Druhé stanovisko evropského inspektora ochrany údajů k přezkumu směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích)

(2009/C 128/04)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na článek 286 této smlouvy,

s ohledem na Listinu základních práv Evropské unie, a zejména na článek 8 této listiny,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů,

s ohledem na směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací,

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,

PŘIJAL TOTO STANOVISKO:

I. ÚVOD

Souvislosti

1. Dne 13. listopadu 2007 Evropská komise přijala návrh, kterým se mění mimo jiné směrnice o soukromí a elektronických komunikacích, k níž se obvykle odkazuje jako ke směrnici o ochraně soukromí v odvětví elektronických komunikací [1] (dále jen „návrh" nebo „návrh Komise"). Dne 10. dubna 2008 přijal EIOÚ stanovisko k uvedenému návrhu Komise, v němž uvedl doporučení ke zlepšení návrhu ve snaze napomoci k zajištění toho, aby navrhované změny vedly k nejlepší možné ochraně soukromí a osobních údajů jednotlivců (dále jen „první stanovisko EIOÚ") [2].

2. EIOÚ uvítal vytvoření povinného systému oznamování narušení bezpečnosti navrhované Komisí, na jehož základě mají společnosti povinnost informovat jednotlivce v případě, že byly jejich osobní údaje ohroženy. Dále rovněž uvítal nové ustanovení umožňující právnickým osobám (např. sdružením spotřebitelů a poskytovatelům internetových služeb) podat žalobu na odesílatele nevyžádaných obchodních sdělení s cílem doplnit stávající nástroje v boji proti nevyžádaným obchodním sdělením („spam").

3. Během projednávání v Parlamentu, které předcházelo prvnímu čtení Evropského parlamentu, poskytl EIOÚ další poradenství prostřednictvím připomínek k vybraným otázkám, které vystaly ve zprávách navržených výbory Evropského parlamentu odpovědnými za přezkum směrnice o univerzální službě [3] a směrnice o soukromí a elektronických komunikacích (dále jen „připomínky") [4]. Připomínky se v první řadě týkaly otázek souvisejících se zpracováním provozních údajů a s ochranou práv duševního vlastnictví.

4. Dne 24. září 2008 Evropský parlament přijal legislativní usnesení o směrnici o soukromí a elektronických komunikacích (dále jen „první čtení") [5] EIOÚ se vyjádřil kladně k několika změnám Evropského parlamentu, které byly přijaty v návaznosti na stanovisko a připomínky EIOÚ uvedené výše. K důležitým změnám patřilo mimo jiné zahrnutí poskytovatelů služeb informační společnosti (tj. společností působících na internetu) do rámce povinnosti oznamovat narušení bezpečnosti. EIOÚ rovněž uvítal změnu umožňující právnickým a fyzickým osobám

[1] Přezkum směrnice o soukromí a elektronických komunikacích je součástí rozsáhlejšího přezkumu, jehož cílem bylo zřídit telekomunikační úřad EU, přezkoumat směrnice 2002/21/ES, 2002/19/ES, 2002/20/ES, 2002/22/ES a 2002/58/ES, jakož i nařízení (ES) č. 2006/2004 (dále jen souhrnně „přezkum telekomunikačního balíčku").

[2] Stanovisko ze dne 10. dubna 2008 k návrhu směrnice, 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), Úř. věst. C 181, 18.7.2008, s. 1.

[3] Směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací (směrnice o univerzální službě), Úř. věst. L 108, 24.4.2002, s. 51.

[4] Připomínky EIOÚ k vybraným otázkám, které vyplynuly ze zprávy Výboru pro vnitřní trh a ochranu spotřebitelů o přezkumu směrnice 2002/22/ES (o univerzální službě) a směrnice 2002/58/ES (o soukromí a elektronických komunikacích), 2. září 2008. K dispozici na adrese: www.edps.europa.eu

[5] Legislativní usnesení Evropského parlamentu ze dne 24. září 2008 o návrhu směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb 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 (KOM(2007) 698 – C6-0420/2007 – 2007/0248(COD)).

podat žalobu na porušení kteréhokoliv ustanovení směrnice o soukromí a elektronických komunikacích (nikoliv pouze na porušení ustanovení o nevyžádaném obchodním sdělení, jak původně navrhovala Komise). Po prvním čtení Parlamentu přijala Komise pozměněný návrh směrnice o soukromí a elektronických komunikacích (dále jen „pozměněný návrh“) ([6]).

5. Dne 27. listopadu 2008 Rada dosáhla politické dohody o přezkumu pravidel týkajících se telekomunikačního balíčku, včetně směrnice o soukromí a elektronických komunikacích, z níž vzejde společný postoj Rady (dále jen „společný postoj“) ([7]). Společný postoj bude předložen Evropskému parlamentu podle čl. 251 odst. 2 Smlouvy o založení Evropského společenství, což může vést k navržení změn ze strany Evropského parlamentu.

Celkový názor na postoj Rady

6. Rada změnila základní prvky znění návrhu a nepřijala mnoho změn přijatých Evropským parlamentem. Ačkoliv společný postoj zcela určitě obsahuje pozitivní prvky, pokud jde o celek, EIOÚ je znepokojen jeho obsahem, zejména proto, že společný postoj nezahrnuje některé pozitivní změny navržené Evropským parlamentem, pozměněným návrhem nebo stanovisky EIOÚ a evropských orgánů pro ochranu údajů vydaných Pracovní skupinou zřízenou podle článku 29. ([8])

7. Naproti tomu byly v několika případech ustanovení pozměněného návrhu a změny Evropského parlamentu, které poskytovaly záruky občanům, vypuštěny či podstatně oslabeny. V důsledku toho je ve společném postoji úroveň ochrany poskytnutá jednotlivcům podstatně oslabena. Proto EIOÚ nyní vydává druhé stanovisko a věří, že v průběhu legislativního procesu v souvislosti se směrnicí o soukromí a elektronických komunikacích budou přijaty nové změny, které obnoví záruky v oblasti ochrany údajů.

8. Toto druhé stanovisko se zaměřuje na některé podstatné obavy a neopakuje všechny body uvedené v prvním stanovisku evropského inspektora ochrany údajů nebo v připomínkách, které platí i nadále. Toto stanovisko se věnuje především těmto otázkám:

— ustanovení o oznamování narušení bezpečnosti;

— rozsah působnosti směrnice o soukromí a elektronických komunikacích v souvislosti se soukromými a veřejně přístupnými soukromými sítěmi;

— zpracování provozních údajů pro bezpečnostní účely;

— možnost právnických osob podat žalobu na porušení směrnice o soukromí a elektronických komunikacích.

9. Při řešení výše uvedených otázek analyzuje toto stanovisko společný postoj Rady a porovnává jej s prvním čtením v Evropském parlamentu a pozměněným návrhem Komise. Stanovisko obsahuje doporučení zaměřená na zjednodušení ustanovení směrnice o soukromí a elektronických komunikacích a na zajištění toho, aby směrnice i nadále odpovídajícím způsobem chránila soukromí a osobní údaje jednotlivců.

II. USTANOVENÍ O OZNAMOVÁNÍ NARUŠENÍ BEZPEČNOSTI

10. EIOÚ podporuje přijetí režimu oznamování narušení bezpečnosti, podle něhož budou orgány a jednotlivci uvědoměni v případě, že jsou jejich osobní údaje ohroženy. ([9]) Oznamování o narušení bezpečnosti může pomoci jednotlivcům přijmout nezbytné kroky ke zmírnění jakýchkoliv potenciálních škod, které z tohoto ohrožení vyplývají. Povinnost zasílat oznámení informující o narušení bezpečnosti kromě toho povzbudí společnosti, aby zlepšovaly bezpečnost údajů, a posílí jejich odpovědnost, pokud jde o osobní údaje, za něž odpovídají.

11. Pozměněný návrh Komise, první čtení Evropského parlamentu a společný postoj Rady představují tři různé přístupy k oznamování narušení bezpečnosti, které se v současné době zvažují. Všechny tři přístupy mají pozitivní aspekty. EIOÚ se však domnívá, že u každého z těchto přístupů existuje prostor pro zlepšení, a doporučuje, aby při zvažování konečných kroků k přijetí režimu oznamování narušení bezpečnosti byla zohledněna doporučení popsaná níže.

([6]) Pozměněný návrh směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb 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, Brusel 6.11.2008 KOM(2008) 723 v konečném znění.

([7]) K dispozici na veřejné webové stránce Rady.

([8]) Stanovisko 2/2008 k přezkumu směrnice 2002/58/ES o soukromí a elektronických komunikacích (neboli *ePrivacy Directive*), které je k dispozici na webové stránce Pracovní skupiny zřízené podle článku 29.

([9]) V tomto stanovisku se používá termín „ohrožený“ pro označení jakéhokoliv náhodného či nedovoleného zničení, ztráty, úpravy nebo neoprávněnému sdělování či zpřístupnění osobních údajů přenášených, uchovávaných či jinak zpracovávaných.

12. Při analýze zmíněných tří režimů oznamování narušení bezpečnosti je třeba zvážit pět kritických bodů: *(i)* definici narušení bezpečnosti; *(ii)* subjekty, na něž se vztahuje oznamovací povinnost (dále jen „zahrnuté subjekty") *(iii)* kritérium pro oznamovací povinnost; *(iv)* určení subjektu odpovědného za stanovení, zda narušení bezpečnosti odpovídá tomuto kritériu či nikoliv a *(v)* příjemci oznámení.

