Drugo mnenje Evropskega nadzornika za varstvo podatkov o pregledu Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah)

(2009/C 128/04)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti in zlasti člena 286 Pogodbe,

ob upoštevanju Listine Evropske unije o temeljnih pravicah in zlasti člena 8 Listine,

ob upoštevanju Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov,

ob upoštevanju Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij.

ob upoštevanju Uredbe (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku teh podatkov ter zlasti člena 41 Uredbe –

SPREJEL NASLEDNJE MNENJE:

I. UVOD

Ozadje

1. Evropska komisija je 13. novembra 2007 sprejela predlog, ki med drugim spreminja direktivo o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij, ponavadi naslovljeno Direktiva o zasebnosti in elektronskih komunikacijah [1] (v nadaljnjem besedilu predlog ali predlog Komisije). ENVP je 10. aprila 2008 sprejel mnenje o predlogu Komisije, v katerem je navedel priporočila za njegovo izboljšanje, s tem pa tudi sam poskušal zagotoviti, da bodo predlagane spremembe omogočile kar se da učinkovito varstvo zasebnosti in osebnih podatkov posameznikov (prvo mnenje ENVP) [2].

2. ENVP je ugodno ocenil predlog Komisije za vzpostavitev obveznega sistema za uradno obveščanje v primeru kršitev varnosti, v okviru katerega bodo morala podjetja uradno obvestiti posameznike, če bodo njihovi osebni podatki ogroženi. Poleg tega je tudi pohvalil novo določbo, ki omogoča pravnim osebam (kot so združenja za varstvo potrošnikov in ponudniki internetnih storitev), da ukrepajo proti pošiljateljem neželene pošte, kar je, poleg obstoječih, dodatni instrument za ukrepanje proti temu pojavu.

3. V razpravah, ki so potekale v Evropskem parlamentu pred prvo obravnavo, je ENVP predstavil nadaljnje nasvete oziroma pripombe glede nekaterih vprašanj, ki so se pojavila v poročilih odborov Evropskega parlamenta, pristojnih za pregled Direktive o univerzalni storitvi [3] in Direktive o zasebnosti in elektronskih komunikacijah (pripombe) [4]. V njih je obravnaval predvsem vprašanja, ki se nanašajo na obdelavo podatkov o prometu in varovanje pravic intelektualne lastnine.

4. Evropski parlament (EP) je 24. septembra 2008 sprejel zakonodajno resolucijo o direktivi o zasebnosti in elektronskih komunikacijah (prva obravnava) [5]. ENVP je pozitivno ocenil več sprememb EP, ki so bile sprejete v skladu z navedenim mnenjem in pripombami ENVP, med njimi vključitev ponudnikov storitev informacijske družbe (podjetij, ki delujejo preko spleta) v obveznosti v zvezi z uradnim obveščanjem o kršitvah varnosti. ENVP je tudi ugodno ocenil spremembo, ki omogoča pravnim in fizičnim osebam ukrepanje v primeru kršitev katerih

[1] Pregled Direktive o zasebnosti in elektronskih komunikacijah je del širšega postopka, katerega cilj je ustanovitev organa EU za telekomunikacijske storitve, pregled direktiv 2002/21/ES, 2002/19/ES, 2002/20/ES, 2002/22/ES in 2002/58/ES ter pregled Uredbe (ES) št. 2006/2004 (v nadaljnjem besedilu pregled telekomunikacijskega svežnja).

[2] Mnenje z dne 10. aprila 2008 o predlogu direktive, ki med drugim o spreminja Direktivo 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), UL C 181, 18.7.2008, str. 1.

[3] Direktiva 2002/22/ES o univerzalni storitvi in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami (Direktiva o univerzalnih storitvah) (UL L 108, 24.4.2002, str. 51).

[4] Pripombe ENVP v zvezo z izbranimi vprašanji na podlagi poročila odbora IMCO o pregledu Direktive 2002/22/ES (univerzalna storitev) in Direktive 2002/58/ES (Direktiva o zasebnosti in elektronskih komunikacijah), 2. september 2008. Na voljo na spletni strani: www.edps.europa.eu

[5] Zakonodajna resolucija Evropskega parlamenta z dne 24. septembra 2008 o predlogu direktive Evropskega parlamenta in Sveta o spremembi Direktive 2002/22/ES o univerzalni storitvi in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju na področju varstva potrošnikov (COM(2007) 698 – C6-0420/2007 – 2007/248(COD).

koli določb direktive o zasebnosti in elektronskih komunikacijah (in ne samo kršitev določb o neželeni pošti, kot je predlagala Komisija). Po prvi obravnavi v Parlamentu je Komisija pripravila spremenjeni predlog Direktive o zasebnosti in elektronskih komunikacijah (v nadaljnjem besedilu spremenjeni predlog) ([6]).

5. Svet je 27. novembra 2008 dosegel politično soglasje o pregledu predpisov o svežnju predlogov o telekomunikacijah, med katerimi je tudi Direktiva o zasebnosti in elektronskih komunikacijah, ki bo predstavljeno kot skupno stališče Sveta (skupno stališče) ([7]). To stališče, ki bo v skladu s členom 251(2) Pogodbe o ustanovitvi Evropske skupnosti posredovano EP, lahko vključuje tudi spremembe, ki jih je predlagal slednji.

Splošno mnenje o skupnem stališču

6. Svet je spremenil bistvene elemente predloga in hkrati ni sprejel več sprememb, ki jih je predlagal EP. Čeprav je skupno stališče Sveta zagotovo tudi pozitivno, je ENVP zaskrbljen zaradi njegove vsebine, zlasti zato, ker vanj niso vključene nekatere pozitivne spremembe, ki so jih predlagali EP, Komisija (v spremenjenem predlogu), ENVP in evropski organi za varstvo podatkov v okviru razprav Delovne skupine iz člena 29 ([8]).

7. Nasprotno, določbe v spremenjenem predlogu Komisije in spremembah EP, ki ščitijo državljane, so v kar nekaj primerih znatno oslabljene ali črtane. Raven varstva posameznikov, kakor je predlagana v skupnem stališču, je tako precej nižja. ENVP je zato pripravil drugo mnenje, saj upa, da bodo v nadaljnji obravnavi Direktive o zasebnosti in elektronskih komunikacijah sprejete nove spremembe, ki bodo ponovno zaščitile državljane.

8. V drugem mnenju se je ENVP osredotočil na nekaj glavnih pomislekov in ni ponovil vseh pripomb, ki jih je navedel v mnenju iz decembra 2005 in so še vedno utemeljene. V njem obravnava zlasti:

— določbe o uradnem obveščanju o kršitvah varnosti;

— področje uporabe Direktive o zasebnosti in elektronskih komunikacijah v zasebnih in v javno dostopnih zasebnih omrežjih;

— obdelavo podatkov o prometu iz varnostnih razlogov;

— možnost, da pravne osebe ukrepajo v primeru kršitev direktive o zasebnosti in elektronskih komunikacijah.

9. Pri obravnavi navedenih vprašanj je ENVP analiziral skupno stališče Sveta in ga primerjal s predlaganimi spremembami EP in spremenjenim predlogom Komisije. V mnenje so vključena priporočila, ki naj bi racionalizirala določbe Direktive o zasebnosti in elektronskih komunikacijah in pomagala zagotoviti, da bo direktiva še naprej ustrezno varovala zasebnost in osebne podatke posameznikov.

II. **DOLOČBE O URADNEM OBVEŠČANJU O KRŠITVAH VARNOSTI**

10. ENVP podpira sprejetje določb o sistemu za uradno obveščanje v primeru kršitev, ki bo zagotavljal, da bodo organi in posamezniki obveščeni, če bodo njihovi osebni podatki ogroženi ([9]). Ta obvestila naj bi omogočila posameznikom, da ublažijo morebitno škodo zaradi ogroženosti. Poleg tega bo obveznost obveščanja o kršitvah spodbudila podjetja, da bodo izboljšala varstvo podatkov in okrepila odgovornost glede osebnih podatkov, s katerimi razpolagajo.

11. Pristopi treh institucij – Komisije v spremenjenem predlogu, Evropskega parlamenta v prvi obravnavi in Sveta v skupnem stališču – v zvezi z obravnavanim sistemom za uradno obveščanje se razlikujejo. Za vsakega od njih so značilni tudi pozitivni vidiki. Kljub temu pa je po mnenju ENVP treba vse tri pristope izboljšati, zato svetuje, naj institucije v zadnjih fazah pred sprejetjem sistema upoštevajo priporočila iz tega mnenja.

([6]) Spremenjeni Predlog direktive Evropskega parlamenta in Sveta o spremembi Direktive 2002/22/ES o univerzalni storitvi in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju na področju varstva potrošnikov, 6.11.2008, COM(2008) 723 konč.

([7]) Na voljo na spletni strani Sveta.

([8]) Mnenje 2/2008 o pregledu direktive 2002/58/ES o zasebnosti in elektronskih komunikacijah, na voljo na spletni strani Delovne skupine iz člena 29.

([9]) V mnenju je uporabljena beseda „ogroženi“, ki se nanaša na vse kršitve varnosti osebnih podatkov zaradi nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

12. Po analizi vseh treh pristopov je ENVP opozoril na pet kritičnih točk, o katerih bo treba še razpravljati: (i) opredelitev kršitve varnosti; (ii) subjekti, za katere velja obveznost uradnega obveščanja (zadevni subjekti); (iii) standard oziroma povod za obveznost obveščanja; (iv) opredelitev subjekta, ki bo odgovoren za odločanje o tem, ali je v določenem primeru kršitve varnosti potrebno obveščanje ali ne; (v) prejemniki obvestila.

