspokojivé úrovně ochrany je nutno přijímat vhodná ochranná opatření ke zvládnutí možných rizik spojených s infrastrukturou systému a s dotčenými osobami. O této věci se nyní pojednává v různých částech návrhu a zaslouží si lepšího zpracování.

Články 10 a 13 návrhu obsahují různá opatření pro bezpečnost údajů a vypočítávají druhy zneužití, jimž je třeba předcházet. EIOÚ vítá, že do těchto článků byla zařazena ustanovení o systematické interní kontrole bezpečnostních opatření.

Článek 59 navrhovaného rozhodnutí a článek 34 navrhovaného nařízení, které upravují sledování a hodnocení, by se však neměly týkat pouze aspektů výkonu, účinnosti vynaložených prostředků a kvality služeb, ale rovněž dodržování právních předpisů zejména v oblasti ochrany údajů. EIOÚ proto doporučuje, aby oblast působnosti těchto článků byla rozšířena o sledování zákonnosti zpracování a o předkládání zpráv o této otázce.

V souladu s čl. 10 odst. 1 písm. f) nebo čl. 18 navrhovaného rozhodnutí a článkem 17 navrhovaného nařízení, týkajících se řádně oprávněných pracovníků majících přístup k údajům, by se mělo dále doplnit, že členské státy (a rovněž Europol a Eurojust) by měly zabezpečit dostupnost přesných uživatelských profilů (které by měly být za účelem kontroly k dispozici kontrolním orgánům členských států). Vedle těchto uživatelských profilů musí členské státy navíc vypracovat úplný seznam totožností uživatelů a musí jej neustále aktualizovat. Totéž platí pro Komisi.

Výčet těchto bezpečnostních opatření doplňují ochranná opatření monitorovacího a organizačního rázu. Článek 14 obou návrhů popisuje podmínky a účel vedení záznamů o veškerých provedených operacích zpracování údajů. Tyto záznamy nejsou uchovávány pouze za účelem monitorování ochrany údajů a zajišťování bezpečnosti údajů, ale i za účelem provádění pravidelných interních kontrol SIS II podle článku 10. Interní kontrolní zprávy přispějí k účinnému plnění úkolů kontrolními orgány, které tak budou moci stanovit nejslabší místa a zaměřit se na ně při svém vlastním kontrolním řízení.

Jak již bylo uvedeno výše, zvýšení počtu přístupových bodů do systému musí být přísně odůvodněno, protože se jím automaticky zvyšuje riziko zneužití. V článku 4 odst. 1 písm. b) návrhů by se proto měla stanovit nutnost konkrétně prokázat potřebu druhého přístupového místa.

V návrzích se jasně nevysvětluje, k čemu je zapotřebí vnitrostátních kopií centrálního systému, což vyvolává značné znepokojení, co se týče celkové úrovně rizika a bezpečnosti systému, jako například:

— Zvýšení počtu kopií zvyšuje riziko zneužití (zvláště vezmeme-li v úvahu existenci nových údajů jako jsou biometrické údaje);

— Údaje, jichž se tyto kopie týkají, nejsou jasně definovány;

— Požadavky na přesnost, kvalitu a dostupnost uvedené v článku 9 představují značný technický problém, a tudíž se jimi zvyšují náklady podle stavu vývoje dostupné technologie;

— Dozor nad těmito kopiemi ze strany vnitrostátních orgánů si vyžádá dodatečné lidské a finanční zdroje, které nemusejí být vždy k dispozici.

Vzhledem k existujícím rizikům není EIOÚ přesvědčen o potřebě vnitrostátních kopií (vzhledem k dostupným technologiím) ani o výhodách, které by jejich používání přineslo. Doporučuje zrušit možnost, aby členské státy používaly vnitrostátní kopie.

Pokud se však budou vnitrostátní kopie pořizovat, EIOÚ připomíná, že jejich používání na vnitrostátní úrovni musí podléhat zásadě přísného omezení účelu zpracování údajů. Obdobně se nesmí do vnitrostátní kopie nahlížet jiným způsobem, než který je stanoven pro centrální databázi.

