ISSN 1725-5163

Úřední věstník C 298

Evropské unie

České vydání

Informace a oznámení

Svazek 48

29. listopadu 2005

Oznámení č. | Obsah | Strana

I *Informace*

Evropský inspektor ochrany údajů

2005/C 298/01 Stanovisko Evropského inspektora ochrany údajů k návrhu směrnice Evropského parlamentu a Rady o uchovávání údajů zpracovaných v souvislosti s poskytováním veřejných služeb elektronických komunikací, kterou se mění směrnice 2002/58/ES (KOM(2005) 438 v konečném znění) 1

I

(Informace)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

Stanovisko Evropského inspektora ochrany údajů k návrhu směrnice Evropského parlamentu a Rady o uchovávání údajů zpracovaných v souvislosti s poskytováním veřejných služeb elektronických komunikací, kterou se mění směrnice 2002/58/ES (KOM(2005) 438 v konečném znění)

(2005/C 298/01)

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 [1] a směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) [2],

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 [3], 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 23. září 2005,

ZAUJAL TOTO STANOVISKO:

I. Úvod

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 nařízení (ES) č. 45/2001 by však současné stanovisko mělo být uvedeno v odůvodnění směrnice.

2. EIOÚ si je vědom toho, že je důležité, aby orgány členských států činné v trestním řízení měly možnost využívat všech potřebných právních nástrojů zejména při boji

(1) Úř. věst. L 281, 23.11.1995, s. 31.

(2) Úř. věst. L 201, 31.7.2002, s. 37.

(3) Úř. věst. L 8, 12.1.2001, s. 1.

s terorismem a jinou závažnou trestnou činností. Zásadním nástrojem těchto orgánů činných v trestním řízení může být náležitá dostupnost některých provozních a polohových údajů veřejných elektronických služeb a může přispět k zajištění fyzické bezpečnosti osob. Dále je vhodné uvést, že k těmto účelům nejsou nezbytně nutné nové nástroje předpokládané v současném návrhu.

3. Stejně tak je zřejmé, že tento návrh má značný dopad na ochranu osobních údajů. Pokud by byl návrh posuzován pouze z hlediska ochrany údajů, pak by provozní a polohové údaje neměly být pro účely vynucování práva vůbec uchovávány. Z důvodu ochrany údajů ukládá směrnice 2002/58/ES jako právní zásadu povinnost vymazat provozní údaje, jejichž uchovávání pro účely spojené s vlastní komunikací (včetně fakturačních účelů) již není nutné. Výjimky z této právní zásady podléhají přísným podmínkám.

4. EIOÚ v tomto stanovisku zdůrazňuje dopad návrhu na ochranu osobních údajů. EIOÚ bere dále v úvahu skutečnost, že bez ohledu na důležitost návrhu pro vynucení práva nemůže mít návrh za následek omezení základního lidského práva na ochranu soukromí.

5. Toto stanovisko EIOÚ musí být vnímáno s ohledem na tyto úvahy. EIOÚ navrhuje vyvážený přístup, kdy hraje hlavní roli nezbytnost a přiměřenost zásahu do ochrany údajů.

6. Co se vlastního návrhu týče, musí být posuzován jako odpověď na podnět Francie, Irska, Švédského království a Spojeného království směřující k rámcovému rozhodnutí o uchovávání údajů zpracovaných a uložených v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo údajů ve veřejných komunikačních sítích za účelem vyšetřování, odhalování a stíhání trestné činnosti včetně terorismu (dále jen „návrh rámcového rozhodnutí“), který byl zamítnut Evropským parlamentem (v rámci konzultačního postupu).

7. EIOÚ nebyl ohledně návrhu rámcového rozhodnutí konzultován, ani k němu z vlastního podnětu nezaujal stanovisko. EIOÚ nemá v současnosti v úmyslu zaujmout stanovisko k návrhu rámcového rozhodnutí, ale v tomto stanovisku bude na tento návrh rozhodnutí v případě potřeby odkazovat.

II. **Obecné připomínky**

Dopad návrhu na ochranu osobních údajů

8. Pro EIOÚ je podstatné, aby návrh respektoval základní práva. Právní opatření, které by narušovalo ochranu zaručovanou právními předpisy Společenství, a zejména judikaturou Soudního dvora a Evropského soudu pro lidská práva, není pouze nepřijatelné, ale rovněž protiprávní. Společenské okolnosti se mohly z důvodu teroristických útoků změnit, ale to nemůže mít za následek ohrožení vysoké úrovně ochrany v právní oblasti. Ochrana je stanovena zákonem bez ohledu na současné potřeby při vynucování práva. Navíc samotná judikatura umožňuje výjimky, jestliže jsou v demokratické společnosti nezbytné.

9. Návrh má přímý dopad na ochranu poskytnutou článkem 8 Evropské úmluvy o ochraně lidských práv a základních svobod. Podle judikatury Evropského soudu pro lidská práva:

— Ukládání informací o jednotlivci je považováno za zásah do soukromého života, i když tyto informace neobsahují žádné citlivé údaje (Amann ([1])).

— Stejně je tomu i při využívání „měření“ telefonických hovorů, které zahrnuje použití zařízení, které automaticky zaznamenává čísla vytočená telefonním přístrojem a čas a délku každého hovoru (Malone ([2])).

— Důvody pro zásah by měly převážit újmu, kterou může vlastní existence dotyčného právního ustanovení osobám působit (Dungeon ([3])).

10. Čl. 6 odst. 2 Smlouvy o EU stanovuje, že Unie ctí základní práva zaručená Evropskou úmluvou o ochraně lidských práv a základních svobod. V předešlém odstavci bylo poukázáno na to, že podle judikatury Evropského soudu pro lidská práva spadá povinnost uchovávat údaje pod článek 8 Evropské úmluvy o ochraně lidských práv a základních svobod a že je vyžadováno přísné odůvodnění, které vyhovuje

([1]) Rozsudek Evropského soudu pro lidská práva ze dne 16. února 2000, ve věci Amann, Sb. rozh. 2000-II, žád. č.: 27798/95.

([2]) Rozsudek Evropského soudu pro lidská práva ze dne 2. srpna 1984, ve věci Malone, Sb. rozh. A 82, žád. č.: 8691/79.