Pregled pristopov Komisije, Sveta in EP

13. Evropski parlament, Svet in Komisija so sprejeli različne pristope glede obveščanja o kršitvah varnosti. EP je v prvi obravnavi spremenil prvotni sistem za obveščanje v primeru kršitev, ki ga je predlagala Komisija ([10]). Po mnenju EP obveznost obveščanja ne velja samo za ponudnike javno razpoložljivih elektronskih komunikacijskih storitev (PPECS), ampak tudi za ponudnike storitev informacijske družbe (ISSP). Poleg tega bi bilo treba po mnenju EP o vseh kršitvah varnosti osebnih podatkov obvestiti nacionalni regulativni organ ali pristojne organe (skupaj organe). Če bi organi ugotovili, da gre za *resne* kršitve, bi zahtevali od PPECS in ISSP, naj nemudoma obvestijo zadevno osebo. Če bi kršitve predstavljale takojšnjo in neposredno nevarnost, bi PPECS in ISSP najprej obvestili posameznike in šele nato organe, kar pomeni, da ne bi čakali na njihovo odločitev. Obveznost obveščanja potrošnika ne bi veljala samo za tiste subjekte, ki bi lahko organom dokazali, da „*so bili sprejeti ustrezni tehnični ukrepi*“ za preprečitev dostopa do podatkov nepooblaščenim osebam.

14. Tudi Svet meni, da bi morali biti obveščeni naročniki in organi, vendar le v primerih, če bi kršitve po mnenju *zadevnega* subjekta pomenile *resno* grožnjo za naročnikovo zasebnost (npr. kraja ali goljufija, fizična škoda, veliko ponižanje ali škodovanje ugledu).

15. V spremenjenem predlogu Komisije je ohranjena obveznost, ki jo je sprejel EP, tj. obveznost obveščanja organov o vseh kršitvah. Kljub temu pa je Komisija v spremenjeni predlog, v nasprotju s Parlamentom, vključila odstopanja, kar pomeni, da naj obveznost obveščanja zadevnih posameznikov ne bi veljala v primerih, če PPEC dokaže pristojnemu organu, da (i) ni „*dokaj verjetno*“, da bi posameznik lahko utrpel škodo (gospodarsko izgubo, družbeno škodo ali krajo identitete), ki bi bila posledica teh kršitev, ali da (ii) so bili sprejeti „*ustrezni tehnološki varnostni ukrepi*“ v zvezi s podatki, na katere se nanaša kršitev. Predlog Komisije torej vključuje analizo škode za posamezne kršitve oziroma obvestila o kršitvah.

([10]) To vprašanje je obravnavano zlasti v naslednjih spremembah EP: 187, 124 do 127 ter 27, 21 in 32.

16. Treba je opozoriti, da bi morali po mnenju EP ([11]) in Komisije o obveznosti obveščanja odločati *organi*, ki bi presodili, ali je kršitev resna, oziroma, ali je dokaj verjetno, da bi lahko povzročila škodo posamezniku. Svet, nasprotno, meni, da naj bi to odločitev sprejeli *zadevni subjekti*.

17. Po mnenju Sveta in Komisije naj bi obveznost obveščanja veljala samo za PPECS in ne tudi za ISSP, kot meni Parlament.

Opredelitev kršitve varnosti

18. ENVP z zadovoljstvom ugotavlja, da vsi trije zakonodajni predlogi vključujejo isto opredelitev obveznosti obveščanja v primeru kršitev varnosti, tj. za „*kršitve, ki povzročijo nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani […]*“ ([12]).

19. Kot je razvidno iz tega mnenja, ENVP pozitivno ocenjuje to opredelitev, saj je dovolj široka, da vključuje večino okoliščin, v katerih bi lahko bilo potrebno obveščanje o kršitvah varnosti.

20. Prvič: opredelitev vključuje primere, ko do podatkov *dostopa nepooblaščena* tretja oseba – kot je vdor v računalniški sistem, tj. strežnik, ki vsebuje osebne podatke, in priklic teh podatkov.

21. Drugič: opredelitev vključuje tudi primere, ko so bili osebni podatki izgubljeni ali razkriti, nepooblaščen dostop pa je treba še dokazati. Gre za primere, ko bi osebni podatki lahko bili izgubljeni (CD-romi, ključi USB ali druge prenosne naprave) ali pa so jih redni uporabniki naredili javnosti dostopne (mapa s podatki o zaposlenih, ki je bila nenamerno in začasno dostopna javnosti preko spleta). Ker pogosto ni dokazov o tem, ali so takšni podatki bili v določenem trenutku dostopni nepooblaščenim tretjim osebam oziroma ali so jih te osebe uporabljale, se zdi primerno, da so takšne okoliščine vključene v opredelitev. Zato ENVP priporoča, da opredelitev ostane v tej obliki. ENVP tudi priporoča, da se opredelitev kršitve varnosti vključi v člen 2 Direktive o zasebnosti in elektronskih komunikacijah, ker bi bilo to bolj skladno s celotno strukturo direktive in bi zagotavljalo večjo jasnost.

([11]) Razen v primerih takojšnje in neposredne nevarnosti, v katerih morajo zadevni subjekti najprej obvestiti potrošnika.

([12]) Člen (2) skupnega stališča in spremenjenega predloga ter člen 3.3 iz prve obravnave EP.

Subjekti, za katere bi morala veljati obveznost obveščanja

22. Po mnenju EP naj bi obveznost obveščanja veljala za PPECS in ISSP. Kljub temu pa Svet in Komisija menita, da naj bi obveznost obveščanja posameznikov v primeru, če je bila kršena varnost in bi lahko bili ogroženi njihovi osebni podatki, veljala le za PPECS, kot so podjetja, ki omogočajo telekomunikacijske storitve, in ponudniki dostopa do interneta. Za druge sektorje, kot so spletne banke, spletna trgovina na drobno, spletne zdravstvene storitve in druge, pa naj ne bi veljala. Kot je pojasnjeno v nadaljnjem besedilu, ENVP meni, da je z vidika javnega reda bistveno, da se zagotovi, da bo obveznost obveščanja veljala tudi za ponudnike storitev informacijske družbe, ki vključujejo spletne banke, ponudnike spletnih zdravstvenih storitev itd.

23. Prvič: ENVP meni, da so podjetja, ki zagotavljajo telekomunikacijske storitve, sicer res izpostavljena kršitvam varnosti, in zato mora zanje veljati obveznost obveščanja, kljub temu pa ugotavlja, da velja isto za vse druge vrste podjetij/ponudnikov. Spletni trgovci na drobno, spletne banke in spletne lekarne so ravno tako izpostavljeni kršitvam varnosti kot telekomunikacijska podjetja, če ne še v večji meri. Po preučitvi tveganj je torej mogoče ugotoviti, da obveznosti obveščanja ne bi smeli omejiti na PPECS. Da je potreben širši pristop, dokazujejo tudi izkušnje drugih držav. V Združenih državah so na primer skoraj vse države (več kot 40 v tem trenutku) sprejele zakonodajo glede obveznosti obveščanja o kršitvah varnosti, ki ima širše področje uporabe in torej ne vključuje samo PPECS, ampak vse subjekte, ki razpolagajo z osebnimi podatki.

24. Drugič: drži, da kršitev varnosti osebnih podatkov, ki jih redno obdelujejo PPECS, lahko vpliva na zasebnost posameznikov. Enako pa velja, če ni ta nevarnost še večja, za osebne podatke, ki jih obdelujejo ISSP. Banke in druge finančne institucije gotovo hranijo strogo zaupne informacije (npr. podatke o bančnih računih), ki bi v primeru razkritja lahko bili uporabljeni za krajo identitete. Še zlasti veliko škodo bi lahko posameznikom povzročilo tudi razkritje zelo občutljivih podatkov v zvezi z zdravstvenim stanjem, ki jih hranijo ponudniki spletnih zdravstvenih storitev. Zato si je treba zaradi vrst osebnih podatkov, katerih varnost bi lahko bila ogrožena, prizadevati za širšo veljavnost obveznosti obveščanja o kršitvah varnosti, ki mora vključevati vsaj ISSP.

25. Pri razpravah o razširitvi področja uporabe tega člena, tj. subjektih, za katere naj bi veljala navedena obveznost, so se pojavili nekateri pravni problemi. Zlasti je bilo poudarjeno, da se Direktiva o zasebnosti in elektronskih komunikacijah na splošno nanaša samo na PPECS, kar naj bi preprečevalo, da bi obveznost obveščanja veljala tudi za ISSP.

26. V tej zvezi želi ENVP opozoriti, da: (i) s pravnega vidika ni nikakršnih ovir, da ne bi področje uporabe nekaterih določb direktive razširili, tj. da se ne bi mogle uporabljati tudi za druge subjekte in ne samo za PPECS; zakonodajalec Skupnosti ima pri odločanju o tem popolnoma proste roke, (ii) veljavna Direktiva o zasebnosti in elektronskih komunikacijah že vključuje določbe, ki se nanašajo na subjekte, ki niso PPECS.

27. Primer: člen 13 se ne uporablja samo za PPECS, ampak za vsa podjetja, ki pošiljajo neželena sporočila, ob predhodni zahtevi za potrditev soglasja. Poleg tega člen 5(3) Direktive o zasebnosti in elektronskih komunikacijah, ki med drugim prepoveduje shranjevanje podatkov, kot so piškotki (*cookies*), v terminalski opremi uporabnikov, ne zavezuje samo PPECS, ampak vse subjekte, ki poskušajo shraniti podatke ali pridobiti dostop do podatkov, ki so shranjeni v računalniški opremi posameznikov. Poleg tega je Komisija v tem zakonodajnem postopku predlagala razširitev področja uporabe člena 5(3) na primere, ko se podobne tehnologije (piškotki/vohunska programska oprema) ne prenašajo samo preko elektronskih komunikacijskih sistemov, ampak tudi z vsemi drugimi možnimi metodami (pri prenosu s spleta ali preko zunanjih računalniških shranjevalnih nosilcev, kot so CD-romi, ključi USB, hitri pomnilniki (*flash drives*) itd.) Vsi ti elementi so pomembni in jih je treba ohraniti, v sedanjih razpravah o področju uporabe pa bi jih morali tudi upoštevati kot precedense.

