I

(Uznesenia, odporúčania a stanoviská)

STANOVISKÁ

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV

Stanovisko európskeho dozorného úradníka pre ochranu údajov k 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)

(2008/C 181/01)

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 o voľnom pohybe týchto údajov ([1]),

so zreteľom na smernicu Európskeho parlamentu a Rady 2002/58 z 12. júla 2002 týkajúcu sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií ([2]),

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 ([3]),

so zreteľom na žiadosť Európskej komisie o stanovisko v súlade s článkom 28 ods. 2 nariadenia (ES) č. 45/2001, doručenú 16. novembra 2007,

PRIJAL TOTO STANOVISKO:

I. ÚVOD

1. Komisia 13. novembra 2007 prijala návrh smernice, ktorou sa okrem iných právnych predpisov mení a dopĺňa aj smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (ďalej len „návrh“ alebo „navrhované zmeny a doplnenia“). Na súčasnú verziu smernice 2002/58/ES sa obvykle, a to aj v tomto stanovisku, odkazuje ako na smernicu o elektronickom súkromí.

([1]) Ú. v. EÚ L 281, 23.11.1995, s. 31.
([2]) Ú. v. EÚ L 201, 31.7.2002, s. 37.
([3]) Ú. v. EÚ L 8, 12.1.2001, s. 1.

2. Cieľom návrhu je zvýšiť ochranu súkromia a osobných údajov jednotlivcov v sektore elektronických komunikácií. To sa nevykonáva celkovým prepracovaním súčasnej smernice o elektronickom súkromí, ale skôr navrhovaním jej zmien a doplnení *ad hoc*, pričom tieto zmeny a doplnenia sa zameriavajú na posilnenie ustanovení súvisiacich s bezpečnosťou a zlepšenie mechanizmov vynucovania práva.

3. Návrh je súčasťou širšej reformy piatich smerníc EÚ v oblasti telekomunikácií (ďalej len „telekomunikačný balík"). Komisia okrem návrhov na preskúmanie telekomunikačného balíka ([1]) zároveň prijala aj návrh nariadenia, ktorým sa zriaďuje Európsky úrad pre trh elektronických komunikácií ([2]).

4. Poznámky v tomto stanovisku sa obmedzujú na navrhované zmeny a doplnenia smernice o elektronickom súkromí, ak takéto navrhované zmeny a doplnenia nevychádzajú z koncepcií a ustanovení uvedených v návrhoch na preskúmanie telekomunikačného balíka. Okrem toho niektoré pripomienky uvedené v tomto stanovisku odkazujú na ustanovenia smernice o elektronickom súkromí, ktoré sa návrhom nemenia ani nedopĺňajú.

5. V tomto stanovisku sa zaoberáme nasledujúcimi témami: i) rozsah pôsobnosti smernice o elektronickom súkromí, konkrétne pokiaľ ide o dotknuté služby (navrhovaná zmena a doplnenie článku 3 ods. 1); ii) oznamovanie narušenia bezpečnosti (navrhované zmeny a doplnenia, ktorými sa dopĺňajú odseky 3 a 4 článku 4); iii) ustanovenia o cookies, spajvéri a podobných zariadeniach (navrhovaná zmena a doplnenie článku 5 ods. 3); iv) žaloby podané poskytovateľmi elektronických komunikačných služieb a inými právnickými osobami (navrhované zmeny a doplnenia, ktorými sa dopĺňa odsek 6 článku 13) a v) posilnenie ustanovení o vynucovaní práva (navrhované zmeny a doplnenia, ktorými sa dopĺňa článok 15a).

Konzultácia s EDPS a širšia verejná konzultácia

6. Komisia 16. novembra 2007 zaslala tento návrh EDPS. EDPS toto oznámenie chápe ako žiadosť o poskytnutie poradenstva inštitúciám a orgánom Spoločenstva v zmysle článku 28 ods. 2 nariadenia (ES) č. 45/2001 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov [ďalej len „nariadenie (ES) č. 45/2001"].

7. Komisia pred prijatím návrhu neformálne konzultovala jeho navrhované znenie s EDPS, čo EDPS uvítal, keďže mu to poskytlo príležitosť predložiť niekoľko návrhov k navrhovanému zneniu ešte predtým, ako ho Komisia prijala. EDPS je rád, že niektoré z jeho návrhov sa v navrhovanom znení zohľadnili.

8. Prijatiu návrhu predchádzala široká verejná konzultácia – postup, ktorý EDPS oceňuje. Komisia v júni 2006 začala verejnú konzultáciu o svojom oznámení o preskúmaní telekomunikačného balíka, v ktorom uviedla svoje názory na situáciu a predložila niekoľko návrhov zmien a doplnení ([3]). Pracovná skupina článku 29 pre ochranu údajov (ďalej len „PS 29"), ktorej je EDPS členom, využila túto príležitosť na to, aby vyjadrila svoje názory k navrhovaným zmenám a doplneniam v stanovisku prijatom 26. septembra 2006 ([4]).

([1]) Navrhované zmeny a doplnenia telekomunikačných smerníc sa predkladajú v týchto návrhoch: i) návrh smernice Európskeho parlamentu a Rady, ktorou sa mení a dopĺňa smernica 2002/21/ES o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby, smernica 2002/19/ES o prístupe a prepojení elektronických komunikačných sietí a príslušných zariadení a smernica 2002/20/ES o povolení na elektronické komunikačné sieťové systémy a služby, 13. novembra 2007, KOM(2007) 697 v konečnom znení; ii) návrh 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, 13. novembra 2007, KOM(2007) 698 v konečnom znení.

([2]) Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa zriaďuje Európsky úrad pre trh elektronických komunikácií, 13. novembra 2007, KOM(2007) 699 v konečnom znení.

([3]) Oznámenie o preskúmaní regulačného rámca EÚ pre elektronické komunikačné siete a služby [SEK(2006) 816], prijaté 29. júna 2006. K oznámeniu je priložený pracovný dokument útvarov Komisie [KOM(2006) 334 v konečnom znení].

([4]) Stanovisko 8/2006 k preskúmaniu regulačného rámca pre elektronickú komunikáciu a služby, zamerané najmä na smernicu o ochrane súkromia v sektore elektronickej komunikácie, prijaté 26. septembra 2006.

Celkový názor EDPS

9. Celkový názor EDPS na návrh je kladný. EDPS plne podporuje ciele Komisie spočívajúce v prijatí návrhu, ktorým sa zvyšuje ochrana súkromia a osobných údajov jednotlivcov v sektore elektronických komunikácií. EDPS víta najmä prijatie systému povinného oznamovania narušenia bezpečnosti (zmeny a doplnenia článku 4 smernice o elektronickom súkromí, ktorými sa dopĺňajú odseky 3 a 4). Oznámenie v prípade narušenia bezpečnosti v súvislosti s údajmi znamená jasné prínosy, zvyšuje zodpovednosť organizácií, je faktorom, ktorý núti spoločnosti zavádzať prísne bezpečnostné oparenia a z hľadiska ochrany informácií umožňuje určovanie najspoľahlivejších technológií. Okrem toho poskytuje poškodeným jednotlivcom príležitosť vykonať kroky na svoju ochranu pred krádežou totožnosti alebo iným zneužitím svojich osobných informácií.