([3]) Rozsudek Evropského soudu pro lidská práva ze dne 22. října 1981, ve věci Dudgeon, Sb. rozh. A 45, žád. č.: 7525/76.

kritériu rozsudku ve věci Dudgeon. Je nutno v plné šíři prokázat nezbytnost a přiměřenost povinnosti uchovávat data.

11. Dále má návrh velký dopad na zásady týkající se ochrany údajů uznávané právními předpisy Společenství:

— Údaje se musí uchovávat po dobu o mnoho delší, než je doba obvyklá u poskytovatelů veřejně dostupných služeb elektronických komunikací nebo u sítí veřejných komunikací (obě služby jsou dále označovány společně jako „poskytovatelé“).

— Na základě směrnice 2002/58/ES, a zejména článku 6, mohou být údaje shromažďovány a ukládány pouze pro účely mající přímý vztah k samotným komunikacím, včetně pro účely fakturace ([1]). Poté musí být údaje vymazány (kromě výjimek). Podle tohoto návrhu je uchovávání pro účely vymáhání trestního práva povinné. Východisko je tedy zcela opačné.

— Směrnice 2002/58/ES zajišťuje zabezpečení a důvěrnost. Tento návrh nemůže mít za následek mezery v této oblasti; jsou nutné přísné záruky a mělo by být vyjasněno omezení účelu.

— Zavedení povinnosti uchovávat údaje, kterou předpokládá tento návrh, směřuje k základním databázím a pro osoby, jichž se uchovávání týká, představuje zvláštní hrozbu. Je možné uvažovat o komerčním využívání údajů, jakož i o využívání údajů „pro činnosti náhodného vyhledávání“ a o vytěžování údajů orgány činnými v trestním řízení nebo národními bezpečnostními službami.

12. V neposlední řadě byly ochrana soukromého života i ochrana osobních údajů uznány v Listině základních práv, jak již bylo uvedeno v důvodové zprávě.

13. Dopad návrhu na ochranu osobních údajů vyžaduje důkladnou analýzu. EIOÚ ve své analýze zohlední výše uvedené prvky a shledá, že je potřebné posílení záruk. Pouhý odkaz na stávající právní rámec ochrany údajů (zejména na směrnice 95/46/ES a 2002/58/ES) není dostačující.

Nezbytnost uchovávání provozních a polohových údajů.

14. EIOÚ připomíná závěr pracovní skupiny článku 29 pro ochranu údajů ze dne 9. listopadu 2004 o rámcovém rozhodnutí. Pracovní skupina prohlásila, že není přijatelné povinné uchovávání provozních údajů za podmínek stanovených v návrhu rámcového rozhodnutí. Tento závěr byl *mimo jiné* založen na tom, že nebyly předloženy žádné důkazy o nutnosti uchovávání údajů pro účely veřejného pořádku, protože analýza prokázala, že značná část provozních údajů požadovaných orgány činnými v trestním řízení nebyla starší šesti měsíců.

15. Podle EIOÚ by měly být výše uvedené důvody pracovní skupiny článku 29 pro ochranu údajů východiskem pro hodnocení tohoto návrhu. Výsledek těchto úvah však není možné pouze přenést do stávajícího návrhu. Je třeba brát v úvahu, že se okolnosti mohou změnit. Podle EIOÚ by pro hodnocení mohl být důležitý následující vývoj.

16. Za prvé byla uvedena některá čísla, která ukazují, že v praxi jsou vyžadovány až rok staré provozní údaje orgány činnými v trestním řízení. Komise, jakož i předsednictví Rady, přikládají význam výzkumu provedenému policií Spojeného království ([2]), který prokazuje, že ačkoliv 85 % provozních údajů, které jsou vyžadovány policií, je mladší šesti měsíců, údaje z období mezi šestým měsícem a jedním rokem jsou využívány při složitém vyšetřování závažnějších trestných činů. Byly předloženy i některé příklady těchto případů. Doba uchovávání v tomto návrhu – 1 rok pro telefonické údaje – odpovídá praxi orgánů činných v trestním řízení.

17. EIOÚ není přesvědčen o tom, že tato statistická čísla představují důkaz pro nezbytnost uchovávání provozních údajů až po dobu jednoho roku. Skutečnost, že v některých případech dostupnost provozních a polohových údajů přispěla k objasnění trestných činů, automaticky neznamená, že tyto údaje jsou (obecně) nutným nástrojem orgánů činných v trestním řízení. Tato statistická čísla však nelze přehlížet. Představují přinejmenším vážný pokus ukázat nezbytnost uchovávání. Tato statistická čísla navíc jasně ukazují, že doba uchovávání delší než jeden rok se s ohledem na stávající praxi orgánů činných v trestním řízení nevyžaduje.

18. Za druhé dává směrnice 2002/58/ES poskytovatelům pouze možnost uchovávat provozní údaje pro účely fakturace a tato možnost není vždy využívána, neboť k uchovávání dat z důvodu fakturace často vůbec nedochází (předplacené karty pro mobilní komunikace, paušály, atd.). V těchto případech,

([1]) Viz také bod 3 tohoto stanoviska.

([2]) Svoboda a bezpečnost, snaha o nalezení správné rovnováhy. Dokument předsednictví Spojeného království ze dne 7. září 2005.

které jsou v praxi stále častější, nejsou provozní a polohové údaje uchovávány, ale jsou ihned po uskutečnění komunikace vymazány. Stejně je tomu i s nezodpovězenými hovory. Toto může mít dopad na účinnost vymáhání práva.

19. Tento vývoj telekomunikačních služeb může navíc vést k narušení fungování vnitřního trhu, *mimo jiné* z důvodu (brzkého) přijetí právních opatření členskými státy podle článku 15 směrnice 2002/58/ES. Například italská vláda nedávno zveřejnila vyhlášku, podle které jsou poskytovatelé povinni ukládat telefonické údaje po dobu čtyř let. Tato povinnost způsobí v určitých členských státech, jako je Itálie, značné náklady.

