Druhé stanovisko Európskeho dozorného úradníka pre ochranu údajov k preskúmaniu smernice 2002/58/ES týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách)

(2009/C 128/04)

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV,

so zreteľom na Zmluvu o založení Európskeho spoločenstva, a najmä na jej článok 286,

so zreteľom na Chartu základných práv Európskej únie, a najmä na jej článok 8,

so zreteľom na smernicu Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov,

so zreteľom na smernicu Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúcu sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií,

so zreteľom na nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov, a najmä na jeho článok 41,

PRIJAL TOTO STANOVISKO:

I. ÚVOD

Kontext

1. Európska komisia prijala 13. novembra 2007 návrh, ktorým sa okrem iného mení smernica o súkromí a elektronických komunikáciách, zvyčajne nazývaná smernica o elektronickom súkromí ([1]) (ďalej len „návrh" alebo „návrh Komisie"). EDPS prijal 10. apríla 2008 stanovisko k návrhu Komisie, v ktorom odporúčal zlepšenia návrhu s cieľom pomôcť zabezpečiť, aby navrhované zmeny vyústili do čo najlepšej ochrany súkromia a osobných údajov jednotlivcov (ďalej len „prvé stanovisko EDPS") ([2]).

2. EDPS privítal návrh Komisie, aby sa vytvoril systém povinného oznamovania narušenia bezpečnosti, ktorý by od spoločností vyžadoval, aby oznamovali jednotlivcom prípady, keď boli ich osobné údaje ohrozené. Okrem toho ocenil nové ustanovenie, ktoré umožňuje právnickým osobám (napr. spotrebiteľským združeniam a poskytovateľom internetového pripojenia) podať návrh na začatie súdneho konania, čím sa dopĺňajú existujúce nástroje na boj proti spamu.

3. Počas parlamentnej rozpravy, ktorá predchádzala prvému čítaniu v Parlamente, vydal EDPS ďalšie rady v podobe pripomienok k vybraným otázkam, ktoré vyvstali v správach vypracovaných výbormi Európskeho parlamentu zodpovednými za preskúmanie smernice o univerzálnej službe ([3]) a smernice o elektronickom súkromí (ďalej len „pripomienky") ([4]). Pripomienky sa týkali najmä otázok súvisiacich so spracúvaním prevádzkových dát a ochranou práv duševného vlastníctva.

4. Európsky parlament (ďalej len „EP") prijal 24. septembra 2008 legislatívne uznesenie k smernici o elektronickom súkromí (Ďalej len „prvé čítanie") ([5]). EDPS zaujal kladné stanovisko k viacerým pozmeňujúcim a doplňujúcim návrhom, ktoré boli prijaté na základe uvedeného stanoviska EDPS a pripomienok. Medzi významné zmeny patrilo začlenenie poskytovateľov služieb informačnej spoločnosti (t. j. spoločnosti s prevádzkou na internete) do rozsahu pôsobnosti povinnosti upozorňovať na narušenia bezpečnosti. EDPS privítal aj pozmeňujúci

([1]) Preskúmavanie smernice o elektronickom súkromí je súčasťou širšieho procesu preskúmavania, ktorý bol zameraný na vytvorenie telekomunikačného orgánu EÚ, preskúmanie smerníc 2002/21/ES, 2002/19/ES, 2002/20/ES, 2002/22/ES a 2002/58/ES, ako aj na preskúmanie nariadenia (ES) č. 2006/2004 (ďalej spolu len „preskúmanie telekomunikačného balíka").

([2]) Stanovisko z 10. apríla 2008 návrhu smernice Európskeho parlamentu a Rady, ktorou sa okrem iných právnych predpisov mení a dopĺňa smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), Ú. v. EÚ C, 181, 18.7.2008, s. 1.

([3]) Smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb (smernica univerzálnej služby), Ú. v. ES L 108, 24.4.2002, s. 51.

([4]) Pripomienky EDPS k vybraným otázkam, ktoré vyplynuli zo správy Výboru pre vnútorný trh a ochranu spotrebiteľa o preskúmaní smernice 2002/22/ES (univerzálna smernica) a smernice 2002/58/ES (elektronické súkromie), 2. september 2008. Dostupné na webovej stránke: www.edps.europa.eu

([5]) Legislatívne uznesenie Európskeho parlamentu z 24. septembra 2008 o návrhu smernice Európskeho parlamentu a Rady, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí, smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci v oblasti ochrany spotrebiteľa (COM(2007) 698 – C6-0420/2007 – 2007/248(COD).

a doplňujúci návrh, ktorý umožňuje právnickým a fyzickým osobám podávať návrhy na začatie konania vo veci porušenia ktoréhokoľvek z ustanovení smernice o elektronickom súkromí (nielen vo veci porušenia ustanovení o spame, ako sa povodne uvádzalo v návrhu Komisie). Po prvom čítaní v Parlamente Komisia prijala zmenený a doplnený návrh smernice o elektronickom súkromí (ďalej len „zmenený a doplnený návrh“) ([6]).

5. Rada 27. novembra 2008 dosiahla politickú dohodu o preskúmaní právnych predpisov tvoriacich telekomunikačný balík vrátane smernice o elektronickom súkromí, ktorá sa zmení na spoločnú pozíciu Rady (ďalej len „spoločná pozícia“) ([7]). Spoločná pozícia Rady, ktorá môže obsahovať pozmeňujúce a doplňujúce návrhy EP, sa mu oznámi podľa článku 251 ods. 2 Zmluvy o založení Európskeho spoločenstva.

Celkové stanovisko k pozícii Rady

6. Rada pozmenila podstatné prvky znenia návrhu a neakceptovala veľa pozmeňujúcich a doplňujúcich návrhov EP. Napriek tomu, že spoločná pozícia jednoznačne obsahuje pozitívne prvky, EDPS má obavy o jej celkový obsah, najmä preto, že sa do nej nezapracovali niektoré pozitívne pozmeňujúce a doplňujúce návrhy EP, návrhy uvedené v zmenenom a doplnenom návrhu, alebo v stanoviskách EDPS a návrhy európskych orgánov na ochranu údajov vydané prostredníctvom pracovnej skupiny článku 29 ([8]).

7. Práve naopak, v niekoľkých prípadoch sa ustanovenia zmeneného a doplneného návrhu a pozmeňujúce a doplňujúce návrhy EP, ktoré občanom ponúkajú záruky ochrany, vypúšťajú alebo zreteľne oslabujú. V dôsledku toho sa úroveň ochrany poskytovaná jednotlivcom v spoločnej pozícii podstatne znížila. EDPS preto vydáva druhé stanovisko, dúfajúc, že počas legislatívneho procesu súvisiaceho so smernicou o elektronickom súkromí sa prijmú nové pozmeňujúce a doplňujúce návrhy, ktorými sa záruky ochrany údajov obnovia.

8. Toto druhé stanovisko sa sústreďuje na niekoľko zásadných otázok a neopakuje všetky argumenty uvedené v prvom stanovisku EDPS, ktoré ostávajú naďalej platné. V tomto stanovisku sa hovorí najmä o týchto otázkach:

— ustanovenia o oznamovaní narušenia bezpečnosti,

— rozsah pôsobnosti smernice o elektronickom súkromí na súkromné a verejne dostupné súkromné siete,

— spracúvanie prevádzkových dát na bezpečnostné účely,

— možnosť právnických osôb podávať návrhy na začatie konania vo veci porušenia smernice o elektronickom súkromí.

9. V stanovisku sa pri riešení uvedených otázok analyzuje spoločná pozícia Rady a porovnáva sa s prvým čítaním Parlamentu a zmeneným a doplneným návrhom Komisie. Stanovisko obsahuje odporúčania zamerané na racionalizáciu ustanovení smernice o elektronickom súkromí a zabezpečenie toho, aby smernica naďalej primeraným spôsobom chránila súkromie a osobné údaje jednotlivcov.

II. USTANOVENIA O OZNAMOVANÍ NARUŠENIA BEZPEČNOSTI

10. EDPS podporuje prijatie mechanizmu oznamovania narušenia bezpečnosti, v rámci ktorého sa orgánom a jednotlivcom bude oznamovať, ak príde k ohrozeniu ich údajov ([9]). Oznámenia o narušení bezpečnosti môžu pomôcť jednotlivcom pri prijímaní krokov potrebných na zmiernenie možných škôd spôsobených ohrozením. Povinnosť posielať oznámenia o narušeniach bezpečnosti bude navyše nabádať spoločnosti k tomu, aby zvyšovali bezpečnosť údajov a svoju zodpovednosť za osobné údaje, ktoré im boli zverené.

11. Zmenený a doplnený návrh Komisie, prvé čítanie Parlamentu a spoločná pozícia Rady predstavujú tri rôzne prístupy k zvažovanému oznamovaniu narušenia bezpečnosti. Každý z nich má kladné stránky. EDPS sa však domnieva, že každý z nich možno vylepšiť a navrhuje, aby sa pred zvážením záverečných krokov smerujúcich k prijatiu mechanizmu oznamovania narušenia bezpečnosti zobrali do úvahy odporúčania uvedené nižšie.

([6]) Zmenený a doplnený návrh smernica európskeho Parlamentu a Rady, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí, smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci v oblasti ochrany spotrebiteľa, Brusel, 6.11.2008, KOM(2008) 723 v konečnom znení.

([7]) K dispozícii na webovej stránke Rady.

([8]) Stanovisko 2/2008 o preskúmaní smernice 2002/58/ES o súkromí a elektronických komunikáciách (smernica o elektronickom súkromí), k dispozícii na webovej stránke pracovnej skupiny článku 29.

([9]) V stanovisku sa výrazom „ohroziť“ odkazuje na akékoľvek porušenie ochrany osobných údajov, ktoré nastalo v dôsledku ich náhodného alebo nezákonného zničenia, straty, pozmenenia, nepovoleného zverejnenia alebo ich sprístupnenia pri prenose, uchovávaní alebo spracúvaní iným spôsobom.

12. Pri analýze týchto troch mechanizmov oznamovania narušenia bezpečnosti je potrebné zvážiť päť kritických bodov: *i*) vymedzenie narušenia bezpečnosti; *ii*) subjekty, na ktoré sa vzťahuje oznamovacia povinnosť (ďalej len „povinné subjekty"); *iii*) norma, na základe ktorej vzniká oznamovacia povinnosť; *iv*) určenie subjektu zodpovedného za stanovenie skutočnosti, či narušenie bezpečnosti porušením normy alebo nie a *v*) príjemcovia oznámenia.

