I

(Usnesení, doporučení a stanoviska)

STANOVISKA

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

Stanovisko evropského inspektora ochrany údajů k návrhu směrnice Evropského parlamentu a Rady, kterou se mění mimo jiné směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích)

(2008/C 181/01)

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]),

s ohledem na směrnici Evropského parlamentu a Rady 2002/58 ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací ([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, a zejména na článek 41 tohoto nařízení ([3]),

s ohledem na žádost o stanovisko v souladu s čl. 28 odst. 2 nařízení (ES) č. 45/2001 obdrženou od Evropské komise dne 16. listopadu 2007,

ZAUJAL TOTO STANOVISKO:

I. ÚVOD

1. Dne 13. listopadu 2007 Komise přijala návrh směrnice, kterou se mění mimo jiné směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (dále jen „návrh“ nebo „pozměňovací návrh“). Stávající znění směrnice 2002/58/ES je obvykle, a to i v tomto stanovisku, označováno jako směrnice o ochraně soukromí v odvětví elektronických komunikací.

([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.

2. Návrh má za cíl zlepšení ochrany soukromí a osobních údajů jednotlivců v odvětví elektronických komunikací, a to prostřednictvím změn *ad hoc*, jež mají za cíl především zpřísnit ustanovení týkající se bezpečnosti a zlepšit stávající donucovací mechanismy.

3. Tento návrh je součástí širší reformy pěti směrnic EU v oblasti telekomunikací („telekomunikační balíček“) Kromě návrhů na přezkum právních předpisů tvořících součást telekomunikačního balíčku ([1]) Komise současně rovněž přijala návrh nařízení o zřízení Evropského úřadu pro trh elektronických komunikací ([2]).

4. Postřehy uvedené v tomto stanovisku se omezují na navržené změny směrnice o ochraně soukromí v odvětví elektronických komunikací, pokud tyto navržené změny nevycházejí z konceptů nebo ustanovení obsažených v návrzích na přezkum telekomunikačního balíčku. Některé připomínky uvedené v tomto stanovisku odkazují k ustanovením směrnice o ochraně soukromí v odvětví elektronických komunikací, jež se návrhem nemění.

5. Toto stanovisko se zabývá následujícími otázkami: i) oblast působnosti směrnice o ochraně soukromí v odvětví elektronických komunikací, zejména dotčené služby (navržená změna čl. 3 odst. 1), ii) oznamování narušení bezpečnosti (navrhovanou změnou je nový čl. 4 odst. 3 a 4), iii) ustanovení o tzv. „cookies“, „spyware“ a podobných zařízeních (navrhovaná změna čl. 5 odst. 3), iv) právní kroky z podnětu poskytovatelů služeb elektronických komunikací a jiných právnických osob (navrhovanou změnou je nový odst. 6 v čl. 13) a v) zpřísnění ustanovení o vynucování (navrhovanou změnou je nový čl. 15a).

Konzultace s EIOÚ a konzultace s širší veřejností

6. Komise zaslala návrh EIOÚ dne 16. listopadu 2007. EIOÚ považuje toto sdělení za žádost o konzultaci orgánů a institucí Společenství podle čl. 28 odst. 2 nařízení (ES) č. 45/2001 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (dále jen „nařízení (ES) č. 45/2001“).

7. Komise tento návrh před jeho přijetím neformálně konzultovala s EIOÚ, což evropský inspektor ochrany údajů uvítal, protože tak dostal příležitost k němu učinit před přijetím Komisí několik připomínek. EIOÚ s potěšením konstatuje, že některé z jeho připomínek byly v tomto návrhu zohledněny.

8. Přijetí návrhu předcházela konzultace široké veřejnosti, což je postup, jejž EIOÚ oceňuje. V lednu 2006 Komise zahájila veřejnou konzultaci svého sdělení o přezkumu telekomunikačního balíčku, v němž Komise uvedla své postoje k situaci a předložila několik návrhů změn ([3]). Pracovní skupina článku 29 pro ochranu údajů, jejímž je EIOÚ členem, využila příležitosti k poskytnutí svého stanoviska k navrhovaným změnám ve stanovisku přijatém dne 26. září 2006 ([4]).

([1]) Navrhované změny směrnic v oblasti telekomunikací jsou předloženy v těchto návrzích: i) návrh směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací, směrnice 2002/19/ES o přístupu k sítím a službám elektronických komunikací a o jejich vzájemném propojení a směrnice 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací, 13. listopadu 2007, KOM(2007) 697 v konečném znění, ii) návrh směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci v oblasti ochrany spotřebitele, 13. listopadu 2007, KOM(2007) 698 v konečném znění.

([2]) Návrh nařízení Evropského parlamentu a Rady o zřízení Evropského úřadu pro trh elektronických komunikací, 13. listopadu 2007, KOM(2007) 699 v konečném znění.

([3]) Sdělení o přezkumu regulačního rámce EU pro sítě a služby elektronických komunikací {SEK(2006) 816} přijaté dne 29. června 2006. Toto sdělení je doplněno o pracovní dokument útvarů Komise {KOM(206) 334 v konečném znění}.

([4]) Stanovisko 8/2006 k přezkumu regulačního rámce pro elektronické komunikace a služby se zaměřením na směrnici o ochraně soukromí v odvětví elektronických komunikací), přijaté dne 26. září 2006.

Obecná stanoviska EIOÚ

9. EIOÚ se k návrhu jako celku staví kladně. EIOÚ plně podporuje cíle Komise ohledně přijetí návrhu, kterým se zlepšuje ochrana soukromí a osobních údajů jednotlivců v odvětví elektronických komunikací. EIOÚ zejména vítá přijetí povinného systému oznamování narušení bezpečnosti (změna článku 4 směrnice o ochraně soukromí v odvětví elektronických komunikací, doplňující odstavce 3 a 4). Dojde-li k úniku údajů, oznámení má jasné výhody, posílí odpovědnost organizací a je faktorem, který nutí společnosti zavést přísnější bezpečnostní opatření a dovoluje nalezení nejspolehlivějších technologií k ochraně informací. Dále umožňuje dotčené osobě příjmout opatření za účelem své vlastní ochrany před krádeží identity nebo proti jinému zneužití svých osobních informací.

10. EIOÚ vítá další změny v návrhu, jako je způsobilost právnických osob s právním zájmem zahájit kroky proti těm, kteří poruší některé z ustanovení směrnice o ochraně soukromí v odvětví elektronických komunikací (změna k článku 13, doplňující odstavec 6). Pozitivní je rovněž posílení vyšetřovacích pravomocí vnitrostátních regulačních orgánů, protože jim to umožní posoudit, zda je jakékoli zpracování údajů provedeno v souladu se zákonem či nikoliv a zjistit porušení (doplnění čl. 15a odst. 3). Opatření umožňující co nejdříve zastavit nezákonné zpracování osobních údajů a porušování soukromí je nezbytné za účelem ochrany práv a svobod osob. Za tímto účelem je velmi vítán navržený čl. 15a odst. 2, jenž uznává pravomoc vnitrostátních regulačních orgánů nařídit zastavení porušování, protože jim umožní okamžitě zastavit zpracovávání, jež vážně porušuje zákon.