Zákonnost zpracování osobních údajů se zakládá na přísném dodržování bezpečnosti a celistvosti údajů. EIOÚ bude tyto postupy účinně sledovat, pokud bude moci sledovat nejen bezpečnost údajů, ale i jejich celistvost prostřednictvím analýzy dostupných protokolů. Proto je nutné doplnit čl. 14 odst. 6 o „celistvost údajů“.

9. **PROJEDNÁVÁNÍ VE VÝBORECH**

V návrzích se předpokládají postupy projednávání ve výborech v několika případech, kdy je třeba přijmout rozhodnutí technického rázu týkající se provádění a řízení SIS II. Jak bylo uvedeno ve stanovisku o VIS a z podobných důvodů, tato rozhodnutí významně ovlivní vlastní provádění zásady účelu a proporcionality.

EIOÚ doporučuje, aby rozhodnutí mající podstatný vliv na ochranu údajů jako například přístup k údajům a zřizování údajů, výměna doplňujících informací, kvalita údajů a slučitelnost mezi záznamy, technická shoda vnitrostátních kopií atd. se přijímala jako nařízení nebo rozhodnutí, nejlépe postupem spolurozhodování ([1]).

([1]) Ve stejném smyslu viz Stanovisko EIOÚ o vízovém informačním systému, bod 3.12, a Stanovisko EIOÚ o návrhu směrnice o uchovávání údajů zpracovávaných v souvislosti s poskytováním veřejných elektronických komunikačních služeb vydané dne 26. září 2005, s. 60.

Ve všech ostatních případech majících vliv na ochranu údajů by měl mít EIOÚ možnost vyjádřit své stanovisko k výběru provedenému těmito výbory.

Poradní úloha EIOÚ by měla být včleněna do článků 60 a 61 rozhodnutí a do článku 35 nařízení.

V případě technických pravidel pro zřizování odkazů mezi záznamy (článek 26 nařízení a článek 46 rozhodnutí) je nutno vysvětlit, čím se odůvodňují postupy v různých výborech (v poradním výboru v případě rozhodnutí a v regulativním výboru v případě nařízení).

10. **INTEROPERABILITA**

Vzhledem k tomu, že dosud chybí sdělení Komise o interoperabilitě mezi vznikajícími systémy EU, je obtížné správně zhodnotit výhody předpokládaného, ale dosud nedefinovaného synergického působení.

V tomto směru by EIOÚ rád odkázal na prohlášení Rady o boji proti terorismu ze dne 25. března 2004, ve kterém se Komise požaduje, aby předložila návrhy ke zvýšení interoperability a synergického působení mezi informačními systémy (SIS, VIS a Eurodac). EIOÚ rovněž poukazuje na probíhající diskusi o tom, kterému subjektu by v budoucnu bylo možné svěřit řízení různých rozsáhlých systémů (viz rovněž bod 3.8 tohoto stanoviska).

EIOÚ již ve svém stanovisku k Vízovému informačnímu systému uvedl, že interoperabilita je rozhodujícím a zásadním požadavkem k zajištění efektivnosti rozsáhlých informačních systémů jako je SIS II. Nabízí možnost soustavně snižovat celkové náklady a vyhýbat se překrývání různorodých opatření, k němuž přirozeně dochází.

— Interoperabilita může rovněž přispět k cíli udržovat vysoký stupeň bezpečnosti v rámci prostoru bez kontrol na vnitřních hranicích mezi členskými státy, a sice tím, že se do všech prvků, které tvoří tuto politiku, zavedou stejné procesní normy. Zásadní je však rozlišovat mezi dvěma úrovněmi interoperability:

  — interoperabilitou mezi členskými státy EU, která je vysoce žádoucí; Záznam zaslaný orgány jednoho členského státu musí být interoperabilní s těmi, které zašlou orgány všech ostatních členských států.

  — interoperabilitou mezi systémy zavedenou z jiných důvodů nebo interoperabilitou se systémy třetích zemí, která je daleko problematičtější.