28. Poleg tega sta Komisija in EP, verjetno pa tudi Svet, predlagala vključitev novega člena 6(6)(a), ki se nanaša na subjekte, ki niso PPECS, in je obravnavan v nadaljnjem besedilu.

29. Če upoštevamo vse pozitivne vidike obveznosti uradnega obveščanja o kršitvah varnosti, je zelo verjetno, da bodo državljani pričakovali koristi od tega ukrepa tudi v primeru, če bodo njihove osebne podatke ogrožali ISSP in ne samo v primeru kršitev s strani PPECS. Pričakovanja državljanov ne bodo uresničena, če na primer ne bodo obveščeni v primeru, če bi spletna banka izgubila podatke o njihovem bančnem računu.

30. Če povzamemo: ENVP je prepričan, da bo cilj določb o obveznem uradnem obveščanju v primeru kršitev varnosti bolje uresničen le, če bodo veljale za PPECS in ISSP.

Primeri, v katerih je obvezno uradno obveščanje

31. Kar zadeva povod za obveznost obveščanja, je po mnenju ENVP, kot je dodatno pojasnjeno v nadaljevanju, izmed treh predlogov najprimernejši pristop iz spremenjenega predloga, tj. „*če je dokaj verjetno*“, da bodo kršitve povzročile škodo: Kljub temu pa je treba zagotoviti, da je „škoda“ dovolj široko opredeljena, da zajema vse vidike negativnih posledic na zasebnost ali druge zakonite interese posameznikov. Sicer bi bilo bolje oblikovati novo opredelitev, v skladu s katero bi bilo obveščanje obvezno „*če je dokaj verjetno, da bo kršitev škodovala posameznikom*“.

32. Kot je bilo poudarjeno v prejšnjem delu, EP, Komisija in Svet predlagajo različne pogoje, pod katerimi je treba obvestiti posameznike (imenovane „povod“ ali „standard“). Očitno je, da bo število obvestil, ki jih bodo prejeli posamezniki, v veliki meri odvisno od predvidenih povodov oziroma standardov.

33. Svet in Komisija predlagata, da naj bi bilo obveščanje obvezno, če je kršitev „*resna grožnja za posameznikovo zasebnost*“ (Svet) in če „*je dokaj verjetno, da bi bile zaradi kršitve ogrožene koristi potrošnikov*“ (Komisija). Po mnenju EP naj bi obveščanje posameznikov bilo odvisno od „*resnosti kršitve*“ (tj. obveščanje posameznikov je obvezno, če se oceni, da je kršitev „*resna*“). Če ta pogoj ni izpolnjen, obveščanje ni obvezno ([13]).

34. Po mnenju ENVP je mogoče trditi, da imajo vsi posamezniki, katerih osebni podatki so bili ogroženi, v vseh okoliščinah pravico, da so o tem seznanjeni. Kljub temu pa bi bilo pravilno, da bi preučili, ali jo to ustrezna rešitev glede na druge interese in stališča.

35. Izražen je bil pomislek, da bi neomejena obveznost obveščanja v primerih ogrožanja varnosti osebnih podatkov lahko povzročila pretirano obveščanje in tozadevna „utrujenost“, kar bi povzročilo desenzibilizacijo. Kot je pojasnjeno v nadaljevanju, je ENVP se ENVP s tem argumentom sicer strinja, čeprav želi hkrati tudi poudariti, da ga skrbi možnost pretiranega obveščanja, ki bi bilo lahko dokaz za vsesplošen neuspeh ppostopkov za izboljšanje varnosti.

36. Kot je bilo že pojasnjeno, se ENVP zaveda morebitnih negativnih posledic pretiranega obveščanja in bi želel pomagati zagotoviti, da pravni okvir, ki bo sprejet v zvezi z obveščanjem o kršitvah varnosti, ne bo imel takšnih posledic. Če naj bi posamezniki bili obveščeni o kršitvah tudi v primeru, kadar te ne povzročajo škode ali stiske, bi lahko na koncu spodkopali enega od ključnih ciljev obveznosti obveščanja, saj bi posamezniki lahko, kar je ironija, spregledali obvestila prav v primerih, kjer bi se dejansko morali zavarovati. Zato je zelo pomembno doseči pravilno ravnotežje pri zagotavljanju premišljenega obveščanja, kajti v primeru, če se posamezniki ne bodo odzivali na prejeta obvestila, bo učinkovitost sistemov za obveščanje bistveno manjša.

37. Da bi sprejeli ustrezen standard, ki ne bi povzročil pretiranega obveščanja, je treba razmišljati ne samo o povodu za obveščanje, ampak tudi o drugih dejavnikih, zlasti o opredelitvi kršitve varnosti in informacijah, ki jih je treba sporočiti posamezniku. V tej zvezi ENVP ugotavlja, da glede na to, da je opredelitev kršitve varnosti široka, vsi trije predlogi omogočajo dokaj pogosto obveščanje. Zaskrbljenost zaradi možnosti pretiranega obveščanja je še toliko večja, ker opredelitev kršitve varnosti zajema vse vrste osebnih podatkov. Čeprav je to po mnenju ENVP pravilen pristop (brez omejevanja vrst osebnih podatkov, za katere velja obveznost obveščanja) – v nasprotju z drugimi pristopi, kot npr.v zakonodaji ZDA, kjer so zahtevki osredotočeni na občutljivost informacij – je vseeno dejavnik, ki ga je treba upoštevati.

38. Glede na navedeno in ob upoštevanju različnih spremenljivk, ki jih je treba obravnavati skupaj, bi bilo po mnenju ENVP primerno, da se določi, v katerih primerih je obveščanje obvezno.

39. V predlagani standard, tj. če kršitev pomeni „*resno tveganje za zasebnost*“ ali je „*dokaj verjetno, da bo povzročilo škodo*“, so v obeh primerih vključene na primer družbena škoda ali škoda ugledu in ekonomska izguba. Ta dva standarda naj bi vključevala vidike izpostavljenosti nevarnosti za krajo identitete zaradi razkritja skritih identifikatorjev kot so številke potnih listov, ter razkritje podatkov o zasebnem življenju posameznika. ENVP ugodno ocenjuje ta pristop. Prepričan je, da sistema obveščanja o kršitvah varnosti ne bi mogli v celoti izkoristiti, če bi vključeval samo kršitve, ki povzročijo ekonomsko izgubo.

([13]) Glede odstopanj od tega pravila glej opombo 11.

40. Glede na predlagana standarda ENVP meni, da je boljši predlog Komisije, tj. opredelitev „*dokaj verjetno, da bo povzročilo škodo*“, saj zagotavlja ustreznejšo raven zaščite posameznikov. Bolj verjetno je, da bo obveznost obveščanja potrebna, če je „*dokaj verjetno*“, da bodo kršitve „*povzročile škodo*“ zasebnosti posameznika, kot v primeru, če predstavljajo „*resno grožnjo*“. Če bi se torej omejili samo na kršitve, ki predstavljajo resno grožnjo zasebnosti posameznika, bi bistveno zmanjšali število kršitev, za katere velja obveznost obveščanja. To pa bi PPECS in ISSP zagotovilo pretirana pooblastila pri odločanju glede nujnosti obveščanja, saj je mnogo lažje utemeljiti ugotovitev, da ne obstaja „*resna grožnja*“, kot trditev, da ni „*dokaj verjetno, da bi lahko nastala*“ škoda. Čeprav je seveda treba preprečiti pretirano obveščanje, je v celoti gledano v primeru dvoma treba zavarovati zasebnost posameznikov, ki morajo biti zaščiteni vsaj v primeru, če je dokaj verjetno, da bi lahko kršitev povzročila škodo. Poleg tega bo izraz „*dokaj verjetno*“ v praksi bolj učinkovit, saj zajema subjekte in pristojne organe, ker zahteva objektivno oceno primera in njegovega ozadja.

41. Poleg tega lahko kršitve varnosti osebnih podatkov povzročijo škodo, ki je lahko zelo različna in jo je težko izmeriti. Dejansko lahko razkritje iste vrste podatkov v različnih okoliščinah povzroči določenemu posamezniku veliko škodo, drugega pa ne prizadene v takšni meri. Standard, ki bi določal, da je škoda materialna, pomembna ali resna, ne bi bil primeren. V predlogu Sveta je na primer zahteva, da ima kršitev *resne* posledice za zasebnost posameznika; glede na zahtevo, da mora kršitev imeti „resne“ posledice, s takšnim pristopom ne bi bila zagotovljena ustrezna zaščita posameznikov, hkrati pa bi tudi vplival na objektivnost presoje.

42. Čeprav ENVP meni, kot je bilo že pojasnjeno, da je „*dokaj verjetno, da se povzroči škoda*“ primeren standard za obveznost obveščanja o kršitvah varnosti, se kljub temu boji, da vanj ne bi bili vključeni vsi primeri, za katere velja obveznost obveščanja, tj. vsi primeri, v katerih je dokaj verjetno, da bodo imele kršitve negativne posledice na zasebnost ali druge zakonite pravice posameznikov. Zato bi bilo treba preučiti naslednjo opredelitev primerov, v katerih je potrebna obveznost obveščanja, tj. „*če je dokaj verjetno, da bo kršitev imela negativne posledice za posameznike*“.