10. EDPS víta ostatné zmeny a doplnenia v návrhu, ako napríklad možnosť právnických osôb s oprávneným záujmom podať žalobu na tých, ktorí porušujú niektoré ustanovenia smernice o elektronickom súkromí (zmeny a doplnenia článku 13, ktorými sa dopĺňa odsek 6). Pozitívne je aj posilnenie vyšetrovacích právomocí vnútroštátnych regulačných orgánov, keďže im umožní posúdiť, či spracovanie údajov je alebo nie je vykonávané v súlade so zákonom, ako aj určiť porušovateľov (doplnenie článku 15a ods. 3). Možnosť čo najskôr zastaviť nezákonné spracúvanie osobných údajov a porušovanie súkromia je nevyhnutným opatrením zameraným na ochranu práv a slobôd jednotlivcov. Na tento účel sa obzvlášť víta navrhovaný článok 15a ods. 2, v ktorom sa uznáva právomoc vnútroštátnych regulačných orgánov nariadiť zastavenie porušovania právnych predpisov, keďže im umožní okamžite ukončiť závažné nezákonné spracúvanie údajov.

11. Prístup vyplývajúci z návrhu, ako aj väčšina navrhovaných zmien a doplnení, sú v súlade s názormi na budúcu stratégiu v oblasti ochrany údajov, ktoré EDPS uviedol vo svojich predchádzajúcich stanoviskách, ako napríklad v stanovisku o vykonávaní smernice o ochrane údajov ([1]). Prístup sa okrem iného zakladá na presvedčení, že aj keď nie sú nevyhnutné nové zásady ochrany údajov, sú potrebné presnejšie pravidlá na riešenie otázok súvisiacich s ochranou údajov, ktoré priniesli nové technológie, ako internet, RFID atď., ako aj nástroje, ktoré prispejú k posilneniu a zefektívneniu právnych predpisov na ochranu údajov, ako sú napríklad právne predpisy umožňujúce právnickým osobám podať žalobu pre porušenie ochrany údajov a zaväzujúce kontrolórov údajov oznamovať narušenie bezpečnosti.

12. EDPS napriek celkovému kladnému prístupu vyplývajúcemu z návrhu vyjadruje poľutovanie nad tým, že návrh nie je taký ambiciózny, akým mohol byť. Uplatňovaním ustanovení uvedených v smernici o elektronickom súkromí od roku 2003, ako aj dôkladnou analýzou tejto otázky sa ukázalo, že niektoré ustanovenia smernice nie sú vôbec jasné, čo vytvára právnu neistotu a problémy s jej dodržiavaním. To je napríklad prípad týkajúci sa rozsahu, v akom sa smernica o elektronickom súkromí vzťahuje na poloverejných poskytovateľov elektronických komunikačných služieb. Očakávalo by sa, že Komisia by využila preskúmanie telekomunikačného balíka, a najmä smernice o elektronickom súkromí, aby vyriešila niektoré pretrvávajúce problémy. Návrh okrem toho pri riešení nových otázok, akou je napríklad zavedenie systému povinného oznamovania narušenia bezpečnosti, ponúka iba čiastočné riešenie, ktoré medzi organizácie povinné oznamovať narušenie bezpečnosti nezahŕňa subjekty, ako sú on-line banky a poskytovatelia on-line zdravotníckych služieb, ktoré spracúvajú veľmi citlivé typy údajov. EDPS vyjadruje poľutovanie nad týmto prístupom.

13. EDPS vyjadruje nádej, že zákonodarca pri prechode návrhu legislatívnym procesom vezme do úvahy pripomienky a návrhy uvedené v tomto stanovisku, smerujúce k vyriešeniu tých otázok, ktoré sa nepodarilo riešiť v návrhu Komisie.

([1]) Stanovisko európskeho dozorného úradníka pre ochranu údajov z 25. júla 2007 k oznámeniu Komisie Európskemu parlamentu a Rade o krokoch nadväzujúcich na pracovný program pre lepšie vykonávanie smernice o ochrane údajov (Ú. v. EÚ C 255, 27.10.2007, s. 1).

II. ANALÝZA NÁVRHU

II.1. Rozsah pôsobnosti smernice o elektronickom súkromí, konkrétne rozsahu dotknutých služieb

14. Kľúčovým problémom platnej smernice o elektronickom súkromí je otázka jej rozsahu uplatňovania. Návrh obsahuje niekoľko pozitívnych prvkov zameraných na vymedzenie a vyjasnenie rozsahu jeho pôsobnosti, konkrétne dotknutých služieb, ktorými sa ďalej zaoberáme v časti i). Navrhované zmeny a doplnenia však nanešťastie neriešia všetky existujúce problémy. Ako sa uvádza ďalej v časti ii), navrhované zmeny a doplnenia, žiaľ, nepredstavujú snahu o rozšírenie rozsahu uplatňovania smernice tak, aby zahŕňala elektronické komunikačné služby v súkromných sieťach.

15. V článku 3 smernice o elektronickom súkromí sa opisujú príslušné služby, inými slovami služby, na ktoré sa vzťahujú povinnosti ustanovené smernicou: „*Táto smernica sa vzťahuje na spracovávanie osobných údajov v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach*“.

16. Služby, ktorých sa smernica o elektronickom súkromí týka, sú preto službami verejných poskytovateľov elektronických komunikačných služieb vo verejných sieťach (providers of public electronic communication services – ďalej len „PPECS“). Vymedzenie PPECS sa ustanovuje v článku 2 písm. c) rámcovej smernice ([1]). Verejné komunikačné siete sa vymedzujú v článku 2 písm. d) rámcovej smernice ([2]). Príklady činnosti PPECS zahŕňajú poskytovanie prístupu k internetu, prenos informácií prostredníctvom elektronických sietí, mobilné a telefónne prepojenia atď.

i) *Navrhovaná zmena a doplnenie článku 3 smernice o elektronickom súkromí: Dotknuté služby majú zahŕňať verejné komunikačné siete podporujúce zariadenia na zber údajov a identifikačné zariadenia*

17. Návrhom sa mení a dopĺňa článok 3 smernice o elektronickom súkromí tým, že sa upresňuje, že verejné elektronické komunikačné siete zahŕňajú „*verejné komunikačné siete podporujúce zariadenia na zber údajov a identifikačné zariadenia*“. V odôvodnení 28 sa vysvetľuje, že vývoj systémov zahŕňajúcich zber informácií vrátane osobných údajov, ktoré používajú rádiové frekvencie, ako napríklad RFID, musí upravovať smernica o elektronickom súkromí, ak sú tieto systémy prepojené alebo využívajú verejné komunikačné siete alebo služby.

18. EDPS považuje toto ustanovenie za pozitívne, keďže vyjasňuje, že viacero systémov RFID patrí do pôsobnosti smernice o elektronickom súkromí, čím sa v súvislosti s týmto bodom odstraňuje určitá neistota a s konečnou platnosťou sa odstraňuje nesprávne pochopenie a nesprávny výklad práva.

19. Aj podľa súčasného článku 3 smernice o elektronickom súkromí sa táto smernica vzťahuje na niektoré systémy RFID. Dochádza k tomu z niekoľkých vzájomne súvisiacich dôvodov. Po prvé, pretože na systémy RFID sa vzťahuje vymedzenie elektronických komunikačných služieb. Po druhé, pretože sa prevádzkujú prostredníctvom elektronickej komunikačnej siete, pokiaľ sú tieto systémy podporované

([1]) Smernica Európskeho parlamentu a Rady (ES) 2002/21 zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (Ú. v. EÚ L 108, 24.4.2002, s. 33). Rámcovou smernicou sa vymedzuje, čo by sa malo rozumieť pod pojmom „elektronická komunikačná služba“, konkrétne: i) „Elektronická komunikačná služba“ je služba, ktorá sa bežne poskytuje za poplatok a ktorá pozostáva z prenosu signálov v sieťach a zahŕňa telekomunikačné a prenosové služby v sieťach. ii) Služby, ktoré poskytujú obsah prenášaný pomocou elektronických komunikačných sietí a služieb, sú vyňaté z vymedzenia elektronických komunikačných služieb. iii) Poskytovanie služieb je zriadenie, prevádzka, riadenie alebo sprístupňovanie siete. iv) Elektronické komunikačné služby nezahŕňajú služby informačnej spoločnosti vymedzené v smernici o elektronickom obchode ako služba/-y, ktorá sa bežne poskytuje za odmenu, na diaľku, elektronickým spôsobom a na základe individuálnej žiadosti príjemcu služieb.