11. Přístup návrhu a většina navrhovaných změn je v souladu s postoji k budoucí politice ochrany údajů, jež byly předloženy v předchozích stanoviscích EIOÚ, jako je stanovisko k provádění směrnice o ochraně údajů ([1]). Tento přístup mimo jiné vychází z přesvědčení, že zatímco nejsou potřeba žádné nové zásady ochrany údajů, je třeba konkrétnějších pravidel pro řešení vzniklých otázek týkajících se ochrany údajů prostřednictvím nových technologií, jako je internet, identifikace na základě rádiové frekvence atd., jakož i nástrojů, jež přispívají k posílení a činí účinnými právní předpisy v oblasti ochrany údajů, jako například ty, jež právním subjektům umožňují zahájit kroky ve věci porušování ochrany údajů a zavazující správce údajů k oznamování narušení bezpečnosti.

12. Přes celkový pozitivní přístup k návrhu EIOÚ lituje, že tento návrh není natolik ambiciózní, jak mohl být. Uplatňování ustanovení obsažených ve směrnici o soukromí v odvětví elektronických komunikací od roku 2003, jakož i důkladný rozbor předmětu ukázaly, že některá z jejích ustanovení nejsou ani zdaleka jasná, vytvářejí právní nejistotu a problémy s dodržováním. To je například otázka týkající se rozsahu, v němž se směrnice o soukromí v odvětví elektronických komunikací vztahuje na poloveřejné poskytovatele služeb elektronické komunikace. Dalo by se očekávat, že Komise využije přezkumu telekomunikačního balíčku, a zejména směrnice o ochraně soukromí v odvětví elektronických komunikací, k vyřešení některých přetrvávajících problémů. Pokud jde o řešení nových otázek, jako je stanovování povinného systému oznamování porušení, návrh nabízí pouze částečné řešení a nezahrnuje do oblasti působnosti organizací povinných oznamovat narušení bezpečnosti subjekty, jež zpracovávají velmi citlivé druhy údajů, jako jsou banky poskytující internetové bankovnictví nebo poskytovatelé zdravotních služeb on-line. EIOÚ tohoto přístupu lituje.

13. EIOÚ věří, že tento návrh projde legislativním procesem a že normotvůrce zohlední připomínky a návrhy obsažené v tomto stanovisku k řešení otázek, jimiž se návrh Komise nezabýval.

([1]) Stanovisko evropského inspektora ochrany údajů ze dne 25. července 2007 ke sdělení Komise Evropskému parlamentu a Radě o pokračování pracovního programu pro lepší provádění směrnice o ochraně osobních údajů (Úř. věst. C 255, 27.10.2007, s. 1).

II. **ROZBOR NÁVRHU**

II.1 **Oblast působnosti směrnice o ochraně soukromí v odvětví elektronických komunikací, zejména pokud jde o služby**

14. Hlavní otázkou ve stávající směrnici o ochraně soukromí v odvětví elektronických komunikací je otázka oblasti působnosti. Tento návrh obsahuje některé pozitivní prvky týkající se definování a objasnění působnosti směrnice, zejména služeb dotčených touto směrnicí, o nichž se pojednává níže v části i). Navrhované změny však bohužel neřeší všechny stávající problémy. Jak je uvedeno v části ii) níže, změny se bohužel nesnaží rozšířit oblast působnosti této směrnice tak, aby zahrnula služby elektronické komunikace v soukromých sítích.

15. V článku 3 směrnice o ochraně soukromí v odvětví elektronických komunikací jsou popsány služby dotčené touto směrnicí, jinak řečeno služby, na něž se povinnosti stanovené v této směrnici použijí: „*Tato směrnice se vztahuje na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích*".

16. Proto jsou směrnicí o ochraně soukromí v odvětví elektronických komunikací dotčeny služby poskytovatele veřejné služby elektronických komunikací ve veřejných sítích. Definice poskytovatele elektronických komunikací je uvedena v čl. 2 odst. c) rámcové směrnice ([1]). Veřejné komunikační sítě jsou definovány v čl. 2 písm. d) rámcové směrnice ([2]). Příklady činností poskytovatele veřejné služby elektronických komunikací ve veřejných sítích zahrnují poskytování přístupu k internetu, přenos sdělení prostřednictvím elektronických sítí, mobilní a telefonní spojení atd.

i) *Navrhovaná změna článku 3 směrnice o ochraně soukromí v odvětví elektronických komunikací: Dotčené služby mají zahrnovat veřejné komunikační sítě podporující zařízení pro shromažďování a identifikaci údajů*

17. Návrh mění článek 3 směrnice o ochraně soukromí v odvětví elektronických komunikací stanovením, že veřejné elektronické komunikační sítě zahrnují „*veřejné komunikační sítě podporující zařízení pro shromažďování a identifikaci údajů*". Ve 28. bodu odůvodnění je uvedeno, že vývoj aplikací, jež mají za následek shromažďování informací, včetně osobních údajů, za použití radiových frekvencí, jako je identifikace na základě radiové frekvence, musí podléhat směrnici o soukromí v odvětví elektronických komunikací, pokud jsou napojeny na sítě či služby veřejné komunikace nebo jich využívají.

18. EIOÚ považuje toto ustanovení za pozitivní, protože se v něm objasňuje, že řada aplikací s identifikací na základě rádiové frekvence spadá do oblasti působnosti směrnice o soukromí v odvětví elektronických komunikací, čímž se v této otázce odstraňuje určitá nejistota a s konečnou platností se odstraňuje nedorozumění nebo nesprávný výklad zákona.

19. Podle stávajícího článku 3 směrnice o soukromí v odvětví elektronických komunikací se na některé aplikace s identifikací na základě rádiové frekvence tato směrnice již vskutku vztahuje. K tomu dochází z několika kumulativních důvodů. Zaprvé proto, že aplikace s identifikací na základě rádiové frekvence spadají do definice elektronických komunikačních služeb. Zadruhé proto, že jsou poskytovány prostřednictvím elektronické komunikační sítě, pokud jsou aplikace podporovány přenosovými systémy,

([1]) Směrnice Evropského parlamentu a Rady 2002/21 ze dne 7. března 2002 o společném regulačním rámci pro sítě a služby elektronických komunikací (Úř. věst. L 108, 24.4.2002, s. 33). Rámcová směrnice vymezuje, co by mělo být chápáno pod výrazem služby elektronických komunikací, konkrétně i) „Služba elektronických komunikací" je služba obvykle poskytovaná za úplatu, která spočívá v přenosu signálů po sítích, včetně telekomunikačních služeb a přenosových služeb v sítích. ii) Služby poskytující obsah přenášený prostřednictvím sítí a služeb elektronických komunikací jsou z definice elektronických komunikačních služeb vyjmuty. iii) Zajišťováním sítě elektronických komunikací rozumí zřízení takové sítě, její provozování, dohled nad ní nebo její zpřístupnění. iv) Služby elektronických komunikací nezahrnují služby informační společnosti, jež jsou definovány ve směrnici o elektronickém obchodu jako služby obvykle poskytované za úplatu na dálku, elektronickými prostředky a na individuální žádost příjemce služby.