43. Takšna opredelitev je primerna tudi z vidika skladnosti z zakonodajo EU o varstvu podatkov. Dejansko so v direktivi o varstvu podatkov velikokrat navedene negativne posledice za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Na primer: člen 18 in uvodna izjava 49, ki obravnavata obveznost registracije postopkov obdelave osebnih podatkov pri organih za varstvo podatkov, omogočata državam članicam odstopanje od te obveznosti v primeru, če „*obdelava zelo verjetno ne bo škodljivo vplivala na pravice in svoboščine posameznikov, na katere se osebni podatki nanašajo*“. Podobna določba je uporabljena v členu 16(6) skupnega stališča, njen namen pa je zagotoviti pravnim osebam možnost ukrepanja proti pošiljateljem neželene pošte.

44. Poleg tega bi lahko glede na navedeno tudi pričakovali, da naj bi bili zadevni subjekti in zlasti organi, ki so pristojni za izvajanje zakonodaje o varstvu podatkov, bolje seznanjeni z navedenim standardom, kar bi pripomoglo k lažjemu odločanju glede tega, ali je obveznost obveščanja v posameznem primeru potrebna ali ne.

Subjekt, ki odloča o tem, ali je obveznost obveščanja v primeru kršitve obvezna ali ne

45. Po mnenju EP (razne v primerih neposredne nevarnosti) in v skladu s spremenjenim predlogom Komisije, naj bi o tem, ali je v določenem primeru kršitve zasebnosti obveščanje posameznika obvezno ali ne, odločali organi držav članic.

46. Po mnenju ENVP imajo ti organi pomembno vlogo pri odločanju o tem, ali je obveščanje obvezno, saj v določeni meri jamčijo za pravilno izvajanje zakonov. Takšen sistem bi lahko podjetjem preprečeval, da bi neustrezno ocenila, da kršitev ni škodljiva/resna, in bi se s tem izognila obveznosti obveščanja, čeprav bi bila ta dejansko potrebna.

47. Po drugi strani pa po mnenju ENVP zbuja pomisleke dejstvo, da bi bil sistem, v katerem bi odločali nacionalni organi, nepraktičen in bi ga težko uporabljali oziroma bi se lahko v praksi izkazalo, da je kontraproduktiven. Lahko bi celo povzročil, da bi bili osebni podatki posameznikov slabše zaščiteni.

48. V skladu s tem pristopom bi se dejansko lahko dogajalo, da bi organi za varstvo podatkov prejemali preveliko količino obvestil o kršitvah varnosti in bi zato z veliko težavo pripravljali potrebne ocene. Treba je opozoriti, da morajo organi pri odločanju o tem, ali je v primeru kršitve potrebno obveščanje, zbrati dovolj notranjih informacij, ki so večinoma tehnično zelo kompleksne in jih je treba obdelati zelo hitro. Glede na to, da je takšno ocenjevanje težavno in da imajo nekateri organi omejene vire, bi se po mnenju ENVP lahko zgodilo, da bodo ti organi s težavo izpolnjevali to obveznost in bi lahko v ta namen prerazporejali vire, zadolžene za druge pomembne prednostne naloge. Poleg tega bi takšen sistem pomenil nepotreben pritisk na te organe; če bi sprejeli odločitev, da kršitev ni resna, posamezniki pa bi zaradi nje kljub temu utrpeli škodo, bi se lahko zgodilo, da bi organi morali prevzeti odgovornost.

49. Navedena težava je še dodatno obremenjujoča, če se upošteva, da je ključni dejavnik pri zmanjševanju tveganja, ki ga povzročijo kršitve varnosti, čas. Če organi ne morajo pripraviti ocene v zelo kratkem času in za to potrebujejo dodatni čas, lahko to poveča škodo, ki jo utrpijo posamezniki. Ironija pa je v tem, da bi bi zato lahko ta dodatni ukrep, ki naj bi zagotovil boljšo zaščito posameznikov, te ščitil slabše kot sistemi, ki temeljijo na neposrednem obveščanju.

50. Zato bi bilo po mnenju ENVP bolj primerno, da bi vzpostavili sistem, ki ga predlaga Svet, tj. sistem, v katerem bi zadevni subjekti odločali, ali je obveznost obveščanja potrebna ali ne.

51. Kljub temu pa je treba preprečiti možnost zlorabe, tj. da bi lahko subjekti odklonili obveščanje v primerih, ko je to izrazito potrebno; zato je nadvse pomembno, da se vključijo v nadaljevanju navedeni zaščitni ukrepi za varstvo podatkov.

52. Prvič: obveznost subjektov, da sami odločajo o tem, ali je obveščanje potrebno, mora biti združena z drugo obveznostjo, tj. zahtevo po obveznem obveščanju organov v primeru vseh kršitev, ki ustrezajo predpisanemu standardu. Subjekti bi morali v teh primerih obvestiti organe o kršitvah in razlogih za njihovo odločitev o obvestilu ter vsebini vseh poslanih obvestil.

53. Drugič: organom je treba dejansko zagotoviti nadzorno vlogo. Pri tem jim mora biti omogočena neobvezna preiskava okoliščin kršitve in možnost, da zahtevajo kakršne koli ustrezne ukrepe za izboljšanje ([14]). Poleg obveščanja posameznikov (če še ni bilo izvedeno), bi morala biti vključena tudi možnost, da naložijo subjektom obveznost za sprejetje ukrepov, s katerimi naj bi preprečili nadaljnje kršitve. V tej zvezi bi morali organi imeti učinkovita pooblastila in vire, pa tudi potrebno svobodo pri odločanju o tem, ali je treba v primeru obvestila o kršitvi varnosti ukrepati ali ne. Z drugimi besedami: na ta način bi lahko zagotovili organom možnost izbire in s tem preiskavo velikih in resnično škodljivih kršitev varnosti ter preverjanje in boljšo usklajenost z zakonodajo.

54. Da bi uresničili navedene cilje, ENVP predlaga, da se poleg pooblastil, dodeljenih v skladu s členom 15(a)(3) Direktive o zasebnosti in elektronskih komunikacijah ter Direktive o varstvu podatkov, vključi naslednje besedilo: *„Če naročnik ali zadevni posameznik še ni bil obveščen o kršitvi, lahko pristojni nacionalni organ po preučitvi zadeva zahteva od PPECS ali ISSP, da pošlje obvestilo.“*

55. Poleg tega ENVP priporoča EP in Svetu, naj potrdita obveznost, ki jo predlaga EP (sprememba št. 122, člen 4(1)(a), tj. da morajo subjekti oceniti in presoditi, kakšno tveganje je povezano z njihovimi sistemi in osebnimi podatki, ki jih nameravajo obdelovati. V skladu s to obveznostjo naj bi subjekti pripravili ustrezno in natančno opredelitev zaščitnih ukrepov, ki jih bodo uporabljali in ki naj bi bili na razpolago organom. V primeru kršitve varnosti bo ta obveznost pomagala zadevnim subjektom – in morda tudi organom v vlogi nadzornikov – pri odločanju o tem, ali bi ogrožanje informacij lahko imelo negativne posledice ali povzročilo škodo posameznikom.

56. Tretjič: obveznost subjektov, da odločajo o obveščanju posameznikov, se mora uporabljati hkrati z obveznostjo beleženja podrobne in celovite notranje revizijske sledi, v okviru katere je treba opisati vse kršitve varnosti in navesti poročila o njih, pa tudi vse ukrepe, ki so bili sprejeti za preprečevanje kršitev v prihodnje. Ta notranja revizijska sled mora biti na razpolago organom pri pregledu in morebitni preiskavi. Omogočilo jim bo izvedbo nadzora. To bi bilo mogoče doseči z vključitvijo naslednjega besedila: *„PPECS in ISSP vodijo in hranijo celovite evidence, v katerih so podrobno navedene vse kršitve, z njimi povezane tehnične informacije in ukrepi za izboljšanje. V evidencah so zabeležena tudi vsa obvestila naročnikom ali zadevnim posameznikom ter pristojnim nacionalnim organom, vključno z datumom in vsebino. Evidence se na zahtevo predložijo pristojnemu organu.“*

57. Da se zagotovi doslednost pri izvajanju predpisanega standarda ter drugih vidikov okvira v zvezi s kršitvami varnosti, kot sta oblika in postopki obveščanja, je seveda treba poskrbeti, da lahko Komisija po posvetovanju z ENVP, Delovno skupino iz člena 29 in drugimi zainteresiranimi stranmi sprejme tehnične izvedbene ukrepe.

([14]) To je zagotovljeno tudi v členu 15(a)(3), ki določa, da *„države članice zagotovijo, da imajo pristojni nacionalni organi in po potrebi drugi nacionalni organi vsa potrebna preiskovalna pooblastila in sredstva ter možnost za pridobitev vseh ustreznih informacij, ki so potrebne za spremljanje in izvrševanje nacionalnih določb, sprejetih na podlagi te direktive“*.

Prejemniki obvestila

58. V zvezi s prejemniki obvestila je ENVP bolj naklonjen izrazom, ki jih navajata EP in Komisija, kot terminologiji, ki jo uporablja Svet. EP je besedo „naročniki“ nadomestil z izrazom „uporabniki“. Komisija uporablja izraza „naročniki“ in „zadevni posamezniki“. V predlogih EP in Komisije prejemniki obvestil niso samo sedanji, ampak tudi nekdanji naročniki in tretje strani, kot so uporabniki, ki so v stiku z zadevnimi subjekti, niso pa njihovi naročniki. ENVP pozitivno ocenjuje ta pristop in zato Evropskemu parlamentu in Svetu priporoča, naj ga ohranita.

59. Kljub temu pa ENVP ugotavlja, da obstaja vrsta nedoslednosti glede na terminologijo, ki jo je EP uporabljal v prvi obravnavi; to napako je treba odpraviti. Na primer: beseda „naročniki“ je bila v večini primerov, ne pa v vseh, zamenjana z besedo „uporabniki“, v drugih primerih je bila vstavljena beseda „potrošniki“. To je treba uskladiti.