Prehľad prístupu Komisie, Rady a EP

13. Európsky parlament, Komisia a Rada zvolil v súvislosti s oznamovaním narušenia bezpečnosti odlišné prístupy. V prvom čítaní EP sa pôvodný mechanizmus oznamovania narušenia bezpečnosti ustanovený v návrhu Komisie pozmenil ([10]). V rámci prístupu EP sa oznamovacia povinnosť vzťahuje nielen na poskytovateľov verejne prístupných služieb elektronickej komunikácie, ale aj na poskytovateľov služieb informačnej spoločnosti (ďalej len „PVSEK" a „PSIS"). V rámci tohto prístupu by sa navyše všetky prípady porušenia ochrany osobných údajov oznamovali národnému regulačnému orgánu alebo príslušným orgánom (ďalej spolu len „orgány"). Ak by orgány určili, že narušenie je *závažné*, žiadali by od PVSEK a PSIS, aby narušenie bezodkladne oznámili dotknutej osobe. V prípade narušení, ktoré predstavujú bezprostredné a priame nebezpečenstvo, by ich PVSEK a PSIS oznamovali jednotlivcom predtým, než ich oznámia orgánom a nečakali by na regulačné rozhodnutie. Na subjekty, ktoré sú schopné preukázať, že „*uplatňujú vhodné technické ochranné opatrenia*", ktoré zabezpečia nečitateľnosť údajov pre kohokoľvek, kto nie je oprávnený k nim pristupovať, sa vzťahuje výnimka z povinnosti oznamovať narušenia spotrebiteľom.

14. V rámci prístupu Rady sa narušenia musia tiež oznamovať účastníkom i orgánom, avšak len v prípadoch, keď narušenie považuje za *vážne riziko* pre súkromie účastníka (t. j. krádež totožnosti alebo podvod s osobnými údajmi, fyzická ujma, závažné poníženie alebo poškodenie dobrého mena) *povinný subjekt*.

15. V zmenenom a doplnenom návrhu Komisie sa ponechala povinnosť oznamovať všetky narušenia orgánom, ktorú ustanovil EP. Na rozdiel od prístupu EP však zmenený a doplnený návrh obsahuje výnimku z oznamovacej povinnosti týkajúcej sa dotknutých jednotlivcov, ak PVSEK pred príslušným orgánom preukáže, že *i*) v dôsledku narušenia bezpečnosti s „*dostatočnou pravdepodobnosťou*" nevznikne žiadna škoda (napr. hospodárska, sociálna alebo krádež totožnosti) alebo, že *ii*) na údaje dotknuté narušením bezpečnosti sa použili „*vhodné technické ochranné opatrenia*". V súvislosti s jednotlivými oznámeniami sa teda v rámci prístupu Komisie používa analýza škôd.

([10]) Ide najmä o pozmeňujúce a doplňujúce návrhy EP č. 187, 124 až 127, ako aj 27, 21 a 32.

16. Je dôležité všimnúť si, že v rámci prístupu EP ([11]) a Komisie sú v konečnom dôsledku za rozhodnutie o závažnosti narušenia bezpečnosti alebo pravdepodobnosti, s akou môže spôsobiť škody, zodpovedné *orgány*. V rámci prístupu Rady sa rozhodnutie ponecháva na *povinných subjektoch*.

17. Prístup Rady i Komisie sa týka len PVSEK a netýka sa, ako v prípade EP, PSIS.

Vymedzenie narušenia bezpečnosti

18. EDPS s potešením konštatuje, že všetky tri legislatívne návrhy obsahujú rovnaké vymedzenie narušenia bezpečnosti: „*porušenie bezpečnosti, ktoré má za následok náhodné, ako aj nezákonné zničenie, stratu, zmenu alebo nedovolené zverejnenie osobných údajov, ktoré sa prenášajú, ukladajú alebo inak spracúvajú […] ako aj umožnenie prístupu k takýmto údajom*" ([12]).

19. Ako sa uvádza nižšie, toto vymedzenie je vítané, pretože je dostatočne široké na to, aby obsiahlo väčšinu relevantných situácií, v ktorých by mohlo byť potrebné oznamovať prípady narušenia bezpečnosti.

20. Po prvé, vymedzenie zahŕňa prípady, keď tretia strana *nedovolene pristúpi* k údajom, ako napríklad v prípade napadnutia servera, ktorý obsahuje osobné údaje, a získania takýchto údajov.

21. Po druhé, toto vymedzenie by zahŕňalo aj situácie, keď došlo k strate alebo zverejneniu osobných údajov, zatiaľ čo nedovolený prístup sa ešte len musí preukázať. Zahŕňalo by to situácie, keď príde k strate osobných údajov (uložených napr. na nosiči CD-ROM, USB disku alebo iných prenosných zariadeniach) alebo ich zverejneniu oprávnenými používateľmi (údaje o zamestnancoch, ktoré sa nechcene a dočasne sprístupnili prostredníctvom internetu). Pretože často nebudú k dispozícii dôkazy o tom, že k takýmto údajom môže prípadne nemôže v budúcnosti pristupovať tretia strana alebo že ich môže alebo nemôže používať, zdá sa byť vhodné, aby sa takéto prípady začlenili do rozsahu pôsobnosti vymedzenia. EDPS preto odporúča zachovanie tohto vymedzenia. EDPS takisto odporúča, aby sa do článku 2 smernice o elektronickom súkromí začlenilo vymedzenie narušenia bezpečnosti, pretože by sa tým dosiahla väčšia konzistentnosť celkovej štruktúry smernice a zabezpečila by sa lepšia zrozumiteľnosť.

([11]) S výnimkou narušení, ktoré predstavujú bezprostredné a priame nebezpečenstvo, kedy musia povinné subjekty najprv informovať spotrebiteľov.

([12]) Článok 2 písm. i) spoločnej pozície a zmeneného a doplneného návrhu a článok 3.3. prvého čítania EP.

Subjekty, na ktoré by sa mala vzťahovať oznamovacia povinnosť

22. V rámci návrhu EP majú oznamovaciu povinnosť PVSEK aj PSIS. V rámci mechanizmov, ktoré navrhujú Rada a Komisia, však majú povinnosť informovať jednotlivcov o narušeniach bezpečnosti, ktoré majú za následok ohrozenie osobných údajov, iba PVSEK, ako napríklad telekomunikačné spoločnosti a poskytovatelia prístupu k internetu. Ostatné odvetvia, ako napríklad on-line banky, on-line maloobchodní predajcovia, on-line poskytovatelia zdravotnej starostlivosti a iné nie sú touto povinnosťou viazané. Z dôvodov uvedených nižšie sa EDPS domnieva, že z hľadiska verejného poriadku je kritické zabezpečiť, aby sa požiadavka na oznamovanie vzťahovala aj na služby informačnej spoločnosti, medzi ktoré patria aj on-line podniky, on-line banky, on-line poskytovatelia zdravotnej starostlivosti atď.

23. Po prvé, EDPS poznamenáva, že hoci v prípade telekomunikačných spoločností ide určite o subjekty, ktoré sú cieľom pokusov o tie druhy narušenia bezpečnosti, ktoré si vyžadujú splnenie oznamovacej povinnosti, to isté platí aj pre iné druhy spoločností/poskytovateľov. Pravdepodobnosť, že sa on-line maloobchodní predajcovia, on-line banky, alebo on-line lekárne stanú terčom pokusov o narušenie bezpečnosti, je rovnaká ako v prípade telekomunikačných spoločností, ak nie väčšia. Po zvážení rizikovosti sa preto nemožno prikloniť na stranu obmedzenia rozsahu pôsobnosti povinnosti oznamovať narušenia bezpečnosti na PVSEK. Potrebu širšieho prístupu dosvedčujú skúsenosti iných krajín. Napríklad v Spojených štátoch takmer všetky štáty (v súčasnosti viac ako 40) prijali zákony o oznamovaní narušení bezpečnosti, ktoré majú širší rozsah uplatniteľnosti a vzťahujú sa nielen na PVSEK, ale na všetky subjekty, ktoré majú v držbe požadované osobné údaje.

24. Po druhé, i keď porušenie ochrany tých druhov osobných údajov, ktoré pravidelne spracúvajú PVSEK, jednoznačne môže mať vplyv na súkromie jednotlivca, to isté platí, ak nie v ešte väčšej miere, pre tie druhy osobných informácií, ktoré spracúvajú PSIS. Je isté, že banky a iné finančné inštitúcie môžu mať v držbe veľmi dôverné informácie (napr. údaje o bankovom účte), ktorých zverejnenie by mohlo umožniť ich využitie na krádež totožnosti. Zverejnenie veľmi citlivých informácií súvisiacich so zdravotným stavom zo strany on-line zdravotníckych služieb by takisto mohlo spôsobiť jednotlivcom obzvlášť veľké škody. Preto si aj takéto druhy osobných údajov, ktoré môžu byť ohrozené, vyžadujú širšie uplatňovanie povinnosti oznamovať narušenia bezpečnosti, zahŕňajúce aspoň PSIS.

25. Voči rozšíreniu rozsahu pôsobnosti príslušného článku, t. j. voči rozsahu subjektov, ktorých sa oznamovacia povinnosť má týkať, boli vznesené isté pripomienky právneho charakteru. Ako prekážka uplatňovania oznamovacej povinnosti aj na PSIS sa poukazovalo najmä na skutočnosť, že celkový rozsah pôsobnosti smernice o elektronickom súkromí sa týka len PVSEK.

26. EDPS by v tomto kontexte chcel pripomenúť, že: *i)* začleneniu iných subjektov než PVSEK do rozsahu pôsobnosti niektorých ustanovení smernice nebráni žiadna právna prekážka. Zákonodarca Spoločenstva má v tomto ohľade voľnú ruku. *ii)* v súčasnej smernici o elektronickom súkromí existujú precedensy uplatňovania na subjekty iné ako PVSEK.