20. Za třetí se vyvíjejí i pracovní metody orgánů činných v trestním řízení: na významu získává aktivní vyšetřování a využívání technické podpory. Tento vývoj vyžaduje, aby orgány používaly odpovídající a přesně stanovené nástroje, které jim umožní výkon jejich činnosti s náležitým ohledem na zásady ochrany údajů. Jedním z nástrojů, které orgány v členských státech obvykle využívají, je zálohování dat nebo zmrazení komunikačních údajů na žádost v souvislosti s konkrétním vyšetřováním. Bylo řečeno, že tento nástroj, který má na tyto zásady menší dopad než nástroj, který je navrhován nyní (uchovávání údajů), nemusí vždy dostačovat, zejména při sledování osob účastnících se terorismu nebo jiné závažné trestné činnosti, které nebyly v minulosti z trestné činnosti podezřívány. Rozhodnutí o tom, zda se jedná o takový případ, však vyžaduje další důkazy.

21. Za čtvrté vzrůstají obavy z teroristických útoků. EIOÚ sdílí názor, který byl vyjádřen v souvislosti s návrhy na uchovávání údajů, že prvořadá je osobní bezpečnost. Společnost musí být chráněna. Proto mají vlády povinnost v případě útoku na společnost projevit, že tuto potřebu ochrany berou náležitě v úvahu, a prošetřit, jestli je třeba reagovat zavedením nových právních opatření. EIOÚ bezpochyby plně podporuje úkol vlád na vnitrostátní i na evropské úrovni, jímž je chránit společnost a prokázat, že pro zabezpečení této ochrany učinily vše potřebné, včetně přijetí nových oprávněných a účinných opatření na základě výsledků jejich šetření.

22. Přestože si je EIOÚ vědom změny okolností, není dosud přesvědčen o nezbytnosti uchovávání provozních a polohových údajů pro účely vymáhání práva, jak je stanoveno v tomto návrhu. Zdůrazňuje důležitost právní zásady stanovené směrnicí 2002/58/ES, podle které musejí být provozní údaje vymazány v okamžiku, kdy jejich uložení pro účely nesouvisející s vlastní komunikací není dále nutné. Předložená statistická čísla rovněž neprokazují, že by stávající právní rámec nenabízel nástroje, které jsou vyžadovány za účelem ochrany fyzické bezpečnosti, ani že by členské státy plně využívaly svých pravomocí, které jim uděluje evropské právo (ovšem bez potřebných výsledků), ke spolupráci v rozsahu stávajícího právního rámce.

23. Pokud by však Evropský parlament a Rada došly po pečlivém zvážení dotčených zájmů k závěru, že je nezbytnost uchovávání provozních a polohových údajů dostatečně prokázána, pak je EIOÚ toho názoru, že uchovávání je možné odůvodnit podle práva Společenství jen za podmínky dodržení zásady přiměřenosti a poskytnutí vhodných záruk v souladu s tímto stanoviskem.

Přiměřenost

24. Přiměřenost navrhovaného nového legislativního opatření závisí na hmotných ustanoveních, ze kterých je opatření složeno: zahrnuje vhodnou a přiměřenou reakci na potřeby společnosti?

25. První úvaha se týká vhodnosti návrhu: může se od návrhu očekávat, že zvýší fyzickou bezpečnost obyvatel Evropské unie? Jedním z důvodů pro zpochybnění vhodnosti, který byl často zmiňován ve veřejných diskuzích, je skutečnost, že provozní a polohové údaje nejsou vždy spojeny s konkrétním jednotlivcem, a proto určení telefonního čísla (nebo čísla počítače v síti) vždy neodhaluje jeho totožnost. Dalším – a ještě závažnějším – důvodem k pochybnostem je otázka, jestli existence obrovských databází umožní orgánům činným v trestním řízení snadno nalézt údaje potřebné pro daný případ.

26. EIOÚ je toho názoru, že uchovávání provozních a polohových údajů není samo o sobě vhodnou a účinnou reakcí. Pro zajištění cíleného a rychlého přístupu orgánů k údajům, které jsou v daném případě potřebné, jsou nutná další opatření. Uchovávání údajů je vhodné a účinné, pouze pokud existují účinné vyhledávací nástroje.

27. Druhá úvaha se týká přiměřenosti reakce. Aby byl návrh přiměřený, měl by:

— omezit dobu uchovávání. Doba musí odpovídat prokázaným potřebám orgánů činných v trestním řízení,

— omezit počet údajů, které se mají ukládat. Tento počet musí odpovídat prokázaným potřebám orgánů činných v trestním řízení a zajistit, aby nebyl možný přístup k údajům o obsahu,

— obsahovat vhodná bezpečnostní opatření, jako například omezení přístupu a následného užití, záruky zabezpečení údajů, a pro osoby, kterých se uchovávání údajů týká, zajištění možnosti uplatnit svá práva.

28. EIOÚ zdůrazňuje význam těchto přísných omezení, která by měla s ohledem na omezení přístupu doprovázena vhodnými zárukami. Je toho názoru, že členské státy nemohou vzhledem k důležitosti těchto tří prvků přijmout v jejich případě doplňující vnitrostátní opatření, která by odporovala zásadě přiměřenosti. Potřeba harmonizace bude upřesněna v části IV.

Vhodná bezpečnostní opatření

29. V důsledku návrhu budou poskytovatelé nakládat s databázemi, ve kterých bude ukládáno značné množství provozních a polohových údajů.

30. Za prvé bude muset návrh zajistit, aby byl přístup k těmto údajům omezený, aby byly využitelné pouze za zvláštních okolností a pro vymezené zvláštní účely.

31. Za druhé budou muset být vhodně chráněny databáze (zabezpečení údajů). Za tím účelem musí být zajištěno na konci doby jejich uchovávání účinné vymazání údajů. Není přípustné žádné zneužívání údajů nebo tzv. „odkládání údajů". Zkrátka to vyžaduje vysokou úroveň zabezpečení údajů a vhodná technická a organizačně-bezpečnostní opatření.

32. Vysoká úroveň zabezpečení údajů je ještě důležitější, neboť sama existence údajů může způsobit poptávku po přístupu a po využití nejméně u tří zájmových skupin:

— u samotných poskytovatelů. Ti se mohou snažit využít údaje pro své vlastní komerční účely. V tomto případě jsou nezbytné záruky, které zabrání kopírování těchto souborů,

— u orgánů činných v trestním řízení: návrh jim poskytuje právo přístupu, ovšem pouze ve zvláštních případech a v souladu s vnitrostátními právními předpisy (čl. 3 odst. 2 návrhu). Přístup k údajům pro účely vytěžování nebo „při činnostech náhodného vyhledávání" není možný. Výměna údajů s orgány jiných členských států by měla být jasně upravena,

— u zpravodajských služeb (odpovídajících za vnitrostátní bezpečnost).