III. **PODROČJE UPORABE DIREKTIVE O ZASEBNOSTI IN ELEKTRONSKIH KOMUNIKACIJAH: JAVNA IN ZASEBNA OMREŽJA**

60. V členu 3(1) sedanje Direktive o zasebnosti in elektronskih komunikacijah je določeno, kdo so subjekti, na katere se nanaša ta direktiva; gre namreč za subjekte, ki obdelujejo podatke „*v zvezi z*“ zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev (v tem besedilu: PPECS) ([15]). Med dejavnosti PPECS štejemo zagotavljanje dostopa do interneta, prenos informacij prek elektronskih omrežij, povezave mobilne in fiksne telefonije itd.

61. Evropski parlament je sprejel spremembo št. 121 v zvezi s členom 3 prvotnega predloga Komisije, na podlagi katere je bilo področje uporabe Direktive o zasebnosti in elektronskih komunikacijah razširjeno, in sicer tako, da zajema: „*obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih in zasebnih komunikacijskih omrežjih in javno dostopnih zasebnih omrežjih v Skupnosti*“ (člen 3(1) Direktive o zasebnosti in elektronskih komunikacijah). Za Svet in Komisijo ta sprememba, žal, ni bila sprejemljiva, zato je nista upoštevala v skupnem stališču in spremenjenem predlogu.

Uporaba direktive o zasebnosti in elektronskih komunikacijah v javno dostopnih zasebnih omrežjih

62. ENVP je naklonjen ohranitvi bistvenega dela spremembe št. 121, saj želi spodbuditi uskladitev mnenj, v nadaljevanju pa navaja tudi druge razloge. Predlaga tudi dodatno spremembo, tj. podrobnejše pojasnilo glede vrst storitev, ki naj bi bile zajete v razširjenem področju uporabe.

63. Zasebna omrežja se pogosto uporabljajo za zagotavljanje elektronskih komunikacijskih storitev, kot je dostop do interneta, neopredeljenemu, potencialno pa zelo velikemu številu ljudi. To denimo drži za dostop do interneta v spletnih kavarnah v hotelih in restavracijah ter na letališčih, vlakih in drugih krajih, ki so dostopni javnosti, kjer ponujajo – pogosto skupaj z drugimi storitvami (pijače, nastanitev itd.) – zaščiteni brezžični dostop (*Wi-Fi*).

64. V vseh navedenih primerih se komunikacijska storitev, torej dostop do interneta, ne zagotavlja javnosti prek javnega omrežja, pač pa prek omrežja, ki bi lahko veljalo za zasebno, saj z njim upravljajo zasebniki. Čeprav gre v zgornjih primerih za zagotavljanje komunikacijskih storitev javnosti, je zaradi vrste omrežja, ki je zasebno in ne javno, *možno*, da tozadevne storitve niso v celoti zajete v direktivi o zasebnosti in elektronskih komunikacijah ali vsaj v nekaterih členih te direktive ([16]). V teh primerih zato niso zaščitene temeljne pravice posameznikov, ki jih zagotavlja ta direktiva. Uporabniki storitev dostopa do interneta prek javnih telekomunikacijskih omrežij in uporabniki istih storitev v zasebnih omrežjih so tako v neenakem pravnem položaju, čeprav so zasebnost in osebni podatki posameznikov v vseh teh primerih enako ogroženi, kot če se storitev izvaja v javnih omrežjih. Zdi se torej, da ni nobene logične osnove, s katero bi bilo mogoče v okviru direktive upravičiti razlikovanje med komunikacijskimi storitvami, ki se zagotavljajo prek zasebnega omrežja, in storitvami, ki jih zagotavlja javno omrežje.

65. ENVP se zato zavzema za spremembo, kot je sprememba št. 121 Evropskega parlamenta, v skladu s katero bi se direktiva o zasebnosti in elektronskih komunikacijah uporabljala tudi za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v *zasebnih* komunikacijskih omrežjih.

66. ENVP se sicer zaveda, da bi lahko takšna formulacija imela nepredvidene in morebitne nenamerne posledice. Že samo zaradi navedbe zasebnih omrežij bi bilo mogoče sklepati, da direktiva zajema tudi primere, za katere je sicer jasno, da ne spadajo v njeno področje uporabe. Možna je na primer ugotovitev, da bi z dobesedno oziroma strogo

([15]) „Ta direktiva se uporabi za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih.“

([16]) Nasprotno pa bi bilo mogoče trditi, da zagotavljanje komunikacijskih storitev javnosti, tudi prek zasebnega omrežja, ureja obstoječi pravni okvir, torej ne glede na to, da gre za zasebno omrežje. V Franciji, na primer, so delodajalci, ki svojim zaposlenim zagotavljajo dostop do interneta, izenačeni s komercialnimi ponudniki dostopa do interneta. Ta razlaga sicer ni splošno uveljavljena.

razlago te formulacije v področje uporabe direktive vključili tudi lastnike domov, ki so opremljeni z WiFi ([17]) in s tem vsem, ki so v njihovem dosegu (običajno v domu), omogočajo zaščiteni brezžični dostop; to pa ni namen spremembe št. 121. Da bi se temu izognili, ENVP predlaga novo besedilo spremembe št. 121, tako da bi področje uporabe direktive o zasebnosti in elektronskih komunikacijah zajemalo *„obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih ali javno dostopnih zasebnih komunikacijskih omrežjih v Skupnosti*".

67. Na ta način bi bilo jasno navedeno, da naj bi se direktiva o zasebnosti in elektronskih komunikacijah nanašala le na tista zasebna omrežja, ki so javno dostopna. Direktiva, katere določbe se uporabljajo *le* za *javno dostopna zasebna omrežja* (in ne za vsa zasebna omrežja), bo zato zajemala le komunikacijske storitve v okviru zasebnih omrežij, ki so namenoma *dostopna* javnosti. S tako formulacijo bo mogoče v še večji meri izpostaviti dejstvo, da je pri ugotavljanju tega, ali zasebno omrežje spada na področje uporabe direktive, ključni dejavnik predvsem *dostopnost* tega omrežja *za širšo javnost*. Povedano drugače, če je omrežje – ne glede na to, ali gre za javno ali zasebno omrežje – namenoma na voljo javnosti zaradi zagotavljanja javne telekomunikacijske storitve, kot je dostop do interneta, tudi če gre pri tem za dopolnilno storitev (npr. hkrati s hotelsko nastanitvijo), je ta vrsta storitve oziroma omrežja zajeta v Direktivi o zasebnosti in elektronskih komunikacijah.

68. ENVP ugotavlja, da je navedeni pristop, ki ga je podprl, in na podlagi katerega se določbe Direktive o zasebnosti in elektronskih komunikacijah uporabljajo za *javno dostopna zasebna omrežja*, v skladu s pristopi številnih držav članic, kjer so oblasti že odločile, da take vrste storitev, vključno s storitvami v povsem zasebnih omrežjih, spadajo na področje uporabe nacionalnih določb o izvajanju navedene direktive ([18]).

69. Zaradi dodatne pravne varnosti subjektov, ki naj bi jih zajemalo novo področje uporabe, bi bilo morda v Direktivo o zasebnosti in elektronskih komunikacijah koristno vključiti tudi opredelitev „javno dostopnih zasebnih omrežij", ki bi se lahko glasila takole: *„Javno dostopno zasebno omrežje pomeni omrežje, s katerim upravljajo zasebniki in do katerega ima širša javnost praviloma neomejen dostop, in sicer proti plačilu ali zastonj oziroma v povezavi z drugimi storitvami ali ponudbami ter ob upoštevanju veljavnih pogojev.*".

70. V praksi to pomeni, da bi direktiva zajemala zasebna omrežja v hotelih in na drugih mestih, kjer širši javnosti zagotavljajo dostop do interneta prek zasebnega omrežja. Nasprotno pa direktiva ne bi urejala komunikacijskih storitev omejene skupine določljivih posameznikov v povsem zasebnih omrežjih. Virtualna zasebna omrežja in domovi uporabnikov, opremljeni z WiFi, tako na primer ne bi spadali v področje uporabe direktive; enako bi veljalo tudi za storitve, ki se zagotavljajo prek omrežij, ki so izključno korporacijska.

Zasebna omrežja v okviru področja uporabe Direktive o zasebnosti in elektronskih komunikacijah

71. Izključitev zasebnih omrežij kot takih, kot je predlagano zgoraj, bi morala veljati za *začasen* ukrep, o katerem bi bilo treba dodatno razpravljati. Ob upoštevanju posledic, ki bi jih izključitev povsem zasebnih omrežij imela za varstvo zasebnosti, ter po drugi strani dejstva, da izključitev zadeva veliko število ljudi, ki do interneta običajno dostopajo prek korporacijskih omrežij, bi bilo treba to vprašanje v prihodnosti morda zares ponovno preučiti. Da bi spodbudil razpravo o tem, ENVP priporoča, da se v Direktivo o zasebnosti in elektronskih komunikacijah vključi uvodna izjava, na podlagi katere bi Komisija izvedla javno posvetovanje glede uporabe te direktive za vsa zasebna omrežja, pri čemer bi sodelovali tudi ENVP, organi za varstvo podatkov in druge zadevne zainteresirane strani. V uvodni izjavi bi lahko poleg tega določili, da bi morala Komisija po opravljenem javnem posvetovanju preučiti rezultate in temu primerno predlagati vključitev novih vrst subjektov, ki bi jih morala zajemati Direktiva o zasebnosti in elektronskih komunikacijah, oziroma njihovo omejitev.