([2]) Verejná komunikačná sieť je elektronická komunikačná sieť používaná úplne alebo prevažne na poskytovanie verejne dostupných elektronických komunikačných služieb.

prenosovým systémom, ktorý zabezpečuje bezdrôtový prenos signálov. A napokon, sieť môže byť verejná a súkromná. Ak je verejná, systémy RFID sa považujú za „dotknuté služby" a teda patria do pôsobnosti smernice o elektronickom súkromí. Navrhovaná zmena a doplnenie však odstráni všetky s tým súvisiace zostávajúce pochybnosti a tak poskytne väčšiu právnu istotu.

20. Ako sa ale uvádza v predchádzajúcom stanovisku EDPS k RFID ([1]), pokiaľ ide o RFID, toto ustanovenie nevylučuje možnú potrebu prijať dodatočné právne nástroje. Takéto opatrenia by sa však mali prijať v inom kontexte, nie ako súčasť tohto návrhu.

ii) *Potreba zahrnúť elektronické komunikačné služby do súkromných alebo polosúkromných sietí*

21. Zatiaľ čo EDPS víta vyššie uvedené vyjasnenie, vyjadruje poľutovanie nad tým, že návrh nerieši otázku stále neurčitejšieho rozlíšenia medzi súkromnými a verejnými sieťami. EDPS ďalej vyjadruje poľutovanie nad tým, že vymedzenie služieb, na ktoré sa vzťahuje smernica o elektronickom súkromí, sa nerozšírilo tak, aby zahŕňalo aj súkromné siete. Článok 3 ods. 1 smernice o elektronickom súkromí sa v súčasnom znení vzťahuje iba na *elektronické komunikačné služby vo verejných sieťach*.

22. EDPS si všíma tendenciu, v dôsledku ktorej sa služby stávajú stále viac kombináciou súkromných a verejných služieb. Ako príklad možno uviesť univerzity, ktoré tisíckam študentov umožňujú používať internet a elektronickú poštu. Schopnosť týchto poloverejných (alebo polosúkromných) sietí obmedzovať súkromie jednotlivcov je zjavná a preto si vyžaduje, aby tento typ služieb podliehal rovnakému súboru pravidiel, aké sa uplatňujú výhradne na verejné siete. Okrem toho súkromné siete, ako napríklad siete zamestnávateľov poskytujúcich zamestnancom prístup k internetu, hotelov alebo majiteľov apartmánov poskytujúcich hosťom telefón alebo elektronickú poštu, ako aj internetových kaviarní, majú vplyv na ochranu údajov a súkromia svojich používateľov, čo znamená, že aj na ne by sa mala vzťahovať pôsobnosť smernice o elektronickom súkromí.

23. Judikatúra niektorých členských štátov už v skutočnosti uplatňuje v súvislosti s elektronickými komunikačnými službami poskytovanými v súkromných sieťach rovnakú povinnosti, ako v prípade služieb poskytovaných vo verejných sieťach ([2]). Aj podľa nemeckého zákona dospeli orgány na ochranu údajov k záveru, že umožnenie používať súkromnú elektronickú poštu v rámci spoločnosti môže zapríčiniť, že táto spoločnosť sa bude považovať za prevádzkovateľa verejných telekomunikačných služieb a teda sa na ňu budú vzťahovať ustanovenia smernice o elektronickom súkromí.

24. Skrátka, rastúci význam zmiešaných (súkromno-verejných) a súkromných sietí v každodennom živote, s úmerne rastúcim rizikom pre osobné údaje a súkromie, oprávňuje potrebu uplatňovať na takéto služby rovnaký súbor pravidiel, aké sa uplatňujú na verejné elektronické komunikačné služby. EDPS sa domnieva, že na tento účel by sa mala smernica zmeniť a doplniť, aby sa rozšíril rozsah jej pôsobnosti tak, aby zahŕňal takéto typy súkromných služieb; s týmto názorom sa stotožňuje aj pracovná skupina článku 29 ([3]).

II.2. **Oznamovanie narušenia bezpečnosti: zmena a doplnenie článku 4**

25. Článok 4 smernice o elektronickom súkromí sa mení a dopĺňa dvomi novými odsekmi (3 a 4), ktorými sa ustanovuje povinnosť oznamovať narušenie bezpečnosti. Podľa článku 4 ods. 3 musia teda PPECS na jednej strane bezodkladne informovať vnútroštátne regulačné orgány o každom narušení bezpečnosti vedúcom k náhodnému alebo nezákonnému zničeniu, strate, pozmeneniu, nepovolenému zverejneniu alebo sprístupneniu osobných údajov prenášaných, uchovávaných alebo iným spôsobom spracúvaných v spojení s poskytovaním elektronických komunikačných služieb (súhrnne „ohrozenie údajov"); na druhej strane PPECS musia informovať aj svojich zákazníkov.

([1]) Stanovisko z 20. decembra 2007 k oznámeniu Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov o rádiofrekvenčnej identifikácii (RFID) v Európe: kroky k politickému rámcu KOM(2007) 96.

([2]) Napríklad v rozsudku parížskeho odvolacieho súdu vo veci *BNP Paribas* v *World Press Online* vynesenom 4. februára 2005 sa uvádza, že nie je rozdiel medzi poskytovateľmi internetových služieb, ktorí poskytovali prístup k internetu na komerčnom základe, a zamestnávateľmi, ktorí poskytovali prístup k internetu svojim zamestnancom.

([3]) Stanovisko 8/2006 k preskúmaniu regulačného rámca pre elektronickú komunikáciu a služby, zamerané najmä na smernicu o ochrane súkromia v sektore elektronickej komunikácie, prijaté 26. septembra 2006.

Prínosy tejto povinnosti

26. EDPS víta tieto ustanovenia (článok 4 ods. 3 a 4), ktorými sa zavádza povinné oznamovanie narušenia bezpečnosti. Oznamovanie narušenia bezpečnosti má z hľadiska ochrany osobných údajov a súkromia pozitívne účinky, čo sa už odskúšalo v Spojených štátoch, kde sú právne predpisy o oznamovaní narušenia bezpečnosti v platnosti už niekoľko rokov.

27. Po prvé, právne predpisy o oznamovaní narušenia bezpečnosti zvyšujú zodpovednosť PPECS, pokiaľ ide o informácie, ktoré boli ohrozené. Zodpovednosť v rámci stratégie ochrany údajov alebo súkromia znamená, že každá organizácia je zodpovedná za informácie, o ktoré sa stará a ktoré má pod kontrolou. Oznamovacia povinnosť je na jednej strane rovnocenná s opätovným vyhlásením, že údaje, ktoré boli ohrozené, sú pod kontrolou PPECS, a že na strane druhej je zodpovednosťou tejto organizácie prijať v súvislosti s takýmito údajmi potrebné opatrenia.

28. Po druhé, ukázalo sa, že existencia oznamovania narušenia bezpečnosti je faktorom, ktorý povzbudzuje investície do bezpečnosti v organizáciách, ktoré spracúvajú osobné údaje. Skutočne už len samotný fakt, že organizácie musia verejne oznamovať narušenie bezpečnosti spôsobuje, že zavádzajú prísnejšie bezpečnostné normy, ktoré chránia osobné informácie a zabraňujú narušeniu bezpečnosti. Oznamovanie narušenia bezpečnosti okrem toho pomôže určovať a vykonávať spoľahlivú štatistickú analýzu, pokiaľ ide o najúčinnejšie bezpečnostné riešenia a mechanizmy. Dlhý čas existoval nedostatok „tvrdých“ údajov o zlyhaní bezpečnosti informácií a nedostatok najvhodnejších technológií na ochranu informácií. Tento problém povinnosť oznamovať narušenie bezpečnosti pravdepodobne vyrieši, ako tomu bolo v prípade zákonov o oznamovaní narušenia bezpečnosti v USA, pretože oznamovaním sa poskytnú informácie o technológiách, ktorá dokážu účinnejšie brániť narušeniu bezpečnosti ([1]).