27. Napríklad článok 13 sa nevzťahuje len na PVSEK, ale na všetky spoločnosti, ktoré zasielajú nevyžiadané správy, a vyžaduje na ich zasielanie predchádzajúci súhlas. Článok 5 ods. 3 smernice o elektronickom súkromí, ktorý okrem iného zakazuje ukladanie informácií ako sú cookies na koncovom zariadení používateľa, je navyše záväzný nielen pre PVSEK, ale pre každého, kto sa usiluje ukladať informácie na koncové zariadenia jednotlivcov, alebo získať prístup k informáciám uloženým na takýchto zariadeniach. Komisia okrem toho v súčasnom legislatívnom procese dokonca navrhuje, aby sa pôsobnosť článku 5 ods. 3 rozšírila z šírenia podobných technológií (cookies/spyware) prostredníctvom elektronických komunikačných systémov aj na všetky ostatné možné metódy (šírenie prostredníctvom sťahovania z internetu alebo externých médií na ukladanie údajov, ako je napr. CD-ROM, USB kľúč, mechaniky bez pohyblivých médií atď.). Všetky tieto prvky sú vítané a mali by sa ponechať, predstavujú však tiež relevantné precedensy pre diskusiu o rozsahu pôsobnosti.

28. Okrem toho Komisia a EP a pravdepodobne aj Rada navrhujú v súčasnom legislatívnom procese nový článok 6 ods. 6a, ktorý sa vzťahuje na iné subjekty ako PVSEK a o ktorom sa pojednáva nižšie.

29. Nakoniec, prihliadajúc na celkové pozitíva vyplývajúce z povinnosti oznamovať narušenia bezpečnosti, je veľmi pravdepodobné, že občania budú očakávať tieto výhody nielen v prípade ohrozenia ich údajov zo strany PVSEK, ale aj zo strany PSIS. Očakávania občanov nemusia byť naplnené napríklad, ak sa im neoznámi, že ich on-line banka stratí stratila údaje o ich účte.

30. Záverom EDPS je presvedčenie, že úplné výhody oznamovania narušení bezpečnosti sa dosiahnu, iba ak rozsah pôsobnosti bude ako povinné subjekty zahŕňať PVSEK aj PSIS.

Norma, na základe ktorej vzniká oznamovacia povinnosť

31. Pokiaľ ide o podnet, na základe ktorého vzniká oznamovacia povinnosť, a ako sa podrobnejšie uvádza nižšie, ESDP sa domnieva, že norma uvedená v zmenenom a doplnenom návrhu slovami „*dostatočná pravdepodobnosť poškodenia*“ je najvhodnejšou spomedzi troch navrhovaných noriem. Je však potrebné zabezpečiť, aby „poškodenie“ bol vymedzené dostatočne široko a vzťahovalo sa na všetky relevantné prípady negatívneho vplyvu na súkromie alebo iné legitímne záujmy jednotlivcov. Inak by bolo vhodnejšie vytvoriť novú normu, podľa ktorej by oznamovacia povinnosť vznikla „*ak je dostatočne pravdepodobné, že narušenie bude mať na jednotlivcov negatívny vplyv*“.

32. Ako sa načrtlo v predchádzajúcom oddiele, podmienky, za ktorých sa musí jednotlivcom poslať oznámenie (ďalej len „podmienky vzniku oznamovacej povinnosti“ alebo „norma“) sú v prístupoch EP, Komisie a Rady odlišné. Je zrejmé, že množstvo oznamov, ktoré budú jednotlivci dostávať, bude závisieť najmä od nastavenia podmienok vzniku oznamovacej povinnosti alebo normy.

33. V rámci mechanizmov Rady a Komisie sa musí oznámenie poslať, ak narušenie predstavuje „*vážne riziko pre súkromie účastníka*“ (Rada) a ak „*je dostatočne pravdepodobné, že v dôsledku narušenia dôjde k poškodeniu záujmov spotrebiteľov*“ (Komisia). V rámci mechanizmu EP je podmienkou vzniku oznamovacej povinnosti „*závažnosť narušenia*“ (t. j. oznámenie jednotlivcom sa vyžaduje, ak sa narušenie posúdi ako „*závažné*“). Oznámenie nie je v prípade nižšej dôležitosti narušenia potrebné ([13]).

34. EDPS rozumie, že ak došlo k ohrozeniu osobných údajov, možno argumentovať, že jednotlivci, ktorým dotknuté údaje patria, majú nárok byť za každých okolností oboznámení o tom, že takýto prípad nastal. Nie je však vôbec na škodu zvážiť, či ide o vhodné riešenie vzhľadom na iné záujmy a okolnosti.

35. Jedným z argumentov je, že povinnosť posielať oznámenia pri každom ohrození osobných údajov, inými slovami bez akýchkoľvek obmedzení, môže viesť k nadmernému zasielaniu takýchto oznamov a „únave“ z nich, čo by mohlo otupiť citlivosť ich vnímania. Ako sa uvádza nižšie, EDPS na tento argument starostlivo prihliada; zároveň však chce zdôrazniť svoje obavy súvisiace s tým, že nadmerné zasielanie oznamov môže byť ukazovateľom rozsiahleho zlyhania bezpečnostných postupov súvisiacich s informáciami.

36. Ako bolo uvedené, EDPS vníma potenciálne negatívne dôsledky nadmerného zasielania oznamov a chcel by pomôcť zabezpečiť, aby sa prijatím právneho rámca pre oznamovanie narušení bezpečnosti takýmto dôsledkom predišlo. Ak by jednotlivci dostávali oznámenia o narušení bezpečnosti často, dokonca aj v situáciách bez negatívnych následkov, škôd alebo núdze, mohol by sa podkopať jeden z kľúčových cieľov zasielania oznamov, pretože jednotlivci by možno tieto oznamy paradoxne ignorovali v prípadoch, keď by skutočne mali prijať opatrenia na svoju ochranu. Vyváženosť je teda pri zasielaní zmysluplných oznámení dôležitá, pretože keby jednotlivci na oznámenia nereagovali, účinnosť oznamovacieho mechanizmu by sa radikálne znížila.

37. Pri prijímaní vhodnej normy, ktorá nespôsobí nadmerné zasielanie oznamov, sa okrem zváženia podmienok vzniku oznamovacej povinnosti musia zohľadniť aj ostatné faktory, najmä vymedzenie narušenia bezpečnosti a informácie, na ktoré sa má oznamovacia povinnosť vzťahovať. EDPS v tomto ohľade poznamenáva, že v rámci uvedených troch navrhovaných prístupov môže byť vzhľadom na široké vymedzenie narušenia bezpečnosti uvedené vyššie objem oznámení vysoký. Obavy súvisiace s nadmerným zasielaním oznámení prehlbuje skutočnosť, že vymedzenie narušenia bezpečnosti sa vzťahuje na všetky druhy osobných údajov. Napriek tomu, že v porovnaní s prístupmi uplatňovanými napr. v USA, kde sa požiadavky sústreďujú na citlivosť informácií, považuje EDPS uvedený prístup (neobmedzovanie osobných údajov podliehajúcich oznamovacej povinnosti podľa ich druhu) za správny, ide o a faktor, ktorý je nutné zohľadniť.

38. Vzhľadom na uvedené skutočnosti a prihliadajúc na rozdielne premenné zvážené spoločne, EDPS považuje za vhodné, aby sa zaviedla norma alebo prah, pod ktorým nebudú oznamy povinné.

39. Zdá sa, že obe navrhované normy, teda narušenie, ktoré je „*vážnym rizikom pre súkromie*“ alebo ktoré predstavuje „*dostatočnú pravdepodobnosť poškodenia*“, v sebe zahŕňajú napríklad poškodenie spoločenského postavenia alebo dobrého mena a hospodársku škodu. Takéto normy by sa napríklad zaoberali prípadmi, keď boli jednotlivci vystavení krádeži totožnosti prostredníctvom zverejnenia neverejných identifikačných údajov, ako je napr. číslo pasu, alebo zverejneniu informácií o ich súkromnom živote. EDPS tento prístup víta. Je presvedčený, že výhody oznámení o narušeniach bezpečnosti by sa nevyužili úplne, ak by sa oznámenia vzťahovali výhradne na narušenia, ktoré spôsobili hospodárske škody.

([13]) K výnimke z tohto pravidla pozri poznámku pod čiarou č. 11.

40. Z uvedených dvoch noriem uprednostňuje EDPS normu Komisie vyjadrenú spojením „*dostatočná pravdepodobnosť poškodenia*“, pretože by jednotlivcom zabezpečila vhodnejšiu úroveň ochrany. Narušenia sa s oveľa väčšou pravdepodobnosťou určia za narušenia, ktoré je potrebné oznámiť, ak z nich vyplýva „*dostatočná pravdepodobnosť poškodenia*“ súkromia jednotlivcov, než keď predstavujú „*vážne riziko*“ takéhoto poškodenia. Ak by sa do vymedzenia začlenili iba narušenia, ktoré predstavujú vážne riziko pre súkromie jednotlivcov, počet narušení, ktoré by sa museli oznámiť, by sa značne znížil. Takýmto vymedzením by sa PVSEK a PSIS umožnila neprimeraná voľnosť pri rozhodovaní o tom, či je potrebné zaslať oznámenie, pretože by pre nich bolo omnoho jednoduchšie zdôvodniť svoje rozhodnutie tým, že neexistuje „*vážne riziko*“ poškodenia, než tým, že neexistuje „*dostatočná pravdepodobnosť poškodenia*“. I keď je jednoznačne potrebné predchádzať nadmernému zasielaniu oznamov, jazýček váh je nutné posunúť v prospech ochrany súkromia jednotlivcov, ktorí by mali byť chránení minimálne vtedy, keď ich narušenie s dostatočnou pravdepodobnosťou môže poškodiť. Spojenie „dostatočná pravdepodobnosť“ bude okrem toho v praxi vhodnejšie pre povinné subjekty i príslušné orgány, pretože si vyžaduje objektívne posúdenie daného prípadu a jeho relevantného kontextu.

41. Narušenia osobných údajov môžu navyše spôsobiť škodu, ktorú ťažko kvantifikovať a ktorá môže byť rozličnej povahy. Zverejnenie rovnakého druhu údajov môže dokonca v závislosti od konkrétnych okolností spôsobiť značnú škodu jednému jednotlivcovi a menšiu škodu inému. Norma, ktorou by sa vyžadovalo, aby bola škoda materiálna, značná alebo závažná, by nebola vhodná. Napríklad prístupom Rady, v rámci ktorého sa vyžaduje, aby narušenie *vážne* ovplyvnilo niekoho súkromie, by sa nezabezpečila dostatočná ochrana jednotlivcov, pretože takáto norma si vyžaduje, aby bol vplyv na súkromie „vážny“ Tým sa tiež otvára priestor pre subjektívne posudzovanie.