([2]) Veřejnou komunikační sítí se rozumí síť elektronických komunikací, která slouží zcela nebo převážně k poskytování veřejně přístupných služeb elektronických komunikací.

jež přenáší signály bezdrátově. A konečně síť může být veřejná nebo soukromá. Pokud je veřejná, aplikace s identifikací na základě rádiové frekvence budou považovány za „dotčené služby", a tak spadají do oblasti působnosti aplikace směrnice o soukromí v odvětví elektronických komunikací. Avšak navržená změna odstraní veškeré zbývající pochybnosti o této věci, a tak poskytne více právní jistoty.

20. Jak je uvedeno v předchozím stanovisku EIOÚ k identifikaci na základě rádiové frekvence ([1]), toto ustanovení samozřejmě nevylučuje možnou potřebu stanovit doplňkové právní nástroje týkající se rádiových identifikačních zařízení. Taková opatření by však měla být přijata v jiné souvislosti, nikoliv jako součást tohoto návrhu.

ii) *Potřeba zahrnout elektronické komunikační služby do soukromých a polosoukromých sítí*

21. Zatímco EIOÚ vítá objasnění popsané níže, lituje, že návrh neřeší otázku stále zastřenějšího rozlišení mezi soukromými a veřejnými sítěmi. EIOÚ dále lituje, že definice služeb, na něž se vztahuje směrnice o ochraně soukromí v odvětví elektronických komunikací, nebyla rozšířena tak, aby zahrnovala soukromé sítě. Podle stávajícího znění se čl. odst. 1 směrnice o ochraně soukromí v odvětví elektronických komunikací vztahuje pouze na *služby elektronické komunikace ve veřejných sítích*.

22. EIOÚ poznamenává, že dochází ve stále větší míře ke spojování soukromých a veřejných služeb. Například univerzity umožňují tisícům studentů používat internet a e-mail. Schopnost poloveřejných (nebo polosoukromých) sítí vstupovat do soukromí jednotlivců je zřetelná, a proto je třeba, aby byl tento druh služby předmětem souboru stejných pravidel, jako jsou ta, jež se vztahují pouze na veřejné sítě. Soukromé sítě, jako sítě zaměstnavatelů poskytující zaměstnancům přístup k internetu, majitelé hotelů nebo apartmánů poskytující hostům telefon a e-mail, jakož i internetové kavárny, mají dopad na ochranu údajů a soukromí uživatelů, z čehož plyne, že by se oblast působnosti směrnice o ochraně soukromí v odvětví elektronických komunikací měla vztahovat i na ně.

23. Judikatura některých členských států již ve skutečnosti spojila služby elektronických komunikací poskytovaných v soukromých sítích se stejnými povinnostmi, jako jsou povinnosti stanovené pro služby veřejné ([2]). Podle německých právních předpisů orgány na ochranu údajů rovněž shledaly, že povolení použití soukromých e-mailů v rámci společnosti může mít za následek, že společnost bude považována za provozovatele veřejných telekomunikačních služeb, a tím spadat pod ustanovení směrnice o ochraně soukromí v odvětví elektronických komunikací.

24. Stručně řečeno, rostoucí význam smíšených (soukromých/veřejných) a soukromých sítí v každodenním životě, společně s odpovídajícím růstem ohrožení osobních údajů a soukromí, zdůvodňuje potřebu použít pro takové služby soubor stejných pravidel, jako jsou ta, jež se používají pro veřejné služby elektronické komunikace. Proto se EIOÚ domnívá, že by směrnice měla být změněna způsobem, jímž by se oblast působnosti rozšířila tak, aby tento druh soukromých služeb zahrnula; Pracovní skupina článku 29 je téhož názoru ([3]).

II.2 **Oznamování narušení bezpečnosti: změna v článku 4**

25. Článek 4 směrnice o ochraně soukromí v odvětví elektronických komunikací je změněn vložením dvou nových odstavců (3 a 4), které stanovují povinnost oznamovat narušení bezpečnosti. Podle čl. 4 odst. 3 jsou poskytovatelé veřejné služby elektronických komunikací ve veřejných sítích nuceni na jedné straně k oznámení vnitrostátním regulačním orgánům, bez zbytečného prodlení, jakéhokoliv narušení bezpečnosti, jež vedlo k náhodnému či protiprávnímu zničení, ztrátě, změně, neoprávněnému sdělení či zpřístupnění osobních údajů přenášených, uchovávaných či jinak zpracovávaných v souvislosti s poskytováním elektronických komunikačních služeb (souborně označeno jako „ohrožení údajů"); na druhé straně jsou poskytovatelé veřejné služby elektronických komunikací rovněž nuceni podat oznámení svým zákazníkům.

([1]) Stanovisko ze dne 20. prosince 2007 ke sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o identifikaci na základě rádiové frekvence (RFID) v Evropě: kroky k rámci politiky KOM(2007) 96.

([2]) Například v rozsudku pařížského odvolacího soudu ve věci *BNP Paribas* v. *World Press Online* vydaného dne 4. února 2005 bylo shledáno, že není rozdíl mezi poskytovatelem internetové služby, jenž poskytnul přístup k internetu na komerčním základě, a zaměstnavatelem, jenž poskytl přístup k internetu svému zaměstnanci.

([3]) Stanovisko 8/2006 k přezkumu regulačního rámce pro elektronické komunikace a služby se zaměřením na směrnici o ochraně soukromí v odvětví elektronických komunikací), přijaté dne 26. září 2006.

Přínos vyplývající z této povinnosti

26. EIOÚ vítá tato ustanovení (čl. 4 odst. 3 a čl. 4 odst. 4) zavádějící povinné oznamování narušení bezpečnosti. Oznamování narušení bezpečnosti má pozitivní dopad z hlediska ochrany osobních údajů a soukromí a bylo již testováno ve Spojených státech amerických, kde jsou právní předpisy týkající se oznámení o porušení na vnitrostátní úrovni v platnosti již několik let.

27. Zaprvé právní předpisy týkající se oznámení porušení zlepšují odpovědnost poskytovatelů veřejné služby elektronických komunikací ohledně informací, jež byly ohroženy. V rámci ochrany údajů nebo politiky v oblasti soukromí se odpovědností rozumí, že každá organizace je odpovědná za informace, jež má na starosti a pod kontrolou. Oznamovací povinnost je rovnocenná s opětovným prohlášením, že na jedné straně údaje, jež byly ohroženy, byly pod kontrolou poskytovatele veřejné služby elektronických komunikací, a na druhé straně, že je v odpovědnosti této organizace přijmout ohledně takových údajů nezbytná opatření.

28. Zadruhé existence oznamování narušení bezpečnosti se ukázala být faktorem, jenž podporuje investice do bezpečnosti v organizacích, jež osobní údaje zpracovávají. Pouhá skutečnost, že se musí narušení bezpečnosti veřejně oznamovat, má vskutku za následek, že organizace uplatňují přísnější bezpečnostní normy, jež chrání osobní informace a předcházejí porušení. Oznamování narušení bezpečnosti dále pomůže nalézt a provést spolehlivé statistické analýzy nejúčinnějších bezpečnostních řešení a mechanismů. Již dlouho existuje nedostatek konkrétních údajů o selhání bezpečnosti informací a o nejvhodnějších technologiích pro ochranu informací. Tento problém je pravděpodobně možno vyřešit pomocí oznamovací povinnosti o narušení bezpečnosti, jak tomu bylo v případě zákonů Spojených států amerických týkajících se oznamování narušení bezpečnosti, protože oznámení poskytne informace o technologiích, jež jsou pro porušení příznivější ([1]).