Shrnutí přístupů Komise, Rady a Evropského parlamentu

13. Evropský parlament, Komise a Rada přijaly různé přístupy k oznamování narušení bezpečnosti. V prvním čtení Evropského parlamentu byl změněn původní režim oznamování narušení bezpečnosti stanovený v návrhu Komise. ([10]) Podle přístupu Evropského parlamentu se oznamovací povinnost vztahuje nejen na poskytovatele veřejně dostupných služeb elektronických komunikací, ale rovněž na poskytovatele služeb informační společnosti. V rámci tohoto přístupu by dále byla veškerá narušení osobních údajů oznámena vnitrostátnímu regulačnímu orgánu nebo příslušným orgánům (dále jen souhrnně „orgány") Pokud by tyto orgány stanovily, že je narušení *závažné*, požadovaly by, aby poskytovatelé veřejně dostupných služeb elektronických komunikací a poskytovatelé služeb informační společnosti neprodleně informovali dotčené osoby. V případě narušení, které představuje bezprostřední a přímé ohrožení, by poskytovatelé veřejně dostupných služeb elektronických komunikací a poskytovatelé služeb informační společnosti oznámili tuto skutečnost jednotlivcům ještě před tím, než informují orgány, a nečekali by na rozhodnutí regulačního orgánu. Výjimka z povinnosti informovat spotřebitele se vztahuje na subjekty, které mohou prokázat orgánům, že *„byla zavedena náležitá opatření technologické ochrany"* činící údaje nečitelnými pro všechny, kdo nemají oprávnění k přístupu k nim.

14. Podle přístupu Rady musí být narušení také oznámeno jak účastníkům, tak orgánům, avšak pouze v případech, kdy se *zahrnuté subjekty* domnívají, že narušení představuje *závažné nebezpečí* pro soukromí účastníka (tj. krádež či podvodné zneužití totožnosti, fyzická újma, hrubá potupa či poškození pověsti).

15. V pozměněném návrhu Komise je zachována povinnost oznámit orgánům všechna narušení, kterou navrhl Evropský parlament. Avšak na rozdíl od přístupu Evropského parlamentu pozměněný návrh obsahuje výjimku z požadavku na oznamování dotčeným jednotlivcům, pokud poskytovatel veřejně dostupných služeb elektronických komunikací prokáže příslušnému orgánu, že *(i)* *„s přiměřenou pravděpodobností"* nedojde v důsledku tohoto narušení k žádné škodě (např. k hospodářské ztrátě, společenské škodě nebo krádeži totožnosti) nebo *(ii)* pokud byla na údaje, u nichž došlo k narušení, použita *„náležitá opatření technologické ochrany"*. Z toho vyplývá, že se v přístupu Komise spojuje oznámení jednotlivcům s analýzou škod.

([10]) Touto otázkou se zabývají zejména tyto změny Evropského parlamentu: 187, 124 až 127, 27, 21 a 32.

16. Je důležité poznamenat, že podle přístupu Evropského parlamentu ([11]) a Komise jsou to *orgány*, které jsou v konečném důsledku oprávněny stanovit, zda je narušení závažné nebo zda může s přiměřenou pravděpodobností způsobit škodu. Naproti tomu v přístupu Rady je rozhodnutí ponecháno na *dotčených subjektech*.

17. Přístup Rady i Komise se vztahuje pouze na poskytovatele veřejně dostupných služeb elektronických komunikací, a nikoliv, jak je tomu v případě přístupu Evropského parlamentu, na poskytovatele služeb informační společnosti.

Definice narušení bezpečnosti

18. EIOÚ vítá, že všechny tři legislativní návrhy obsahují stejnou definici oznamování narušení bezpečnosti, které je vymezeno jako *„narušení bezpečnosti, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně či neoprávněnému vyzrazení nebo zpřístupnění osobních údajů přenášených, uchovávaných nebo jinak zpracovávaných […]"* ([12])

19. Jak je podrobněji uvedeno níže, tato definice je vítána, protože je dostatečně široká, aby zahrnula většinu příslušných situací, v nichž by mohlo být zaručeno oznamování narušení bezpečnosti.

20. Zaprvé, tato definice zahrnuje případy, kdy došlo k *neoprávněnému přístupu* k osobním údajům ze strany třetí osoby, jako je neoprávněné vniknutí na servery obsahující osobní údaje a získání takových informací.

21. Zadruhé, tato definice by rovněž zahrnula situace, v nichž došlo ke ztrátě nebo vyzrazení osobních údajů, přičemž neoprávněný přístup je třeba ještě prokázat. Jednalo by se o takové situace, kdy mohlo dojít ke ztrátě osobních údajů (např. CD-ROMů, USB klíčů nebo jiných přenosných zařízení) nebo ke zveřejnění řádnými uživateli (složka s údaji zaměstnance nedopatřením a dočasně zpřístupněná pro veřejně dostupnou oblast prostřednictvím internetu). Vzhledem k tomu, že často nebude k dispozici důkaz o tom, že k těmto údajům může nebo nemůže mít v daném okamžiku přístup třetí osoba nebo že tyto údaje může využít, zdá se být vhodné zahrnout tyto případy do rozsahu této definice. Proto EIOÚ doporučuje tuto definici zachovat. EIOÚ rovněž doporučuje zahrnout definici narušení bezpečnosti do článku 2 směrnice o soukromí a elektronických komunikacích, protože by to více odpovídalo celkové struktuře směrnice a zajistilo by to větší jasnost.

([11]) Vyjma případů bezprostředního a přímého ohrožení; v takovém případě musí zahrnuté subjekty nejprve informovat spotřebitele.

([12]) Článek 2 písm. i) společného postoje a pozměněného návrhu a čl. 3 odst. 3 prvního čtení Evropského parlamentu.

Subjekty, na něž by se měla vztahovat oznamovací povinnost

22. Oznamovací povinnost v rámci přístupu Evropského parlamentu se vztahuje na poskytovatele veřejně dostupných služeb elektronických komunikací a na poskytovatele služeb informační společnosti. Avšak podle režimů Rady a Komise budou mít oznamovací povinnost vůči jednotlivcům pouze poskytovatelé veřejně dostupných služeb elektronických komunikací, jako jsou telekomunikační společnosti a poskytovatelé přístupu k internetu, a to v případě, že dojde k narušení bezpečnosti vedoucí k ohrožení osobních údajů. Jiné oblasti činnosti, jako jsou například internetové banky, internetoví maloobchodníci, internetoví poskytovatelé zdravotnických služeb a jiní nejsou touto povinností vázáni. Z níže uvedených důvodů se EIOÚ domnívá, že z hlediska veřejné politiky je nutné zajistit, aby se na služby informační společnosti, které zahrnují internetové podniky, internetové banky, internetové poskytovatele zdravotnických služeb a další, rovněž vztahovala oznamovací povinnost.

23. Zaprvé, EIOÚ uvádí, že ačkoliv telekomunikační společnosti jsou jistě cílem narušení bezpečnosti, které odůvodňuje oznamovací povinnost, totéž platí pro jiné druhy společností či poskytovatelů. Pravděpodobnost narušení bezpečnosti v případě internetových maloobchodníků, internetových bank, on-line lékáren je stejná, ne-li vyšší, jako v případě telekomunikačních společností. Na základě zvážení rizik se proto nelze přiklonit k omezení rozsahu požadavku oznamovat narušení údajů na poskytovatele veřejně dostupných služeb elektronických komunikací. Potřebu širšího přístupu dokládají zkušenosti jiných zemí. Například téměř všechny státy ve Spojených státech amerických (nyní je jich více než 40) přijaly zákony o oznamování narušení bezpečnosti, které mají širší oblast působnosti a zahrnují nejen poskytovatele veřejně dostupných služeb elektronických komunikací, ale všechny subjekty mající požadované osobní údaje.

24. Zadruhé, i když je zřejmé, že narušení těch druhů osobních údajů, které jsou pravidelně zpracovávány poskytovateli veřejně dostupných služeb elektronických komunikací, může mít dopad na soukromí jednotlivců, totéž platí, ne-li ještě ve větší míře, pro druhy osobních informací zpracovávaných poskytovateli služeb informační společnosti. Banky a jiné finanční instituce mohou mít zcela jistě k dispozici vysoce důvěrné informace (např. údaje o bankovních účtech), jejichž vyzrazení může umožnit využití pro účely krádeže totožnosti. Rovněž vyzrazení velmi citlivých údajů týkajících se zdraví prostřednictvím zdravotních služeb on-line může jednotlivce velmi poškodit. Ty druhy osobních údajů, které mohou být ohroženy, proto rovněž vyžadují širší použití oznamování narušení bezpečnosti, které by zahrnovalo alespoň poskytovatele služeb informační společnosti.

25. Proti rozšíření oblasti působnosti tohoto článku, tj. subjektů, na které se vztahuje tento požadavek, byly vzneseny některé právní námitky. Zejména skutečnost, že celková oblast působnosti směrnice o soukromí a elektronických komunikacích se týká pouze poskytovatelů veřejně dostupných služeb elektronických komunikací, byla uvedena jako překážka uplatnění oznamovací povinnosti rovněž na poskytovatele služeb informační společnosti.

26. V této souvislosti by chtěl EIOÚ připomenout, že: *(i)* neexistuje žádná právní překážka pro zahrnutí dalších subjektů do oblasti působnosti některých ustanovení této směrnice, společně s poskytovateli veřejně dostupných služeb elektronických komunikací. To je zcela na uvážení normotvůrce Společenství. *(ii)* ve stávající směrnici o soukromí a elektronických komunikacích jsou jiné precedenty ohledně použití na jiné subjekty, než jsou poskytovatelé veřejně dostupných služeb elektronických komunikací.