42. I keď spojenie „*dostatočná pravdepodobnosť poškodenia*“ sa zdá byť, ako sa uvádza vyššie, vhodnou normou pre oznamy o narušeniach bezpečnosti, EDPS je naďalej znepokojený tým, že nemusí zahŕňať všetky situácie, v ktorých by sa oznámenie jednotlivcom malo poslať, t. j. všetky situácie, keď nastáva dostatočná pravdepodobnosť negatívnych vplyvov na súkromie alebo iné legitímne záujmu jednotlivcov. Z týchto dôvodov by sa mohla zvážiť norma, podľa ktorej by oznámenie bolo povinné, „*ak je dostatočne pravdepodobné, že narušenie bude mať na jednotlivcov negatívny vplyv*“.

43. Ďalšou výhodou takejto alternatívnej normy je jej súlad s legislatívou EÚ v oblasti ochrany údajov. V smernici o ochrane údajov sa často odkazuje na nepriaznivý vplyv na práva a slobody dotknutých osôb. Napríklad v článku 18 a odôvodnení 49, ktoré hovoria o povinnosti oznamovať operácie spracúvania údajov orgánom členských štátov na ochranu údajov, umožňujú členským štátom povoliť výnimku z tejto povinnosti v prípadoch, kedy spracúvanie „*nebude nepriaznivo vplývať na práva a slobodu údajových subjektov*“. Podobné znenie sa použilo v článku 16 ods. 6 spoločnej pozície, aby sa právnickým osobám umožnila dávať návrhy na začatie konania proti šíriteľom spamu.

44. Ak zoberieme uvedené skutočnosti do úvahy, dá sa navyše očakávať, že povinné subjekty a najmä orgány príslušné na presadzovanie legislatívy v oblasti ochrany údajov budú s uvedenou normou oboznámené vo väčšej miere, čím sa uľahčí ich posudzovanie toho, či dané narušenie napĺňa normu.

Subjekt, ktorý má určiť, či narušenie bezpečnosti napĺňa normu

45. V rámci prístupu EP (okrem prípadov bezprostredného nebezpečenstva) a podľa zmeneného a doplneného návrhu Komisie budú za určovanie toho, či narušenie bezpečnosti napĺňa normu, na základe ktorej vzniká povinnosť poslať oznam dotknutému jednotlivcovi, zodpovedať za členské štáty.

46. EDPS sa domnieva, že účasť orgánov je pri určovaní skutočnosti, či bola norma naplnená, dôležitá, pretože je do istej miery zárukou správneho uplatňovania práva. Takýto systém môže zabrániť spoločnostiam, aby neprimerane posudzovali narušenia ako bezpečné/nedôležité a vyhýbať sa tak oznamovaniu v prípadoch, keď je v skutočnosti potrebné.

47. Na druhej strane sa EDPS obáva, že systém, v rámci ktorého posudzovanie povinne vykonávajú orgány, môže byť nepraktický a náročný na uplatňovanie, alebo sa môže v praxi ukázať ako kontraproduktívny. Môže tak dokonca spôsobiť oslabenie záruk ochrany údajov jednotlivcov.

48. V rámci takéhoto prístupu je pravdepodobné, že orgány na ochranu údajov budú zaplavené oznamami o narušeniach bezpečnosti a možno budú čeliť pri ich posudzovaní vážnym ťažkostiam. Je dôležité pamätať na to, že ak majú orgány posúdiť, či narušenie napĺňa normu, musia mať k dispozícii dostatočné interné informácie, často zložitej technickej povahy, ktoré budú musieť veľmi rýchlo spracúvať. Prihliadajúc na zložitosť posudzovania a skutočnosť, že niektoré orgány majú obmedzené zdroje, EDPS sa obáva, že pre orgány bude veľmi zložité vyhovieť tejto povinnosti a že by to mohlo odlákať zdroje od ostatných dôležitých priorít. Takýto systém by navyše mohol dostať orgány pod neprimeraný tlak; ak sa napríklad rozhodnú, že narušenie nie je závažné, a jednotlivci budú napriek tomu poškodení, orgány by mohli byť brané na zodpovednosť.

49. Uvedené ťažkosti sa ešte viac prehĺbia, ak sa zohľadní, že pri minimalizácii rizík vyplývajúcich z narušení bezpečnosti zohráva kľúčovú úlohu čas. Pokiaľ orgány nie sú schopné vypracovať posudok vo veľmi krátkych lehotách, dodatočný čas, ktorý na to potrebujú, môže zväčšiť škodu, ktorú utrpia dotknutí jednotlivci. Takýto dodatočný krok, ktorý má zabezpečiť väčšiu ochranu jednotlivcov, preto môže paradoxne poskytovať nižšiu úroveň ochrany, ako systémy založené na priamom oznamovaní.

50. EDPS sa preto nazdáva, že by bolo vhodnejšie zriadiť systém, v rámci ktorého by posudky o tom, či narušenie bezpečnosti napĺňa normu, vypracúvali povinné subjekty, ako navrhuje Rada.

51. Aby sa však predchádzalo riziku možného zneužívania, napríklad ak by subjekty odmietali oznamy posielať aj v situáciách, kedy je zrejmé, že tak majú urobiť, je nesmierne dôležité, aby sa ustanovili isté záruky ochrany údajov opísané nižšie.

52. Po prvé, povinnosť príslušných subjektov určiť, či musia poslať oznam, musí byť samozrejme sprevádzaná ďalšou povinnosťou oznamovať orgánom všetky narušenia, ktoré naplnili normu. Povinné subjekty by mali byť v takýchto prípadoch povinné informovať orgány o danom narušení a dôvodoch, na základe ktorých rozhodli o oznámení, ako aj o obsahu všetkých poslaných oznamov.

53. Po druhé, orgánom sa musí zveriť úloha skutočných dozorcov. Pri vykonávaní tejto úlohy sa musí orgánom umožniť (nesmie to však byť povinnosť) vyšetriť okolnosti daného narušenia a žiadať, aby boli prijaté vhodné nápravné opatrenia ([14]). Malo by ísť nielen o posielanie oznamov jednotlivcom (ak sa ešte neuskutočnilo), ale aj o schopnosť uložiť povinnosť prijať opatrenia na predchádzanie ďalším narušeniam. Orgánom by sa v tomto ohľade mali poskytnúť účinné právomoci a zdroje a potrebná voľnosť pri rozhodovaní, kedy zareagovať na oznámenie o narušení bezpečnosti. Inými slovami, orgánom by sa takto umožnilo selektívne správanie a účasť na vyšetrovaní napr. veľkých, naozaj škodlivých prípadov narušenia bezpečnosti a overovaní a presadzovaní dodržiavania zákonných požiadaviek.

54. Aby bolo možné dosiahnuť uvedený cieľ, EDPS odporúča, aby sa okrem právomocí uznaných na základe smernice o elektronickom súkromí, ako napr. v článku 15a ods. 3 a smernice o ochrane údajov doplnil tento text: „*Ak dotknutému účastníkovi alebo jednotlivcovi zatiaľ nebol oznam poslaný, príslušný národný orgán môže po zvážení povahy narušenia prikázať PVSEK alebo PSIS, aby oznam poslal.*“

55. EDPS navyše EP a Rade odporúča, aby potvrdili návrh EP (pozmeňujúci a doplňujúci návrh č. 122, článok 4 ods. 1a), ktorý subjektom ukladá povinnosť, aby pre ich systémy a osobné údaje, ktoré zamýšľajú spracúvať, vypracovali posudok rizikovosti. Subjekty na základe tejto povinnosti vypracujú na mieru šité a presné vymedzenie bezpečnostných opatrení, ktoré sa prijmú v ich prípade a ktoré by mali mať orgány k dispozícii. Ak nastane narušenie bezpečnosti, táto povinnosť pomôže povinným subjektom a v konečnom dôsledku aj orgánom plniacim dozornú úlohu určiť, či ohrozenie daných informácií môže mať na jednotlivcov negatívny vplyv alebo im spôsobiť škodu.

56. Po tretie, povinnosť subjektov určovať, či musia poslať jednotlivcovi oznámenie, musí sprevádzať povinnosť udržiavať podrobné a komplexné záznamy na účely auditu, ktoré budú obsahovať popis všetkých narušení, ktoré sa vyskytli, ako aj oznamov, ktoré sa kvôli nim zaslali, a všetky opatrenia, ktoré sa prijali, aby sa narušeniam v budúcnosti predchádzalo. Tieto záznamy na účely auditu musia mať orgány k dispozícii na preskúmanie a potenciálne vyšetrovanie. To im umožní vykonávať ich dozornú úlohu. Dalo by sa to dosiahnuť prijatím napríklad takéhoto textu: „*PVSEK a PSIS vedú a uchovávajú komplexné záznamy o všetkých narušeniach bezpečnosti, ktoré sa vyskytli, relevantné technické informácie, ktoré s nimi súvisia, ako aj záznamy o prijatých nápravných opatreniach. Záznamy musia obsahovať aj odkaz na všetky oznámenia vydané pre dotknutých účastníkov alebo jednotlivcov a príslušné národné orgány vrátane ich dátumu a obsahu. Záznamy sa predkladajú príslušným národným orgánom základe ich žiadosti.*“

57. Samozrejme, aby bolo možné zabezpečiť konzistentnosť pri vykonávaní tejto normy, ako aj ďalších dôležitých aspektov rámca pre narušenia bezpečnosti, ako je napr. formát a postupy pre oznamovanie, bolo by vhodné, keby Komisia po porade s EDPS, pracovnou skupinou článku 29 a príslušnými zainteresovanými stranami prijala technické vykonávacie opatrenia.

([14]) V článku 15a ods. 3 sa tieto dozorné právomoci uznávajú, pretože sa v ňom ustanovuje, že „členské štáty zabezpečia, aby príslušné vnútroštátne orgány a prípadne iné vnútroštátne orgány mali všetky vyšetrovacie právomoci a zdroje nevyhnutné na monitorovanie a vynucovanie vnútroštátnych predpisov prijatých podľa tejto smernice vrátane možnosti získavať všetky relevantné informácie.“

Príjemcovia oznámení

58. Pokiaľ ide o príjemcov oznámení, EDPS uprednostňuje terminológiu EP a Komisie pre terminológiou Rady. EP nahradil slovo „účastníci" slovom „užívatelia". Komisia používa „účastníkov" a „príslušných jednotlivcov". Znením použitým EP i Komisiou by sa medzi príjemcov oznámení začlenili nielen súčasní účastníci, ale aj bývalí účastníci a tretie strany, ako napríklad užívatelia, ktorí sú vo vzťahu s niektorými povinnými subjektami bez toho, aby boli ich účastníkmi. EDPS tento prístup víta a vyzýva EP a Komisiu, aby ho zachovali.