29. Díky oznamování narušení bezpečnosti si dále jednotlivci uvědomují nebezpečí, jemuž jsou vystaveni, když jsou ohroženy jejich osobní údaje, a mohou lépe přijmout nezbytná opatření ke zmírnění takových nebezpečí. Například jsou-li ohroženy bankovní údaje, jednotlivec, jenž je informován, může rozhodnout o změně údajů týkajících se přístupu k jeho bankovnímu účtu tak, aby se zabránilo tomu, aby tyto informace někdo získal a využil jich k nezákonným účelům (obvykle se hovoří o „krádeži identity"). Souhrnně řečeno tato povinnost snižuje pravděpodobnost, že se jednotlivci stanou obětí krádeže identity, a rovněž může pomoci obětem přijmout nezbytné kroky k vyřešení problémů.

Nedostatky navrhované změny

30. Zatímco EIOÚ vítá systém oznamování narušení bezpečnosti stanovený čl. 4 odst. 3 a čl. 4 odst. 4, upřednostnil by jeho použití v širší míře tak, aby byli zahrnuti poskytovatelé služeb informační společnosti. To by znamenalo, že by se tento zákon vztahoval rovněž na banky on-line, podniky on-line, poskytovatele zdravotních služeb on-line atd ([2]).

31. Rovněž existují důvody, které ospravedlňují uložit poskytovatelům veřejných služeb elektronických komunikací oznamování narušení bezpečnosti, týkající se jiných organizací, jež rovněž zpracovávají velké množství osobních údajů, jejichž sdělení by mohlo být pro subjekty údajů obzvláště poškozující. Sem spadají banky on-line, zprostředkovatelé údajů a další poskytovatelé on-line, jako ti, kteří zpracovávají citlivé údaje (jež zahrnují údaje o zdraví, politické názory atd.). Ohrožení informací držených bankami on-line a podniky on-line, jež mohou zahrnovat nejen čísla bankovních účtů, ale rovněž podrobnosti o kreditních kartách, mohou podnítit krádež identity, a v tomto případě je pro jednotlivce důležité, aby byli informováni s cílem přijmout nezbytná opatření. V posledním uvedeném případě (zdravotní služby on-line) jednotlivci utrpí zcela jistě újmu neekonomické povahy, ne-li újmu finanční.

([1]) Viz zpráva „*Ekonomika bezpečnosti a vnitřní trh*", již pro Evropskou agenturu pro bezpečnost sítí a informací vypracovali Prof. Ross Anderson, Rainer Böhme, Richard Clayton a Tyler Moore. Zpráva je k dispozici na: http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Poskytovatelé služeb informační společnosti jsou definováni ve směrnici o elektronickém obchodu jako služba/služby, obvykle poskytovaná/poskytované za úplatu na dálku elektronickými prostředky a na individuální žádost příjemce služeb.

32. Rozšířením oblasti působnosti povinnosti se výše popsaný přínos očekávaný od jejího uložení neomezí na jednu oblast činnosti, tedy na oblast poskytovatelů veřejné služby elektronických komunikací, ale rozšíří se na služby informační společnosti obecně. Uložení oznamovacích povinností poskytovatelům služeb informační společnosti, jako jsou banky on-line, nejen zvýší jejich odpovědnost, ale rovněž je motivuje ke zpřísnění svých bezpečnostních opatření, a tím zabrání možným narušením bezpečnosti v budoucnu.

33. Existují jiné precedenty, kde se směrnice o ochraně soukromí v odvětví elektronických komunikací již uplatňuje na jiné subjekty než na poskytovatele veřejné služby elektronických komunikací, jako je článek 5 o důvěrnosti sdělení a článek 13 o spamu. Tím se potvrzuje, že normotvůrce v minulosti velmi moudře přijal rozhodnutí rozšířit oblast působnosti některých ustanovení směrnice o ochraně soukromí v odvětví elektronických komunikací, protože měl pocit, že to bylo vhodné a nezbytné. EIOÚ věří, že normotvůrce v současné době bez váhání zaujme podobný rozumný a flexibilní přístup a rozšíří oblast působnosti použití článku 4 s cílem zahrnout poskytovatele služeb informační společnosti. Za tímto účelem by bylo postačující vložit do čl. 4 odst. 3 tento odkaz na provozovatele služeb informační společnosti: „V případě narušení bezpečnosti, jež vedlo k náhodnému či … poskytovatel veřejně přístupných služeb elektronických komunikací a poskytovatel služeb informační společnosti … o tomto narušení neprodleně uvědomí dotčeného účastníka a vnitrostátní regulační orgán".

34. EIOÚ považuje tuto povinnost a její použití jak pro poskytovatele veřejných služeb elektronických komunikací, tak pro poskytovatele služeb informační společnosti za první krok vývoje, jejž je možno případně použít na všechny správce údajů obecně.

Specifický právní rámec týkající se narušení bezpečnosti, jenž má být vyřešen prostřednictvím postupu projednávání ve výborech

35. Tento návrh se nezabývá řadou otázek souvisejících s povinností poskytovat oznámení o narušení bezpečnosti. Příklady otázek, jež je třeba řešit, jsou okolnosti oznámení, formát a použitelné postupy. Namísto toho čl. 4 odst. 4 návrhu ponechává tato rozhodnutí k přijetí prostřednictvím postupu projednávání ve výborech ([1]), jmenovitě v Komunikačním výboru zřízeném článkem 22 rámcové směrnice, v souladu s rozhodnutím Rady ze dne 28. června 1999. Taková opatření by byla zejména přijata v souladu s článkem 5 rozhodnutí Rady ze dne 28. června 1999, jež stanoví pravidla pro regulační postup, pokud jde o „*opatření obecného významu, jejichž předmětem je uplatnění základních ustanovení základních aktů*".

36. EIOÚ není proti možnosti ponechat všechny tyto záležitosti na oblast prováděcích právních předpisů. Přijetím právních předpisů postupem projednávání ve výborech se pravděpodobně zkrátí legislativní proces. Postup spolurozhodování rovněž pomůže zajistit harmonizaci, jež je cílem, jehož by mělo být s konečnou platností dosaženo.

37. Při zohlednění velkého množství otázek, jež bude třeba prováděcími opatřeními vyřešit, a jejich závažnosti, jak je zdůrazněno níže, se zdá být vhodné zabývat se jimi společně v jednom právním předpise, a nikoli formou postupného přístupu, v němž by některé otázky byly řešeny ve směrnici o ochraně soukromí v odvětví elektronických komunikací a jiné by byly ponechány na prováděcí právní předpisy. Tak je třeba uvítat přístup Komise, jenž spočívá v ponechání těchto rozhodnutí na prováděcí právní předpisy, jež mají být přijaty po konzultaci s EIOÚ a snad i s jinými zúčastněnými stranami (viz bod níže).