27. Například článek 13 se použije nejen na poskytovatele veřejně dostupných služeb elektronických komunikací, ale na kteroukoliv společnost, která zasílá nevyžádaná sdělení, k čemuž je vyžadován předchozí souhlas. Kromě toho čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, který mimo jiné zakazuje uchovávání informací, jako jsou „cookies", v koncových zařízeních uživatelů, je závazný nejen pro poskytovatele veřejně dostupných služeb elektronických komunikací, ale rovněž pro všechny, kdo se pokoušejí ukládat informace nebo získat přístup k informacím uloženým v koncovém zařízení jednotlivců. V rámci stávajícího legislativního procesu navíc Komise dokonce navrhla rozšířit použití čl. 5 odst. 3 na případy, kdy podobné technologie (cookies/spyware) nejsou přenášeny pouze prostřednictvím systémů elektronické komunikace, ale jakýmkoliv jiným možným způsobem (přenášení stahováním z internetu nebo prostřednictvím externího paměťového média, např. CD-ROMu, USB klíče, flash disků atd.). Všechny tyto prvky jsou vítány a měly by být zachovány, ale rovněž by měly stanovit důležitý precedens pro stávající diskusi o oblasti působnosti.

28. Dále v rámci stávajícího legislativního procesu Komise a Evropský parlament a pravděpodobně i Rada navrhly nový čl. 6 odst. 6a, projednávaný níže, který se vztahuje na jiné subjekty, než jsou poskytovatelé veřejně dostupných služeb elektronických komunikací.

29. A konečně, s ohledem na obsáhlé pozitivní prvky vyplývající z povinnosti oznamovat narušení bezpečnosti budou občané s velkou pravděpodobností očekávat tyto přínosy nejen pokud byly jejich osobní údaje ohroženy ze strany poskytovatelů veřejně dostupných služeb elektronických komunikací, ale rovněž ze strany poskytovatelů služeb informační služby. Očekávání občanů nemusí být splněna, pokud například nejsou informováni v případě, že internetová banka ztratila informace o jejich bankovním účtu.

30. Souhrnně řečeno, EIOÚ je přesvědčen, že plného přínosu vyplývajícího z oznamování narušení bezpečnosti bude lépe dosaženo pouze tehdy, pokud budou do oblasti zahrnutých subjektů spadat vedle poskytovatelů veřejně dostupných služeb elektronických komunikací i poskytovatelé služeb informační společnosti.

Kritérium pro oznamovací povinnost

31. Pokud jde o podnět k oznámení, EIOÚ se domnívá, jak je dále vysvětleno níže, že kritérium „*přiměřené pravděpodobnosti poškození*“ uvedené v pozměněném návrhu jako je ze tří navrhovaných kritérií nejvhodnější. Nicméně je důležité zajistit, aby „poškození“ bylo dostatečně široké k pokrytí všech příslušných případů negativních dopadů na soukromí nebo jiné oprávněné zájmy jednotlivců. Jinak by bylo vhodnější stanovit nové kritérium, na jehož základě by oznamování bylo povinné „*pokud by narušení s přiměřenou pravděpodobností mohlo poškodit jednotlivce*“.

32. Jak bylo naznačeno v předchozí části, podmínky, za nichž musí být učiněno oznámení jednotlivcům (dále jako „podnět“ nebo „kritérium“) se liší podle přístupu Evropského parlamentu, Komise a Rady. Je zřejmé, že objem oznámení, která jednotlivec obdrží, bude z velké části záviset na podnětu nebo kritériu stanovených pro oznámení.

33. Podle režimů Rady a Komise musí být oznámení provedeno, pokud narušení představuje „*závažné narušení soukromí účastníka*“ (Rada) a pokud „*poškození zájmu spotřebitele je v důsledku narušení přiměřeně pravděpodobné*“ (Komise). Podle režimu Evropského parlamentu je podnětem pro oznámení jednotlivci „*závažnost narušení*“ (tj. oznámení jednotlivcům se vyžaduje, pokud je porušení považováno za „*závažné*“). Oznámení není nezbytné, pokud není dosaženo tohoto prahu ([13]).

34. EIOÚ chápe, že pokud došlo k ohrožení osobních údajů, lze namítnout, že jednotlivci, jimž tyto údaje náleží, mají za všech okolností právo o této události vědět. Nicméně je však správné uvažovat o tom, zda se jedná o vhodné řešení se zřetelem na jiné zájmy a ohledy.

35. Bylo poznamenáno, že povinnost zaslat oznámení při každém ohrožení osobních údajů, jinak řečeno bez omezení, může vést k nadměrnému oznamování a „únavě z oznamování“, což by mohlo mít za následek ztrátu citlivosti. Jak je uvedeno níže, EIOÚ považuje tento argument za důležitý; avšak současně chce zdůraznit své obavy týkající se nadměrného oznamování, které by mohlo být možným ukazatelem širokosáhlého selhání informačních bezpečnostních postupů.

36. Jak je uvedeno výše, EIOÚ vidí možné negativní důsledky nadměrného oznamování a chtěl by pomoci zajistit, aby právní rámec přijatý ohledně oznamovací povinnosti při narušení bezpečnosti neměl tento následek. Pokud by jednotlivcům byla zasílána častá oznámení o narušení bezpečnosti, a to i v situacích, v nichž nedochází k poškození, ztrátě nebo nesnázím, může dojít k tomu, že budou narušeny klíčové cíle poskytování oznámení, protože jednotlivci mohou paradoxně ignorovat oznámení v těch případech, v nichž ve skutečnosti musí přijmout kroky k tomu, aby se ochránili. Úsilí o nalezení správné rovnováhy při poskytování smysluplného oznámení je proto důležité, neboť pokud jednotlivci na přijatá oznámení nereagují, účinnost režimů oznamování je značně omezena.

37. S cílem přijmout odpovídající kritérium, které nepovede k nadměrnému oznamování, je třeba vedle zohlednění podnětu pro oznámení zvážit i jiné faktory, zejména definici narušení bezpečnosti a informace, na něž se vztahuje oznamovací povinnost. V tomto ohledu EIOÚ poznamenává, že podle tří navrhovaných přístupů může být objem oznámení vysoký, a to vzhledem k výše projednávané široké definici narušení bezpečnosti. Tato obava ohledně nadměrného oznamování je umocněna skutečností, že se definice narušení bezpečnosti vztahuje na všechny druhy osobních údajů. Ačkoliv se EIOÚ domnívá, že se jedná o správný přístup (neomezovat typy osobních údajů, na něž se vtahuje oznamování), narozdíl od jiných přístupů, jako jsou právní předpisy USA, v nichž se požadavky zaměřují na citlivost údajů, jedná se o faktor, který je třeba vzít v úvahu.

38. S ohledem na výše uvedené skutečnosti a při celkovém zohlednění různých proměnných EIOÚ považuje za vhodné stanovit práh nebo normu, při jejichž nedosažení není oznamování povinné.

39. Zdá se, že obě navrhovaná kritéria, tj. že narušení představuje „vážné *ohrožení soukromí*“ nebo „*přiměřeně pravděpodobné poškození*“, zahrnují například společenské poškození nebo poškození dobré pověsti a hospodářskou ztrátu. Tato kritéria by se například zaměřila na případy, kdy je jednotlivec vystaven krádeži totožnosti prostřednictvím zveřejnění neveřejných identifikátorů, jako jsou čísla pasů, jakož i zveřejnění informací o soukromém životě jednotlivce. EIOÚ tento přístup vítá. Je přesvědčen, že přínosů oznamovací povinnosti při narušení bezpečnosti by nebylo plně dosaženo, pokud by se režim oznamování vztahoval pouze na narušení vedoucí k hospodářské újmě.

([13]) Viz poznámka pod čarou 11 týkající se výjimky z tohoto pravidla.

40. Ze dvou navrhovaných kritérií EIOÚ upřednostňuje kritérium Komise „*přiměřeně pravděpodobné způsobení škody*“, protože by se tak zajistila vhodnější míra ochrany jednotlivců. Narušení povedou mnohem pravděpodobněji k oznamování, pokud existuje „*přiměřená pravděpodobnost způsobení škody*“ soukromí jednotlivců, než pokud mají představovat „*závažné nebezpečí*“ vzniku takové škody. Proto pokud by do oblasti působnosti byla zahrnuta pouze narušení představující závažné nebezpečí pro soukromí jednotlivců, bylo by značně omezeno množství narušení, která musí být oznámena. Zahrnutí pouze takových narušení by poskytovatelům veřejně dostupných služeb elektronických komunikací a poskytovatelům služeb informační společnosti udělilo nadměrnou pravomoc rozhodnout o tom, zda je oznámení nutné, protože by pro ně bylo mnohem snadnější odůvodnit závěr, že neexistuje žádné „*závažné nebezpečí*“, než že k nebezpečí „*s přiměřenou pravděpodobností nedojde*“. Zatímco je třeba zcela jistě zabránit nadměrnému oznamování, je třeba v případě pochybností rozhodnout ve prospěch ochrany soukromých zájmů jednotlivců a jednotlivci by měli být chráněni přinejmenším v případě, že jim narušení s přiměřenou pravděpodobností způsobí škodu. Navíc spojení „*přiměřeně pravděpodobně*“ bude účinnější v praxi, a to jak pro zahrnuté subjekty, tak pro příslušné orgány, protože vyžaduje objektivní posouzení případu a jeho příslušných souvislostí.