59. EDPS však upozorňuje na niekoľko terminologických nezrovnalostí v návrhu EP z prvého čítania, ktoré by sa mali napraviť. Napríklad slovo „účastníci" sa vo väčšine prípadov nahradilo slovom „užívatelia", ale v niektorých prípadoch slovom „spotrebitelia". Terminológia by sa mala zjednotiť.

III. ROZSAH PÔSOBNOSTI SMERNICE O ELEKTRONICKOM SÚKROMÍ: VEREJNÉ A SÚKROMNÉ SIETE

60. V článku 3 ods. 1 platnej smernice o elektronickom súkromí sa ustanovujú subjekty, ktorých sa smernica predovšetkým týka, t. j. tie, ktoré spracúvajú údaje „v súvislosti s" poskytovaním verejne dostupných služieb elektronickej komunikácie vo verejných sieťach (PVSEK) ([15]). Príklady činnosti PVSEK zahŕňajú poskytovanie prístupu k internetu, prenos informácií prostredníctvom elektronických sietí, mobilné a telefónne prepojenia atď.

61. EP prijal pozmeňujúci a doplňujúci návrh č. 121, ktorým sa mení článok 3 pôvodného návrhu Komisie, v rámci ktorého sa mal rozsah pôsobnosti smernice o elektronickom súkromí rozšíriť tak, aby zahŕňal „*spracovávanie osobných údajov v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných a súkromných komunikačných sieťach a verejne dostupných súkromných sieťach v Spoločenstve […]*" (článok 3 ods. 1 smernice o elektronickom súkromí). Rada a Komisia však nanešťastie nemohli tento pozmeňujúci a doplňujúci návrh akceptovať a preto ho nezapracovali do spoločnej pozície ani zmeneného a doplneného návrhu.

Uplatňovanie smernice o elektronickom súkromí na verejne dostupné súkromné siete

62. Z dôvodov uvedených nižšie a s cieľom napomôcť konsenzu nabáda EDPS na zachovanie podstaty pozmeňujúceho a doplňujúceho návrhu 121. EDPS navyše navrhuje začlenenie zmeny a doplnenia, ktorými by sa presnejšie vymedzili druhy služieb, ktoré by patrili do rozšíreného rozsahu pôsobnosti.

63. Súkromné siete sa často používajú na poskytovanie služieb elektronickej komunikácie, ako je napr. internet, nevymedzenému počtu ľudí, ktorý môže byť vysoký. Ide napríklad o prístup k internetu v internetových kaviarňach, ako aj o prístupové body Wi-Fi, ktoré sú k dispozícii v hoteloch , reštauráciách, na letiskách, vo vlakoch a iných zariadeniach prístupných verejnosti, kde sa takéto služby často poskytujú ako doplnok k iným službám (nápoje, ubytovanie atď.).

64. Vo všetkých uvedených príkladoch sa nejaká komunikačná služba, napr. internet, sprístupňuje verejnosti nie cez verejnú sieť, ale cez sieť, ktorú možno považovať za súkromnú, t. j. za súkromne prevádzkovanú sieť. Navyše, i keď v uvedenom príklade sa komunikačné služby poskytujú verejnosti, keďže sieť je súkromná a nie verejná, na poskytovanie takýchto služieb sa údajne smernica o elektronickom súkromí nevzťahuje vôbec, alebo len čiastočne ([16]). Základné práva jednotlivcov, ktoré garantuje smernica o elektronickom súkromí, nie sú preto v takýchto prípadoch chránené a užívatelia, ktorí využívajú služby prístupu k internetu prostredníctvom súkromných verejných telekomunikačných prostriedkov, sa v porovnaní s užívateľmi, ktorí využívajú tie isté služby prostredníctvom verejných telekomunikačných prostriedkov, ocitajú v nerovnakej právnej situácii. Táto situácia vzniká napriek tomu, že súkromie jednotlivcov a osobné údaje existujú vo všetkých takýchto prípadoch v rovnakej miere, ako keď sa na poskytnutie služby použijú verejné siete. V súhrne sa zdá, že rozdielne zaobchádzanie s komunikačnými službami poskytovanými prostredníctvom súkromných sietí a službami poskytovanými prostredníctvom verejných sietí na základe danej smernice nemá opodstatnenie.

65. EDPS by preto podporil zmenu a doplnenie, ako napr. pozmeňujúci a doplňujúci návrh EP č. 121, na základe ktorého by sa smernica o elektronickom súkromí vzťahovala aj na spracúvanie osobných údajov v súvislosti s poskytovaním verejne dostupných služieb elektronickej komunikácie v súkromných komunikačných sieťach.

66. EDPS však uznáva, že takéto ustanovenie by mohlo mať nepredvídateľné a možno aj nezamýšľané dôsledky. Dokonca aj púhy odkaz na súkromné siete by bolo možné vykladať ako odkaz na situácie, na ktoré sa

([15]) „Táto smernica sa vzťahuje na spracovávanie osobných údajov v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach."

([16]) Argumentovať možno naopak i tak, že keďže sa komunikačná služba poskytuje verejnosti, na poskytovanie takýchto služieb sa platný právny rámec vzťahuje, aj keď je sieť súkromná. Napríklad vo Francúzsku sa zamestnávatelia, ktorí svojim zamestnancom poskytujú prístup k internetu, považujú v tomto ohľade za rovnocenných s komerčnými poskytovateľmi internetu. Tento výklad nie je všeobecne akceptovaný.

podľa zámerov táto smernica nemá vzťahovať. Mohlo by sa napríklad tvrdiť, že doslovný alebo prísny výklad takéhoto ustanovenia by do rozsahu pôsobnosti smernice zahrnul aj majiteľov domácností vybavených Wi-Fi sieťami ([17]), ktoré umožňujú pripojenie sa každému v ich dosahu (zvyčajne v danej domácnosti), a to napriek tomu, že to nie je zámerom pozmeňujúceho a doplňujúceho návrhu č. 121. Aby sa takémuto dôsledku zabránilo, EDPS navrhuje zmenu znenia pozmeňujúceho a doplňujúceho návrhu č. 121, ktorou by sa do rozsahu pôsobnosti smernice o elektronickom súkromí začlenilo *„spracúvanie osobných údajov v súvislosti s poskytovaním verejne dostupných služieb elektronickej komunikácie vo verejných komunikačných sieťach alebo súkromných komunikačných sieťach, ku ktorým má prístup verejnosť, v Spoločenstve, …“*.

67. Pomohlo by to vyjasniť, že smernica o elektronickom súkromí by sa vzťahovala len na súkromé siete, ku ktorým má prístup verejnosť. Tým, že sa ustanovenia smernice o elektronickom súkromí budú vzťahovať *výhradne* na súkromné siete, ku ktorým má prístup verejnosť (a nie na všetky súkromné siete), ustanoví sa obmedzenie, na základe ktorého sa smernica bude vzťahovať len na komunikačné služby poskytované prostredníctvom súkromných sietí, ktoré sa *úmyselne* sprístupnia verejnosti. Takáto formulácia tiež zdôrazní skutočnosť, že *dostupnosť* súkromnej siete *pre širokú verejnosť* je kľúčovým faktorom pri určovaní toho, či sa na danú situáciu vzťahuje smernica (navyše k ustanoveniu o verejne dostupných komunikačných službách). Inými slovami, nezávisle na tom, či je sieť verejná alebo súkromná, ak sa úmyselne sprístupní verejnosti s cieľom poskytovať verejnú komunikačnú službu, ako napríklad pripojenie k internetu, dokonca aj ak je takáto služba doplnkom k inej službe (napr. ubytovanie v hoteli), na takýto druh služby/siete by sa smernica o elektronickom súkromí vzťahovala.

68. EDPS poznamenáva, že uvedený prístup, v rámci ktorého by sa ustanovenia smernice o elektronickom súkromí vzťahovali na verejne dostupné súkromné siete, zodpovedá prístupom, ktoré zaujalo niekoľko členských štátov, v ktorých už orgány uznali, že takéto druhy služieb, ako aj služby poskytované v čisto súkromných sieťach, spadajú do rozsahu pôsobnosti vnútroštátnych ustanovení, ktorými sa smernica o elektronickom súkromí vykonáva ([18]).

69. Aby sa posilnila právna istota vo vzťahu k subjektom, na ktoré sa bude vzťahovať nový rozsah pôsobnosti, do smernice o elektronickom súkromí by sa mohla začleniť zmena a doplnenie na vymedzenie „verejne dostupných súkromných sietí“, ktorá by mohla znieť takto: *„verejne dostupná súkromná sieť je súkromne prevádzkovaná sieť, ku ktorej má široká verejnosť po odsúhlasení podmienok súvisiacich s jej používaním bežne neobmedzený prístup za poplatok alebo v rámci iných služieb alebo ponúk.“*

70. V praxi by takýto prístup znamenal, rozsah pôsobnosti smernice by sa vzťahoval aj na súkromné siete v hoteloch a iných zriadeniach, ktoré poskytujú prístup k internetu širokej verejnosti. Naopak, na poskytovanie komunikačných služieb v čisto súkromných sieťach, kde sa služba poskytuje obmedzenej skupine identifikovateľných jednotlivcov, by sa smernica nevzťahovala. Nevzťahovala by sa teda napríklad na virtuálne súkromné siete a domácnosti spotrebiteľov so sieťami Wi-Fi. Rovnako by sa nevzťahovala na čisto podnikové siete.

Súkromné siete, na ktoré by sa uplatňovala smernica o elektronickom súkromí

71. Vylúčenie súkromných sietí ako takých, ako sa uvádza vyššie, by sa malo považovať za prechodné opatrenie, o ktorom by sa malo v budúcnosti rokovať. Vzhľadom na vplyv vylúčenia čisto súkromných sietí ako takých na oblasť ochrany súkromia na jednej strane a na skutočnosť, že súkromné siete používa veľké množstvo ľudí, ktorí zvyčajne pristupujú k internetu cez podnikové siete na druhej strane, je možné, že túto otázku bude potrebné v budúcnosti ešte zvážiť. Z tohto dôvodu a s cieľom podporiť diskusie o tejto otázke EDPS odporúča, aby sa do smernice o elektronickom súkromí začlenilo odôvodnenie, podľa ktorého by Komisia uskutočnila verejnú diskusiu o uplatňovaní smernice o elektronickom súkromí na všetky súkromné siete, pričom do nej prispeje EDPS, orgány na ochranu údajov a ďalšie relevantné zainteresované strany. Okrem toho by sa v odôvodnení mohlo uviesť, že Komisia by mala na základe verejnej diskusie vypracovať vhodný návrh na rozšírenie alebo obmedzenie druhov subjektov, na ktoré by sa mala smernica o elektronickom súkromí vzťahovať.