Otázky, jež bude třeba vyřešit prostřednictvím prováděcích opatření

38. Význam prováděcích opatření je mnohem zřejmější, pokud si uvědomíme otázky, jež bude třeba prostřednictvím prováděcích opatření řešit. Prováděcí opatření mohou stanovit normy, podle nichž musí být doručena oznámení. Specifikují například, v čem spočívá narušení bezpečnosti, podmínky, za nichž musí být podána oznámení jednotlivcům a orgánům, termíny pro oznámení a podání oznámení.

([1]) Postupy tvorby zákonů v ES, jež zahrnují výbory složené ze zástupců vlád členských států na úrovni státních úředníků.

39. EIOÚ se domnívá, že směrnice o ochraně soukromí v odvětví elektronických komunikací by neměla, zejména v článku 4, obsahovat žádnou výjimku z oznamovací povinnosti. V tomto ohledu je EIOÚ spokojen s přístupem Komise obsaženém v článku 4, jenž stanoví oznamovací povinnost a nepředpokládá z ní žádnou výjimku, avšak umožňuje, aby tato otázka byla spolu s jinými řešena v prováděcích právních předpisech. Ačkoliv si je EIOÚ vědom argumentů, jež by mohly ospravedlnit stanovení některých výjimek z povinnosti, EIOÚ upřednostňuje, aby tato i jiné otázky byly důkladně vyřešeny prostřednictvím prováděcích právních předpisů, a to po důkladném a celkovém projednání všech příslušných témat. Jak je uvedeno výše, komplexní povaha otázek souvisejících s povinností poskytovat oznámení o narušení bezpečnosti, včetně toho, zda jsou výjimky nebo omezení vhodné, si vyžaduje, aby tyto otázky byly řešeny jednotným způsobem, tj. v rámci jednoho právního předpisu, který se zabývá výlučně tímto tématem.

Konzultace s EIOÚ a potřeba širší konzultace

40. Při zohlednění rozsahu, v němž budou mít prováděcí opatření dopad na ochranu osobních údajů jednotlivců, je důležité, aby před přijetím těchto opatření Komise provedla řádné konzultace. Proto EIOÚ vítá čl. 4 odst. 4 návrhu, jenž výslovně stanoví, že před přijetím prováděcích opatření Komise konzultuje evropského inspektora ochrany údajů. Taková opatření se nebudou ochrany osobních údajů a soukromí jednotlivců pouze dotýkat, nýbrž na ni budou mít významný dopad. Proto je důležité požádat o stanovisko EIOÚ, jak vyžaduje článek 41 nařízení (ES) č. 45/2001.

41. Vedle konzultace EIOÚ může být vhodné zahrnout ustanovení, jimiž se stanovuje, že návrh prováděcích opatření bude podléhat veřejné konzultaci, s cílem obdržet stanovisko a podpořit sdílení zkušeností s osvědčenými postupy v této věci. Tím bude poskytnut vhodný postup předkládání stanovisek nejen pro průmysl, ale rovněž pro jiné zúčastněné strany, včetně dalších orgánů pro ochranu údajů a pro Pracovní skupiny článku 29. Potřeba veřejné konzultace sílí, vezme-li se v úvahu, že postupem pro přijetí právních předpisů je postup projednávání ve výborech, s omezeným zásahem Evropského parlamentu.

42. EIOÚ poznamenává, že se v čl. 4 odst. 4 návrhu předpokládá, že Komise bude před přijetím prováděcích pravidel rovněž konzultovat Evropský úřad pro trh elektronických komunikací. V tomto ohledu EIOÚ oceňuje zásadu konzultování Evropského úřadu pro trh elektronických komunikací jakožto držitele zkušeností a znalostí Evropské agentury pro bezpečnost sítí a informací týkajících se otázek sítě a bezpečnosti informací. Do zřízení Evropského úřadu pro trh elektronických komunikací může být vhodné jako dočasné řešení zakotvit v navrhované změně (čl. 4 odst. 4) konzultaci Evropské agentury pro bezpečnost sítí a informací.

II.3 **Ustanovení o tzv. „cookies“, „spyware“ a podobných zařízeních: změny v čl. 5 odst. 3**

43. Článek 5 odst. 3 směrnice o ochraně soukromí v odvětví elektronických komunikací se zabývá otázkou technologií, jež umožňují přístup k informacím a ukládání informací v koncovém zařízení uživatele prostřednictvím sítí elektronické komunikace. Příkladem použití čl. 5 odst. 3 je použití tzv. „cookies“ ([1]). Jiné příklady obsahují použití technologií, jako je „spyware“ a trojské koně (programy skryté ve zprávách nebo v jiném zdánlivě nezávadném software). Cíl takových technologií a účely jsou velmi rozdílné; zatímco některé jsou zcela neškodné a pro uživatele spíše užitečné, jiné jsou jednoznačně velmi škodlivé a představují ohrožení.

([1]) Cookies jsou umístěny prostřednictvím poskytovatelů služeb informační společnosti (webové stránky) do koncového zařízení uživatele za různými účely, včetně rozpoznání návštěvníka při opětovné návštěvě webové stránky. V praxi to znamená, že když je cookie odesláno uživateli internetu webovou stránkou, je počítači uživatele přiděleno jedinečné číslo (tj. počítač, jenž obdržel cookies z webové stránky A se stane „počítačovým držitelem cookie 111“). Webová stránka si ponechá toto číslo jako odkaz. Nevymaže-li uživatel počítače, který obdržel cookie 111, tento soubor s cookie, napříště, když uživatel navštíví stejnou webovou stránku, bude stránka moci identifikovat počítač jako držitele cookie 111. Webová stránka si z toho samozřejmě odvodí, že tento počítač ji již dříve navštívil. Mechanismus, jenž umožňuje webové stránce rozpoznat počítač jako již známého návštěvníka, je jednoduchý. Obsahuje-li navštěvující počítač cookies, jako je cookie 111, a navštíví stránku, jež při předchozí návštěvě toto cookie vytvořila, bude hledat na pevném disku uživatele číslo souboru s tímto cookie. Pokud vyhledávač uživatele nalezne soubor s cookie, jenž odpovídá referenčnímu číslu uloženému webovou stránkou, informuje webovou stránku, že počítač obsahuje cookie 111.

44. Článek 5 odst. 3 směrnice o ochraně soukromí v odvětví elektronických komunikací stanoví podmínky, jež se použijí při získávání přístupu ke koncovému zařízení nebo ukládání informací na něj u uživatelů využívajících mimo jiné výše uvedené technologie. Podle čl. 5 odst. 3 zejména i) musí uživatelé internetu získávat jasné a úplné informace podle směrnice 95/46/ES, mimo jiné o účelech zpracování, a ii) musí uživatelé internetu smět odmítnout takové zpracování, tj. nepřistoupit na zpracování informací získaných z jejich koncového zařízení.

Přínos navrhované změny

45. Stávající čl. 5 odst. 3 směrnice o ochraně soukromí v odvětví elektronických komunikací omezuje její oblast působnosti na situace, v nichž je přístup k informacím a ukládání informací v koncovém zařízení uživatele prováděno prostřednictvím *sítí elektronických komunikací*. To zahrnuje výše uvedené situace týkající se využití cookies, jakož i jiných technologií, jako je „spyware" dodávaný prostřednictvím sítí elektronických komunikací. Avšak není ani zdaleka jasné, zda se čl. 5 odst. 3 použije v situacích, v nichž se podobné technologie šíří prostřednictvím software umístěného na externím paměťovém médiu a stahují se do koncového zařízení uživatele. Vzhledem k tomu, že ohrožení soukromí existuje nezávisle na komunikačním kanálu, omezení čl. 5 odst. 3 na jeden komunikační kanál je nešťastné.