41. Narušení osobních údajů může dále způsobit škodu, kterou je obtížné kvantifikovat a která se může lišit. Zveřejnění stejného druhu údajů může skutečně v závislosti na konkrétních okolnostech způsobit značnou škodu jednomu jednotlivci a menší škodu jinému. Kritérium, které by vyžadovalo, aby škoda byla hmotná, významná nebo závažná, by nebylo vhodné. Například přístup Rady, který vyžaduje, aby narušení *závažně* ovlivnilo něčí soukromí, by poskytl neodpovídající ochranu jednotlivcům, neboť takové kritérium vyžaduje, aby byl dopad na soukromí „závažný“. Navíc vzniká prostor pro subjektivní posouzení.

42. Výše uvedené spojení „*přiměřeně pravděpodobné poškození*“ se sice zdá být vhodným kritériem pro oznamování narušení bezpečnosti, EIOÚ se však i nadále obává, že by sem nemusely spadat všechny situace, v nichž je oznámení jednotlivcům zaručeno, tj. všechny situace, v nichž existuje přiměřená pravděpodobnost negativního dopadu na soukromí nebo jiná zákonná práva jednotlivců. Z tohoto důvodu by mohla být zváženo kritérium, které by vyžadovalo oznámení, „*pokud by narušení s přiměřenou pravděpodobností poškodilo jednotlivce*“.

43. Toto alternativní kritérium má další výhodu v tom, že je v souladu s právními předpisy EU v oblasti ochrany údajů. Směrnice o ochraně údajů vskutku často odkazuje k poškození práv a svobod subjektů údajů. Například článek 18 a 49. bod odůvodnění, které se zabývají povinností registrovat zpracování údajů u orgánů pro ochranu osobních údajů, opravňují členské státy k výjimce z této povinnosti v případech, v nichž zpracování „*nejsou způsobilá poškodit práva a svobody subjektů údajů*“. Podobné znění je použito v čl. 16 odst. 6 společného postoje s cílem umožnit právnickým osobám podat žalobu na spammery.

44. Dále by s ohledem na výše uvedené bylo možno rovněž očekávat, že zahrnuté subjekty, a zejména příslušné orgány k prosazování právních předpisů na ochranu údajů, budou důvěrněji seznámeny s výše uvedenými kritérii, což usnadní jejich posouzení toho, zda příslušné narušení odpovídá požadovanému kritériu.

Subjekt určující, zda narušení bezpečnosti odpovídá kritériu či nikoliv

45. Podle přístupu Evropského parlamentu (vyjma případů přímého ohrožení) a pozměněného návrhu Komise bude na orgánech členských států, aby určily, zda narušení bezpečnosti odpovídá kritériu, které je podnětem pro povinnost informovat dotčené jednotlivce.

46. EIOÚ je přesvědčen, že zapojení určitého orgánu hraje důležitou roli při určování toho, zda bylo splněno kritérium, neboť je to do určité míry zárukou správného uplatňování právních předpisů. Takový režim může zabránit tomu, aby společnosti nesprávně posuzovaly narušení jako neškodlivé či nezávažné, a tím se vyhnuly oznamování v případech, kdy je takové oznamování ve skutečnosti nezbytné.

47. Na druhé straně se EIOÚ obává, že režim, na jehož základě mají orgány provádět posouzení, může být nepraktický a jeho uskutečnění obtížné, nebo se může ukázat, že je kontraproduktivní. Dokonce tak mohou být oslabena opatření na ochranu údajů pro jednotlivce.

48. Podle tohoto přístupu budou orgány na ochranu údajů pravděpodobně zaplaveny oznámeními narušení bezpečnosti a mohou čelit závažným obtížím při provádění nezbytných posouzení. Je důležité mít na paměti, že orgánům bude třeba poskytnout dostatečné důvěrné informace, často komplexní technické povahy, které budou muset velmi rychle zpracovat za účelem posouzení toho, zda narušení bezpečnosti odpovídá kritériu,. Vzhledem k obtížím s posuzováním a ke skutečnosti, že některé orgány mají omezené zdroje, se EIOÚ obává, že bude pro orgány velmi obtížné splnit tuto povinnost a že by mohla ubírat zdroje určené pro jiné důležité priority. Takový režim může dále vyvíjet na orgány nepřiměřený tlak; pokud rozhodnou, že narušení není závažné, a jednotlivci přesto utrpí škodu, orgány by skutečně mohly být považovány za odpovědné.

49. Výše uvedená obtíž je ještě závažnější, pokud zohledníme, že čas je klíčovým faktorem při minimalizaci nebezpečí vyplývajících z narušení bezpečnosti. Nejsou-li orgány schopny provést posouzení během velmi krátké doby, může dodatečná lhůta, kterou orgány vyžadují pro provedení posouzení, zvýšit škody způsobené dotčeným jednotlivcům. Tento další krok, který má zajistit větší ochranu jednotlivcům, tak může paradoxně vést k tomu, že poskytnutá ochrana bude nižší, než u systémů založených na přímém oznamování.

50. Z výše uvedených důvodů se EIOÚ domnívá, že by bylo vhodnější vytvořit systém, v němž by měly příslušné subjekty posoudit, zda narušení odpovídá kritériu či nikoliv, jak to stanoví přístup Rady.

51. Avšak aby se zabránilo nebezpečí možného zneužití, například pokud jde o subjekty odmítající učinit oznámení za okolností, v nichž se oznámení zcela jasně vyžaduje, je nanejvýš důležité zahrnout jistá bezpečnostní opatření na ochranu údajů uvedená níže.

52. Zaprvé, povinnost určit, zda je třeba učinit oznámení, kterou mají zahrnuté subjekty, musí být samozřejmě doplněna další povinností vyžadující povinně oznamovat orgánům všechna narušení odpovídající požadovanému kritériu. Příslušné subjekty by v takových případech měly mít povinnost informovat orgány o narušení a o důvodech jejich rozhodnutí ohledně oznámení a o obsahu jakéhokoliv učiněného oznámení.

53. Zadruhé, orgánům musí být udělena skutečná dozorčí úloha. Při plnění této úlohy musí být orgánům povoleno, nikoliv však přikázáno, vyšetřit okolnosti narušení a požadovat odpovídající nápravné opatření ([14]). To by mělo zahrnovat nejen oznamování jednotlivcům (pokud se tak ještě nestalo), ale rovněž možnost uložení povinnosti učinit kroky k zabránění dalších narušení. Orgánům by měly být v tomto ohledu uděleny účinné pravomoci a zdroje a musí mít nezbytnou volnost k tomu, aby rozhodly, kdy je třeba reagovat na oznámení narušení bezpečnosti. Jinak řečeno, umožnilo by to orgánům, aby byly selektivní a prováděly vyšetřování například rozsáhlých a skutečně závažných narušení bezpečnosti, přičemž by ověřovaly a prosazovaly plnění požadavků právních předpisů.

54. S cílem dosáhnout výše uvedeného, a vedle pravomocí přiznaných v rámci směrnice o soukromí a elektronických komunikacích, jako je čl. 15a odst. 3 a směrnice o ochraně údajů, doporučuje EIOÚ vložit toto znění: „*Nebylo-li dotčenému účastníkovi nebo jednotlivci již zasláno oznámení, může příslušný vnitrostátní orgán po zvážení povahy narušení požadovat, aby tak učinili poskytovatelé veřejně dostupných služeb elektronických komunikací nebo poskytovatelé služeb informační společnosti*.“

55. EIOÚ dále doporučuje Evropskému parlamentu a Radě, aby potvrdily povinnost navrženou Evropským parlamentem (změna č. 122, čl. 4. odst. 1a), podle níž mají subjekty provádět posuzování rizik a jejich identifikaci ve svých systémech a v osobních údajích, které mají v úmyslu zpracovat. Na základě této povinnosti vypracují subjekty upravenou a přesnou definici bezpečnostních opatření, která budou použita v jejich případě a která by měly být orgánům k dispozici. Dojde-li k narušení bezpečnosti, pomůže tato povinnost zahrnutým subjektům, a případně rovněž orgánům při jejich dozorčí úloze, určit, zda ohrožení takové informace může mít za následek nepříznivý dopad na jednotlivce nebo ho může poškodit.

56. Zatřetí, povinnost zahrnutých subjektů určit, zda musí učinit oznámení jednotlivcům, musí být doplněna povinností vést podrobný a komplexní záznam interního auditu uvádějící všechna narušení, k nimž došlo, a všechna související oznámení, jakož i všechna opatření přijatá s cílem zabránit budoucím narušením. Tento záznam vnitřního auditu musí být orgánům k dispozici za účelem přezkumu a možného prošetření. Umožní to orgánům plnit jejich dozorčí úlohu. Toho by mohlo být dosaženo přijetím níže uvedeného znění: „*Poskytovatelé veřejně dostupných služeb elektronických komunikací a poskytovatelé služeb informační společnosti vedou a uchovávají komplexní záznamy podrobně uvádějící všechna narušení bezpečnosti, k nimž došlo, příslušné související technické informace a přijatá nápravná opatření. Záznamy rovněž obsahují odkaz na všechna oznámení určená dotčeným účastníkům nebo jednotlivcům a příslušným vnitrostátním orgánům, včetně jejich data a obsahu. Záznamy se na požádání poskytnou příslušnému vnitrostátnímu orgánu*.“

57. Aby byla zajištěna soudržnost při zavádění tohoto kritéria, jakož i jiné důležité aspekty rámce týkajícího se narušení bezpečnosti, jako je formát a postupy pro oznamování, bylo by samozřejmě vhodné, aby Komise po konzultaci s EIOÚ, s Pracovní skupinou zřízenou podle článku 29 a s příslušnými zúčastněnými stranami přijala technická prováděcí opatření.