72. Ustrezno bi bilo treba spremeniti tudi različne člene navedene direktive, tako da se bodo vse izvedbene določbe v zvezi z javnimi omrežji izrecno nanašale tudi na javno dostopna zasebna omrežja.

IV. **OBDELAVA PODATKOV O PROMETU IZ VARNOSTNIH RAZLOGOV**

73. Družbe, ki zagotavljajo varnostne storitve, so med zakonodajnim postopkom v zvezi z revizijo Direktive o zasebnosti in elektronskih komunikacijah izjavile, da bi bilo treba v direktivo vnesti določbo, s katero bi upravičili zbiranje podatkov o prometu in s tem zagotovili učinkovito spletno varnost.

([17]) Običajno gre za brezžično lokalno omrežje (*Local Area Network* – LAN).

([18]) Glej opombo 16.

74. Evropski parlament je zato v besedilo vnesel spremembo št. 181 o oblikovanju novega člena 6(6)(a), s katerim bi bilo izrecno dovoljeno obdelovanje podatkov o prometu iz varnostnih razlogov: „*Brez poseganja v skladnost z določbami, razen člena 7 Direktive 95/46/EC in člena 5 te direktive, se lahko podatki o prometu obdelajo za zakoniti interes kontrolorja podatkov za namene uvajanja tehničnih ukrepov za zagotovitev varnosti omrežja in informacij javnih storitev elektronskih komunikacij, javnega ali zasebnega omrežja elektronskih komunikacij, storitev informacijske družbe ali s tem povezane terminalske in elektronskokomunikacijske opreme, kot je opredeljeno v členu 4(c) Uredbe (ES) št. 460/2004 Evropskega parlamenta in Sveta z dne 10. marca 2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij, razen kadar nad temi interesi ne prevlada interes posameznikovih temeljnih pravic in svoboščin. Obdelava mora biti omejena na to, kar je nujno potrebno za izvajanje določene/takšne varnostne dejavnosti.*“.

75. V spremenjenem predlogu Komisije je ta sprememba načeloma upoštevana, črtana pa je odločilna klavzula, katere namen je bil zagotoviti spoštovanje drugih določb direktive in ki se glasi: „*Brez poseganja v […] … določbe te direktive […]*“. Svet je sprejel preoblikovano različico, v kateri so pomembne določbe o zaščiti in uravnoteženosti interesov iz spremembe št. 181 še nekoliko bolj oslabljene, saj se sedaj glasi takole: „*Podatki o prometu se lahko obdelujejo, kolikor je to potrebno za zagotovitev varnosti omrežij in informacij, kot je opredeljena v členu 4(c) Uredbe (ES) 460/2004 Evropskega parlamenta in Sveta z dne 10. marca 2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij*“.

76. Kot je podrobneje obrazloženo v nadaljevanju, je člen 6(6)(a) nepotreben, obstaja pa tudi nevarnost zlorabe, zlasti če bi bil sprejet brez pomembnih zaščitnih ukrepov, klavzul o upoštevanju drugih določb direktive ter uravnoteženosti interesov. ENVP zato priporoča črtanje tega člena ali vsaj zagotovitev, da bodo vsi tovrstni členi vsebovali zaščitne ukrepe, in sicer po vzoru spremembe št. 181, ki jo je sprejel Evropski parlament.

Pravni razlogi za obdelavo podatkov o prometu, ki veljajo za elektronske komunikacijske storitve in druge upravljavce podatkov na podlagi sedanje zakonodaje na področju varstva podatkov

77. Ponudniki javno razpoložljivih elektronskih komunikacijskih storitev lahko zakonito obdelujejo podatke o prometu ob upoštevanju omejitev iz člena 6 Direktive o zasebnosti in elektronskih komunikacijah; v skladu s tem členom je tovrstna obdelava dovoljena le za nekatere namene, kot so denimo obračunavanje, medsebojno povezovanje in trženje. Ta obdelava lahko poteka le ob upoštevanju natančno določenih pogojev – v primeru trženja je to privoljenje posameznikov. V skladu s členom 7 Direktive o varstvu podatkov – ta določa, da lahko upravljavci podatkov obdelujejo osebne podatke ob upoštevanju vsaj ene od naštetih pravnih podlag oziroma pravnih razlogov – lahko poleg tega podatke o prometu obdelujejo tudi drugi upravljavci podatkov, kot so ponudniki storitev informacijske družbe.

78. Eden od primerov takšne pravne podlage je člen 7(a) Direktive o varstvu podatkov, v katerem je določeno, da je potrebna privolitev posameznika, na katerega se nanašajo osebni podatki. Če želi na primer spletni trgovec na drobno obdelovati podatke o prometu zaradi razpošiljanja oglasnih ali tržnih gradiv, mora za to pridobiti privoljenje posameznika. Drug primer pravne podlage iz člena 7 v nekaterih primerih npr. dopušča, da lahko podatke o prometu iz varnostnih razlogov obdelujejo tudi podjetja za varovanje, ki nudijo varnostne storitve; to je utemeljeno s členom 7(f), v katerem je določeno, da lahko upravljavci podatkov obdelujejo osebne podatke le, „*če je obdelava potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja stranka ali stranke, ki so jim osebni podatki posredovani, razen kadar nad takimi interesi prevladajo temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo […]*“ V Direktivi o varstvu podatkov ni posebej določeno, v katerih primerih bi obdelava osebnih podatkov ustrezala tej zahtevi. Tovrstne odločitve zato sprejemajo upravljavci podatkov, in sicer za vsak primer posebej, pogosto s soglasjem nacionalnih organov za varstvo podatkov in drugih organov.

79. Preučiti bi bilo treba medsebojno učinkovanje člena 7 Direktive o varstvu podatkov ter predlaganega člena 6(6)(a) Direktive o zasebnosti in elektronskih komunikacijah; v slednjem je podrobno opisano, kaj je potrebno za izpolnjevanje zahtev iz navedenega člena 7(f). Člen 6(6)(a) namreč z odobritvijo obdelave podatkov o prometu, s čimer naj bi zagotovili varnost omrežja in informacij, omogoča takšno obdelavo zaradi zakonitih interesov, za katere si prizadeva upravljavec podatkov.

80. Kot je obrazloženo v nadaljevanju, ENVP meni, da predlagani člen 6(6)(a) ni niti potreben niti koristen. S pravnega vidika načeloma pravzaprav ni potrebe po tem, da bi bilo treba ugotavljati, ali določena dejavnost obdelovanja podatkov, v tem primeru je to obdelava podatkov o prometu iz varnostnih razlogov, izpolnjuje zahteve iz člena 7(f) Direktive o varstvu podatkov, pri čemer je morda potrebna privolitev posameznika na podlagi člena 7(a). Kot je bilo že navedeno, o tem ponavadi odločijo upravljavci podatkov, torej podjetja, in sicer, glede izvajanja, po posvetovanju z organi za varstvo podatkov, po potrebi pa o tem odločajo tudi sodišča. ENVP na splošno meni, da je za zakonito obdelavo podatkov o prometu iz varnostnih razlogov v specifičnih primerih, ki ne vpliva na temeljne pravice in svoboščine posameznikov, verjetno,

da bo ustrezala zahtevam iz člena 7(f) Direktive o varstvu podatkov. V obeh direktivah, tisti o varstvu podatkov ter Direktivi o zasebnosti in elektronskih komunikacijah, poleg tega ni nobenih drugih primerov izločevanja ali posebne obravnave določenih vrst dejavnosti obdelave podatkov v skladu z merili iz člena 7(f), prav tako pa tudi ni nobenih dokazov, da bi bile take izjeme potrebne. Ravno nasprotno, glede na povedano se zdi, da bi v številnih primerih taka dejavnost popolnoma ustrezala določbam sedanjega besedila. Pravna določba, s katero naj bi to oceno potrdili, je zato načeloma nepotrebna.

Člen 6(6)(a) – različice Evropskega parlamenta, Sveta in Komisije

81. Kot je bilo že obrazloženo, je sprememba št. 181, ki jo je sprejel Evropski parlament, sicer nepotrebna, vseeno pa je treba poudariti, da so bila pri njenem oblikovanju v določeni meri upoštevana načela zasebnosti in varstva podatkov, določena v zakonodaji o varstvu podatkov. V spremembi št. 181, ki jo je pripravil Evropski parlament, bi lahko varstvu podatkov in zasebnosti dali še večji poudarek, če bi vanjo na primer vključili besede „v posebnih primerih“ in s tem zagotovili selektivno uporabo tega člena, ali pa z določitvijo specifičnega obdobja hrambe.

82. Sprememba št. 181 ima nekaj pozitivnih strani. Potrjuje, da bi morala obdelava potekati v skladu z vsemi drugimi načeli varstva podatkov, ki veljajo za obdelavo osebnih podatkov: „*Brez poseganja v skladnost z določbami […] Direktive 95/46/ES in […] te direktive*“. Sprememba št. 181 sicer dopušča obdelavo podatkov iz varnostnih razlogov, vendar hkrati v enaki meri upošteva interese subjekta, ki obdeluje podatke o prometu, ter interese posameznikov, katerih podatki se obdelujejo; takšna obdelava podatkov je torej mogoča le v primeru, kadar interes subjekta, ki obdeluje podatke, ne prevlada nad interesom temeljnih pravic in svoboščin posameznikov („*razen kadar nad temi interesi ne prevlada interes posameznikovih temeljnih pravic in svoboščin*“). Ta zahteva je bistvena, saj je z njo mogoče upravičiti obdelovanje podatkov o prometu v specifičnih primerih, ne pa tudi obdelavo svežnjev podatkov o prometu.