29. A napokon, vďaka oznamovaniu narušenia bezpečnosti sú si jednotlivci vedomí rizík, ktorým čelia, keď sú ich osobné údaje ohrozené, pričom im zároveň pomáha prijať opatrenia nevyhnutné na zmiernenie takéhoto rizika. Ak boli ohrozené napríklad bankové údaje, jednotlivec, ktorý bol informovaný, sa môže rozhodnúť, že zmení prístupové údaje k svojmu bankovému účtu, aby zabránil niekomu získať a zneužiť ich na nezákonné účely (čo sa obvykle označuje ako „krádež totožnosti“). Ak to zhrnieme, táto povinnosť znižuje pravdepodobnosť, že sa jednotlivci stanú obeťami krádeže totožnosti a môže tiež obetiam pomôcť prijať opatrenia potrebné na riešenie problémov.

Nedostatok navrhovanej zmeny a doplnenia

30. Aj keď EDPS vyjadruje potešenie v súvislosti so systémom oznamovania narušenia bezpečnosti, ktorý sa ustanovuje v článku 4 ods. 3 a 4, uprednostnil by ich uplatňovanie v širšom rozsahu, aby zahŕňali aj poskytovateľov služieb informačnej spoločnosti. To by znamenalo, že zákon by sa vzťahoval aj na on-line banky, on-line podnikateľské subjekty, on-line poskytovateľov zdravotníckych služieb atď. ([2]).

31. Dôvody, ktoré oprávňujú, aby sa oznamovanie narušenia bezpečnosti uplatňovalo aj na poskytovateľov verejných elektronických komunikačných služieb, t. j. PPECS, existujú aj v prípade iných organizácií, ktoré tiež spracúvajú veľké počty osobných údajov, ktorých zverejnenie môže dotknuté osoby obzvlášť poškodiť. Týka sa to on-line bánk, sprostredkovateľov údajov a iných on-line poskytovateľov, ako napríklad tých, ktorí spracúvajú citlivé údaje (ktoré zahŕňajú zdravotné údaje, politické názory a pod.). Zneužitie informácií, ktorými disponujú banky a on-line podnikateľské subjekty, ktoré sa môže týkať nielen čísiel bankových účtov, ale aj údajov kreditných kariet, môže spôsobiť krádež totožnosti, pričom v takom prípade je pre jednotlivca podstatné, aby bol informovaný s cieľom prijať potrebné opatrenia. Ak by v druhom prípade (on-line zdravotnícke služby) nebola spôsobená finančná škoda, určite jednotlivci by pri zneužití citlivých informácií pravdepodobne utrpeli inú ako hospodársku škodu.

([1]) Pozri správu „*Ekonomika bezpečnosti a vnútorný trh*“, ktorú na objednávku ENISA vypracovali prof. Ross Anderson, Rainer Böhme, Richard Clayton a Tyler Moore. Správa je k dispozícii na: http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Poskytovatelia služieb informačnej spoločnosti sa vymedzujú v smernici o elektronickom obchode ako služba/-y, ktorá sa bežne poskytuje za odmenu, na diaľku, elektronickým spôsobom a na základe individuálnej žiadosti príjemcu služieb.

32. Zväčšením rozsahu tejto povinnosti sa okrem toho vyššie opísané prínosy, očakávané na základe uloženia tejto povinnosti, neobmedzia iba na jeden sektor činnosti, a to sektor poskytovateľov verejne dostupných elektronických komunikačných služieb, ale všeobecne sa rozšíria na služby informačnej spoločnosti. Uloženie povinnosti oznamovať narušenie bezpečnosti poskytovateľom služieb informačnej spoločnosti, akými sú on-line banky, nielen zvýši ich zodpovednosť, ale bude tiež motivovať takýchto aktérov, aby posilnili svoje bezpečnostné opatrenia a zabránili tak možnému narušeniu bezpečnosti v budúcnosti.

33. Existujú iné prípady, v ktorých sa smernica o elektronickom súkromí už uplatňuje na iné subjekty než PPECS, ako napríklad podľa článku 4 o dôvernosti správ a článku 13 o spame. To potvrdzuje, že zákonodarca sa v minulosti veľmi múdro rozhodol rozsah uplatňovania určitých ustanovení smernice o elektronickom súkromí rozšíriť, pretože bol presvedčený, že je to vhodné a potrebné. EDPS vyjadruje nádej, že v súčasnosti zákonodarca nebude váhať a zaujme podobne citlivý a pružný prístup a rozšíri rozsah uplatňovania článku 4 tak, aby zahŕňal poskytovateľov služieb informačnej spoločnosti. Na tento účel by postačovalo vložiť do článku 4 ods. 3 takýto odkaz na poskytovateľov služieb informačnej spoločnosti: „Ak dôjde k narušeniu bezpečnosti vedúcemu k náhodnému alebo … poskytovateľ verejne dostupných elektronických komunikačných služieb a poskytovateľ služieb informačnej spoločnosti … o takomto narušení informuje dotknutého účastníka a vnútroštátny regulačný orgán“.

34. EDPS vníma túto povinnosť a jej uplatňovanie na PPECS, ako aj na poskytovateľov služieb informačnej spoločnosti, ako prvý krok vývoja, ktorý sa napokon môže vzťahovať všeobecne na všetkých kontrolórov údajov.

Osobitný právny rámec pre narušenie bezpečnosti, ktorý sa má riešiť prostredníctvom komitológie

35. Návrh nerieši viacero otázok týkajúcich sa povinnosti poskytovať oznámenie o narušení bezpečnosti. Príkladmi otázok, ktoré je potrebné riešiť, sú okolnosti oznámenia, forma a príslušné postupy. Namiesto toho sa článkom 4 ods. 4 návrhu ponechávajú tieto rozhodnutia na prijatie prostredníctvom „komitologického“ výboru ([1]), konkrétne Výboru pre komunikácie, ktorý sa zriadil podľa článku 22 rámcovej smernice na základe rozhodnutia Rady z 28. júna 1999. Takéto opatrenia by sa prijímali konkrétne v súlade s článkom 5 rozhodnutia Rady z 28. júna 1999, v ktorom sa ustanovujú pravidlá regulačného postupu, pokiaľ ide o „*opatrenia so všeobecnou pôsobnosťou určené na uplatňovanie podstatných ustanovení základných právnych aktov*“.

36. EDPS nie je proti možnosti ponechať všetky tieto otázky na vykonávacie právne predpisy. Prijatie právneho predpisu prostredníctvom komitologického postupu pravdepodobne skráti legislatívny proces. Komitológia tiež pomôže zaistiť harmonizáciu, ktorá je určite žiadaným cieľom.

37. Ak sa berie do úvahy veľký počet otázok, ktorými sa bude potrebné zaoberať vo vykonávacích opatreniach, ako aj ich význam, ako sa zvýrazňuje ďalej, zdá sa byť vhodné riešiť ich radšej spoločne jedným právnym predpisom, než po častiach – v dôsledku čoho by sa niektoré otázky riešili v smernici o elektronickom súkromí a riešenie iných by sa ponechalo na vykonávacie právne predpisy. Preto je potrebné uvítať prístup Komisie, ktorý spočíva v ponechaní týchto rozhodnutí na vykonávacie právne predpisy, ktoré sa prijmú po konzultácii s EDPS a snáď aj s inými zúčastnenými stranami (pozri nasledujúci bod).