([14]) Článek 15a odst. 3 uznává tuto dohlížecí pravomoc stanovením, že „členské státy zajistí, aby příslušné vnitrostátní orgány a případně další vnitrostátní orgány měly veškerou vyšetřovací pravomoc a zdroje nezbytné ke sledování a vynucování vnitrostátních předpisů přijatých podle této směrnice, včetně možnosti získat všechny příslušné informace, jež k tomu mohou potřebovat.“

Příjemci oznámení

58. Pokud jde o příjemce oznámení, EIOÚ upřednostňuje terminologii Evropského parlamentu a Komise před terminologií Rady. Evropský parlament nahradil slovo „účastníci" slovem „uživatelé". Komise používá pojmy „uživatelé" a „dotčený jednotlivec". Znění Evropského parlamentu i znění Komise by mezi příjemce oznámení nezahrnula pouze stávající účastníky, ale rovněž bývalé účastníky a třetí osoby, jako jsou uživatelé, kteří jsou ve spojení s některými zahrnutými subjekty bez toho, aniž by se stali jejich účastníky. EIOÚ tento přístup vítá a vyzývá Evropský parlament a Radu, aby jej zachovaly.

59. EIOÚ si však uvědomuje mnoho nesrovnalostí, pokud jde o terminologii v prvním čtení EP, jimiž je třeba se zabývat. Například slovo „účastníci" bylo ve většině případů, nikoliv však ve všech, nahrazeno slovem „uživatelé", v jiných případech slovem „spotřebitelé". To je třeba harmonizovat.

III. OBLAST PŮSOBNOSTI SMĚRNICE O SOUKROMÍ A ELEKTRONICKÝCH KOMUNIKACÍCH: VEŘEJNÉ A SOUKROMÉ SÍTĚ

60. V čl. 3 odst. 1 stávající směrnice o soukromí a elektronických komunikacích jsou stanoveny subjekty, jichž se tato směrnice v první řadě týká, tj. ty, které zpracovávají údaje *„ve spojení s"* poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných sítích ([15]). Příklady činností poskytovatelů veřejně dostupných služeb elektronických komunikací zahrnují poskytování přístupu k internetu, přenos informací prostřednictvím elektronických sítí, mobilní a telefonní spojení atd.

61. Evropský parlament předložil změnu č. 121, kterou se mění článek 3 původního návrhu Komise, podle níž byla oblast působnosti směrnice o soukromí a elektronických komunikacích rozšířena tak, aby zahrnula *„zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných a soukromých komunikačních sítích a veřejně dostupných soukromých sítí ve Společenství, […]* " (čl. 3 odst. 1 směrnice o soukromí a elektronických komunikacích). Pro Radu a Komisi bylo bohužel obtížné přijmout tuto změnu, a proto tento přístup nezapracovaly do společného postoje ani do pozměněného návrhu.

Použití směrnice o soukromí a elektronických komunikacích na veřejně přístupné soukromé sítě

62. Z níže uvedených důvodů a s cílem podpořit shodu EIOÚ vybízí k tomu, aby byla zachována podstata změny č. 121. EIOÚ kromě toho navrhuje zahrnout změnu, která pomůže dále objasnit druhy služeb, na něž by se vztahovala rozšířená oblast působnosti.

63. Soukromé sítě se často používají k poskytování služeb elektronických komunikací, jako je přístup k internetu neurčenému množství osob, které může být velké. Jedná se například o přístup na internet v internetových kavárnách a prostřednictvím přístupových bodů Wi-Fi v hotelích, restauracích, na letištích, ve vlacích a v jiných zařízeních přístupných veřejnosti, kde jsou takové služby často poskytovány jako doplněk k jiným službám (nápoje, ubytování apod.)

64. Ve všech výše uvedených příkladech jsou komunikační služby, např. přístup k internetu, poskytovány veřejnosti nikoliv prostřednictvím veřejné sítě, ale spíše prostřednictvím sítě, která může být považována za soukromou, tj. prostřednictvím soukromě provozované sítě. Ačkoliv ve výše uvedených případech jsou komunikační služby poskytovány veřejnosti, druh použité sítě je spíše soukromý než veřejný, poskytování těchto služeb proto *pravděpodobně* není pokryto celou směrnicí o soukromí a elektronických komunikacích nebo alespoň některými z jejích článků ([16]). Základní práva jednotlivců zaručená směrnicí o soukromí a elektronických komunikacích proto nejsou v těchto případech chráněna a pro uživatele, kteří využívají téhož přístupu ke službě připojení na internet prostřednictvím veřejných telekomunikačních prostředků, vzniká ve vztahu k těm, kteří využívají přístup prostřednictvím soukromých telekomunikačních prostředků, nerovný právní stav. To vše i navzdory skutečnosti, že ohrožení soukromí jednotlivců a osobních údajů ve všech těchto případech je stejné jako v případě, že jsou k přenášení služeb použity veřejné sítě. Souhrnně řečeno, zdá se, že není *důvod*, který by podle této směrnice ospravedlňoval různý přístup ke komunikačním službám poskytovaným prostřednictvím soukromé sítě a k těm, které jsou poskytovány prostřednictvím veřejné sítě.

65. Proto by EIOÚ podpořil změnu, jako je změna č. 121 Evropského parlamentu, podle níž by se směrnice o soukromí a elektronických komunikacích rovněž použila na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronické komunikace v *soukromých* komunikačních sítích.

66. EIOÚ však uznává, že toto znění by mohlo mít nepředvídatelné a případně nezamýšlené důsledky. Pouhý odkaz k soukromým sítím by vskutku mohl být vykládán tak, že se vztahuje na situace, na něž se tato směrnice zcela jistě

([15]) „Tato směrnice se vztahuje na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích."

([16]) Naopak by bylo možné namítnout, že vzhledem k tomu, že jsou komunikační služby poskytovány veřejnosti, i když je síť soukromá, vztahuje se na poskytování těchto služeb stávající právní rámec, a to i navzdory skutečnosti, že síť je soukromá. Například ve Francii se zaměstnavatelé poskytující přístup k internetu svým zaměstnancům považují za rovnocenné poskytovatelům přístupu na internet, kteří nabízí přístup k internetu na komerčním základě.- Tento výklad není v široké míře přijímán.

vztahovat nemá. Například by bylo možno tvrdit, že doslovný nebo přesný výklad tohoto znění by mohl do oblasti působnosti směrnice zahrnout domácnosti ([17]) vybavené připojením Wi-Fi, které umožňuje připojení komukoliv v jejich okolí (obvykle v domácnosti); i když to není cílem změny č. 121. Aby se zabránilo takovému výsledku, EIOÚ navrhuje změnu formulace změny č. 121, kterou se do oblasti působnosti směrnice o soukromí a elektronických komunikacích zahrnuje „*zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných nebo veřejně přístupných soukromých komunikačních sítích ve Společenství, …*“

67. To by pomohlo objasnit, že se směrnice o soukromí a elektronických komunikacích vztahuje pouze na soukromé sítě, které jsou veřejně přístupné. Použitím ustanovení směrnice o soukromí a elektronických komunikacích *pouze* na *veřejně přístupné soukromé sítě* (a nikoliv na všechny soukromé sítě) se použití směrnice omezí tak, aby se vztahovala pouze na služby komunikace poskytované v soukromých sítích, které jsou záměrně *zpřístupňovány* veřejnosti. Tato formulace pomůže ještě více zdůraznit, že *dostupnost* soukromé sítě *široké veřejnosti* je klíčovým faktorem při stanovování toho, zda se směrnice bude na daný případ vztahovat (vedle poskytování veřejně dostupných komunikačních služeb). Jinak řečeno, bez ohledu na to, zda je síť veřejná nebo soukromá, je-li síť záměrně zpřístupněná veřejnosti s cílem poskytnout službu veřejné komunikace, jako je přístup k internetu, a to i když se jedná o doplňkovou službu k jiné službě (např. ubytování v hotelu), směrnice o soukromí a elektronických komunikacích by se na tento druh služby či sítě vztahovala.

68. EIOÚ poznamenává, že výše podpořený přístup, podle nějž se směrnice o soukromí a elektronických komunikacích použije na *veřejně přístupné soukromé sítě*, je v souladu s přístupy přijatými v několika členských státech, v nichž orgány již považují takové druhy služeb, jakož i služby poskytované prostřednictvím zcela soukromých sítí, za spadající do oblasti působnosti vnitrostátních ustanovení provádějících směrnici o soukromí a elektronických komunikacích ([18]).

69. S cílem dosáhnout větší právní jistoty ohledně subjektů, na něž se vztahuje nová oblast působnosti, by mohlo být užitečné zahrnout do směrnice o soukromí a elektronických komunikacích změnu definující „veřejně přístupné soukromé sítě“, jež by mohla zní takto: „*veřejně přístupnou soukromou sítí se rozumí soukromě provozovaná síť, k níž má široká veřejnost zpravidla neomezený přístup, za úplatu i zdarma nebo ve spojení s jinými službami nebo nabídkami, pod podmínkou přijetí platných podmínek.*“

([17]) Obvykle bezdrátové místní sítě (LAN).
([18]) Viz poznámka pod čarou 16.

70. V praxi by výše uvedený přístup znamenal, že by se na soukromé sítě v hotelích a jiných zařízeních, které poskytují přístup k internetu široké veřejnosti prostřednictvím soukromé sítě, směrnice vztahovala. Naproti tomu by se nevztahovala na poskytování komunikačních služeb ve zcela soukromých sítích, v nichž je služba omezena na určitou skupinu identifikovatelných jednotlivců. Proto by se například na virtuální soukromé sítě a na domácnosti spotřebitelů vybavené Wi-Fi směrnice nevztahovala. Rovněž by se nevztahovala na služby poskytované prostřednictvím výlučně korporátních sítí.