83. Spremenjena različica spremembe, ki jo je pripravil Svet, ima nekaj pohvale vrednih elementov; v njej so obdržali izraz „*nujno potrebno*“, s čimer je poudarjeno omejeno področje uporabe tega člena. Toda v različici Sveta ni več navedenih zaščitnih ukrepov glede varstva podatkov in zasebnosti. Načeloma sicer veljajo splošne določbe o varstvu podatkov, ne glede na specifično sklicevanje pri vsakem primeru posebej, toda člen 6(6)(a) v različici Sveta bi bilo mogoče kljub temu razumeti tako, kot da dopušča neomejeno obdelavo podatkov o prometu, ne da bi bilo treba pri tem upoštevati kakršne koli zaščitne ukrepe glede varstva podatkov in zasebnosti, ki se sicer uporabljajo pri obdelavi podatkov o prometu. Slednje bi torej lahko zbirali, hranili in jih nadalje uporabljali brez upoštevanja načel varstva podatkov in izpolnjevanja specifičnih obveznosti, ki sicer veljajo za zadevne strani, kot je na primer načelo kakovosti ali obveznost poštene in zakonite obdelave ter obveznost varovanja zaupnosti podatkov in njihove varne hrambe. Glede na to, da v različici Sveta ni nobenega sklicevanja na veljavna načela varstva podatkov, ki določajo roke za hrambo informacij, oziroma na to, da v členu niso določeni nobeni tozadevni specifični roki, bi bilo mogoče to različico razumeti tudi tako, da dopušča zbiranje in obdelavo podatkov o prometu iz varnostnih razlogov za nedoločen čas.

84. V nekaterih delih besedila je Svet poleg tega predvidel manj zavezujoče določbe o varovanju zasebnosti, saj je uporabljena bolj splošna formulacija. V njem na primer ni več sklicevanja na „*zakoniti interes upravljavca podatkov*“, kar zbuja dvom glede vrst subjektov, ki bi lahko izkoristili to izjemo. Nadvse pomembno je, da se vsem uporabnikom ali pravnim osebam prepreči, da bi se s to spremembo okoristili.

85. Nedavne izkušnje v Evropskem parlamentu in Svetu so pokazale, da je s predpisi težko določiti obseg in pogoje za zakonito obdelavo podatkov iz varnostnih razlogov. Le malo verjetno je, da bi se bilo mogoče s kakršnim koli obstoječim ali bodočim členom izogniti tveganju zaradi preširoke uporabe navedene izjeme iz kakršnih koli drugih razlogov, ki niso izključno varnostni; ravno tako se ne bi bilo mogoče izogniti temu, da bi izjemo izkoristili subjekti, ki do tega sicer niso upravičeni. To pa še ne pomeni, da podatkov sploh ne bi smeli obdelovati na ta način. Toda možnosti za tako obdelavo in obseg njene izvedbe bi bilo morda lažje oceniti na ravni izvajanja. Subjekti, ki bi želeli obdelovati podatke na ta način, bi se morali o področju uporabe in pogojih posvetovati z organi za varstvo podatkov in po možnosti z Delovno skupino iz člena 29. Druga možnost pa je, da se v Direktivo o zasebnosti in elektronskih komunikacijah vnese člen, ki bi dopuščal obdelavo podatkov o prometu iz varnostnih razlogov, za kar pa bi bilo potrebno tudi izrecno dovoljenje organov za varstvo podatkov.

86. ENVP je ob upoštevanju tveganja, ki ga člen 6(6)(a) predstavlja za temeljno pravico do varstva podatkov in zasebnosti posameznikov, ter dejstva, da je ta člen (kakor je obrazloženo v tem mnenju) s pravnega vidika nepotreben, zato sklenil, da bi bila najboljša rešitev črtanje celotnega predlaganega člena.

87. Če bi bilo kljub nasprotnemu priporočilu ENVP vseeno sprejeto kakršno koli besedilo po vzoru katere koli od trenutnih različic člena 6(6)(a), bi moralo v vsakem primeru vsebovati prej navedene zaščitne ukrepe glede varstva podatkov. Ravno tako bi ga bilo treba tudi primerno vključiti v sedanji člen 6, po možnosti kot nov odstavek 2(a).

V. **MOŽNOST PRAVNIH OSEB, DA UKREPAJO OB KRŠITVAH DIREKTIVE O ZASEBNOSTI IN ELEKTRONSKIH KOMUNIKACIJAH**

88. Evropski parlament je sprejel spremembo št. 133, ki ponudnikom dostopa do interneta in drugim pravnim osebam, kot so združenja potrošnikov, omogoča, da lahko sprožijo sodni postopek zaradi kršitve katere koli določbe Direktive o zasebnosti in elektronskih komunikacijah ([19]). Vendar te spremembe Komisija in Svet nista sprejela. ENVP meni, da gre za izredno dobrodošlo spremembo in priporoča, da se jo ohrani.

89. Da bi lahko dojeli, kako pomembna je ta sprememba, je treba vedeti, da škoda, ki je na področju zasebnosti in varstva podatkov povzročena posamezniku, ponavadi ni zadosten razlog za uvedbo sodnega postopka. Posamezniki običajno ne gredo na sodišče, če so prejeli neželeno elektronsko pošto ali če je bilo njihovo ime pomotoma vneseno v imenik. Ta sprememba bi združenjem potrošnikov in sindikatom, ki zastopajo skupne interese potrošnikov, omogočila, da v njihovem imenu sprožijo sodni postopek. Tudi raznovrstnejši mehanizmi uveljavljanja bi po vsej verjetnosti pripomogli k boljši usklajenosti, s tem pa k učinkoviti uporabi določb Direktive o zasebnosti in elektronskih komunikacijah.

90. Pravni okviri nekaterih držav članic vključujejo pravne precedense, na podlagi katerih je že predvidena možnost kolektivnega pravnega sredstva; z njim naj bi potrošnikom oziroma interesnim skupinam omogočili, da lahko od strani, ki jim je povzročila škodo, zahtevajo nadomestilo.

91. V drugih državah članicah imajo poleg tega potrošniki in interesne skupine (ter *prizadeti konkurent*) v skladu s predpisi o konkurenci ([20]) pravico, da lahko vložijo tožbo proti kršitelju. Podjetja, ki kršijo predpise o konkurenci, se bodo namreč s tem najbrž okoristila, saj se potrošniki, ki so utrpeli le manjšo škodo, ponavadi le stežka odločajo za tožbo. To utemeljitev bi lahko smiselno uporabili tudi na področju varstva podatkov in zasebnosti.

92. Kot je bilo že navedeno, pa je še bolj pomembno, da lahko pravne osebe, kot so združenja potrošnikov in PPECS, vložijo tožbo, saj je s tem položaj potrošnikov močnejši, spodbuja pa se tudi splošna skladnost z zakonodajo o varstvu podatkov. Če podjetjem, ki kršijo predpise, grozi večja verjetnost tožbe, si bodo najbrž bolj prizadevala za skladnost z zakonodajo o varstvu podatkov, kar bo dolgoročno izboljšalo spoštovanje zasebnosti in varstvo potrošnikov. ENVP zato glede na vse navedeno poziva Evropski parlament in Svet, naj sprejmeta določbo, ki bo pravnim osebam omogočala, da lahko sprožijo sodni postopek zaradi kršitve katere koli določbe Direktive o zasebnosti in elektronskih komunikacijah.

VI. **SKLEP**

93. Skupno stališče Sveta, besedilo Evropskega parlamenta iz prve obravnave in spremenjeni predlog Komisije vsebujejo bolj ali manj pozitivne elemente, ki bi pripomogli k boljši zaščiti zasebnosti posameznikov in njihovih osebnih podatkov.

94. Toda ENVP meni, da še vedno obstajajo možnosti za izboljšave, zlasti kar zadeva skupno stališče Sveta, iz katerega so bile, žal, črtane nekatere spremembe, ki jih je predlagal Evropski parlament, da bi s tem pripomogel k ustrezni zaščiti zasebnosti posameznikov in njihovih osebnih podatkov. Zato poziva Evropski parlament in Svet, naj ponovno uvedeta zaščitne ukrepe glede zasebnosti, ki jih je Parlament sprejel v prvi obravnavi.

95. ENVP poleg tega meni, da bi bilo treba racionalizirati nekatere določbe direktive. Še zlasti to velja za določbe o kršitvah varnosti; ENVP je namreč mnenja, da bodo vse prednosti uradnega obvestila o kršitvi najbolj prišle do izraza, če bo že v zasnovi ustrezno določen pravni okvir. ENVP pa tudi meni, da bi bilo treba izboljšati in pojasniti formulacijo nekaterih določb navedene direktive.

96. Glede na navedeno ENVP poziva Evropski parlament in Svet, naj si še bolj prizadevata, da bodo posamezne določbe Direktive o zasebnosti in elektronskih komunikacijah bolje in jasneje formulirane, hkrati pa poskrbita tudi za to, da bodo znova uvedene spremembe, ki jih je Evropski parlament sprejel v prvi obravnavi in katerih namen je zagotoviti ustrezno raven zasebnosti in varstva podatkov. V točkah 97, 98, 99 in 100 v nadaljevanju so povzeta vsa odprta vprašanja; navedena pa so tudi nekatera priporočila in predlagane določene rešitve. ENVP poziva vse udeležene strani, naj jih upoštevajo pri dokončnem sprejetju direktive o zasebnosti in elektronskih komunikacijah.

Kršitev varnosti

97. Evropski parlament, Komisija in Svet so sprejeli različne pristope glede uradnega obveščanja o kršitvi varnosti. Navedeni trije modeli se med drugim razlikujejo glede subjektov, za katere velja ta obveznost, standarda oziroma povoda za uradno obvestilo, posameznikov, na katere se nanašajo osebni podatki in so upravičeni do obvestila itd. Evropski parlament in Svet morata storiti vse, kar je v njuni moči, in oblikovati zanesljiv pravni okvir v zvezi s kršitvami varnosti. Zato bi morala:

([19]) Člen 13(6) – prva obravnava v Evropskem parlamentu.