Otázky, ktoré bude potrebné riešiť prostredníctvom vykonávacích opatrení

38. Význam vykonávacích opatrení sa zvýrazňuje, ak dokážeme podrobne predvídať otázky, ktoré bude potrebné riešiť prostredníctvom vykonávacích opatrení. Vykonávacie opatrenia môžu určiť normy, na základe ktorých sa oznámenia musia doručovať. Budú napríklad určovať, čo predstavuje narušenie bezpečnosti, podmienky, na základe ktorých sa musia doručovať oznámenia jednotlivcom a orgánom, lehotu oznamovania.

([1]) Zákonodarné postupy v ES, na ktorých sa zúčastňujú výbory zložené zo zástupcov vlád členských štátov na úrovni štátnych zamestnancov.

39. EDPS sa domnieva, že smernica o elektronickom súkromí a najmä článok 4 by nemali obsahovať žiadnu výnimku z oznamovacej povinnosti. EDPS v tejto súvislosti potešil prístup Komisie vyjadrený v článku 4, v ktorom sa ustanovuje oznamovacia povinnosť a nepredpokladá sa žiadna výnimka z tohto ustanovenia, no umožňuje sa riešiť túto a iné otázky prostredníctvom vykonávacích právnych predpisov. Hoci si EDPS uvedomuje argumenty, ktoré by mohli oprávňovať ustanovenie určitých výnimiek z tejto povinnosti, uprednostňuje, aby sa táto a iné otázky dôkladne riešili prostredníctvom vykonávacích právnych predpisov po dôkladnej a komplexnej diskusii o všetkých predmetných otázkach. Ako sa už uviedlo, komplexný charakter otázok týkajúcich sa povinnosti poskytovať oznámenie narušenia bezpečnosti vrátane toho, či sú vhodné výnimky a obmedzenia, si vyžaduje jednotný prístup, t. j. prostredníctvom jedného právneho predpisu, ktorý sa zaoberá výhradne touto otázkou.

Konzultácia s EDPS a potreba rozšírenia konzultácie

40. Ak sa zohľadní rozsah, v ktorom vykonávacie opatrenia ovplyvnia ochranu osobných údajov jednotlivcov, je potrebné, aby sa Komisia pred prijatím týchto opatrení zapojila do vhodného procesu konzultácií. Z tohto dôvodu EDPS víta článok 4 ods. 4 návrhu, v ktorom sa výslovne ustanovuje, že Komisia pred prijatím vykonávacích opatrení konzultuje s európskym dozorným úradníkom pre ochranu údajov. Také opatrenia sa budú nielenže týkať ochrany osobných údajov a súkromia jednotlivcov, ale budú mať na ňu aj významný vplyv. Preto je dôležité žiadať EDPS o poradenstvo, ako sa to vyžaduje na základe článku 41 nariadenia (ES) č. 45/2001.

41. Okrem konzultácie s EDPS by možno bolo vhodné doplniť ustanovenie o tom, že v záujme získania poradenstva a podpory výmeny skúseností s najlepšími postupmi v týchto záležitostiach bude návrh vykonávacích opatrení predmetom verejnej konzultácie. To poskytne nielen odvetviu, ale aj iným zúčastneným stranám vrátane ostatných orgánov pre ochranu údajov a pracovnej skupine článku 29 vhodný prostriedok na predkladanie ich názorov. Potreba verejnej konzultácie sa zvýrazňuje, ak si uvedomíme, že tieto právne predpisy sa prijímajú na základe komitologického postupu, a teda s obmedzenou účasťou Európskeho parlamentu.

42. EDPS berie na vedomie, že v článku 4 ods. 4 sa predpokladá, že Komisia bude pred prijatím vykonávacích pravidiel konzultovať aj s Úradom pre trh elektronických komunikácií. EDPS v tejto súvislosti oceňuje zásadu konzultovať s Úradom pre trh elektronických komunikácií ako depozitárom skúseností a znalostí ENISA v oblasti otázok bezpečnosti sietí a informácií. V navrhovanej zmene a doplnení (článok 4 ods. 4) sa do zriadenia Úradu pre trh elektronických komunikácií môže ako vhodné prechodné riešenie ustanoviť konzultácia s ENISA.

II.3. **Ustanovenie o cookies, spajvéri a podobných zariadeniach: zmena a doplnenie článku 5 ods. 3**

43. V článku 5 ods. 3 sa rieši otázka technológií, ktoré umožňujú prístup k informáciám a uchovávanie informácií v koncovom zariadení užívateľa prostredníctvom elektronických komunikačných sietí. Príkladom uplatňovania článku 5 ods. 3 je používanie cookies ([1]). Iné príklady sa týkajú používania technológií, ako je spajvér (skryté špionážne programy) a trójske kone (programy skryté v správach alebo iných zjavne nevinných softvéroch). Ciele takýchto technológií a účely sú mimoriadne rôznorodé – zatiaľ čo niektoré sú dokonale neškodné alebo dokonca pre užívateľa užitočné, iné ciele sú jasne veľmi škodlivé a ohrozujúce.

([1]) Cookies sa ukladajú prostredníctvom ISSP (prevádzkovateľov webových stránok) v koncovom zariadení užívateľa na rôzne účely, vrátane identifikácie návštevníka, keď opätovne navštevuje webové miesto. Ak sa v praxi cookie zasiela užívateľovi internetu prostredníctvom webového miesta, počítaču užívateľa sa pridelí špecifické číslo (napr. počítač, ktorému sa doručili cookies z webového miesta A sa stáva „počítačovým držiteľom cookie 111“). Webové miesto si toto číslo ponechá ako referenčný údaj. Ak užívateľ alebo užívatelia počítača, ktorý obdržal cookie 111, nevymažú súbor cookies, pri ďalšej návšteve rovnakého webového miesta bude toto miesto schopné identifikovať tento počítač ako držiteľa cookie 111. Webové miesto si prirodzene odvodí, že tento počítač ho už v minulosti navštívil. Mechanizmus, ktorý webovému miestu umožňuje identifikáciu počítača ako opakovaného návštevníka, je jednoduchý. Ak navštevujúci počítač drží cookies, ako je cookie 111, a navštívi miesto, ktoré pri predchádzajúcej návšteve toto cookie vytvorilo, prehľadá pevný disk užívateľa s cieľom nájsť číslo súboru tohto cookie. Ak užívateľov prehľadávač nájde súbor cookie, ktorý zodpovedá referenčnému číslu, ktoré si vedie webové miesto, informuje webové miesto o tom, že počítač uchováva cookie 111.

44. V článku 5 ods. 3 smernice o elektronickom súkromí sa ustanovujú podmienky, ktoré sa uplatňujú pri získaní prístupu ku koncovému zariadeniu alebo uchovávaní informácií na koncovom zariadení užívateľov s použitím, okrem iného, uvedených technológií. Podľa článku 5 ods. 3 sa najmä i) používateľom internetu musia poskytnúť jasné a komplexné informácie v súlade so smernicou 95/46/ES, medzi iným aj o účeloch spracovania a ii) používateľom internetu sa musí umožniť odmietnuť takéto spracovanie, t. j. umožniť zvoliť si, aby sa informácie získané z ich koncového zariadenia nespracúvali.

Prínosy navrhovanej zmeny a doplnenia

45. V súčasnom článku 5 ods. 3 smernice o elektronickom súkromí sa obmedzuje rozsah jeho uplatňovania na situácie, keď sa prístup k informáciám a uchovávanie informácií v koncovom zariadení užívateľa vykonáva prostredníctvom *elektronických komunikačných sietí*. To zahŕňa vyššie opísanú situáciu v súvislosti s používaním cookies, ako aj iných technológií, ako spajvér, ktoré sa prenášajú prostredníctvom elektronických komunikačných sietí. Vôbec však nie je jasné, či sa článok 5 ods. 3 uplatňuje v situáciách, keď sa podobné technológie (cookies/spajvér a im podobné) distribuujú prostredníctvom softvéru, ktorý sa poskytuje na externých médiách na uchovávanie údajov, a sťahujú do koncového zariadenia užívateľa. Ak sa vezme do úvahy, že ohrozenie súkromia existuje nezávisle od komunikačného kanála, obmedzenie článku 5 ods. 3 iba na jeden komunikačný kanál je nešťastné.