33. EIOÚ, pokud jde o přístup zpravodajských služeb, poznamenává, že podle článku 33 Smlouvy o EU a článku 64 Smlouvy o ES nemají zásahy v rámci třetího a prvního pilíře vliv na výkon pravomocí členských států, které jim byly uloženy s ohledem na zachování veřejného pořádku a zajištění vnitřní bezpečnosti. Podle EIOÚ vedou tato ustanovení k tomu, že Evropská unie nemá pravomoc omezit přístup bezpečnostních nebo zpravodajských služeb k údajům, které poskytovatelé uchovávají. Jinými slovy, právo Evropské unie se nevztahuje ani na přístup těchto služeb k provozním a polohovým údajům poskytovatelů, ani na následné využití informací, které tyto služby získaly. Toto je prvek, který musí být při hodnocení návrhu zohledněn. Je na členských státech, aby přijaly nezbytná opatření k úpravě přístupu zpravodajských služeb k údajům.

34. Za třetí mají následky uvedené v předešlých odstavcích významný dopad na osobu, které se údaje týkají. Je třeba stanovit doplňující záruky, které zajistí, aby tato osoba mohla jednoduchým způsobem a včas uplatnit svá práva vyplývající z jejího postavení. EIOÚ zdůrazňuje, že je potřeba účinně kontrolovat přístup a další užití, přičemž upřednostňuje provádění této kontroly prostřednictvím soudních orgánů členských států. Záruky by se měly použít rovněž v případě přístupu k provozním údajům a jejich následného užití ze strany orgánů jiného členského státu.

35. EIOÚ v této souvislosti odkazuje na podněty směřující k novému právnímu rámci o ochraně údajů, který se použije pro orgány činné v trestním řízení (třetí pilíř Smlouvy o EU). Dle jeho názoru tento právní rámec vyžaduje dodatečné záruky a nemůže se omezit pouze na opětovné potvrzení obecných zásad týkajících se ochrany údajů, které jsou obsažené v prvním pilíři. ([1])

36. Za čtvrté existuje přímá souvislost mezi vhodností bezpečnostních opatření a náklady na tato opatření. Vhodná právní úprava uchovávání údajů proto musí obsahovat podněty vybízející poskytovatele k investování do technické infrastruktury. Poskytovatelům mohou být např. hrazeny dodatečné náklady na vhodná bezpečnostní opatření.

37. Celkem vzato by vhodná bezpečnostní opatření měla:

— omezit přístup a další užití údajů,

— stanovit vhodná technická a organizační bezpečnostní opatření k ochraně databází. To zahrnuje i náležité vymazání údajů na konci doby uchovávání a reaguje na

([1]) Viz obdobně písemné stanovisko k vymáhání práva a výměně informací v EU přijaté na jarní konferenci evropských institucí o ochraně údajů, která se konala v Krakově ve dnech 25. a 26. dubna 2005.

poptávku příslušných zájmových skupin po přístupu k údajům a jejich využití,

— zajistit výkon práva osob, kterých se uchovávané údaje týkají, a to nejen opakováním obecných zásad vztahujících se k ochraně údajů,

— obsahovat podněty, které poskytovatele povzbudí k investování do technické infrastruktury.

III. Právní základ a návrh rámcového rozhodnutí

38. Návrh je založen na Smlouvě o ES, zejména na jejím článku 95, a jeho účelem je harmonizace povinností poskytovatelů ve vztahu ke zpracovávání a uchovávání provozních a polohových údajů podle jeho článku 1. Podle návrhu mají být údaje poskytovány pouze příslušným vnitrostátním orgánům v přesně vymezených případech, které souvisejí s trestnou činností, ale podrobnější stanovení účelu a přístupu k údajům i jejich dalšího užití je ponecháno na pravomoci členských států, s výhradou uplatnění záruk stávajícího rámce Společenství na ochranu údajů.

39. Návrh má v tomto ohledu omezenější rozsah působnosti než rámcové rozhodnutí, které vychází z čl. 31 odst.1 písm. c) Smlouvy o EU a které obsahuje dodatečná ustanovení o přístupu k uchovávaným údajům, jakož i ustanovení upravující žádosti o přístup ze strany ostatních členských států. Důvodová zpráva předkládá odůvodnění tohoto omezení oblasti působnosti návrhu. Zpráva uvádí, že přístup a výměna informací mezi příslušnými orgány činnými v trestním řízení spadají mimo oblast působnosti Smlouvy o ES.

40. EIOÚ toto tvrzení obsažené v důvodové zprávě nepřesvědčilo. Hlavním cílem zásahu Společenství, který je založen na článku 95 Smlouvy o ES (vnitřní trh), musí být odstranění překážek pro obchod. Zásah musí podle judikatury Soudního dvora skutečně vhodným způsobem přispět k odstranění takové překážky. Při svém zásahu však musí zákonodárné orgány Společenství ctít základní práva (čl. 6 odst. 2 Smlouvy o EU, viz část II tohoto stanoviska). Vzhledem k tomu může stanovení pravidel o uchovávání údajů na úrovni Společenství vyžadovat, aby bylo na úrovni Společenství řešeno i dodržování základních práv. Jestliže zákonodárné orgány Společenství nemohly stanovit pravidla pro přístup a užití údajů, nemohly splnit svou povinnost uloženou článkem 6 Smlouvy o EU, neboť posledně zmiňovaná pravidla jsou nezbytná pro zajištění toho, aby byly údaje uchovávány za podmínky náležitého respektování základních práv. Podle EIOÚ nelze pravidla pro přístup, užití a výměnu údajů oddělit od povinnosti spojené s uchováváním údajů.

41. EIOÚ připouští, že členským státům náleží pravomoc ustavit příslušné orgány. Stejně je tomu i se soudní ochranou a uspořádáním orgánů činných v trestním řízení. Akt společenství však může členským státům stanovit podmínky pro určení příslušných orgánů, soudní kontrolu nebo pro využívání právní ochrany ze strany občanů. Tato ustanovení zajišťují, aby na vnitrostátní úrovni byly k dispozici vhodné postupy, které zaručí plnou účinnost aktu, včetně úplného dodržování právních předpisů týkajících se ochrany údajů.