Jedním z ochranných opatření, jež lze přijmout k omezení účelu systému a k zamezení neplánované funkce („function creep"), je použití odlišných technologických norem. Navíc by měla být důkladně zdokumentována jakákoli forma interakce mezi dvěma odlišnými systémy. Interoperabilita by nikdy neměla vést k tomu, aby orgán, kterému není povolen přístup k určitým údajům nebo jejich použití, mohl tento přístup získat prostřednictvím jiného informačního systému. Nakolik to lze po přečtení návrhů posoudit, tak se například zdá, že SIS II nebude v prvních létech obsahovat Systém automatické identifikace otisků prstů (AFIS); je v nich pouze zmínka o budoucím vyhledávači na základě biometrických údajů. Pokud se předpokládá scénář, podle něhož se bude používat systémů automatické identifikace otisků prstů z jiných systémů EU, mělo by to být jasně popsáno spolu s ochrannými opatřeními, jichž je zapotřebí pro takové synergie.

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 mu měl být předložen.

11. **SOUHRN ZÁVĚRŮ**

11.1 **Obecné body**

1. EIOÚ vítá celou řadu kladných aspektů těchto návrhů, které ve srovnání se současnou situací představují v některých bodech zlepšení. Uznává, že ustanovení o ochraně údajů byla všeobecně zpracována velmi pečlivě.

2. EIOÚ zdůrazňuje, že i přes svou složitost by nový právní režim měl

   — zajistit vysokou úroveň ochrany údajů,

   — být spolehlivý jak pro občany, tak pro orgány, které si vyměňují údaje,

   — být důsledný, pokud jde o jeho použití v různých rámcích (v rámci prvního nebo třetího pilíře).

3. Doplnění nových prvků do SIS II, jimiž se zvyšuje případný dopad systému na životy lidí, by navíc mělo jít ruku v ruce s přísnějšími ochrannými opatřeními, která jsou v tomto stanovisku popsána. Jedná se zejména o toto:

— Přístup k údajům v SIS II nelze novým orgánům povolit bez toho, aniž by byl řádně zdůvodněn. Měl by být také co nejvíce omezen, ať už se to týká přístupných údajů anebo osob, jimž je přístup povolen.

— Propojení záznamů nesmí vést, a to ani nepřímo, ke změně přístupových práv.

— Dosud nepřijaté právní předpisy nelze považovat za platný důvod pro zadávání údajů do SIS II (záznamy pro účely odepření vstupu).

— Měl by se znovu přezkoumat právní základ pro přístup orgánů odpovědných za vydávání osvědčení o registraci vozidel, protože tento přístup je určen především pro boj proti trestné činnosti.

— EIOÚ uznává, že použitím biometrických údajů lze zlepšit přínos systému i pomoc obětem krádeže totožnosti. Jak se však zdá, dopad zařazení těchto údajů není dostatečně domyšlen a jejich spolehlivost se přeceňuje.

11.2 **Konkrétní poznámky**

1. EIOÚ vítá souhlas Komise s tím, že nařízení 45/2001 se vztahuje na veškerou činnost Komise při zpracování údajů v SIS II, protože toto přispěje k zajištění důsledného a jednotného uplatňování pravidel o ochraně základních práv a svobod osob v souvislosti se zpracováním osobních údajů.

2. Aby bylo zaručeno přísné omezení účelu zpracování údajů na vnitrostátní úrovni, doporučuje EIOÚ zařadit do návrhů o SIS II (zejména do článku 21 navrhovaného nařízení a článku 40 navrhovaného rozhodnutí) ustanovení za stejným účelem jako ve stávajícím čl. 102 odst. 4 Schengenské úmluvy, čímž se omezí možnost členských států stanovit takové využití údajů, které není předpokládáno ve zněních o SIS II.

3. Pro udělení přístupu k údajům v SIS II by pro všechny orgány měly platit tyto přísné podmínky:

— Přístup musí být slučitelný s obecným účelem SIS II a musí být v souladu s jeho právním základem.