46. EIOÚ je proto spokojen se změnou čl. 5 odst. 3, jenž po odstranění odkazu na „sítě elektronické komunikace" ve skutečnosti rozšíří oblast působnosti použití čl. 4 odst. 3. Doplněná verze čl. 5 odst. 3 vskutku zahrnuje obě situace, kdy je přístup k informacím i ukládání informací v koncovém zařízení uživatele prováděno prostřednictvím sítí elektronických komunikací, ale rovněž prostřednictvím externího paměťového média, jako je CD, CD-ROM, USB klíče atd.

Technické ukládání pro účely usnadnění přenosu

47. Poslední věta čl. 5 odst. 3 směrnice o ochraně soukromí v odvětví elektronických komunikací zůstává ve změněném znění beze změn. Podle poslední věty požadavky první věty čl. 5 odst. 3 „*nebrání technickému ukládání nebo takovému přístupu, jehož jediným účelem je provedení nebo usnadnění přenosu sdělení prostřednictvím sítě elektronických komunikací, nebo je-li to nezbytně nutné pro poskytování služeb informační společnosti* …". Takto se povinná pravidla první věty čl. 5 odst. 3 (potřeba poskytovat informace a nabídnout možnost odmítnout) nepoužijí, má-li přístup ke koncovému zařízení uživatele nebo ukládání informací jediný účel, a to *usnadnit* přenos, nebo je-li naprosto nezbytné pro poskytování služeb informační společnosti požadovaných uživatelem.

48. Směrnice nepopisuje, kdy má přístup k informacím nebo jejich ukládání jediný cíl usnadnit přenos nebo poskytování informací. Jedním příkladem, na něž by se jasně vztahovala výjimka, je vytvoření připojení k internetu. Je to proto, že pro vytvoření připojení k internetu je nezbytné získat IP adresu ([1]). Počítač koncového uživatele bude požádán, aby sdělil poskytovateli přístupu k internetu některé informace o sobě, a v návaznosti na to mu poskytovatel přístupu k internetu poskytne IP adresu. V tomto případě bude uložená informace v koncovém zařízení uživatele předána poskytovateli přístupu k internetu pro účely poskytnutí přístupu k internetu uživateli. V takovém případě je poskytovatel přístupu k internetu osvobozen od povinnosti oznámit toto shromažďování informací a poskytnout právo k odmítnutí, pokud je to třeba k poskytování služby.

49. Je-li uživatel připojen k internetu a chce-li si prohlédnout určitou webovou stránku, musí odeslat zprávu na server, na němž je webová stránka umístěna. Sever odpoví, zda ví, kam zaslat informaci, tj. zda zná IP adresu uživatele. Vzhledem k tomu, jak je tato adresa uložena, je opět požádána webová stránka, již chce uživatel navštívit, o informace pro přístup na koncové zařízení uživatele internetu. Tato operace by jednoznačně rovněž spadala do oblasti působnosti uvedené výjimky. V takových případech se zdá být vhodné pohybovat se mimo oblast působnosti použití požadavků čl. 5 odst. 3.

([1]) IP adresa (adresa internetového protokolu) je jedinečná adresa, jíž některá elektronická zařízení používají ke vzájemné identifikaci a komunikaci na počítačové síti za použití standardu internetového protokolu (IP) – jednodušeji řečeno, adresa počítače. Veškerá zařízení připojená k síti – včetně směrovačů, přepínačů, počítačů, serverů infrastruktury (např. NTP, DNS, DHCP, SNMP atd.), tiskáren, internetových faxů a některých telefonů – mohou mít svou vlastní adresu, jež je v rámci dané sítě jedinečná. Některé IP adresy mají být jedinečné v rámci celosvětového internetu, zatímco jiné musí být jedinečné pouze v rámci podniku.

50. EIOÚ považuje za vhodné osvobodit od potřeby informovat a umožnit odmítnutí ve výše uvedených případech, je-li technické ukládání nebo přístup ke koncovému zařízení uživatele *nezbytné* pouze pro provedení přenosu sdělení prostřednictvím sítě elektronické komunikace. Totéž se použije, je-li technické ukládání nebo přístup zcela nezbytný pro poskytování služeb informační společnosti. EIOÚ však nepovažuje za potřebné osvobodit od povinnosti poskytovat informace a nabídnout právo k odmítnutí v takových případech, kdy má technické ukládání nebo přístup za cíl pouze *usnadnění* přenosu sdělení. Například podle poslední věty tohoto článku nemůže mít subjekt údajů prospěch z informace a práva odmítnout zpracování jeho údajů, pokud cookies shromažďují jazykové preference nebo jeho umístění (např. Belgie, Čína), protože tento druh cookies by mohl být vydáván za takový, jenž má za cíl usnadnit přenos sdělení. EIOÚ si je vědom toho, že na úrovni softwaru může subjekt údajů ve skutečnosti ukládání cookies odmítnout nebo měnit. Žádné právní ustanovení však dostatečně jasně nezajišťuje, aby byl subjekt údajů formálně oprávněn hájit svá práva ve výše uvedené souvislosti.

51. Aby se tomuto důsledku zabránilo, EIOÚ navrhuje učinit malou změnu poslední části čl. 5 odst. 3, jež sestává ve vypuštění slova „usnadnění" z této věty: „*nebrání technickému ukládání nebo takovému přístupu, jehož jediným účelem je provedení nebo usnadnění přenosu sdělení prostřednictvím sítě elektronických komunikací, nebo je-li to nezbytně nutné pro poskytování služeb informační společnosti …*".

II.4 **Právní kroky zahájené poskytovateli veřejné služby elektronických komunikací a právními osobami: doplnění odstavce 6 do článku 13**

52. Navrhovaný čl. 13 odst. 6 stanoví správní opravné prostředky pro každou fyzickou i právnickou osobu s oprávněným zájmem, zejména pro poskytovatele služeb elektronické komunikace, jež mají obchodní zájem bojovat proti těm, kteří poruší článek 13 směrnice o ochraně soukromí v odvětví elektronických komunikací. Tento článek se zabývá zasíláním nevyžádaných obchodních sdělení.

53. Navrhovaná změna umožní například poskytovatelům přístupu k internetu bojovat proti odesílatelům nevyžádaných obchodních sdělení kvůli zneužívání jejich sítí, zažalovat subjekty za padělání adres odesílatele nebo neoprávněný vstup do serverů s cílem využít je jako místa pro odesílání nevyžádaných obchodních sdělení atd.