([20]) Glej na primer člen 8 nemškega zakona o nepošteni konkurenci (*Gesetz gegen den unlauteren Wettbewerb* – UWG).

— v besedilih Evropskega parlamenta, Sveta in Komisije *pustiti nespremenjeno* opredelitev kršitve varnosti, saj je ta dovolj široka, da zajame večino situacij, v katerih bi bila potrebno uradno obvestilo o kršitvi varnosti;

— kar zadeva subjekte, za katere naj bi veljala predlagana zahteva glede uradnega obvestila, *vključiti* ponudnike storitev informacijske družbe. Spletni trgovci na drobno, spletne banke in spletne lekarne so ravno tako izpostavljeni kršitvam varnosti kot telekomunikacijska podjetja, če ne še v večji meri. Državljani pričakujejo, da bodo obveščeni ne le o kršitvah varnosti, ki jih utrpijo ponudniki dostopa do interneta, temveč zlasti, kadar se to zgodi spletnim bankam in lekarnam;

— kar zadeva povod za uradno obvestilo, je standard iz spremenjenega predloga, tj. *da je dokaj verjetno, da bodo [podatki] ogroženi*, ustrezno, saj zagotavlja funkcionalnost sistema. Treba pa je zagotoviti, da je „škoda" dovolj široko opredeljena, da zajema vse vidike negativnih posledic na zasebnost ali druge zakonite interese posameznikov. Sicer bi bilo sicer bolje oblikovati novo opredelitev, v skladu s katero bi bilo obveščanje obvezno, *„če je mogoče upravičeno pričakovati, da bo kršitev škodovala posameznikom"*. V predlogu Sveta je zahteva, da ima kršitev *resne* posledice za zasebnost posameznika; glede na zahtevo, da mora kršitev imeti „resne" posledice, s takšnim pristopom ne bi bila zagotovljena ustrezna zaščita posameznikov, hkrati pa bi vplival na objektivnost presoje.

— vključitev ustreznega organa, ki naj bi odločil o tem, ali mora zadevni subjekt obvestiti posameznike, ima zagotovo tudi pozitivne strani, vendar se lahko zgodi, da ta rešitev ne bo praktična in jo bo težko uveljavljati ter da bo povzročila preusmeritev sredstev, ki so sicer namenjena za druge pomembne prioritete. ENVP se boji, da v primeru, če oblasti ne bodo zmožne izredno hitre reakcije, tak sistem lahko celo oslabi varstvo posameznikov in po nepotrebnem obremeni organe oblasti. ENVP zato na splošno svetuje, da se *vzpostavi* sistem, na podlagi katerega zadevni subjekti sami ocenijo, ali je uradno obvestilo potrebno ali ne;

— da bi organom omogočili preverjanje ocen, ki jih zadevni subjekti pripravijo v zvezi s tem, ali je uradno obvestilo potrebno ali ne, *uvesti* naslednje zaščitne ukrepe:

  — *zagotoviti*, da so takšni subjekti zavezani organe oblasti uradno obvestiti o vseh kršitvah, ki izpolnjujejo predpisani standard;

  — *poskrbeti*, da imajo organi oblasti vlogo nadzornika, kar jim omogoča selektivnost, s tem pa učinkovitost. Da bi to tudi dosegli, se v besedilo vnese naslednji stavek: *„Če naročnik ali posameznik, na katerega se podatki nanašajo, še ni bil obveščen o kršitvi, lahko pristojni nacionalni organ po preučitvi zadeve zahteva od PPECS ali ISSP, da pošlje obvestilo."*

  — *sprejeti* novo določbo, ki bi subjekte zavezovala k beleženju podrobne in celovite revizijske sledi v podjetju. To bi bilo mogoče doseči s sprejetjem naslednje formulacije: *„PPECS in ponudniki storitev informacijske družbe vodijo in hranijo celovite evidence, v katerih so podrobno navedene vse kršitve, z njimi povezane tehnične informacije in ukrepi za izboljšanje. V evidencah so zabeležena tudi vsa obvestila naročnikom ali zadevnim posameznikom ter pristojnim nacionalnim organom, vključno z datumom in vsebino. Evidence se na zahtevo predložijo pristojnemu nacionalnemu organu."*

— da se zagotovi doslednost pri izvajanju okvira v zvezi s kršitvami varnosti, *poskrbeti*, da lahko Komisija po posvetovanju z ENVP, delovno skupino iz člena 29 in drugimi zainteresiranimi stranmi sprejme tehnične izvedbene ukrepe;

— kar zadeva posameznike, ki bi jih bilo treba obvestiti o kršitvi, *uporabiti* terminologijo Komisije ali Evropskega parlamenta, torej „zadevni posamezniki" oziroma „prizadeti uporabniki", saj vključuje vse posameznike, katerih osebni podatki so bili ogroženi.

Javno dostopna zasebna omrežja

98. Javnost ima pogosteje kot prek javnih omrežij dostop do komunikacijskih storitev prek omrežij, s katerimi upravljajo zasebniki (npr. zaščiteni brezžični dostop (*Wi-Fi*) v hotelih in na letališčih), ti pa v direktivi niso zajeti. Evropski parlament je sprejel spremembo št. 121 (člen 3), ki področje uporabe direktive razširja na javna in zasebna komunikacijska omrežja pa tudi javno dostopna zasebna omrežja. Evropski parlament in Svet bi zato morala:

— *ohraniti* bistveni del spremembe št. 121, vendar jo *preoblikovati*, tako da bo področje uporabe direktive o zasebnosti in elektronskih komunikacijah zajemalo le *„obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih ali javno dostopnih zasebnih komunikacijskih omrežjih v Skupnosti"*. Omrežja, s katerimi upravljajo izključno zasebniki (za razliko od javno dostopnih zasebnih omrežij) v direktivi ne bi bila izrecno zajeta;

— ustrezno *spremeniti* različne izvedbene določbe v zvezi z javnimi omrežji, da se bodo izrecno nanašale tudi na javno dostopna zasebna omrežja;

— *vključiti* spremembo, s katero se opredeli, da *„javno dostopno zasebno omrežje pomeni omrežje, s katerim upravljajo zasebniki in do katerega ima širša javnost praviloma neomejen dostop, in sicer proti plačilu ali zastonj oziroma v povezavi z drugimi storitvami ali ponudbami ter ob upoštevanju veljavnih pogojev“*. Za subjekte, ki naj bi jih zajemalo novo področje uporabe, bo to pomenilo dodatno pravno varnost;

— *sprejeti* novo uvodno izjavo, ki bo Komisiji omogočila izvedbo javnega posvetovanja glede uporabe Direktive o zasebnosti in elektronskih komunikacijah za vsa zasebna omrežja, pri čemer bi sodelovali tudi ENVP, delovna skupina iz člena 29 ter druge zadevne zainteresirane strani. V njej bi lahko pojasnili, da bi morala Komisija po opravljenem javnem posvetovanju predlagati ustrezno vključitev novih vrst subjektov, ki bi jih morala zajemati direktiva o zasebnosti in elektronskih komunikacijah, oziroma njihovo omejitev.

Obdelava podatkov o prometu iz varnostnih razlogov

99. Evropski parlament je na prvi obravnavi sprejel spremembo št. 181 (člen 6(6)(a)), ki dovoljuje obdelovanje podatkov o prometu iz varnostnih razlogov. Svet je v skupnem stališču sprejel nov pristop, v katerem so nekateri zaščitni ukrepi glede zasebnosti nekoliko manj strogi. ENVP zato Evropskemu parlamentu in Svetu priporoča, naj:

— ta člen v celoti *zavrneta*, ker je nepotreben, obstaja pa tudi nevarnost zlorabe, kar bi lahko preveč ogrozilo varstvo podatkov in zasebnost posameznikov;

— če bi bila kljub temu sprejeta katera od različic po vzoru sedanjega besedila člena 6(6)(a), vanj *vključita* zaščitne ukrepe glede varstva podatkov, obravnavane v tem mnenju (po vzoru ukrepov iz spremembe, ki jo je predlagal Evropski parlament).

Ukrepi v zvezi s kršitvami Direktive o zasebnosti in elektronskih komunikacijah

100. Evropski parlament je sprejel spremembo št. 133 (člen 13(6)), ki pravnim osebam omogoča, da lahko sprožijo sodni postopek zaradi kršitve katere koli določbe navedene direktive. Toda Svet te spremembe, žal, ni podprl. Svet in Evropski parlament bi morala:

— *odobriti* določbo, ki pravnim osebam, kot so združenja potrošnikov in poslovna združenja, omogoča, da lahko sprožijo sodni postopek zaradi kršitve katere koli določbe navedene direktive (in ne le zaradi kršitve določb o neželeni elektronski pošti, kakor je trenutno določeno v skupnem stališču in spremenjenem predlogu). Raznovrstnejši mehanizmi uveljavljanja bodo pripomogli k boljši usklajenosti, s tem pa k učinkoviti uporabi določb celotne Direktive o zasebnosti in elektronskih komunikacijah.

Reševanje izziva

101. Evropski parlament in Svet morata pri vseh navedenih vprašanjih najti odgovor na vprašanje, kako oblikovati ustrezna pravila in določbe, ki bodo izvedljivi, funkcionalni in v katerih bosta upoštevani pravica do zasebnosti ter pravica do varstva podatkov posameznikov. ENVP pričakuje, da si bodo vse udeležene strani po svojih najboljših močeh prizadevale, da bi rešile ta izziv, in upa, da bo k temu prispevalo tudi to mnenje.

V Bruslju, 9. januarja 2009

Peter HUSTINX

Evropski nadzornik za varstvo podatkov