Soukromé sítě v oblasti působnosti směrnice o soukromí a elektronických komunikacích

71. Vyloučení soukromých sítí samo o sobě, jak je navrženo výše, by mělo být považováno za dočasné opatření, o němž by se mělo dále jednat. S ohledem na jedné straně na důsledky, které má vyloučení zcela soukromých sítí jako takových pro soukromí, a na druhé straně na skutečnost, že to má dopad na velký počet osob, které se obvykle připojují k internetu prostřednictvím korporátních sítí, bude možná v budoucnosti třeba tuto věc ještě jednou zvážit. Z tohoto důvodu a s cílem podpořit diskusi o tomto tématu EIOÚ doporučuje vložit do směrnice o soukromí a elektronických komunikacích bod odůvodnění, podle něhož by Komise provedla veřejnou konzultaci o použití směrnice o soukromí a elektronických komunikacích na všechny soukromé sítě, a to s použitím informací od EIOÚ, orgánů na ochranu osobních údajů a dalších příslušných zúčastněných stran. Tento bod odůvodnění by mohl dále stanovit, že v důsledku veřejné konzultace by Komise měla předložit odpovídající návrh na rozšíření nebo omezení druhů subjektů, na něž by se měla směrnice o soukromí a elektronických komunikacích vztahovat.

72. Kromě výše uvedeného by měly být jednotlivé články směrnice o soukromí a elektronických komunikacích odpovídajícím způsobem změněny tak, aby všechna provozní ustanovení výslovně odkazovala vedle veřejných sítí i k veřejně dostupným soukromým sítím.

IV. ZPRACOVÁNÍ PROVOZNÍCH ÚDAJŮ PRO BEZPEČNOSTNÍ ÚČELY

73. Během legislativního procesu týkajícího se přezkumu směrnice o soukromí a elektronických komunikacích trvaly společnosti poskytující bezpečnostní služby na tom, že je nezbytné vložit do směrnice o soukromí a elektronických komunikacích ustanovení opravňující ke shromažďování provozních údajů s cílem zaručit účinnou bezpečnost on-line.

74. Proto Evropský parlament vložil změnu č. 181, kterou se zavádí nový čl. 6 odst. 6a, jež by výslovně opravňoval ke zpracování provozních údajů pro bezpečnostní účely: „*Aniž je dotčeno dodržování jiných ustanovení, než je článek 7 směrnice 95/46/ES a článek 5 této směrnice, provozní údaje mohou být zpracovávány v oprávněném zájmu správce údajů za účelem provádění technických opatření, která mají zajistit bezpečnost sítí a informací veřejných služeb elektronických komunikací, veřejné či soukromé sítě elektronických komunikací, služeb informační společnosti či souvisejícího koncového zařízení nebo zařízení elektronické komunikace, jak je stanoveno v čl. 4 písm. c) nařízení Evropského parlamentu a Rady (ES) č. 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací, s výjimkou případů, kdy nad těmito zájmy převáží zájmy týkající se základních práv a svobod subjektu údajů. Toto zpracování se musí omezit pouze na skutečnosti, které jsou pro účely těchto bezpečnostních činností zcela nezbytné*“.

75. Pozměněný návrh Komise tuto změnu v zásadě přijal, avšak byla odstraněna klíčová klauzule, kterou mělo být zajištěno dodržování ostatních ustanovení uvedené směrnice, znějící takto: „*Aniž je dotčena […]… této směrnice*“). Rada přijala přepracovanou verzi, které ještě více oslabuje důležitou ochranu a vyvážení zájmů, které byly zapracovány do změny č. 181, a to přijetím tohoto znění: „*Provozní údaje lze zpracovávat v míře nezbytně nutné k zajištění […] bezpečnosti sítě a informací podle definice čl. 4 písm. c) nařízení Evropského parlamentu a Rady (ES) 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací.*“

76. Jak je dále objasněno níže, čl. 6 odst. 6a není nutný a může být zneužit, zejména pokud bude přijat v podobě, která neobsahuje důležitá bezpečnostní opatření, klauzule respektující jiná ustanovení uvedené směrnice a vyvážení zájmů. Proto EIOÚ doporučuje tento článek odmítnout, nebo alespoň zajistit, aby jakýkoliv takový článek týkající se této otázky obsahoval druhy bezpečnostních opatření, které byly zahrnuty do změny č. 181 ve znění přijatém EP.

Právní důvody pro zpracování provozních údajů použitelné na služby elektronických komunikací a na jiné správce údajů podle stávajících právních předpisů o ochraně údajů

77. Rozsah, v němž poskytovatelé veřejně dostupných služeb elektronických komunikací mohou zákonně zpracovat provozní údaje, je upraven podle článku 6 směrnice o soukromí a elektronických komunikacích, který omezuje zpracování provozních údajů na omezené účely, jako je účtování, propojení a marketing. Toto zpracování může být provedeno pouze za zvláštních podmínek, jako je souhlas jednotlivců v případě marketingu. Kromě toho mohou jiní správci údajů, jako jsou poskytovatelé služeb informační společnosti, zpracovávat provozní údaje podle článku 7 směrnice o ochraně údajů, který stanoví, že správci údajů mohou zpracovávat osobní údaje, pokud je splněn alespoň jeden z právních základů uvedených na seznamu, přičemž na tyto právní základy se rovněž odkazuje jako na právní důvody.

78. Příkladem jednoho takového právního základu je čl. 7 písm. a) směrnice na ochranu údajů, který vyžaduje souhlas subjektu údajů. Například pokud si intranetový maloobchodní prodejce přeje zpracovat provozní údaje pro účely zaslání reklamních či marketingových materiálů, musí obdržet souhlas jednotlivce. Jiný právní základ stanovený v článku 7 může v některých případech umožnit zpracování provozních údajů pro bezpečnostní účely například bezpečnostními společnostmi nabízejícími bezpečnostní služby. To je založeno na čl. 7 písm. f), který stanoví, že správci údajů mohou zpracovat osobní údaje, pokud je to „*nezbytné pro uskutečnění oprávněných zájmů správce nebo třetí osoby či osob, kterým jsou údaje sdělovány, za podmínky, že nepřevyšují zájem na základních právech a svobodách subjektu údajů*“. Směrnice na ochranu údajů blíže nestanoví případy, v nichž by zpracování osobních údajů splňovalo tento požadavek. Toto určení provádějí správci údajů pro každý případ zvlášť, často se souhlasem vnitrostátních orgánů na ochranu údajů a jiných orgánů.

79. Je třeba zvážit souvislost mezi článkem 7 směrnice o ochraně údajů a navrhovaným čl. 6 odst. 6a směrnice o soukromí a elektronických komunikacích. Navrhovaný článek 6 odst. 6a stanoví okolnosti, za nichž by byly splněny požadavky čl. 7 písm. f) uvedené výše. Tím, že povoluje zpracování provozních údajů s cílem pomoci zajistit bezpečnost sítí a informací, čl. 6 odst. 6a samozřejmě umožňuje takové zpracování pro účely oprávněného zájmu sledovaného správcem údajů.

80. Jak je podrobněji objasněno níže, EIOÚ se domnívá, že navrhovaný čl. 6 odst. 6a není nezbytný ani užitečný. Z právního hlediska je totiž v zásadě zbytečné stanovit, zda konkrétní druh činnosti související se zpracováním údajů, v tomto případě zpracování provozních údajů pro bezpečnostní účely, splňuje nebo nesplňuje požadavky čl. 7 písm. f) směrnice o ochraně údajů, a v takovém případě může být souhlas jednotlivce nezbytný podle čl. 7 písm. a). Jak je uvedeno výše, toto posouzení obvykle provedou správci údajů, tj. společnosti, a to na úrovni provádění a za konzultace s orgány na ochranu údajů; v případě potřeby toto posouzení provádějí soudy. Obecně řečeno, EIOÚ se domnívá, že ve zvláštních případech oprávněné zpracování údajů pro bezpečnostní účely

prováděné bez ohrožení základních práv a svobod jednotlivců pravděpodobně splní požadavky čl. 7 písm. f) směrnice o ochraně údajů, a proto je možno je provádět. Navíc v oblasti ochrany údajů a směrnice o soukromí a elektronických komunikacích není jiný precedent pro specifikování nebo poskytnutí zvláštního přístupu k některým druhům činností zpracování údajů, které by splnily požadavky čl. 7 písm. f), a nebylo prokázáno, že je takové výjimky zapotřebí. Naopak, jak je uvedeno výše, se zdá, že v mnoha případech by tento druh činnosti bylo možno bez obtíží zařadit do rámce stávajícího znění. Proto je právní ustanovení, které potvrzuje toto posouzení, v zásadě zbytečné.

Znění čl. 6 odst. 6a podle Evropského parlamentu, Rady a Komise

81. Jak je uvedeno výše, ačkoliv je to zbytečné, je třeba zdůraznit, že změna č. 181 ve znění přijatém Evropským parlamentem byla navržena v určité míře s ohledem na zásady pro ochranu soukromí a údajů zakotvené v právních předpisech o ochraně údajů. Změna Evropského parlamentu č. 181 by se mohla více zabývat zájmem na ochraně údajů a soukromí, například vložením slov „ve zvláštních případech" s cílem zajistit selektivní uplatňování tohoto článku nebo začleněním období zachovávajícího stávající stav.