46. EDPS preto vyjadruje potešenie nad zmenou a doplnením článku 5 ods. 3, ktorým sa vďaka odstráneniu odkazu na „elektronické komunikačné siete“ v skutočnosti rozšíril rozsah uplatňovania článku 5 ods. 3. Zmenená a doplnená verzia článku 5 ods. 3 zahŕňa obe situácie, v ktorých sa tak prístup k informáciám, ako aj ich uchovávanie v koncovom zariadení užívateľa, vykonáva prostredníctvom elektronických komunikačných sietí, ale aj prostredníctvom iných externých médií na uchovávanie údajov, akými sú CD, CD-ROM, USB kľúče atď.

Technické uloženie na účel uľahčenia prenosu

47. Posledná veta článku 5 ods. 3 smernice o elektronickom súkromí zostáva vo svojej zmenenej a doplnenej verzii nezmenená. Podľa tejto poslednej vety požiadavka prvej vety článku 5 ods. 3 *„nebráni akémukoľvek technickému uloženiu alebo prístupu na účely výlučne výkonu alebo uľahčenia prenosu správy prostredníctvom elektronickej komunikačnej siete alebo, ak je to nevyhnutne potrebné, na poskytovanie služieb informačnej spoločnosti …“*. Záväzné pravidlá prvej vety článku 5 ods. 3 (potreba poskytnúť informácie a možnosť odmietnuť) sa teda nebudú uplatňovať, ak jediným účelom prístupu ku koncovému zariadeniu užívateľa alebo uloženia informácií je *uľahčenie* prenosu, alebo ak je to potrebné výlučne na poskytovanie služieb informačnej spoločnosti, ktoré vyžaduje užívateľ.

48. V smernici sa neuvádza, kedy je jediným účelom prístupu alebo uloženia informácií uľahčenie prenosu alebo poskytnutie informácií. Situáciou, ktorej sa táto výnimka jasne týka, je zriadenie pripojenia k internetu. Je to preto, lebo na zriadenie pripojenia k internetu je potrebné získať IP adresu ([1]). Poskytovateľ prístupu k internetu požiada počítač koncového užívateľa, aby mu o sebe uviedol určité informácie a poskytovateľ prístupu k internetu následne poskytne počítaču IP adresu. V tomto prípade sa informácie uložené v koncovom zariadení koncového užívateľa prenesú k poskytovateľovi prístupu k internetu s cieľom poskytnúť tomuto užívateľovi prístup k internetu. V tomto prípade sa na poskytovateľa prístupu k internetu nevzťahuje povinnosť oznámiť toto získanie informácií, ani poskytnúť právo odmietnuť, pokiaľ je to potrebné na poskytnutie tejto služby.

49. Ak si užívateľ chce prezerať dané webové miesto a už bol pripojený k internetu, musí zaslať požiadavku serveru, ktorý toto webové miesto hostí. Tento server bude reagovať, ak vie, kam má zaslať informácie, t. j. ak pozná IP adresu užívateľa. Kvôli spôsobu, ako sa táto adresa uchováva, webové miesto, ktoré chce užívateľ navštíviť, sa opäť požiada, aby vykonalo prístup k informáciám na koncovom zariadení používateľa internetu. Aj táto transakcia by jasne patrila medzi výnimky. Zdá sa byť skutočne vhodné, aby sa na tieto prípady nevzťahovali požiadavky článku 5 ods. 3.

([1]) IP adresa (Internet Protocol address) je jedinečnou adresou, ktorú určité elektronické zariadenia používajú na vzájomnú identifikáciu a komunikáciu v počítačovej sieti využívajúcej normu internetového protokolu (IP) – ide jednoducho o počítačovú adresu. Každé účastnícke sieťové zariadenie – vrátane smerovačov, prepínačov, počítačov, infraštruktúrnych serverov (napr. NTP, DNS, DHCP, SNMP atď.), tlačiarní, internetových faxov a niektorých telefónov – môže mať svoju vlastnú adresu, ktorá je v rámci konkrétnej siete jedinečná. Niektoré IP adresy by mali byť jedinečné v rámci globálneho internetu, zatiaľ čo iné musia byť jedinečné iba v rámci podniku.

50. EDPS považuje za vhodnú výnimku z potreby informovať a z poskytnutia možnosti odmietnuť v situáciách, akými sú uvedené príklady, ak je technické uloženie alebo prístup ku koncovému zariadeniu užívateľa *nevyhnutný* výlučne na účel vykonania prenosu správy v elektronickej komunikačnej sieti. To isté platí aj vtedy, ak je technické uloženie alebo prístup nevyhnutný výlučne v záujme poskytovania služieb informačnej spoločnosti. EDPS však nepovažuje za potrebné vyňatie z povinnosti poskytovať informácie a ponúkať právo odmietnuť v tých situáciách, v ktorých je účelom technického uloženia alebo prístupu iba *uľahčenie* prenosu správ. Napríklad podľa poslednej vety tohto článku nesmie dotknutá osoba využívať informácie a právo odmietnuť spracovanie svojich údajov, ak cookies zachytávajú jej jazykové preferencie alebo polohu (napr. Belgicko, Čína), keďže tento druh cookies sa môže uvádzať ako cookies, ktorých účelom je uľahčenie prenosu správ. EDPS si je vedomý, že na úrovni softvéru sa v praxi dotknutým osobám poskytuje možnosť odmietnuť alebo upraviť uchovávanie cookies. To však nemá dostatočne jasnú oporu v žiadnom právnom ustanovení, ktoré by dotknutú osobu oprávňovalo brániť v uvedenom kontexte svoje práva.

51. EDPS s cieľom zabrániť takémuto výsledku navrhuje vykonať menšiu zmenu a doplnenie poslednej časti článku 5 ods. 3 spočívajúce vo vymazaní slova „uľahčenie“ z poslednej vety: „*To nebráni akémukoľvek technickému uloženiu alebo prístupu na účely výkonu alebo uľahčenia prenosu správy v elektronickej komunikačnej sieti alebo, ak je to nevyhnutne potrebné, na zabezpečenie služby informačnej spoločnosti …*“.

II.4. **Žaloby podané PPECS a právnickými osobami: doplnenie odseku 6 do článku 13**

52. V navrhovanom článku 13 ods. 6 sa ustanovujú občianskoprávne opravné prostriedky pre každú fyzickú alebo právnickú osobu, ktorá má oprávnený záujem, a to najmä pre poskytovateľov elektronických komunikačných služieb, v ktorých obchodnom záujme je bojovať proti tým, ktorí porušujú článok 13 smernice o elektronickom súkromí. Tento článok sa zaoberá zasielaním nevyžiadaných komerčných správ.

53. Navrhovaná zmena a doplnenie napríklad umožní poskytovateľom prístupu k internetu, aby bojovali proti šíriteľom spamu z dôvodu zneužívania svojich sietí, aby podávali žaloby na subjekty, ktoré falšujú adresy odosielateľov alebo prenikajú do serverov s cieľom používať ich na preposielanie spamu atď.