42. EIOÚ předkládá další otázku, která se vztahuje k právnímu základu. Zákonodárným orgánům Společenství přísluší výběr odpovídajícího právního základu, jakož i vhodných zákonodárných postupů. Tento výběr není posláním EIOÚ. EIOÚ se však za stávajícího stavu vzhledem k tomu, že se tu jedná o důležité základní otázky, vyslovuje pro upřednostnění postupu spolurozhodování. Pouze tento postup stanovuje průhledný rozhodovací proces s plným zapojením všech tří institucí a s náležitým dodržením zásad, na kterých je založena Evropská unie.

IV. Potřeba harmonizace

43. Návrh směrnice harmonizuje typy údajů, které se mají uchovávat, dobu jejich uchovávání i účely, ke kterým lze tyto údaje postoupit příslušným orgánům. Návrh předpokládá úplnou harmonizaci těchto prvků. V tomto ohledu má zcela jinou povahu než návrh rámcového rozhodnutí, který stanovuje minimální pravidla.

44. EIOÚ, s ohledem na fungování vnitřního trhu, potřeby orgánů činných v trestním řízení, Evropský soud pro lidská práva a zásady ochrany údajů, zdůrazňuje potřebu úplné harmonizace těchto prvků.

45. Pokud jde o fungování vnitřního trhu, harmonizace povinnosti uchovávat údaje odůvodňuje výběr právního základu návrhu (čl. 95 ES). Ponecháním základních rozdílů v právních předpisech členských států by nebylo odstraněno stávající narušení vnitřního trhu elektronických komunikací, které je *mimo jiné* zapříčiněno (brzkým) přijetím právních opatření členskými státy podle čl. 15 směrnice 2002/58/ES (viz bod 19 tohoto stanoviska).

46. Tento význam se ještě zvyšuje, neboť značný počet elektronických komunikací se dotýká pravomocí více než jednoho členského státu. Názornými příklady jsou: přeshraniční telefonické hovory, roaming, přechod hranic *během* mobilní komunikace a využití poskytovatele v členském státu, ve kterém nemá dotčená osoba bydliště.

47. V této souvislosti by nedostatek harmonizace navíc mohl způsobit újmu potřebám orgánů činných v trestním řízení, neboť příslušné orgány by musely splňovat rozdílné právní požadavky. Mohlo by tak dojít k narušení výměny informací mezi orgány členských států.

48. Na závěr EIOÚ odkazuje na svou odpovědnost podle článku 41 nařízení (ES) č. 45/2001 a zdůrazňuje, že úplná harmonizace hlavních prvků obsažených v návrhu je nezbytná pro splnění požadavků Evropského soudu pro lidská práva a zásad ochrany údajů. Jakékoli právní opatření ukládající povinnost uchovávat provozní a polohové údaje, pokud má být z hlediska ochrany údajů přijatelné a pokud má splňovat požadavky nezbytnosti a přiměřenosti, musí jasně vymezovat množství údajů, které mají být uchovávány, dobu jejich uchovávání a (účely pro) přístup a další užití údajů.

V. **Připomínky k článkům návrhu**

Článek 3: Povinnost uchovávat údaje

49. Článek 3 je zásadním ustanovením návrhu. Čl. 3 odst. 1 stanovuje povinnost uchovávat provozní a polohové údaje, přičemž čl. 3 odst. 2 zavádí zásadu omezení účelu. Čl. 3 odst. 2 stanovuje tři významná omezení. Uchovávané údaje mohou být poskytovány pouze:

— příslušným vnitrostátním orgánům,

— v přesně vymezených případech,

— za účelem prevence, vyšetřování, odhalování a stíhání závažné trestné činnosti, jako je např. terorismus a organizovaný zločin.

Čl. 3 odst. 2 odkazuje na vnitrostátní právní předpisy členských států, které mají upřesnit další omezení.

50. EIOÚ vítá čl. 3 odst. 2 jako významné ustanovení, ale domnívá se, že omezení nejsou dostatečně upřesněna, že přístup a další užití by měly být směrnicí výslovně upraveny, a že je potřeba stanovit doplňující záruky. Jak bylo uvedeno v části III tohoto stanoviska, EIOÚ není přesvědčen o tom, že nezahrnutí (upřesňujících) ustanovení o přístupu a dalším užití provozních a polohových údajů je nevyhnutelným důsledkem právního základu návrhu (článku 95 Smlouvy o ES). Toto vede k následujícím poznámkám.

51. Za prvé: není přesně stanoveno, že ostatní dotčené subjekty, jako např. poskytovatelé, nemají přístup k údajům. Poskytovatelé mohou podle článku 6 směrnice 2002/58/ES zpracovávat provozní údaje pouze po dobu, po kterou jsou údaje uchovávány pro účely účtování. Podle EIOÚ není odůvodněn jiný přístup poskytovatelů a dalších příslušných subjektů k údajům než ten, který je předvídán směrnicí 2002/58/ES, a to za podmínek stanovených v této směrnici.

52. EIOÚ doporučuje do textu návrhu doplnit ustanovení, které zajistí, aby k těmto údajům neměly přístup jiné subjekty než příslušné orgány. Toto ustanovení by mohlo znít takto: „údaje mohou být přístupné nebo zpracovávané pouze pro účely podle čl. 3 odst. 2“ nebo „poskytovatelé účinně zajistí, aby byl přístup udělen pouze příslušným orgánům“.

53. Za druhé: zdá se, že omezení na přesně vymezené případy zakazuje běžný přístup „při činnostech náhodného vyhledávání“ a vytěžování údajů. Znění návrhu by však mělo stanovit, že údaje mohou být poskytovány pouze v souvislosti s potřebami vyšetřování příslušného trestného činu.

54. Za třetí: EIOÚ vítá skutečnost, že účel přístupu je omezen na závažné trestné činnosti, jako jsou např. terorismus a organizovaný zločin. V jiných méně závažných případech by přístup k provozním a polohovým údajům nebyl zcela přiměřený. EIOÚ však vyjadřuje své pochybnosti o tom, zda je toto omezení dostatečně přesné, a to zejména v případech, kdy se bude o přístup žádat v souvislosti s jinou závažnou trestnou činností, než je terorismus a organizovaný zločin. Praxe v členských státech bude odlišná. V části IV tohoto stanoviska EIOÚ zdůraznil potřebu úplné harmonizace hlavních prvků obsažených v návrhu. EIOÚ proto doporučuje omezit ustanovení na *určité* závažné trestné činnosti.