— Nutnost přístupu k datům v SIS II musí být prokázána.

— Využití údajů musí být definováno výslovně a omezujícím způsobem.

— Podmínky přístupu musí být správně definovány a vymezeny. Zejména by se měl vést aktuálně platný seznam osob, kterým je povolen přístup do SIS II, a to včetně Europolu a Eurojustu Skutečnost, že těmto orgánům byl udělen přístup k údajům v SIS II, nemůže být v žádném případě důvodem, aby do systému zadávaly nebo v něm aktualizovaly údaje, které nejsou užitečné pro konkrétní záznam, jehož jsou součástí.

— Dobu uchovávání údajů nelze prodlužovat, pokud to není nutné vzhledem k účelu, pro který byly údaje zadány.

4. V konkrétních případech Europolu a Eurojustu vybízí EIOÚ Komisi, aby omezujícím způsobem definovala úkoly, jejichž plnění by ospravedlňovalo jejich přístup do systému. Přístup Europolu a Eurojustu by se měl navíc omezit na údaje o osobách, jejichž jméno se již objevuje v jejich souborech. Rovněž se navrhuje, aby v případě Europolu a Eurojustu byl schválen jen jeden přístupový bod.

5. Pokud jde o záznamy pro účely odepření vstupu, měla by se ustanovení založená na dosud nepřijatých právních předpisech buď stáhnout nebo přeformulovat takovým způsobem – založeným na platných právních předpisů –, aby osoby přesně věděly, která opatření mohou vůči nim orgány přijmout.

6. Doby uchovávání údajů byly prodlouženy bez řádného zdůvodnění. Nebude-li předloženo přesvědčivé zdůvodnění, měly by se tyto lhůty vrátit na současnou délku, zejména v případě záznamů pro účely utajeného sledování nebo zvláštních kontrol.

7. Úloha Komise je popsána tak, že Komise nese odpovědnost za opertivní řízení. Připojíme-li k tomu její velmi důležitou úlohu při vývoji a údržbě systému, měla by se úloha Komise považovat za úlohu kontrolora svého druhu. Tato úloha jde dále než je úloha zpracovatele údajů, ale zároveň je omezenější než u normálního kontrolora, protože Komise nemá přístup k údajům zpracovávaným v SIS II.

   V rámci této úlohy by se mělo do článku 12 obou návrhů doplnit, že Komise by měla pravidelně navrhovat zavádění nových technologií, které představují špičku ve svém oboru a jimiž se zvýší úroveň ochrany údajů i bezpečnosti.

8. Pokud jde o členské státy, je zapotřebí objasnit, které orgány budou kontrolory.

9. Pokud jde o informování subjektu údajů:

   — V navrhovaném nařízení by se měly do seznamu doplnit některé informace, a sice: doba uchovávání údajů, existence práva požadovat přezkum rozhodnutí nebo podat odvolání proti rozhodnutí o pořízení záznamu, možnost získat pomoc od orgánu pro ochranu údajů a existence opravných prostředků.

     Pokud jde o chvíli, kdy mají být tyto informace sděleny, měla by se kromě toho doplnit povinnost poskytnout informace o záznamu především v rozhodnutí, na němž se záznam zakládá.

   — V navrhovaném rozhodnutí by se měl článek 50 pozměnit tak, aby právo být informován nebylo podmíněno žádostí subjektu údajů.

10. Pokud jde o lhůty pro odpověď na žádost o přístup, stanovení těchto lhůt v návrzích je vítáno. Stanoví-li se tyto lhůty i ve vnitrostátních právních předpisech, mělo by být jasně uvedeno, že by měly platit lhůty, které jsou pro subjekt údajů nejpříznivější.

    Bylo by také užitečné stanovit, že při výkonu práva na přístup jsou orgány pro ochranu údajů povinny aktivně spolupracovat.