72. Okrem uvedených skutočností by sa články smernice o elektronickom súkromí mali zmeniť a doplniť tak, aby sa vo všetkých príslušných ustanoveniach výslovne odkazovalo okrem verejných sietí aj na verejne dostupné súkromné siete.

IV. SPRACÚVANIE PREVÁDZKOVÝCH DÁT NA BEZPEČNOSTNÉ ÚČELY

73. Počas legislatívneho procesu súvisiaceho s preskúmaním smernice o elektronickom súkromí spoločnosti, ktoré poskytujú bezpečnostné služby, presadzovali, že je potrebné, aby sa do smernice o elektronickom súkromí začlenilo ustanovenie, ktorým sa legitimizuje zhromažďovanie údajov, aby bolo možné zaručiť účinnú on-line bezpečnosť.

([17]) Zvyčajne ide o miestne siete (LAN).
([18]) Pozri poznámku pod čiarou č. 16.

74. EP preto vložil do smernice pozmeňujúci a doplňujúci návrh č. 181, ktorým sa vytvoril nový článok 6 ods. 6a, ktorým by sa výslovne povolilo spracúvanie prevádzkových údajov na bezpečnostné účely. „*Bez toho, aby tým bolo dotknuté dodržiavanie ustanovení okrem článku 7 smernice 95/45/ES a článku 5 tejto smernice, prevádzkové údaje sa môžu spracovávať z oprávneného záujmu kontrolóra údajov na účely uplatnenia technických opatrení na zaistenie bezpečnosti siete a informácií, ako je vymedzené v článku 4 písm. c) nariadenia (ES) 1 č. 460/2004 Európskeho parlamentu a Rady z 10. marca 2004, ktorým sa vytvorila Európska agentúra pre bezpečnosť sietí a informácií, ďalej na účely verejnej elektronickej komunikačnej služby, verejnej alebo súkromnej elektronickej komunikačnej siete, služieb informačnej spoločnosti alebo súvisiacich terminálov a elektronických komunikačných zariadení s výnimkou prípadov, keď takéto záujmy prevýšia záujmy základných práv a slobôd dotknutej osoby. Takéto spracovávanie je obmedzené len na tie skutočnosti, ktoré sú absolútne nevyhnutné na účely uvedenej bezpečnostnej činnosti.*“

75. V zmenenom a doplnenom návrhu Komisie sa tento pozmeňujúci a doplňujúci návrh v zásade akceptoval, odstránila sa však kľúčová klauzula v znení „*Bez toho, aby tým bolo dotknuté […] … tejto smernice*“, ktorá mala zabezpečiť, aby sa ostatné ustanovenia smernice dodržiavali. Rada prijala preformulované znenie, ktorým sa dôležité ochrany a vyváženie záujmov zabudované do pozmeňujúceho a doplňujúceho návrhu č. 181 ešte viac oslabili: „*Prevádzkové dáta sa môžu spracúvať v rozsahu nevyhnutne potrebnom na zabezpečenie […] siete a zaistenie informačnej bezpečnosti, ako sa vymedzuje v článku 4 písm. c) nariadenia Európskeho parlamentu a Rady (ES) č. 460/2004 z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií.*“

76. Ako sa vysvetľuje nižšie, článok 6 ods. 6a nie je potrebný a môže sa zneužívať, najmä ak sa prijme v podobe, ktorá nebude obsahovať dôležité záruky, klauzuly o dodržiavaní ostatných ustanovení smernice a vyváženie záujmov. EDPS preto odporúča, aby sa tento článok neprijal, alebo aby aspoň každý takýto článok obsahoval rovnaké druhy záruk, ako pozmeňujúci a doplňujúci návrh č. 181, ktorý prijal EP.

Právne dôvody pre spracúvanie prevádzkových dát vzťahujúce sa na elektronické komunikačné služby a iných kontrolórov podľa platných právnych predpisov na ochranu údajov

77. Rozsah, v ktorom môžu poskytovatelia verejne dostupných služieb elektronickej komunikácie legálne spracúvať prevádzkové dáta, je upravený v článku 6 smernice o elektronickom súkromí, v ktorom sa obmedzuje spracúvanie prevádzkových dát na zopár účelov, ako napr. fakturácia, platby za spojenie a marketing. Spracúvanie je podmienené osobitnými podmienkami, ako napríklad súhlas jednotlivcov v prípade marketingu. Iní kontrolóri, ako napr. poskytovatelia služieb informačnej spoločnosti môžu okrem toho spracúvať prevádzkové dáta podľa článku 7 smernice o ochrane údajov, ktorá ustanovuje, že kontrolóri môžu osobné údaje spracúvať, ak je to v súlade s aspoň jedným z vymenovaných právnych základov, ktoré sa nazývajú aj právnymi dôvodmi.

78. Príkladom jedného takéhoto právneho základu je článok 7 písm. a) smernice o ochrane údajov, podľa ktorého sa vyžaduje súhlas dotknutej osoby. Ak napríklad on-line obchodník chce spracovať prevádzkové dáta na účely zasielania reklamných alebo marketingových materiálov, musí získať súhlas daného jednotlivca. Ďalším právnym základom uvedeným v článku 7 sa v niektorých príkladoch povoľuje spracúvanie prevádzkových údajov na bezpečnostné účely, napríklad bezpečnostnými spoločnosťami, ktoré ponúkajú bezpečnostné služby. Základom je v tomto prípade písmeno f) článku, v ktorom sa ustanovuje, že kontrolóri môžu spracúvať osobné údaje, ak je to „*nevyhnutné pre účely legitímnych záujmov, ktoré plní kontrolór, alebo tretia strana alebo strany, ktorým sú údaje odhalené, s výnimkou, ak takéto záujmy sú prevýšené záujmami týkajúcimi sa základných práv a slobôd osoby pracujúcej s údajmi …*“ Smernica o ochrane údajov neobsahuje konkrétne prípady, v ktorých by spracúvanie osobných údajov túto požiadavku spĺňalo. Rozhodnutia prijímajú kontrolóri od prípadu k prípadu, často po dohode s vnútroštátnymi orgánmi na ochranu údajov alebo inými orgánmi.

79. Vzájomné vzťahy medzi článkom 7 smernice o ochrane údajov a navrhovaným článkom 6 ods. 6a smernice o elektronickom súkromí by sa mali zvážiť. Navrhovaný článok 6 ods. 6a je skonkrétnením okolností, za ktorých možno splniť požiadavku uvedené v uvedenom článku 7 písm. f). Článok 6 ods. 6a, tým, že povoľuje spracúvanie prevádzkových dát na účely zaistenia bezpečnosti siete a informácií, umožňuje toto spracúvanie na účely legitímnych záujmov, ktoré plní kontrolór.

80. Ako sa vysvetľuje nižšie, EDPS sa nazdáva, že článok 6 ods. 6a nie je potrebný, ani prospešný. Z právneho hľadiska je v podstate zbytočné, aby sa ustanovovalo, či konkrétny druh spracovania údajov, v tomto prípade spracúvanie údajov na bezpečnostné účely, spĺňa požiadavky článku 7 písm. f) smernice o ochrane osobných údajov alebo nie, pričom ak nie, na základe článku 7 psím. a) by bol potrebný súhlas dotknutého jednotlivca. Ako sa uvádza vyššie, takéto posúdenie v praxi uskutočňujú zvyčajne kontrolóri, t. j. spoločnosti, po porade s orgánmi na ochranu údajov, pričom v prípade potreby ho uskutočňujú súdy. EDPS sa vo všeobecnosti domnieva, že v konkrétnych prípadoch bude legitímne spracúvanie prevádzkových dát na bezpečnostné účely vykonávané bez toho, aby sa ohrozili základné práva a slobody jednotlivcov, pravdepodobne spĺňať požiadavky článku 7 písm. f) smernice o ochrane osobných údajov, a bude ho

preto možné vykonávať. Navyše, v smerniciach o ochrane údajov a o elektronickom súkromí neexistuje žiaden precedens pre vyčlenenie niektorých druhov spracúvania údajov, ktoré by spĺňali požiadavky článku 7 písm. f), ani pre ustanovenie osobitného zaobchádzania s takýmito druhmi spracúvania, pričom potreba takejto výnimky sa nikdy ani nepreukázala. Ako sa uvádza vyššie, zdá sa, že takýto druh činnosti by za mnohých okolností súčasnému zneniu bez problémov vyhovoval Právne ustanovenie, ktorým by sa potvrdilo takéto posudzovanie, preto v zásade nie je potrebné.

Verzie článku 6 ods. 6a podľa EP, Rady a Komisie

81. Ako sa uvádza vyššie, i keď je pozmeňujúci a doplňujúci návrh č. 181, ako ho prijal EP, nepotrebný, jeho znenie v istej miere zohľadňuje zásady ochrany súkromia a údajov stelesnené v právnych predpisoch na ochranu údajov. Pozmeňujúcim a doplňujúcim návrhom EP č. 181 by sa mohla otázka ochrany údajov a súkromia ďalej upraviť napríklad prostredníctvom vloženia spojenia „v osobitných prípadoch“, čím by sa zabezpečilo selektívne uplatňovanie uvedeného článku, alebo začlenením konkrétneho ochranného obdobia.

82. Pozmeňujúci a doplňujúci návrh EP č. 181 obsahuje niekoľko pozitívnych prvkov. Potvrdzuje, že spracúvanie musí byť v súlade so všetkými ostatnými zásadami ochrany údajov uplatniteľnými na spracúvanie osobných údajov („*Bez toho, aby tým bolo dotknuté dodržiavanie ustanovení smernice 95/45/ES a […] tejto smernice*“). Navyše, i keď návrh č. 181 umožňuje spracúvanie prevádzkových dát na bezpečnostné účely, vytvára rovnováhu medzi záujmami subjektu, ktorý spracúva prevádzkové dáta, a záujmami jednotlivcov, ktorých údaje sa spracúvajú, pretože takéto spracúvanie je možné, len ak záujmy jednotlivcov v oblasti základných práv a slobôd nie sú nadradené záujmom takéhoto subjektu („*s výnimkou prípadov, keď takéto záujmy prevýšia záujmy základných práv a slobôd dotknutej osoby*“). Táto požiadavka má zásadný charakter, pretože sa ňou môže povoliť spracúvanie prevádzkových dát v osobitných prípadoch; nepovoľuje však subjektom, aby prevádzková dáta spracúvali hromadne.