54. Smernica o elektronickom súkromí nebola jasná v tom, či poskytuje PPECS právo podať žalobu voči spamerom, pričom PPECS iba vo veľmi malom počte prípadov podali žalobu na súd pre porušenie článku 13 v znení ustanovenom v právnych predpisoch členských štátov ([1]). Tým, že návrh uznáva dôvod žaloby poskytovateľov elektronických komunikačných služieb na ochranu svojich obchodných záujmov zároveň potvrdzuje, že zámerom smernice o elektronickom súkromí je ochrana nielen jednotlivých účastníkov, ale aj poskytovateľov elektronických komunikačných služieb.

55. EDPS vyjadruje spokojnosť s tým, že návrhom sa pre poskytovateľov elektronických komunikačných služieb ustanovuje možnosť mať obchodný záujem na podaní žaloby voči spamerom. Okrem výnimočných okolností jednotliví účastníci nemajú peniaze ani stimuly na podanie žaloby tohto druhu na súd. Naopak poskytovatelia prístupu k internetu a iní PPECS majú finančnú silu a technologickú spôsobilosť na to, aby vyšetrovali spamové kampane, identifikovali narušiteľov a zdá, že je len vhodné, aby mali právo podávať žaloby proti spamerom.

56. EDPS oceňuje navrhované zmeny a doplnenia, najmä pokiaľ by umožňovali aj združeniam spotrebiteľov a odborovým zväzom zastupujúcim záujmy spotrebiteľov, ktorým sa hromadne zasielajú nevyžiadané správy, aby v ich mene podávali žaloby na súdy. Ako sa už uviedlo, škoda spôsobená dotknutej osobe, ktorej sa zasiela spam, ak sa posudzuje jednotlivo, sama osebe obvykle nie je dostatočne rozsiahla na to, aby táto osoba podala žalobu na súd. Pokiaľ ide všeobecne o narušenie súkromia

([1]) Prípadom, v ktorom k tomu došlo, je vec Microsoft corporation/Paul McDonald t/a Bizards UK [2006 All Er (D) 153].

a ochrany údajov, EDPS už v skutočnosti toto opatrenie navrhol vo svojom stanovisku ku krokom nadväzujúcim na pracovný program pre lepšie vykonávanie smernice o ochrane údajov ([1]). Podľa názoru EDPS sa mohlo v návrhu zájsť ešte ďalej a navrhnúť skupinové žaloby, čím by sa skupiny občanov oprávnili na spoločný postup vo veciach týkajúcich sa ochrany osobných údajov. V prípade spamu, keďže spam dostáva veľký počet jednotlivcov, majú skupiny jednotlivcov možnosť spájať sa a podávať skupinové žaloby proti spamerom.

57. EDPS vyjadruje poľutovanie najmä nad tým, že návrh obmedzuje možnosť právnických osôb podniknúť právne kroky v situáciách, keď došlo k porušeniu článku 13 smernice, t. j. v situáciách, keď bolo porušené ustanovenie o nevyžiadaných e-mailových správach. Na základe navrhovanej zmeny a doplnenia by právnické osoby skutočne nemohli podniknúť právne kroky v súvislosti s porušením iných ustanovení smernice o elektronickom súkromí. Napríklad platné ustanovenie neumožňuje právnickej osobe, akou je napríklad združenie spotrebiteľov, podať žalobu proti poskytovateľovi prístupu k internetu, ktorý zverejnil osobné údaje miliónov zákazníkov. Vynucovanie smernice o elektronickom súkromí ako celého právneho predpisu, nielen predmetného článku, by sa značne zlepšilo, ak by sa ustanovenie článku 13 ods. 6 zovšeobecnilo, aby sa umožnilo právnickým osobám podať žalobu pre porušenie akéhokoľvek ustanovenia smernice o elektronickom súkromí.

58. EDPS na riešenie tohto problému navrhuje zmeniť článok 13 ods. 6 na samostatný článok (článok 14). Okrem toho by sa znenie článku 13 ods. 6 malo mierne zmeniť a doplniť takto: tam, kde sa uvádza „*podľa tohto článku*“, by sa malo uviesť „podľa tejto smernice“.

II.5. **Posilnenie ustanovení o vynucovaní: doplnenie článku 15a**

59. Smernica o elektronickom súkromí neobsahuje ustanovenia výslovne o vynucovaní. Namiesto toho odkazuje na časť smernice o ochrane údajov o vynucovaní ([2]). EDPS víta nový článok 15a návrhu, ktorý sa na základe tejto smernice zaoberá výslovne otázkami vynucovania.

60. Po prvé, EDPS poznamenáva, že predpokladom opatrení zameraných na účinné vynucovanie v tejto oblasti, ako to vyžaduje navrhovaný článok 15a ods. 3, je, že vnútroštátne orgány majú právomoc viesť vyšetrovanie s cieľom získať potrebné informácie. Dôkazy o porušení ustanovení smernice o elektronickom súkromí sú veľmi často v elektronickej podobe a môžu sa uchovávať na rôznych počítačoch a v rôznych zariadeniach alebo sieťach. V tejto súvislosti je dôležité, aby sa orgánom činným v trestnom konaní poskytla možnosť získať povolenie na prehliadku, na základe ktorého sa im udelí oprávnenie na vstup, prehliadku a zabavenie.

61. Po druhé, EDPS víta najmä navrhovanú zmenu a doplnenie, t. j. článok 15a ods. 2, podľa ktorého vnútroštátne regulačné orgány musia mať právomoc vydať zákaz, t. j. zastaviť porušovanie právnych predpisov, a musia mať potrebné právomoci a zdroje na vyšetrovanie. Vnútroštátne regulačné orgány vrátane vnútroštátnych orgánov pre ochranu údajov by mali mať právomoc ukladať zákazy, na základe ktorých by porušovatelia museli prestať s činnosťou, ktorou sa porušuje smernica o elektronickom súkromí. Zákazy alebo právomoc nariadiť zastavenie porušovania sú užitočným nástrojom v prípade pretrvávajúceho spôsobu správania, ktorým sa porušujú práva jednotlivcov. Zákazy budú veľmi užitočným nástrojom na zastavenie porušovania smernice o elektronickom súkromí, napríklad porušenia článku 13 o nevyžiadaných komerčných správach, ktoré samotnou svojou povahou predstavujú pretrvávajúci spôsob správania.

62. Po tretie, návrh umožňuje Komisii prijať technické vykonávacie opatrenia, ktoré majú zabezpečiť účinnú cezhraničnú spoluprácu pri vynucovaní vnútroštátnych právnych predpisov (navrhovaný odsek 4 článku 15a). Doterajšie skúsenosti zo spolupráce zahŕňajú dohodu uzavretú z iniciatívy Komisie, ktorou sa stanovuje spoločný postup zaobchádzania so sťažnosťami týkajúcimi sa spamu.

([1]) Stanovisko európskeho dozorného úradníka pre ochranu údajov k oznámeniu Komisie Európskemu parlamentu a Rade o krokoch nadväzujúcich na pracovný programu pre lepšie vykonávanie smernice o ochrane údajov (Ú. v. EÚ C 255, 27.10.2007, s. 1).

([2]) Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov.

63. EDPS sa domnieva, že ak právne predpisy budú podporovať regulátorov, aby pomáhali svojim partnerom v iných krajinách, nepochybne pomôžu cezhraničnému vynucovaniu práva. Preto je vhodné, aby návrh umožnil Komisii vytvoriť podmienky na zabezpečenie cezhraničnej spolupráce vrátane postupov pre výmenu informácií.

III. ZÁVERY A ODPORÚČANIA

64. EDPS tento návrh v celom rozsahu víta. Navrhované zmeny a doplnenia posilňujú ochranu súkromia a osobných údajov jednotlivcov v sektore elektronických komunikácií, pričom sa to zabezpečuje s citom, bez neoprávneného a nevyhnutného zaťažovania organizácií. EDPS sa konkrétne domnieva, že pokiaľ navrhované zmeny a doplnenia náležite spĺňajú svoj očakávaný cieľ, z väčšej časti by sa nemali upravovať. V bode 69 sa uvádzajú zmeny a doplnenia, ktoré by sa podľa EDPS nemali upravovať.