82. Změna 181 obsahuje některé pozitivní prvky. Potvrzuje, že zpracování by mělo být ve shodě se všemi ostatními zásadami pro ochranu údajů, které se vztahují na zpracování osobních údajů („*Aniž je dotčeno…dodržování ustanovení […] směrnice 95/46/ES a […] této směrnice*"). Dále ačkoliv změna č. 181 dovoluje zpracování provozních údajů z bezpečnostních důvodů, usiluje o rovnováhu mezi zájmy subjektu, který zpracovává provozní údaje, a zájmy jednotlivců, jejichž údaje jsou zpracovány tak, že takové zpracování údajů může být provedeno pouze tehdy, pokud nad zájmy ohledně základních práv a svobod jednotlivců nepřeváží zájmy subjektu zpracovávajícího údaje („*s výjimkou případů, kdy nad těmito zájmy převáží zájmy týkající se základních práv a svobod subjektu údajů*"). Tento požadavek je důležitý, protože může umožnit zpracování provozních údajů pro zvláštní účely, avšak neumožní subjektu zpracovávajícímu údaje zpracovat provozní údaje hromadně.

83. Přepracované znění této změny předložené Radou obsahuje vítané prvky, jako je zachování slov „*zcela nezbytné*", což zdůrazňuje omezenou oblast působnosti tohoto článku. Nicméně ze znění Rady byla vypuštěna ochrana údajů a ochrana soukromí uvedené výše. Zatímco se v zásadě použijí obecná ustanovení na ochranu údajů, bez ohledu na to, zda je v každém případě učiněn zvláštní odkaz, znění čl. 6 odst. 6a navržené Radou může být interpretováno tak, že poskytuje pravomoc ke zpracování provozních údajů podle uvážení, aniž by se na ně vztahovala jakákoliv ochrana údajů a ochrana soukromí, jež se vztahuje na každé zpracování provozních údajů. Proto by bylo možno argumentovat, že provozní údaje je možno shromažďovat, uchovávat a dále využívat, aniž by musely být splněny zásady pro ochranu údajů a zvláštní povinnosti, které se jinak použijí na odpovědné strany, jako je zásada kvality nebo povinnost spravedlivého a zákonného zpracování a zachování důvěrnosti a bezpečnosti údajů. Vzhledem k tomu, že není učiněn žádný odkaz na použitelné zásady pro ochranu údajů, které stanoví časové lhůty pro uchovávání informací nebo zvláštní časové lhůty v rámci tohoto článku, znění Rady je možno vykládat tak, že umožňuje shromažďování a zpracování provozních údajů pro bezpečnostní účely na nestanovené časové období.

84. Rada navíc v některých částech znění zmírnila ochranu soukromí možným rozšířením formulace. Například byl odstraněn odkaz na „*oprávněný zájem správce údajů*", čímž vznikly pochybnosti ohledně druhů subjektů, které by mohly využít této výjimky. Je nanejvýš důležité zabránit uživatelům nebo právním subjektům, aby této změny využili.

85. Nedávné zkušenosti v Evropském parlamentu a Radě ukazují, že je obtížné zákonem stanovit rozsah a podmínky, za nichž může být zpracování údajů pro bezpečnostní účely zákonně provedeno. Je nepravděpodobné, že by kterýkoliv stávající nebo budoucí článek odstranil zjevné riziko příliš širokého použití výjimky z jiných důvodů než z výlučně bezpečnostních nebo použití ze strany subjektů, které by neměly mít možnost využít této výjimky. To neznamená, že k takovému zpracování nemůže nikdy dojít. Avšak to, zda a do jaké míry může být prováděno, lze lépe posoudit na úrovni provádění. Subjekty, které si přejí účastnit se takového zpracování, by měly projednat rozsah a podmínky s orgány na ochranu údajů a případně s Pracovní skupinou článku 29. Nebo by směrnice o soukromí a elektronických komunikacích mohla zahrnovat článek umožňující zpracování provozních údajů pro bezpečnostní účely, po výslovném schválení ze strany orgánů na ochranu údajů.

86. Při současném zohlednění nebezpečí, které čl. 6 odst. 6a představuje pro základní právo na ochranu údajů a soukromí jednotlivců, a skutečnosti, že z právního hlediska je tento článek zbytečný, jak je uvedeno ve stanovisku, EIOÚ dospěl k závěru, že nejlepší řešení by bylo, kdyby byl čl. 6 odst. 6a celý vypuštěn.

87. Mělo-li by být vedle znění stávajícího čl. 6 odst. 6a přijato nějaké znění odporující doporučení EIOÚ, mělo by v každém případě obsahovat výše projednané opatření na ochranu údajů. Rovněž by mělo být řádně začleněno do stávající struktury článku 6, nejlépe jako nový odstavec 2a.

V. **MOŽNOST PRÁVNÍCH OSOB PODAT ŽALOBU NA PORUŠENÍ SMĚRNICE O SOUKROMÍ A ELEKTRONICKÝCH KOMUNIKACÍCH**

88. Evropský parlament předložil změnu č. 133 umožňující poskytovatelům přístupu k internetu a jiným právním subjektům, jako jsou sdružení spotřebitelů, podat žalobu na porušení některého z ustanovení směrnice o soukromí a elektronických komunikacích ([19]). Bohužel ji Komise ani Rada nepřijaly. EIOÚ považuje tuto změnu za velmi pozitivní a doporučuje její zachování.

89. Pro pochopení důležitosti této změny je třeba si uvědomit, že v oblasti ochrany soukromí a údajů škoda způsobená jednotlivé osobě obvykle sama o sobě nedostačuje k podání žaloby k soudu. Jednotlivci se obvykle samostatně neobracejí na soud kvůli spamům nebo kvůli tomu, že jejich jméno bylo neoprávněně zaneseno do seznamu. Tato změna by umožnila sdružením spotřebitelů a odborům zastupujícím zájmy spotřebitelů podat jejich jménem hromadnou žalobu k soudu. Větší rozmanitost donucovacích mechanismů pravděpodobně rovněž podpoří větší shodu, a je proto v zájmu účinného použití ustanovení směrnice o soukromí a elektronických komunikacích.

90. V právních rámcích některých členských států jsou právní precedenty, které již předpokládají možnost kolektivního odškodnění s cílem umožnit spotřebitelům nebo zájmovým skupinám požadovat náhradu škody od strany, která škodu způsobila.

91. Soutěžní právo některých členských států ([20]) navíc opravňuje spotřebitele, zájmové skupiny (vedle *poškozeného konkurenta*) podat žalobu proti subjektu, který se dopouští porušování. *Důvodem* tohoto přístupu je, že ze situace pravděpodobně těží společnosti jednající v rozporu se soutěžním právem, protože spotřebitelé, kteří utrpěli pouze nepatrnou škodu, obvykle žalobu nepodávají. Tento důvod je možno obdobně použít v oblasti ochrany údajů a soukromí.

92. Důležitější je, jak je uvedeno výše, že právo právních subjektů, jako jsou sdružení spotřebitelů a poskytovatelé veřejně dostupných služeb elektronických komunikací, podávat žaloby posiluje postavení spotřebitelů a podporuje celkovou shodu s právními předpisy na ochranu údajů. Jsou-li společnosti, které se dopouštějí porušování, vystaveny většímu riziku soudního řízení, pravděpodobně budou více investovat do zajištění souladu s právními předpisy v oblasti ochrany údajů, což z dlouhodobého hlediska zlepší úroveň ochrany soukromí a spotřebitele. Ze všech těchto důvodů EIOÚ vyzývá Evropský parlament a Radu k přijetí ustanovení, které právním subjektům umožní podat žalobu na porušení kteréhokoliv ustanovení směrnice o soukromí a elektronických komunikacích.

VI. **ZÁVĚR**

93. Společný postoj Rady, první čtení v Evropském parlamentu a pozměněný návrh Komise obsahují v různé míře pozitivní prvky, které slouží k posílení ochrany soukromí a osobních údajů jednotlivce.

94. Avšak EIOÚ se domnívá, že existuje prostor pro zlepšení, zejména pokud jde o společný postoj Rady, který bohužel nezachoval některé změny Evropského parlamentu, které mají za cíl pomoci zajistit odpovídající ochranu soukromí a osobních údajů jednotlivce. EIOÚ naléhavě vyzývá Evropský parlament a Radu k opětovnému začlenění opatření na ochranu soukromí obsažených v prvním čtení Evropského parlamentu.

95. EIOÚ se dále domnívá, že by bylo vhodné zjednodušit některá ustanovení této směrnice. To zejména platí v případě ustanovení týkajících se narušení bezpečnosti, protože EIOÚ se domnívá, že oznamování narušení bude mít největší přínos, bude-li právní rámec stanoven od samého počátku. EIOÚ se v neposlední řadě domnívá, že by bylo vhodné zlepšit a objasnit znění některých ustanovení této směrnice.

96. S ohledem na výše uvedené EIOÚ naléhavě vyzývá Evropský parlament a Radu, aby zvýšily úsilí ke zlepšení a objasnění některých ustanovení směrnice o soukromí a elektronických komunikacích a současně aby znovu začlenily změny přijaté v prvním čtení Evropského parlamentu zaměřené na poskytování ochrany soukromí a údajů na odpovídající úrovni. Za tímto účelem jsou v níže uvedených bodech 97, 98, 99 a 100 shrnuta příslušná témata a předloženy některá z doporučení a návrhů. EIOÚ vyzývá všechny zúčastněné strany, aby je zohlednily, protože projednávání směrnice o soukromí a elektronických komunikacích směřuje ke konečnému přijetí.