83. Preformulované znenie pozmeňujúceho a doplňujúceho návrhu, ktoré vypracovala Rada, obsahuje prvky, ktoré si zasluhujú uznanie, ako napríklad zachovanie spojenia „*nevyhnutne potrebnom*“, ktorým sa zdôrazňuje obmedzený rozsah pôsobnosti uvedeného článku. Verzia Rady však neobsahuje záruky ochrany súkromia a údajov uvedené vyššie. Hoci ustanovenia na ochranu údajov v zásade platia nezávisle od osobitných odkazov v jednotlivých prípadoch, verziu článku 6 ods. 6a Rady možno vykladať ako ustanovenie, ktoré ponecháva úplne voľnú ruku pri rozhodovaní o všetkých prípadoch spracúvania prevádzkových údajov bez akýchkoľvek záruk ochrany súkromia alebo údajov. Možno preto argumentovať, že prevádzkové dáta možno zhromažďovať, uchovávať a ďalej používať bez toho, aby bolo nutné dodržiavať zásady ochrany údajov a osobitné povinnosti, ktoré sa inak vzťahujú na zodpovedné subjekty, ako je napríklad zásada kvality alebo povinnosť spravodlivého a zákonného spracúvania, ako aj povinnosť zachovávať dôvernosť a bezpečnosť údajov. Navyše, pretože v danom článku sa neodkazuje na platné zásady ochrany údajov, ktorými sa stanovujú časové obmedzenia uchovávania údajov, ani na konkrétne lehoty, verziu Rady možno vykladať ako ustanovenie, ktoré umožňuje zhromažďovanie a spracúvanie prevádzkových dát na bezpečnostné účely počas nešpecifikovaného časového obdobia.

84. Rada okrem toho oslabila ochranu súkromia v niektorých častiach textu, pretože použila formulácie, ktoré môžu byť vykladané voľnejšie. Napríklad sa odstránil odkaz na „*oprávnený záujem kontrolóra*“, čo vyvoláva pochybnosti o druhu subjektov, ktoré by mohli túto výnimku využívať. Je mimoriadne dôležité, aby sa predišlo tomu, aby tento pozmeňujúci a doplňujúci návrh mohol využívať ľubovoľný používateľ alebo právny subjekt.

85. Nedávne skúsenosti v EP a Rade ukazujú, že rozsah, v ktorom možno legálne spracúvať údaje na bezpečnostné účely, aj podmienky takéhoto spracúvania, je ťažko vymedziť zákonom. Žiaden už platný alebo v budúcnosti prijatý článok pravdepodobne neodstráni zjavné riziko príliš voľného uplatňovania výnimky z dôvodov, ktoré nesúvisia výlučne s bezpečnosťou, alebo subjektami, ktoré by túto výnimku využívať nemali. To neznamená, že inak by takéto spracúvaniu nebolo možné. Skutočnosť, či by ho bolo možné vykonať a v akom rozsahu, však možno lepšie posúdiť na úrovni vykonávania. Subjekty, ktoré chcú takéto spracúvanie vykonávať, by o jeho rozsahu a podmienkach mali rokovať s orgánmi na ochranu údajov a možno aj s pracovnou skupinou článku 29. Alternatívne by sa do smernice o elektronickom súkromí mohol začleniť článok, ktorým by sa umožnilo spracúvanie prevádzkových dát na bezpečnostné účely po výslovnom povolení orgánov na ochranu údajov.

86. Vzhľadom na to, že riziká, ktoré článok 6 ods. 6 predstavuje z hľadiska základného práva na ochranu údajov a súkromia jednotlivcov, ako aj na skutočnosť, že podľa tohto stanoviska nie je článok z právneho hľadiska potrebný, EDPS dospel k záveru, že najlepším výsledkom by bolo úplné vypustenie navrhovaného článku 6 ods. 6a.

87. Ak by sa napriek odporúčaniu EDPS prijalo akékoľvek uznesenie v zmysle ktorejkoľvek zo súčasných verzií článku 6 ods. 6a, v každom prípade by malo obsahovať záruky ochrany údajov uvedené vyššie. Tiež by sa malo riadne integrovať do súčasnej štruktúry článku 6, najlepšie ako nový odsek 2a.

V. **MOŽNOSŤ PRÁVNICKÝCH OSÔB PODÁVAŤ NÁVRHY NA ZAČATIE KONANIA VO VECI PORUŠENIA SMERNICE O ELEKTRONICKOM SÚKROMÍ**

88. EP prijal pozmeňujúci a doplňujúci návrh č. 133, ktorý dáva poskytovateľom pripojenia na internet a iným právnym subjektom, ako sú napr. spotrebiteľské združenia, možnosť podávať návrhy na začatie konanie vo veci porušenia ktoréhokoľvek z ustanovení smernice o elektronickom súkromí ([19]). Žiaľ, Komisia ani Rada ho neakceptovali. EDPS považuje uvedený návrh za veľmi kladný a odporúča jeho ponechanie.

89. Pri chápaní dôležitosti tohto návrhu je potrebné si uvedomiť, že v oblasti súkromia a ochrany údajov škoda, ktorá sa spôsobila jednotlivcovi, posudzovaná od prípadu k prípadu, zvyčajne sama osebe nepostačuje na to, aby daná jednotlivec podal návrh na začatie konania. Jednotlivci zvyčajne nechodia sami na súd pretože sa im doručuje spam, alebo pretože boli neoprávnene začlenení do zoznamu príjemcov. Uvedený návrh by umožňoval spotrebiteľským združeniam a odborom zastupujúcim záujmy spotrebiteľov na kolektívnej úrovni podávať návrhy na začatie konania v ich mene. Podpora širšieho dodržiavania ustanovení smernice o elektronickom súkromí by sa pravdepodobne dala dosiahnuť väčšou rozmanitosťou mechanizmov presadzovania, ktoré sú teda v záujme ich účinného uplatňovania.

90. V právnych rámcoch niektorých členských štátov existujú právne precedensy, ktorými sa už ustanovila možnosť kolektívneho uplatňovania nárokov na nápravu, aby sa spotrebiteľom alebo záujmovým skupinám umožnilo nárokovať si odškodnenie od subjektu, ktorý škodu spôsobil.

91. Zákony o hospodárskej súťaži ([20]) niektorých členských štátov okrem toho ustanovujú právo spotrebiteľov a záujmových skupín (navyše k dotknutému konkurenčnému subjektu) podať návrh na začatie konania proti subjektu, ktorý zákon porušil. Opodstatnením pre takýto prístup je skutočnosť, že spoločnosti porušujúce zákony o hospodárskej súťaži z takéhoto porušovania pravdepodobne profitujú, pretože spotrebitelia, ktorých škody sú marginálne, vo všeobecnosti s podaním žaloby váhajú. Takéto opodstatnenie možno primerane uplatňovať aj v oblasti ochrany údajov a súkromia.

92. Čo je dôležitejšie, ako sa uvádza vyššie, oprávnenie právnych subjektov, ako sú napr. spotrebiteľské združenia, na podávanie žalôb, podporuje postavenie spotrebiteľov a dodržiavanie právnych predpisov na ochranu údajov vo všeobecnej rovine. Ak budú spoločnosti, ktoré porušujú zákon, čeliť väčšiemu riziku súdnych sporov, pravdepodobne budú viac investovať do súladu s právnymi predpismi na ochranu údajov, čím sa v dlhodobom horizonte zvýši ochrana súkromia a spotrebiteľov. EDPS na základe všetkých uvedených príčin vyzýva EP a Radu, aby prijali ustanovenie, ktorým sa právnym subjektom umožní podávať návrhy na začatie konania vo veci porušenia ktoréhokoľvek z ustanovení smernice o elektronickom súkromí.

VI. **ZÁVER**

93. Spoločná pozícia Rady, prvé čítanie EP a zmenený a doplnený návrh Komisie obsahujú – v rozličnej miere – kladné prvky, ktoré by slúžili na posilnenie ochrany súkromia a osobných údajov jednotlivcov.

94. EDPS sa však domnieva, že priestor na zlepšenie existuje, najmä pokiaľ ide o spoločnú pozíciu Rady, v ktorej sa žiaľ neponechali niektoré z pozmeňujúcich a doplňujúcich návrhov EP, ktorých cieľom je pomôcť zabezpečiť primeranú úroveň ochrany súkromia a osobných údajov jednotlivcov. EDPS nalieha na EP a Radu, aby obnovili záruky súkromia navrhnuté v prvom čítaní EP.

95. EDSP sa okrem toho domnieva, že by bolo vhodné, aby sa niektoré ustanovenia smernice zracionalizovali. Obzvlášť to platí pre ustanovenia o narušení bezpečnosti, pretože EDPS sa nazdáva, že výhody vyplývajúce z oznamov o narušeniach bezpečnosti sa zúročia v plnej miere, ak bude právny rámec vhodne „nastavený“ od samotného začiatku. EDPS sa nakoniec domnieva, že formulácie niektorých ustanovení smernice by bolo vhodné zlepšiť a vyjasniť.

96. Vzhľadom na uvedené skutočnosti EDPS nalieha na EP a Radu, aby zintenzívnili úsilie o zlepšenie a vyjasnenie niektorých ustanovení smernice o elektronickom súkromí a súčasne obnovili pozmeňujúce a doplňujúce návrhy EP prijaté v prvom čítaní, ktorých cieľom je zabezpečiť primeranú úroveň ochrany súkromia a osobných údajov. V bodoch 97, 98, 99 a 100 sa preto sumarizujú otázky, ktoré je potrebné riešiť, a predkladajú sa v nich odporúčania a návrhy znenia. EDPS vyzýva všetky zúčastnené strany, aby tieto odporúčania a návrhy v procese smerujúcom k záverečnému prijatiu smernice o elektronickom súkromí zohľadnili.