11. Pokud jde o právo na opravné prostředky, EIOÚ navrhuje vypustit územní omezení z článku 30 a z článku 52.

12. Pokud jde o pravomoci vnitrostátních orgánů pro ochranu údajů:

   — v nařízení: je nutno vzít v úvahu, že vnitrostátní orgány pro ochranu údajů mohou vykonávat ve vztahu k SIS II všechny pravomoci, které jsou jim svěřeny na základě článku 28 směrnice 95/46/ES; ve znění navrhovaného nařízení by toto mělo být jasně vyjádřeno.

   — Pokud jde o navrhované rozhodnutí: kontrolním orgánům by se mělo dostat stejných pravomocí jako v nařízení/směrnici.

13. Pokud jde o pravomoci EIOÚ: EIOÚ by měl mít možnost vykonávat všechny své pravomoci podle nařízení 45/2001, přičemž by ale bral v úvahu omezené pravomoci, které má Komise ohledně samotných údajů.

14. Pokud jde o koordinovaný dozor: v návrzích se rovněž uznává nutnost koordinovat kontrolní činnost různých orgánů, které se na ní podílejí. EIOÚ vítá skutečnost, že návrhy v zásadě obsahují prvky potřebné k navázání spolupráce mezi orgány odpovědnými za dozor na vnitrostátní a na evropské úrovni. Tato ustanovení (článek 31 navrhovaného nařízení a článek 53 navrhovaného rozhodnutí) by však měla být co do obsahu koordinace jasnější.

15. Články 10 a 13 návrhu obsahují různá opatření ohledně bezpečnosti údajů; EIOÚ vítá, že do nich byla zařazena ustanovení o systematické interní kontrole bezpečnostních opatření.

   — Článek 59 navrhovaného rozhodnutí a článek 34 navrhovaného nařízení, které upravují sledování a hodnocení, by se však neměly týkat pouze aspektů výkonu, účinnosti vynaložených prostředků a kvality služeb, ale rovněž dodržování právních předpisů zejména v oblasti ochrany údajů. Tato ustanovení by měla být odpovídajícím způsobem změněna.

   — V souladu s čl. 10 odst. 1 písm. c) nebo čl. 18 navrhovaného rozhodnutí a článkem 17 navrhovaného nařízení by se mělo dále doplnit, že členské státy, Europol a Eurojust by měly zabezpečit dostupnost přesných uživatelských profilů (které by měly být za účelem kontroly k dispozici kontrolním 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.

   — Zákonnost zpracování osobních údajů se zakládá na přísném dodržování bezpečnosti a celistvosti údajů. EIOÚ by měl být s to účinně sledovat nejen bezpečnost údajů, ale i jejich celistvost prostřednictvím analýzy dostupných protokolů. Proto je nutné doplnit čl. 14 odst. 6 o „celistvost údajů“.

16. Použití vnitrostátních kopií může znamenat celou řadu dalších rizik. EIOÚ není přesvědčen o potřebě vnitrostátních kopií (vezmeme-li v úvahu dostupné technologie) ani o výhodách, jichž by jejich používání přineslo. Doporučuje vyhnout se možnosti, že by členské státy používaly vnitrostátní kopie, nebo tuto možnost alespoň značně omezit. Pokud se však budou vnitrostátní kopie pořizovat, jejich používání na vnitrostátní úrovni musí podléhat zásadě přísného omezení účelu zpracování údajů. Obdobně se nesmí do vnitrostátní kopie nahlížet jiným způsobem, než je stanoveno pro centrální databázi.

17. Pokud jde o postup projednávání ve výborech: Rozhodnutí mající podstatný vliv na ochranu údajů by se měla přijímat jako nařízení nebo rozhodnutí, nejlépe postupem spolurozhodování. Bude-li postupu projednávání ve výborech skutečně použito, pak by měla být poradní úloha EIOÚ včleněna do článků 60 a 61 rozhodnutí a do článku 35 nařízení.

18. Interoperabilita systémů nemůže být zavedena v rozporu se zásadou omezení účelu a jakýkoli návrh v této věci by měl být EIOÚ předložen.

V Bruselu dne 19. října 2005.

Peter HUSTINX

Evropský inspektor ochrany údajů