55. Za čtvrté: oproti návrhu rámcového rozhodnutí neobsahuje tento návrh ustanovení o přístupu. Podle názoru EIOÚ by neměl být v této směrnici opomíjen přístup a další užití údajů. Jsou totiž neoddělitelnou součástí předmětu právní úpravy (viz část III tohoto stanoviska).

56. EIOÚ doporučuje doplnění návrhu o jeden nebo více článků, které by upravovaly přístup příslušných orgánů k provozním a polohovým údajům a další užití těchto údajů. Tyto články by měly být schopny zajistit, aby údaje byly používány pouze pro účely stanovené v čl. 3 odst. 2, aby orgány zajistily správnost, důvěrnost a bezpečnost získaných údajů a aby byla data vymazána, pokud již nejsou pro prevenci, vyšetřování, odhalování a stíhání určité trestné

činnosti dále potřebné. Dále by mělo být stanoveno, aby přístup k údajům podléhal ve zvláštních případech soudní kontrole členských států.

57. Za páté: návrh neobsahuje dodatečné záruky ochrany údajů. Body odůvodnění pouze odkazují na záruky obsažené ve stávajících právních předpisech, zejména ve směrnicích 95/46/ES a 2002/58/ES. EIOÚ vzhledem k zvláštnímu významu (doplňujících) záruk nesouhlasí s tímto omezeným přístupem k ochraně údajů (viz část II tohoto stanoviska).

58. EIOÚ proto doporučuje vložit odstavec o ochraně údajů. Do tohoto odstavce mohou být vložena předcházející doporučení, která se týkají čl. 3 odst. 2, jakož i další ustanovení o ochraně údajů, např. ustanovení související s uplatněním práva osob, jichž se uchovávané údaje týkají (viz část II tohoto stanoviska), se správností dat a zabezpečením údajů a s provozními a polohovými údaji o osobách, které nejsou podezřelé z páchání trestné činnosti.

Článek 4: Kategorie údajů, jež mají být uchovávány

59. EIOÚ obecně vítá tento článek a související přílohu z těchto důvodů:

— zvolený způsob právní úpravy s funkčním popisem, který je obsažen v hlavní části směrnice, a s technickými podrobnostmi uvedenými v příloze. Ten je dostatečně pružný, aby náležitě odpovídal technickému vývoji, a poskytuje právní jistotu občanům,

— rozdělení údajů na telekomunikační a internetové, přestože toto rozdělení není z technického hlediska natolik významné. Vzhledem k ochraně údajů je však toto rozdělení důležité, neboť v rámci internetu není zřetelná hranice mezi obsahovými a provozními údaji (viz např. čl. 1 odst. 2 směrnice, který stanoví, že informace vyhledávaná na internetu je údajem o obsahu),

— úroveň harmonizace: návrh předpokládá vysokou úroveň harmonizace s úplným seznamem kategorií údajů, jež mají být uchovávány (oproti rámcovému rozhodnutí, které obsahuje minimální seznam a členským státům ponechává širokou možnost doplnění údajů). Z hlediska ochrany údajů je zásadní úplná harmonizace (viz část IV).

60. EIOÚ doporučuje tyto změny:

— Druhý odstavec článku 4 by měl obsahovat přesnější kritéria zajišťující, že nebudou uvedeny údaje o obsahu. Měla by být doplněna tato věta: „Příloha nesmí obsahovat údaje, které odhalují obsah komunikace."

— Článek 5 nabízí možnost změny přílohy směrnicí Komise (postupem projednávání ve výborech). EIOÚ doporučuje, aby při změnách přílohy, které mají významný dopad na ochranu údajů, byl upřednostněn postup pomocí směrnice v souladu s postupem spolurozhodování. ([1])

Článek 7: Doba uchovávání údajů

61. EIOÚ vítá skutečnost, že doba uchovávání údajů v tomto návrhu je podstatně kratší, než doba, kterou stanovuje návrh rámcového rozhodnutí:

— S odkazem na pochybnosti vyjádřené v tomto stanovisku o prokázání nezbytnosti uchovávání provozních údajů po dobu nejvýše jednoho roku odráží období jednoho roku praxi orgánů činných v trestním řízení *uvedené* na základě statistických údajů poskytnutých Komisí a předsednictvím Rady.

— Tyto statistické údaje rovněž ukazují, že kromě výjimečných případů neodpovídá uchovávání údajů po delší dobu praxi orgánů činných v trestním řízení.

— Kratší doba v délce šesti měsíců stanovená pro údaje elektronických komunikací, které využívají výlučně nebo zejména internetových protokolů, je významná s ohledem na ochranu údajů, neboť uchovávání internetových komunikací vede k zakládání rozsáhlých databází (tyto údaje nejsou obvykle uchovávány pro účely fakturace), vymezení oproti údajům o obsahu je nejasné a uchovávání po dobu delší šesti měsíců neodpovídá praxi orgánů činných v trestním řízení.

62. V textu by mělo být upřesněno:

— doba uchovávání šest měsíců, případně jeden rok, je maximální dobou uchovávání,

([1]) Viz obdobně stanovisko EIOÚ ze dne 23. března 2005 k návrhu nařízení Evropského parlamentu a Rady o vízovém informačním systému (VIS) a výměně údajů o krátkodobých vízech mezi členskými státy (bod 3.12).

— po uplynutí doby uchovávání jsou údaje vymazány. Text by měl dále upřesnit způsob vymazání údajů. Dle EIOÚ musí poskytovatel vymazávat údaje prostřednictvím automatických prostředků nejméně jednou za den.

Článek 8: Požadavky pro ukládání uchovávaných údajů

63. Tento článek je úzce spojen s čl. 3 odst. 2 a obsahuje důležité ustanovení zajišťující možnost omezení přístupu v přesně vymezených případech pouze k takovým údajům, které jsou konkrétně vyžadovány. Článek 8 a čl. 3 odst. 2 předpokládají, že poskytovatelé postoupí vyžádané údaje příslušným orgánům, přičemž tyto orgány nemají k těmto databázím přímý přístup. EIOÚ doporučuje výslovné uvedení tohoto předpokladu do textu.