Narušenia bezpečnosti

97. Európsky parlament, Komisia a Rada zaujali k oznamovaniu narušenia bezpečnosti odlišné postoje. Rozdiely medzi týmito troma modelmi sa týkajú okrem iného povinných subjektov, noriem alebo podmienok vzniku oznamovacej povinnosti, dotknutých osôb s právom byť informovaný atď. EP a Rada musia vyvinúť čo najväčšie úsilie o to, aby vypracovali solídny právny rámec pre inštitúciu narušenia bezpečnosti. Preto by mali:

([19]) Článok 13 ods. 6 prvého čítania EP.

([20]) Pozri napr. § 8 UWG – nemecký zákon o nekalej hospodárskej súťaži.

— *Zachovať* vymedzenie narušenia bezpečnosti uvedené v zneniach EP, Rady a Komisie, pretože je dostatočne široké na to, aby obsiahlo väčšinu relevantných situácií, v ktorých by mohlo byť potrebné oznamovať prípady narušenia bezpečnosti.

— Pokiaľ ide o subjekty, na ktoré sa má vzťahovať navrhovaná oznamovacia povinnosť, *začleniť* poskytovateľov služieb informačnej spoločnosti. Pravdepodobnosť, že sa on-line maloobchodní predajcovia, on-line banky, alebo on-line lekárne stanú terčom pokusov o narušenie bezpečnosti, je rovnaká ako v prípade telekomunikačných spoločností, ak nie väčšia. Občania budú očakávať nielen to, že im narušenia bezpečnosti budú oznamovať poskytovatelia pripojenia na internet, ale najmä, že im ich budú oznamovať ich on-line banky a on-line lekárne.

— Pokiaľ ide o podmienku vzniku oznamovacej povinnosti, spojenie *„dostatočná pravdepodobnosť poškodenia“* uvedené v zmenenom a doplnenom návrhu je vhodnou normou, ktorá zabezpečuje funkčnosť mechanizmu. Je však potrebné zabezpečiť, aby „poškodenie“ bol vymedzené dostatočne široko a vzťahovalo sa na všetky relevantné prípady negatívneho vplyvu na súkromie alebo iné legitímne záujmy jednotlivcov. Inak by bolo vhodnejšie vytvoriť novú normu, podľa ktorej by oznamovacia povinnosť vznikla *„ak je dostatočne pravdepodobné, že narušenie bude mať na jednotlivcov negatívny vplyv“*. Prístupom Rady, v rámci ktorého sa vyžaduje, aby narušenie *vážne* ovplyvnilo niekoho súkromie, by sa nezabezpečila dostatočná ochrana jednotlivcov, pretože takáto norma si vyžaduje, aby bol vplyv na súkromie „vážny“ Tým sa tiež otvára priestor pre subjektívne posudzovanie.

— I keď má zaangažovanie orgánov do rozhodovania o tom, či má povinný podnik daným jednotlivcom oznámenie poslať, pozitívne dôsledky, môže byť jeho uplatňovanie nepraktické a zložité a môže odlákať zdroje od ostatných dôležitých priorít. Ak by orgány neboli schopné reagovať extrémne rýchlo, EDSP sa obáva, že takýto systém by dokonca mohol ochranu jednotlivcov zmenšiť a dostať orgány pod neprimeraný tlak. EDPS teda z celkového hľadiska odporúča *zriadenie systému*, v rámci ktorého by skutočnosť, či je potrebné poslať oznámenie, posudzovali povinné subjekty.

— S cieľom umožniť orgánom vykonávať dozor na posudkami povinných subjektov týkajúcich sa skutočnosti, či je potrebné poslať oznámenie, *zaviesť* tieto záruky:

  — *zabezpečiť*, aby takéto subjekty povinne oznamovali orgánom všetky prípady narušenia bezpečnosti, ktoré napĺňajú príslušnú normu.

  — *ustanoviť* dozornú úlohu orgánov, ktorá im umožní konať v záujme efektívnosti selektívne. Použiť s týmto cieľom tento text: *„Ak dotknutému účastníkovi alebo jednotlivcovi zatiaľ nebol oznam poslaný, príslušný národný orgán môže po zvážení povahy narušenia prikázať PVSEK alebo PSIS, aby oznam poslal.“*

  — prijať nové ustanovenie, ktorým sa od subjektov bude vyžadovať, aby udržiavali podrobné a komplexné záznamy na účely auditu. Dalo by sa to dosiahnuť prijatím napríklad takéhoto textu: *„PVSEK a PSIS vedú a uchovávajú komplexné záznamy o všetkých narušeniach bezpečnosti, ktoré sa vyskytli, relevantné technické informácie, ktoré s nimi súvisia, ako aj záznamy o prijatých nápravných opatreniach. Záznamy musia obsahovať aj odkaz na všetky oznámenia vydané pre dotknutých účastníkov alebo jednotlivcov a príslušné národné orgány vrátane ich dátumu a obsahu. Záznamy sa na základe žiadosti predkladajú príslušnému orgánu.“*

— Aby sa zabezpečila jednotnosť pri vykonávaní rámca pre narušenia bezpečnosti, *umožniť* Komisii prijímať, po porade s EDPS, pracovnou skupinou článku 29 a inými relevantnými zainteresovanými stranami, technické vykonávacie opatrenia.

— Pokiaľ ide o jednotlivcov, ktorým sa majú poslať oznámenia, použiť termíny Komisie alebo EP, teda „príslušní jednotlivci“ alebo „postihnutí užívatelia“, pretože zahŕňajú všetkých jednotlivcov, ktorých osobné údaje boli ohrozené.

Verejne dostupné súkromné siete

98. Komunikačné služby sa verejnosti často ponúkajú nie cez verejné, ale cez súkromne prevádzkované siete (napr. prístupové body Wi-Fi, ktoré sú k dispozícii v hoteloch alebo na letiskách), na ktoré sa údajne smernica nevzťahuje. EP prijal pozmeňujúci a doplňujúci návrh č. 121 (článok 3), ktorým rozsah pôsobnosti smernice rozšíril na verejné a súkromné komunikačné siete, ako aj na verejne dostupné súkromné siete. EP a Rada by v tejto súvislosti mohli:

— *Zachovať* podstatu pozmeňujúceho a doplňujúceho návrhu č. 121, ale *zmeniť* jeho znenie tak, aby sa do rozsahu pôsobnosti smernice o elektronickom súkromí začlenilo *„spracúvanie osobných údajov v súvislosti s poskytovaním verejne dostupných služieb elektronickej komunikácie vo verejných komunikačných sieťach alebo súkromných komunikačných sieťach, ku ktorým má prístup verejnosť, v Spoločenstve“*. Čisto súkromne prevádzkované siete (na rozdiel od súkromných komunikačných sietí, ku ktorým má prístup verejnosť) by do rozsahu pôsobnosti výslovne nespadali.

— zodpovedajúcim spôsobom zmeniť a doplniť všetky príslušné ustanovenia tak, aby sa v nich výslovne odkazovalo okrem verejných sietí aj na verejne dostupné súkromné siete.

— *doplniť* vymedzenie v znení: „*verejne dostupná súkromná sieť je súkromne prevádzkovaná sieť, ku ktorej má široká verejnosť po odsúhlasení podmienok súvisiacich s jej používaním bežne neobmedzený prístup za poplatok alebo v rámci iných služieb alebo ponúk*.“ Zvýši sa tým právna istota vo vzťahu k subjektom, na ktoré sa bude vzťahovať nový rozsah pôsobnosti.

— *prijať* nové odôvodnenie, podľa ktorého by Komisia uskutočnila verejnú diskusiu o uplatňovaní smernice o elektronickom súkromí na všetky súkromné siete, pričom do nej prispeje EDPS, pracovná skupina článku 29 ďalšie relevantné zainteresované strany. EP a Rada by tiež mali uviesť, že Komisia by mala na základe verejnej diskusie vypracovať vhodný návrh na rozšírenie alebo obmedzenie druhov subjektov, na ktoré by sa mala smernica o elektronickom súkromí vzťahovať.

Spracúvanie prevádzkových dát na bezpečnostné účely

99. EP prijal v prvom čítaní pozmeňujúci a doplňujúci návrh č. 181 (článok 6 ods. 6a), ktorým povoľuje spracúvanie prevádzkových dát na bezpečnostné účely. Rada v spoločnej pozícii prijala nové znenie, ktorým sa niektoré záruky ochrany súkromia oslabili EDPS preto v tomto ohľade odporúča, aby EP a Rada:

— *zamietli* tento článok, pretože nie je potrebný a v prípade jeho zneužitia by mohol ohroziť ochranu údajov a súkromia jednotlivcov.

— Alternatívne, ak sa má nejaký variant súčasného znenia článku 6 ods. 6a predsa len prijať, EP a Rada by doňho mali *včleniť* záruky ochrany údajov uvedené v tomto stanovisku (podobné zárukám uvedeným v pozmeňujúcom a doplňujúcom návrhu EP).

Podávanie návrhov na začatie konania vo veci porušenia smernice o elektronickom súkromí

100. Parlament prijal pozmeňujúci a doplňujúci návrh č. 133 (článok 13 ods. 6), ktorý dáva právnym subjektom možnosť podávať návrhy na začatie konanie vo veci porušenia ktoréhokoľvek z ustanovení smernice o elektronickom súkromí. Rada ho nanešťastie nezachovala. Rada a EP by mali:

— *potvrdiť* ustanovenie, ktoré dáva právnym subjektom, ako sú napr. spotrebiteľské združenia a odbory, právo podávať návrhy na začatie konania vo veci porušenia ktoréhokoľvek z ustanovení smernice o elektronickom súkromí (nielen vo veci porušenia ustanovení o spame, čo je prístup, ktorý sa zaujal v spoločnej pozícii a zmenenom a doplnenom návrhu). Väčšou rozmanitosťou mechanizmov presadzovania sa podporí širšie dodržiavanie a účinné uplatňovanie ustanovení smernice o elektronickom súkromí ako celku.

Výzvy

101. EP a Rada musia vo všetkých uvedených otázkach čeliť výzve, ktorá pozostáva vo vypracovaní noriem a ustanovení, ktoré sú súčasne použiteľné v praxi, funkčné a ktoré rešpektujú práva na súkromie a ochranu údajov jednotlivcov. EDPS dúfa, že zúčastnené strany vyvinú maximálne úsilie o vyriešenie týchto výziev a že toto stanovisko k tomu prispeje.

V Bruseli 9. januára 2009

Peter HUSTINX

Európsky dozorný úradník pre ochranu údajov