54. Směrnice o ochraně soukromí v odvětví elektronických komunikací nebyla jasná, pokud jde to, zda mají poskytovatelé veřejné služby elektronických komunikací právo podat žalobu na odesílatele nevyžádaných obchodních sdělení, a poskytovatelé veřejných služeb elektronických komunikací jen zřídka podávali k soudu žalobu ohledně porušení článku 13 na základě právních předpisů členských států ([1]). Uznáním příčiny žaloby poskytovatelů veřejné služby elektronických komunikací na ochranu jejich obchodních zájmů návrh potvrzuje, že směrnice o ochraně soukromí v odvětví elektronických komunikací má za cíl nejen ochranu jednotlivých účastníků, ale i poskytovatelů služeb elektronické komunikace.

55. EIOÚ je spokojen, že návrh zavádí pro poskytovatele služeb elektronické komunikace mající obchodní zájem možnost podat žalobu proti odesílatelům nevyžádaných obchodních sdělení. S výjimkou výjimečných případů jednotliví účastníci nemají peníze ani motivaci k podání takového druhu žaloby k soudu. Naproti tomu poskytovatelé přístupu k internetu a jiní poskytovatelé veřejné služby elektronických komunikací mají finanční prostředky a technologické možnosti k vyšetřování spamových kampaní s cílem nalézt pachatele a zdá se být pouze vhodné, aby měli právo učinit proti odesílatelům nevyžádaných obchodních sdělení právní kroky.

56. EIOÚ navrhovanou změnu oceňuje zejména s ohledem na to, že by rovněž umožnila povolit sdružením spotřebitelů a odborům zastupujících zájmy spotřebitelů, jimž přicházejí nevyžádaná obchodní sdělení, aby učinili u soudu právní kroky jejich jménem. Jak je uvedeno výše, škoda, již utrpěl subjekt údajů, jemuž byla zaslána nevyžádaná obchodní sdělení, není sama o sobě obvykle dostatečná k tomu, aby zahájil právní kroky před soudem. EIOÚ ve skutečnosti již navrhnul toto opatření týkající se porušení soukromí a ochrany údajů v obecném vyjádření ve svém stanovisku o pokračování pracovního

([1]) Jedním z případů byla věc Microsoft corporation v. Paul McDonald t/a Bizards UK (2006 All Er (D) 153).

programu pro lepší provádění směrnice o ochraně osobních údajů ([1]). Podle názoru EIOÚ by mohl návrh jít dále a navrhnout skupinové žaloby opravňující skupinu občanů společně využít skupinové žaloby ve věcech týkajících se ochrany osobních údajů. V případě nevyžádaného obchodního sdělení, jež obdrží velký počet jednotlivců, existuje pro skupiny jednotlivců možnost, aby se spojily a podaly proti odesílatelům nevyžádaných obchodních sdělení skupinovou žalobu.

57. EIOÚ zejména lituje toho, že návrh omezuje pro právnické osoby možnost přijetí právních kroků v případech porušení článku 13 této směrnice, tj. v případech, kdy dojde k porušení ustanovení o nevyžádaných e-mailových sděleních. Podle navržené změny by právnické osoby nemohly přijmout právní kroky týkající se porušení jiných ustanovení směrnice o ochraně soukromí v odvětví elektronických komunikací. Například stávající ustanovení neumožňuje právnické osobě, jako je sdružení spotřebitelů, přijmout právní kroky proti poskytovateli přístupu na internet, jenž sdělil osobní údaje milionů zákazníků. Vynucování směrnice o ochraně soukromí v odvětví elektronických komunikací jako celku, nikoliv jen tohoto článku, by se značně zlepšilo, kdyby byl čl. 6 odst. 3 zobecněn s cílem umožnit právnickým osobám přijmout právní kroky při porušení kteréhokoliv ustanovení směrnice o ochraně soukromí v odvětví elektronických komunikací.

58. Pro vyřešení tohoto problému EIOÚ navrhuje změnit čl. 16 odst. 3 na samostatný článek (článek 14). Dále by mělo být mírně upraveno znění čl. 13 odst. 6, a to takto: Namísto „*podle tohoto článku*“ by mělo být „podle této směrnice“.

II.5 **Posílení ustanovení o vynucování: doplnění článku 15a**

59. Směrnice o ochraně soukromí v odvětví elektronických komunikací neobsahuje výslovná ustanovení o vynucování. Namísto toho odkazuje k části o vynucování směrnice na ochranu údajů ([2]). EIOÚ vítá nový článek 15a návrhu, jenž se otázkou vynucování této směrnice výslovně zabývá.

60. Zaprvé, EIOÚ poznamenává, že účinná politika vynucování v této oblasti předpokládá, jak vyžaduje navrhovaný čl. 15a odst. 3, že vnitrostátní orgány mají vyšetřovací pravomoci pro shromažďování nezbytných informací. Doklad o porušení ustanovení směrnice o ochraně soukromí v odvětví elektronických komunikací je velmi často elektronické povahy a je možno jej uložit na různých počítačích, zařízeních nebo sítích. V této souvislosti je pro donucovací orgány důležité, aby jim byl umožněn vstup, prohlídka a případně zabavení předmětu doličného.

61. Zadruhé, EIOÚ zejména vítá navrhovanou změnu, tj. čl. 15a odst. 2, podle nějž vnitrostátní regulační orgány musí mít pravomoc nařídit soudní příkazy, tj. zastavení porušování, a mají nezbytné vyšetřovací pravomoci a zdroje. Vnitrostátní regulační orgány, včetně vnitrostátních orgánů na ochranu údajů, by měly mít pravomoc udělit soudní příkaz požadující, aby pachatelé zastavili činnost, jež směrnici o ochraně soukromí v odvětví elektronických komunikací porušuje. Soudní příkazy nebo pravomoc nařídit zastavení porušování jsou užitečným nástrojem v případě pokračování jednání, jež porušuje práva jednotlivce. Soudní příkazy budou pro zastavení porušování směrnice o ochraně soukromí v odvětví elektronických komunikací velmi užitečné, jako například při porušení článku 13 o nevyžádaných obchodních sděleních, jež je ze své povahy pokračující chování.

62. Zatřetí návrh umožňuje Komisi nařídit technická prováděcí opatření s cílem zajistit účinnou přeshraniční spolupráci při vynucování vnitrostátních právních předpisů (navrhovaná změna čl. 15a odst. 4). Zkušenosti spolupráce do současné doby zahrnují dohodu stanovenou v iniciativě Komise stanovující společný postup pro zpracování přeshraničních stížností na nevyžádaná obchodní sdělení.

([1]) Stanovisko evropského inspektora ochrany údajů ke sdělení Komise Evropskému parlamentu a Radě o pokračování pracovního programu pro lepší provádění směrnice o ochraně osobních údajů (Úř. věst. C 255, 27.10.2007, s. 1).

([2]) 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.

63. EIOÚ se domnívá, že pokud právní předpisy podporují regulační orgány při pomoci jejich protějškům v jiných zemích, bezpochyby to napomůže přeshraničnímu vynucování. Proto je vhodné, aby návrh umožnil Komisi vytvořit podmínky pro zajištění přeshraniční spolupráce, včetně postupů pro sdílení informací.

III. **ZÁVĚRY A DOPORUČENÍ**

64. EIOÚ návrh plně vítá. Navrhované změny posílí ochranu soukromí a osobních údajů jednotlivců v odvětví elektronické komunikace a činí tak velmi lehkou formou, bez vytváření neoprávněných a zbytečných zátěží pro organizace. Řečeno konkrétněji, EIOÚ se domnívá, že z větší části by navrhované změny neměly být upravovány, pokud řádně splňují sledovaný cíl. V bodě 69 níže jsou uvedeny změny, u nichž EIOÚ věří, že zůstanou bez úprav.