65. EDPS sa bez ohľadu na celkove kladné posúdenie návrhu domnieva, že niektoré jeho zmeny a doplnenia by sa mali zlepšiť v záujme účinného zabezpečenia náležitej ochrany osobných údajov a súkromia jednotlivcov. To platí najmä vzhľadom na ustanovenia o oznamovaní narušenia bezpečnosti a ustanovenia, ktorými sa riešia žaloby pre porušenie ustanovení o spame, podané poskytovateľmi elektronických komunikačných služieb. EDPS okrem toho vyjadruje ľútosť nad tým, že návrh nerieši niektoré otázky, ktorými sa primerane nezaoberá ani platná smernica o elektronickom súkromí, čím tento revízny návrh stráca príležitosť vyriešiť pretrvávajúce problémy.

66. Na vyriešenie oboch problémov, t. j. otázok, ktorými sa primerane nezaoberá návrh a tých, ktoré sa neriešia vôbec, sa v tomto stanovisku predkladajú určité formulačné návrhy. V bodoch 67 a 68 sú zhrnuté problémy a navrhuje sa osobitné znenie. EDPS vyzýva zákonodarcu, aby ich vzal do úvahy pri prechode návrhu legislatívnym procesom.

67. Zmeny a doplnenia uvedené v návrhu, v ktorých by EDPS dôrazne odporúčal úpravy, zahŕňajú:

i) **Oznamovanie narušenia bezpečnosti**: Ako sa uviedlo, navrhovaná zmena a doplnenie, ktorým sa dopĺňa *článok 4 ods. 4*, sa vzťahuje na poskytovateľov služieb elektronickej komunikácie vo verejných sieťach (ISP, prevádzkovatelia siete), ktorí sú povinní oznamovať vnútroštátnym regulačným orgánom a svojim zákazníkom narušenie bezpečnosti. EDPS s touto povinnosťou plne súhlasí. EDPS sa však domnieva, že táto povinnosť by sa mala vzťahovať aj na poskytovateľov služieb informačnej spoločnosti, ktorí často spracúvajú citlivé osobné údaje. Túto povinnosť by teda mali dodržiavať aj on-line banky a poisťovatelia, on-line poskytovatelia zdravotníckych služieb a všetky ostatné on-line podnikateľské subjekty.

Na tento účel EDPS navrhuje vložiť do článku 4 ods. 3 tento odkaz na poskytovateľov služieb informačnej spoločnosti: „Ak dôjde k narušeniu bezpečnosti … poskytovateľ verejne dostupných elektronických komunikačných služieb *a poskytovateľ služieb informačnej spoločnosti* … o takomto narušení informuje dotknutého účastníka a vnútroštátny regulačný orgán“.

ii) **Žaloby podané poskytovateľmi verejných elektronických komunikačných služieb vo verejných sieťach**: Ako sa uviedlo, navrhovanou zmenou a doplnením, ktorým sa dopĺňa *článok 13 ods. 6*, sa pre jednotlivca a právnickú osobu, najmä poskytovateľov elektronických komunikačných služieb, ustanovujú občianskoprávne opravné prostriedky s cieľom bojovať proti porušovaniu článku 13 smernice o elektronickom súkromí, ktorý sa zaoberá spamom. EDPS je s týmto ustanovením spokojný. Zároveň však nepovažuje za opodstatnené, aby sa táto nová možnosť obmedzovala na porušenie článku 13. EDPS navrhuje, aby sa právnickým osobám umožnilo podávať žaloby pre porušenie akéhokoľvek ustanovenia smernice o elektronickom súkromí.

EDPS na dosiahnutie tohto cieľa navrhuje zmeniť článok 13 ods. 6 na samostatný článok (článok 14). Okrem toho by sa znenie článku 13 ods. 6 malo mierne zmeniť a doplniť takto: tam, kde sa uvádza „*podľa tohto článku*“, by sa malo uviesť „podľa tejto smernice“.

68. Rozsah uplatňovania smernice o elektronickom súkromí, ktorá sa v súčasnosti obmedzuje na prevádzkovateľov verejných elektronických komunikačných sietí, je jednou z otázok, ktoré sa v návrhu nepodarilo vyriešiť a ktoré vyvolávajú najväčšie obavy. EDPS sa domnieva, že smernica by sa mala zmeniť a doplniť s cieľom rozšíriť jej uplatňovanie tak, aby zahŕňala poskytovateľov elektronických komunikačných služieb aj v zmiešaných (súkromno-verejných) a súkromných sieťach.

69. Zmeny a doplnenia, ktoré by EDPS dôrazne odporúčal ponechať bez úprav, zahŕňajú:

i) **RFID**: Navrhovaná zmena a doplnenie *článku 3*, podľa ktorého elektronické komunikačné siete zahŕňajú *„verejné komunikačné siete podporujúce zariadenia na zber údajov a identifikačné zariadenia“*, je úplne vyhovujúce. Toto ustanovenie je veľmi pozitívne, keďže vyjasňuje, že viacero systémov RFID musí vyhovovať smernici o elektronickom súkromí, čím sa v tejto otázke odstraňuje určitá právna neistota.

ii) **Cookies/spajvér**: Je potrebné uvítať navrhovanú zmenu a doplnenie *článku 5 ods. 3*, pretože vďaka nemu sa povinnosť informovať a poskytnúť právo namietať voči tomu, aby sa cookies/spajvér uchovávali na koncovom zariadení užívateľa, bude uplatňovať aj vtedy, keď sa takéto zariadenia umiestňujú prostredníctvom externých médií na uchovávanie údajov, ako sú CD-ROM, USD kľúče. EDPS však navrhuje, aby sa vykonala menšia zmena a doplnenie poslednej časti článku 5 ods. 3, ktoré spočíva vo vymazaní slova „uľahčenie“ z poslednej vety.

iii) **Možnosť komitologického postupu s konzultáciou EDPS a podmienky/obmedzenia oznamovacej povinnosti**: Navrhovaná zmena a doplnenie, ktorým sa do článku 4 dopĺňa odsek 4 súvisiaci s oznamovaním narušenia bezpečnosti, ponecháva rozhodnutie o komplexných otázkach súvisiacich s okolnosťami/formou/postupmi týkajúcimi sa systému oznamovania narušenia bezpečnosti v rámci komitologického postupu, a to po vyžiadaní si poradenstva EDPS. EDPS výrazne podporuje tento jednotný prístup. Právne predpisy o oznamovaní narušenia bezpečnosti sú samostatnou témou, ktorou je potrebné zaoberať sa po dôkladnej diskusii a analýze.

S touto záležitosťou súvisí požiadavka niektorých zainteresovaných strán na zapracovanie výnimiek z povinnosti oznamovať narušenie bezpečnosti do článku 4 ods. 4. EDPS je dôrazne proti takémuto prístupu. Radšej by uprednostnil, aby sa celkový predmet oznamovania, spôsob oznamovania a okolnosti, v ktorých sa môže oznámenie skrátiť alebo nejako obmedziť, analyzovali holisticky po uskutočnení riadnej diskusie.

iv) **Vynucovanie**: Navrhovaná zmena a doplnenie, ktorým sa dopĺňa *článok 15a*, obsahuje mnoho dôležitých prvkov, ktoré je potrebné ponechať a ktoré prispejú k zabezpečeniu účinného dodržiavania právnych predpisov, vrátane posilnenia vyšetrovacích právomocí vnútroštátnych regulačných orgánov (článok 15a ods. 3) a vzniku právomoci vnútroštátnych regulačných orgánov prikázať zastavenie porušovania právnych predpisov.

V Bruseli 10. apríla 2008

Peter HUSTINX

európsky dozorný úradník pre ochranu údajov