64. Ustanovení by mělo být upřesněno takto:

— poskytovatelé postoupí vyžádané údaje orgánům (viz bod 63),

— poskytovatelé by měli instalovat potřebnou technickou sestavu včetně vyhledávačů, aby umožnili cílený přístup k přesně stanoveným údajům,

— poskytovatelé by měli zajistit, aby byl přístup do databází z technických důvodů umožněn pouze jejich pracovníkům s přesně vymezenou technickou odpovědností, přičemž jsou tito pracovníci vyrozuměni o citlivé povaze údajů a své pracovní činnosti vykonávají v souladu s přísnými vnitřními předpisy o důvěrnosti,

— postoupení údajů by mělo probíhat bez nepřiměřených průtahů a bez odhalení provozních a polohových údajů, které nejsou pro účely žádosti nezbytné.

Článek 9: Statistika

65. Povinnost poskytovatelů předkládat výroční statistické výkazy pomáhá orgánům Společenství sledovat účinnost provádění a uplatňování stávajícího návrhu. Jsou potřebné vhodné informace.

66. Podle EIOÚ je tato povinnost uplatněním zásady průhlednosti. Evropský občan má právo znát míru účinnosti uchovávání údajů. Z tohoto důvodu by měl být poskytovatel také povinen vést záznamy o přístupech a provádět systematický (vnitřní) audit, který umožní vnitrostátním orgánům pro ochranu údajů kontrolovat praktické uplatňování pravidel o ochraně údajů ([1]). Návrh by měl být v tomto ohledu změněn.

Článek 10: Náklady

67. Jak již bylo uvedeno v části II, existuje přímá souvislost mezi vhodností bezpečnostních opatření a náklady na tato opatření nebo, řečeno jinak, mezi bezpečností a náklady. EIOÚ považuje článek 10, který umožňuje náhradu prokázaných dodatečných nákladů, za významné ustanovení, které by mohlo sloužit poskytovatelům jako pobídka, aby investovali do technické infrastruktury.

68. Podle odhadů hodnocení dopadu předloženého EIOÚ Komisí jsou náklady na uchovávání údajů značné. V případě velkých poskytovatelů sítí a služeb by náklady mohly převyšovat 150 milionů EUR za dobu dvanácti měsíců uchovávání, s ročními provozními náklady ve výši přibližně 50 milionů EUR. ([2]) Nejsou však k dispozici žádné statistické údaje o nákladech na doplňující bezpečnostní opatření, jako jsou např. nákladné vyhledávače (viz poznámka k článku 6), ani o (odhadovaných) finančních dopadech plné náhrady dodatečných nákladů poskytovatelům.

69. Podle EIOÚ je k posouzení návrhu v plném rozsahu zapotřebí přesnějších statistických údajů. EIOÚ navrhuje upřesnění finančních dopadů návrhu v důvodové zprávě.

70. Co se ustanovení článku 10 týče, měl by být v textu tohoto ustanovení vyjasněn vztah mezi vhodností bezpečnostních opatření a náklady. Návrh by měl dále stanovit minimální normy bezpečnostních opatření, které mají být přijaty poskytovateli, aby jim vznikl nárok na náhradu ze strany členského státu. Podle EIOÚ nemůže být určení těchto

([1]) Viz rovněž stanovisko EIOÚ ze dne 23. března 2005 k návrhu nařízení Evropského parlamentu a Rady o vízovém informačním systému (VIS) a výměně údajů o krátkodobých vízech mezi členskými státy (bod 3.9)

([2]) Komise odkazuje na údaje ETNO (Evropského sdružení provozovatelů v odvětví komunikací) a na zprávu poslance Evropského parlamentu Alvara k návrhu rámcového rozhodnutí.

norem ponecháno zcela na členských státech. Tím by mohla být ohrožena úroveň harmonizace, o kterou tato směrnice usiluje. Dále je třeba zohlednit skutečnost, že členské státy ponesou finanční důsledky této náhrady.

Článek 11: Změna směrnice 2002/58/ES

71. Měl by být vyjasněn vztah k čl. 15 odst. 1 směrnice 2002/58/ES, neboť tento návrh zbavuje toto ustanovení značné části jeho obsahu. Odkazy v čl. 15 odst. 1 směrnice 2002/58/ES na články 6 a 9 (stejné směrnice) by měly být zrušeny nebo přinejmenším změněny tak, aby vyjasnily, že členské státy již nemají dále pravomoc přijímat právní předpisy, které se vztahují na trestné činnosti doplňující tento stávající návrh. Je třeba odstranit veškeré nejasnosti ohledně zbývajících pravomocí členských států – například pokud jde o uchovávání údajů ve vztahu k „méně" závažné trestné činnosti.

Článek 12: Hodnocení

72. EIOÚ vítá, že návrh obsahuje článek o hodnocení směrnice do tří let od jejího vstupu v platnost. Hodnocení je navíc významné z hlediska pochybností o vhodnosti a přiměřenosti návrhu.

73. Z tohoto hlediska doporučuje EIOÚ stanovit ještě přísnější povinnost, která obsahuje tyto prvky:

— hodnocení by se mělo skládat z hodnocení účinnosti uplatňování směrnice, z hlediska orgánů činných v trestním řízení, jakož i z hodnocení dopadu na základní práva osob, jichž se uchovávání údajů týká. Komise by měla zahrnout veškeré dostupné důkazy, které by mohly toto hodnocení ovlivnit,

— hodnocení by mělo probíhat pravidelně (nejméně každé 2 roky),

— Komise by měla být povinna případně předložit návrh na změny tohoto návrhu (jako u článku 18 směrnice 2002/58/ES).

VI. **Závěry**

Předběžné podmínky

74. Pro EIOÚ je zásadní, aby návrh respektoval základní práva. Právní opatření, které by poškozovalo ochranu zaručenou právem Společenství, a zejména judikaturou Soudního dvora a Evropského soudu pro lidská práva, je nejen nepřípustné, ale také protiprávní.

75. Nezbytnost a přiměřenost povinnosti uchovávat údaje musí být v plném rozsahu prokázána.

76. K nezbytnosti: EIOÚ si je vědom změny okolností, avšak není přesvědčen o nezbytnosti uchovávání provozních a polohových údajů pro účely vymáhání práva, tak jak je stanovena tímto návrhem.