Narušení bezpečnosti

97. Evropský parlament, Komise i Rada přijaly různé přístupy k oznamování narušení bezpečnosti. Mezi těmito třemi modely jsou rozdíly mimo jiné pokud jde o subjekty, na něž se vztahuje povinnost, kritérium nebo podnět pro oznámení, subjekty údajů oprávněné k tomu, aby jim bylo podáno oznámení, atd. Je třeba, aby Evropský parlament a Rada učinily vše pro vypracování pevného právního rámce pro případy narušení bezpečnosti. Za tímto účelem by Evropský parlament a Rada měly:

([19]) Článek 13 odst. 6 prvního čtení Evropského parlamentu.
([20]) Viz například § 8 německého zákona o nekalé soutěži (UWG).

— *zachovat* definici narušení bezpečnosti ve zněních Evropského parlamentu, Rady a Komise, protože je dostatečně široká k tomu, aby zahrnula většinu situací, v nichž by mělo být oznámení narušení bezpečnosti zaručeno;

— *zahrnout* poskytovatele služeb informační společnosti, s ohledem na oblast působnosti subjektů, na něž se vztahuje navržený požadavek na oznamování. Pravděpodobnost, že u internetových maloobchodníků, internetových bank a on-line lékáren dojde k narušení bezpečnosti, je stejná, ne-li vyšší, jako v případě telekomunikačních společností. Občané budou očekávat, že jim bude podáno oznámení nejen v případě, že se poskytovatelé přístupu k internetu stanou předmětem narušení bezpečnosti, ale zejména tehdy, stane-li se to jejich internetovým bankám a on-line lékárnám.

— Pokud jde o podnět k oznámení, kritérium „*přiměřená pravděpodobnost poškození*“ uvedené v pozměněném návrhu je vhodným kritériem, které zajistí funkčnost režimu. Nicméně je důležité zajistit, aby pojem „poškození“ byl dostatečně široký k pokrytí všech příslušných případů negativních dopadů na soukromí nebo jiné oprávněné zájmy jednotlivců. V opačném případě by bylo vhodnější stanovit nové kritérium, na jehož základě by oznamování bylo povinné „*pokud by narušení s přiměřenou pravděpodobností mohlo poškodit jednotlivce*“. Přístup Rady, který vyžaduje, aby narušení *závažně* narušilo něčí soukromí, by poskytl jednotlivcům nedostatečnou ochranu, protože takové kritérium vyžaduje, aby byl dopad na soukromí „závažný“. Navíc vzniká prostor pro subjektivní posouzení.

— I když má účast orgánu na stanovení, zda musí dotčený subjekt podat oznámení jednotlivcům, zcela jistě pozitivní účinky, v praxi může být obtížné účast orgánu zajistit a rovněž by to mohlo odebírat zdroje z jiných důležitých priorit. Nemohou-li orgány reagovat velmi rychle, EIOÚ se obává, že takový systém může dokonce oslabit ochranu jednotlivců a vyvinout nepřiměřený tlak na orgány. EIOÚ proto doporučuje *vytvořit* systém, v němž je na dotčených subjektech, aby posoudily, zda musí provést oznámení.

— *Provést* níže uvedená ochranná opatření s cílem umožnit orgánům výkon dozoru nad posouzením učiněným zahrnutými subjekty ohledně toho, zda učinit oznámení:

  — *zajistit*, aby takové subjekty byly povinny podat oznámení orgánům o všech narušeních, které odpovídají požadovanému kritériu;

  — *pověřit* orgány dozorčí úlohou, která jim umožní postupovat selektivně, a být tak efektivní. Za účelem dosažení výše uvedeného je třeba vložit toto znění: „*Nebylo-li dotčenému účastníkovi nebo jednotlivci již učiněno oznámení, může příslušný vnitrostátní orgán, po zvážení povahy narušení, požadovat po poskytovatelích veřejně dostupných služeb elektronických komunikací nebo poskytovatelích služeb informační společnosti, aby tak učinili.*“

  — *přijmout* nové ustanovení požadující po subjektech, aby vedly podrobné a komplexní záznamy vnitřního auditu. Toho by mohlo být dosaženo přijetím tohoto znění: „*Poskytovatelé veřejně dostupných služeb elektronických komunikací a poskytovatelé služeb informační společnosti vedou a uchovávají komplexní záznamy podrobně uvádějící všechna narušení bezpečnosti, k nimž došlo, příslušné technické informace s nimi související a přijatá nápravná opatření. Záznamy rovněž obsahují odkaz ke všem oznámením vydaným dotčeným účastníkům nebo jednotlivcům a příslušným vnitrostátním orgánům, včetně jejich data a obsahu. Záznamy budou na požádání poskytnuty příslušnému vnitrostátnímu orgánu.*“

— *Umožnit* Komisi přijmout technická prováděcí opatření, a to po předchozí konzultaci s EIOÚ, Pracovní skupinou zřízenou podle článku 29 a dalšími příslušnými zúčastněnými stranami, aby se zajistila soudržnost při provádění rámce týkajícího se narušení bezpečnosti.

— Pokud jde o jednotlivce, kterým má být podáno oznámení, *použít* terminologii Komise nebo Evropského parlamentu „dotčení jednotlivci“ nebo „poškození uživatelé“, protože zahrnuje všechny jednotlivce, jejichž osobní údaje byly ohroženy.

Veřejně dostupné soukromé sítě

98. Služby komunikace jsou často zpřístupňovány veřejnosti nikoliv prostřednictvím veřejných sítí, ale prostřednictvím soukromě provozovaných sítí (*např.* přístupové body Wi-Fi v hotelích a na letištích), na něž se směrnice patrně nevztahuje. Evropský parlament přijal změnu č. 121 (článek 3) rozšiřující oblast působnosti této směrnice tak, aby byly zahrnuty veřejné a soukromé komunikační sítě, jakož i veřejně přístupné soukromé sítě. V tomto ohledu by Evropský parlament a Rada měly:

— *zachovat* podstatu změny č. 121, ale *přeformulovat znění* tak, aby do oblasti působnosti směrnice o soukromí a elektronických komunikacích spadalo pouze „*zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných nebo veřejně přístupných komunikačních sítích ve Společenství*“. Výslovně zahrnuty by nebyly pouze soukromě provozované sítě (na rozdíl od veřejně přístupných soukromých sítí);

— *změnit* odpovídajícím způsobem všechna operativní ustanovení tak, aby se společně s veřejnými sítěmi výslovně odkazovalo k veřejně přístupným soukromým sítím;

— *zahrnout* změnu definující „*veřejně přístupnou soukromou síť, kterou se rozumí soukromě provozovaná síť, k níž má široká veřejnost zpravidla neomezený přístup, za úplatu i zdarma nebo ve spojení s jinými službami nebo nabídkami, pod podmínkou přijetí platných podmínek*“. Tím se zajistí větší právní jistota, pokud jde o subjekty, na něž se vztahuje nová oblast působnosti;

— *přijmout* nový bod odůvodnění, jehož prostřednictvím by Komise prováděla veřejnou konzultaci o použití směrnice o soukromí a elektronických komunikacích na všechny soukromé sítě, a to s použitím informací od EIOÚ, Pracovní skupiny zřízené podle článku 29 a jiných zúčastněných stran. Dále je třeba upřesnit, že v návaznosti na veřejné konzultace by Komise měla předložit odpovídající návrh na rozšíření nebo omezení druhů subjektů, na něž by se měla směrnice o soukromí a elektronických komunikacích vztahovat.

Zpracování provozních údajů pro bezpečnostní účely

99. V prvním čtení Evropského parlamentu byla přijata změna č. 181 (čl. 6 odst. 6a opravňující ke zpracování provozních údajů pro bezpečnostní účely. Ve společném postoji Rady bylo přijato nové znění oslabující některá opatření na ochranu soukromí. V tomto ohledu EIOÚ doporučuje Evropskému parlamentu a Radě:

— *zamítnout* tento článek jako celek, protože je zbytečný, a pokud by byl zneužit, mohl by příliš ohrozit ochranu údajů a soukromí jednotlivců;

— nebo, v případě, že bude přijata nějaká změna stávajícího znění čl. 6 odst. 6a, *začlenit* opatření na ochranu údajů projednávaná v tomto stanovisku (podobná těm, která jsou uvedena ve změně Evropského parlamentu).

Podání žaloby na porušení směrnice o soukromí a elektronických komunikacích

100. Parlament přijal změnu č. 133 (čl. 13 odst. 6) umožňující právním subjektům podat žalobu na porušení kteréhokoliv ustanovení uvedené směrnice. Rada tuto změnu bohužel nezachovala. Rada a Evropský parlament by měly:

— *potvrdit* ustanovení umožňující právním subjektům, jako jsou sdružení spotřebitelů a odborová sdružení, využít práva na podání žaloby na porušení kteréhokoliv ustanovení této směrnice (nejen na porušení ustanovení o spamech, jak stanoví stávající přístup obsažený ve společném postoji a v pozměněném návrhu). Větší různorodost donucovacích mechanismů podpoří vyšší úroveň shody a účinné používání směrnice o soukromí a elektronických komunikacích jako celku.

Plnění úkolů

101. Ve všech výše uvedených záležitostech musí Evropský parlament a Rada vypracovat řádná pravidla a ustanovení, která jsou proveditelná i funkční a zároveň dodržují právo na soukromí a ochranu údajů jednotlivců. EIOÚ věří, že zúčastněné strany učiní maximum, aby tento úkol splnily, a doufá, že toto stanovisko k jejich úsilí přispěje.

V Bruselu dne 9. ledna 2009.

Peter HUSTINX

Evropský inspektor na ochranu údajů