65. Bez ohledu na celkově pozitivní hodnocení návrhu se EIOÚ domnívá, že některé z jeho změn by měly být zlepšeny s cílem zajistit, aby účinně poskytly řádnou ochranu osobních údajů a soukromí jednotlivců. To zejména platí pro ustanovení o oznamování narušení bezpečnosti a pro ta, jež se zabývají právními kroky zahájenými poskytovateli služeb elektronických komunikací z důvodu porušení ustanovení o nevyžádaných obchodních sděleních. EIOÚ dále lituje, že se návrhem nedaří řešit některé otázky, jež řádně neřešila stávající směrnice o ochraně soukromí v odvětví elektronických komunikací, čímž se nevyužila příležitost tohoto přezkumu vyřešit přetrvávající problémy.

66. K vyřešení obou problémů, tj. otázek, jež nejsou řešeny v tomto návrhu řádně, a těch, jež nejsou řešeny vůbec, se v tomto stanovisku předkládají některé návrhy. V bodech 67 a 68 jsou problémy shrnuty a navržena konkrétní znění. EIOÚ vyzývá normotvůrce, aby je zohlednil během legislativního procesu, jímž bude návrh procházet.

67. Změny obsažené v tomto návrhu, u nichž by EIOÚ důrazně apeloval na provedení úprav, zahrnují:

i) **Oznamování narušení bezpečnosti**: Jak je uvedeno, navrhovaná změna doplňující *čl. 4 odst. 4* se použije na poskytovatele veřejných služeb elektronických komunikací ve veřejných sítích (poskytovatelé internetových služeb, provozovatelé sítí), kteří jsou nuceni oznámit vnitrostátním regulačním orgánům a svým zákazníkům narušení bezpečnosti. EIOÚ tuto povinnost plně podporuje. EIOÚ se domnívá, že tato povinnost by se měla rovněž vztahovat na poskytovatele služeb informační společnosti, kteří často zpracovávají citlivé osobní informace. Takto by uvedenou povinnost musely plnit rovněž banky a pojišťovny on-line, poskytovatelé zdravotních služeb on-line a jiné podniky on-line.

Za tímto účelem EIOÚ navrhuje vložit do čl. 4 odst. 3 tento odkaz na poskytovatele služeb informační společnosti: „V případě narušení bezpečnosti … poskytovatel veřejně přístupných služeb elektronických komunikací a *poskytovatel služeb informační společnosti* … o tomto narušení neprodleně uvědomí dotčeného účastníka a vnitrostátní regulační orgán“.

ii) **Právní kroky zahájené poskytovateli veřejných služeb elektronických komunikací ve veřejných sítích**: Jak bylo uvedeno, navrhovaná změna doplňující *čl. 13 odst. 6* stanoví správní opravné prostředky pro každou fyzickou nebo právnickou osobu, zejména pro poskytovatele služeb elektronické komunikace, v souvislosti s porušením článku 13 směrnice o ochraně soukromí v odvětví elektronických komunikací, jenž se týká nevyžádaných obchodních sdělení. EIOÚ je s tímto ustanovením spokojen. EIOÚ však nevidí důvod, přič by měla být tato nová možnost omezena na porušení článku 13 směrnice. EIOÚ navrhuje umožnit právnickým osobám přijmout právní kroky v případě porušení kteréhokoliv ustanovení směrnice o ochraně soukromí v odvětví elektronických komunikací.

K dosažení výše uvedeného cíle EIOÚ navrhuje změnit čl. 16 odst. 3 na samostatný článek (článek 14). Dále by mělo být mírně upraveno znění čl. 13 odst. 6, a to takto: Namísto „*podle tohoto článku*“ by mělo být „podle této směrnice“.

68. Oblast působnosti směrnice o ochraně soukromí v odvětví elektronických komunikací, jež je v současné době omezena na poskytovatele veřejných sítí elektronických komunikací, je jednou z nejvíce znepokojujících otázek, kterou se návrhem nepodařilo vyřešit. EIOÚ se domnívá, že by směrnice měla být změněna tak, aby byla rozšířeno její použití, s cílem zahrnout poskytovatele služeb elektronické komunikace rovněž do smíšených (soukromých/veřejných) a soukromých sítí.

69. Změny, u nichž by EIOÚ důrazně apeloval na provedení změn, zahrnují:

i) **Identifikace na základě rádiové frekvence**: Navrhovaná změna *článku 3*, podle níž sítě elektronických komunikací zahrnují *„veřejné komunikační sítě podporující zařízení pro sběr a identifikaci údajů“*, je plně postačující. Toto ustanovení má velmi pozitivní význam, protože objasňuje, že řada aplikací s identifikací na základě rádiové frekvence musí odpovídat směrnici o ochraně soukromí v odvětví elektronických komunikací, a tak odstraňuje určitou právní nejistotu ve věci tohoto bodu.

ii) **Cookies/spyware**: Navrhovanou změnu *čl. 5 odst. 3* je třeba uvítat, protože v důsledku toho se povinnost informovat a poskytnout právo k odmítnutí mít uloženy cookies nebo spyware v koncovém zařízení, rovněž použije, pokud jsou tato zařízení umístěna prostřednictvím externího paměťového média, jako je CD-ROM, USB klíče atd. EIOÚ však navrhuje, aby byla učiněna malá změna v poslední části čl. 5 odst. 3, a to aby bylo vypuštěno slovo „usnadnění“.

iii) **Volba projednávání ve výborech s konzultací evropského inspektora ochrany údajů a podmínky a omezení oznamovací povinnosti**: Navrhovaná změna doplňující čl. 4 odst. 4 ohledně oznamování narušení bezpečnosti ponechává rozhodnutí o složitých otázkách ohledně podmínek, formátu či postupů systému oznamování narušení bezpečnosti na postupu projednávání ve výborech po vyžádání stanoviska EIOÚ. EIOÚ tento jednotný přístup důrazně podporuje. Právní předpisy týkající se oznamování narušení bezpečnosti představují samostatné téma, jež je třeba vyřešit po důkladném projednání a analýze.

S touto otázkou souvisí požadavek některých zúčastněných stran navrhnout výjimky z povinnosti oznamovat narušení bezpečnosti v čl. 4 odst. 4. EIOÚ tento přístup důrazně odmítá. Spíše je pro to, aby celá otázka oznamování – jak oznamovat, za jakých podmínek je možno oznámení redukovat nebo nějak jinak omezit – byla analyzována jako celek, a to po důkladném projednání.

iv) **Vynucování**: Navrhovaná změna doplňující *článek 15a* obsahuje mnoho užitečných prvků, jež je třeba zachovat, což přispěje k zajištění účinné shody, včetně posílení vyšetřovacích pravomocí vnitrostátních regulačních orgánů (čl. 15 a odst. 3) a zavedení pravomoci vnitrostátních regulačních orgánů s cílem zastavit porušování.

V Bruselu dne 10. dubna 2008.

Peter HUSTINX

evropský inspektor ochrany údajů