77. EIOÚ předložil v tomto stanovisku svůj názor na přiměřenost tohoto návrhu. To v první řadě znamená, že uchovávání provozních a polohových údajů není samo o sobě vhodným nebo účinným řešením. Jsou nutná doplňující opatření, která např. zajistí, aby dotčené orgány měly ve zvláštním případě cílený a rychlý přístup k potřebným údajům. V druhé řadě by návrh měl:

— omezit dobu uchovávání. Doba musí odpovídat potřebám orgánů činných v trestním řízení,

— omezit počet údajů, které mají být ukládány. Tento počet musí odpovídat potřebám orgánů činných v trestním řízení a zajistit, aby nebyl možný přístup k údajům o obsahu,

— obsahovat vhodná bezpečnostní opatření.

Celkové posouzení

78. EIOÚ zdůrazňuje význam té skutečnosti, že toto znění návrhu předpokládá úplnou harmonizaci hlavních prvků návrhu, zejména druhů údajů, které mají být uchovávány, dobu, po kterou mají být údaje uchovávány, jakož i (účely pro) přístup a další užití údajů.

79. V některých otázkách je nezbytné další vyjasnění, které například zajistí dostatečné vymazání údajů na konci doby uchovávání a účinně zabrání přístupu a využití údajů ze strany příslušných zájmových skupin.

80. Pro přijatelnost návrhu z hlediska ochrany údajů považuje EIOÚ za zásadní tyto body:

— doplnění návrhu o zvláštní ustanovení o přístupu k provozním a polohovým údajů ze strany příslušných orgánů a o dalším užití těchto údajů, jako zásadní a neoddělitelné součásti předmětné úpravy,

— doplnění návrhu o další dodatečné záruky ochrany údajů (oproti pouhému odkazu na záruky, které existují ve stávajících právních předpisech, zejména na směrnici 95/46/ES a směrnici 2002/58/ES), které *mimo jiné* zajistí osobám, kterých se uchovávání údajů týká, možnost uplatnit svá práva,

— doplnění návrhu o další pobídky pro poskytovatele, aby investovali do vhodné technické infrastruktury, včetně finančních pobídek. Tato infrastruktura může být vhodná, pouze pokud budou existovat účinné vyhledávače.

Doporučení změn návrhu

81. K čl. 3 odst. 2:

— doplnění ustanovení, kterým bude zajištěno, aby kromě příslušných orgánů neměly k údajům přístup jiné subjekty. Toto ustanovení by mohlo znít takto: „údaje mohou být přístupné nebo zpracovávané pouze pro účely podle čl. 3 odst. 2“ nebo „poskytovatelé účinně zajistí, aby byl přístup udělen pouze příslušným orgánům“,

— upřesnění, že údaje mohou být poskytnuty pouze v případě, že jsou vyžadovány v souvislosti se zvlášť vymezenou trestnou činností,

— omezení ustanovení na *určité* závažné trestné činnosti,

— doplnění návrhu jedním nebo více články o přístupu k provozním a polohovým údajům ze strany příslušných orgánů a o dalším užití údajů a ustanovením, že přístup bude v členských státech ve zvláštních případech podroben soudní kontrole,

— začlenění odstavce o ochraně údajů.

82. K článkům 4 a 5:

— doplnění článku 4 druhého pododstavce následující větou: „Příloha nesmí obsahovat údaje, které odhalují obsah komunikace.“,

— upřesnění, že změny přílohy, které mají podstatný dopad na ochranu údajů, by měly být prováděny prostřednictvím směrnice podle postupu spolurozhodování.

83. K článku 7, upřesnění textu:

— doba uchovávání šest měsíců, případně jeden rok, je maximální dobou uchovávání,

— po uplynutí doby uchovávání jsou údaje vymazány. Text by měl rovněž vyjasnit způsob vymazání údajů, zejména prostřednictvím poskytovatele a automatizovanými prostředky, nejméně jednou za den.

84. K článku 8, upřesnění textu:

— poskytovatelé postoupí vyžádané údaje orgánům,

— poskytovatelé by měli instalovat potřebnou technickou sestavu včetně vyhledávačů, aby umožnili cílený přístup k přesně stanoveným údajům,

— poskytovatelé by měli zajistit, aby byl přístup do databází z technických důvodů umožněn pouze jejich pracovníkům s přesně stanovenou technickou odpovědností, přičemž jsou tito pracovníci vyrozuměni o citlivé povaze údajů a své činnosti vykonávají v souladu s přísnými vnitřními předpisy o důvěrnosti,

— postoupení údajů by mělo probíhat bez nepřiměřených průtahů a bez odhalení provozních a polohových údajů, které nejsou pro účely žádosti nezbytné.

85. K článku 9:

— doplnění ustanovení o povinnosti poskytovatele vést záznamy o přístupech a provádět systematický (vnitřní) audit, který umožní vnitrostátním orgánům pro ochranu údajů kontrolovat praktické uplatňování pravidel o ochraně údajů.

86. K článku 10:

— v textu ustanovení by měl být vyjasněn vztah mezi vhodností bezpečnostních opatření a náklady,

— doplnění minimálních norem bezpečnostních opatření, které mají být přijaty poskytovateli, aby jim vznikl nárok na náhradu ze strany členského státu,

— vyjasnění finančních důsledků návrhu v důvodové zprávě.

87. K článku 11:

— změna čl. 15 odst. 1 směrnice 2002/58/ES na základě zrušení odkazů na články 6 a 9 (stejné směrnice) nebo přinejmenším jejich změna, která vyjasní, že členské státy již nemají dále pravomoc přijímat takové právní předpisy, které se vztahují na trestné činnosti doplňující tento stávající návrh.

88. K článku 12, změna ustanovení o hodnocení:

— hodnocení by mělo zahrnovat hodnocení účinnosti uplatňování směrnice,

— hodnocení by mělo probíhat pravidelně (nejméně každé 2 roky),

— Komise by měla být povinna případně předložit návrh na změny tohoto návrhu (jako u článku 18 směrnice 2002/58/ES).

V Bruselu dne 26. září 2005.

Peter HUSTINX

Evropský inspektor ochrany údajů