I

(Resolucije, priporočila in mnenja)

MNENJA

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Mnenje evropskega nadzornika za varstvo podatkov o predlogu direktive Evropskega parlamenta in Sveta, med drugim o spremembi Direktive 2002/58/ES Evropskega parlamenta in Sveta o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (direktiva o zasebnosti in elektronskih komunikacijah)

(2008/C 181/01)

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 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ([1]),

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 ([2]),

ob upoštevanju Uredbe (ES) št. 45/2001/ES 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 takih podatkov ter zlasti člena 41 Uredbe ([3]),

ob upoštevanju prošnje za mnenje v skladu s členom 28(2) Uredbe (ES) št. 45/2001, ki ga je 16. novembra 2007 prejel od Evropske komisije –

SPREJEL NASLEDNJE MNENJE:

I. **UVOD**

1. Komisija je 13. novembra 2007 sprejela predlog direktive, med drugim o spremembi Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (v nadaljnjem besedilu: predlog oziroma predlagane spremembe). Sedanjo različico Direktive 2002/58/ES običajno – tudi v tem mnenju – imenujemo direktiva o zasebnosti in elektronskih komunikacijah.

([1]) UL L 281, 23.11.1995, str. 31.
([2]) UL L 201, 31.7.2002, str. 37.
([3]) UL L 8, 12.1.2001, str. 1.

2. Cilj predloga je boljše varstvo zasebnosti in osebnih podatkov posameznikov na področju elektronskih komunikacij. Tega pa ne želi doseči s popolnim preoblikovanjem obstoječe direktive o zasebnosti in elektronskih komunikacijah, pač pa s predlaganimi ad hoc spremembami navedene direktive, katerih cilj je zlasti okrepitev določb, povezanih z varnostjo, ter izboljšanje mehanizmov nadzora.

3. Navedeni predlog je del obsežnejše reforme petih direktiv EU o telekomunikacijah (telekomunikacijski sveženj). Komisija pa je poleg priprave predlogov o pregledu telekomunikacijskega svežnja ([1]) obenem sprejela predlog uredbe o ustanovitvi evropskega organa za trg elektronskih komunikacij ([2]).

4. Pripombe v tem mnenju se nanašajo izključno na predlagane spremembe direktive o zasebnosti in elektronskih komunikacijah, razen če se te predlagane spremembe sklicujejo na pojme oziroma določbe iz predlogov o pregledu telekomunikacijskega svežnja. Nekatere pripombe v tem mnenju se poleg tega nanašajo na določbe direktive o zasebnosti in elektronskih komunikacijah, ki jih predlog ne spreminja.

5. V mnenju so obravnavana naslednja vprašanja: *(i)* področje uporabe direktive o zasebnosti in elektronskih komunikacijah, zlasti zadevne storitve (predlagana sprememba člena 3(1)); *(ii)* obveščanje o kršitvi varnosti (predlagana sprememba, doda se člen 4(3) in (4); *(iii)* določbe o piškotkih, vohunski programski opremi in podobnih napravah (predlagana sprememba člena 5(3)); *(iv)* sodni postopki, ki jih sprožijo ponudniki elektronskih komunikacijskih storitev in druge pravne osebe (predlagana sprememba, doda se člen 13(6)) ter *(v)* okrepljene določbe o nadzoru izvajanja direktive (predlagana sprememba, doda se člen 15a).

Posvetovanje z ENVP in širše javno posvetovanje

6. Komisija je predlog poslala ENVP 16. novembra 2007. ENVP razume to sporočilo kot prošnjo za svetovanje institucijam in organom Skupnosti, kot to določa člen 28(2) Uredbe (ES) št. 45/2001 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (v nadaljnjem besedilu: Uredba (ES) št. 45/2001).

7. Komisija se je z ENVP o osnutku predloga neuradno posvetovala še pred sprejetjem, kar je ENVP ocenil pozitivno, saj je s tem dobil priložnost, da poda nekaj predlogov v zvezi z osnutkom predloga, še preden ga je Komisija sprejela. Z zadovoljstvom ugotavlja, da so bili nekateri njegovi predlogi v dokumentu tudi upoštevani.

8. Pred sprejetjem predloga je bilo opravljeno obsežno javno posvetovanje, kar ENVP odobrava. Komisija je junija 2006 začela javno posvetovanje glede sporočila o pregledu telekomunikacijskega svežnja, v okviru katerega je predstavila svoja stališča o razmerah ter predlagala nekatere spremembe ([3]). Ob tej priložnosti so mnenje o predlaganih spremembah predložili tudi v Delovni skupini o varstvu podatkov (Delovna skupina iz člena 29), katere član je tudi ENVP; sprejeto je bilo 26. septembra 2006 ([4]).

([1]) Predlagane spremembe direktiv o telekomunikacijah so predstavljene v naslednjih predlogih: *(i)* Predlog direktive Evropskega parlamenta in Sveta o spremembah Direktiv 2002/21/ES o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve, 2002/19/ES o dostopu do elektronskih komunikacijskih omrežij in pripadajočih naprav ter o njihovem medomrežnem povezovanju in 2002/20/ES o odobritvi elektronskih komunikacijskih omrežij in storitev, 13. november 2007, COM(2007) 697 konč.; *(ii)* 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, 13. november 2007, COM(2007) 698 konč.

([2]) Predlog uredbe Evropskega parlamenta in Sveta o ustanovitvi organa za trg evropskih elektronskih komunikacij, 13. november 2007, COM(2007) 699 konč.

([3]) Sporočilo o pregledu regulativnega okvira EU za elektronska komunikacijska omrežja in storitve (SEC (2006) 816), sprejeto 29. junija 2006. Dopolnjeno je bilo z delovnim dokumentom služb Komisije (COM (206) 334 konč.).

([4]) Mnenje 8/2006 o pregledu regulativnega okvira za elektronske komunikacije in storitve s poudarkom na direktivi o zasebnosti in elektronskih komunikacijah, sprejeto 26. septembra 2006.

Splošno mnenje ENVP

9. ENVP ima glede predloga na splošno pozitivno mnenje. V celoti podpira cilje, ki so Komisijo vodili pri sprejetju predloga za boljše varstvo zasebnosti in osebnih podatkov posameznikov na področju elektronskih komunikacij. Zlasti pozitivno ocenjuje sprejetje sistema obveznega obveščanja o kršitvah varnosti (sprememba člena 4 direktive o zasebnosti in elektronskih komunikacijah, dodana sta odstavka 3 in 4). Če pride do kršitve v zvezi s podatki, se obveščanje o tem izkaže za očitno prednost, saj poudari odgovornost organizacij, podjetja prisili k izvajanju strogih varnostnih ukrepov ter omogoči določitev najzanesljivejših tehnologij za zaščito informacij. Obveščanje poleg tega prizadetim posameznikom omogoča, da ustrezno ukrepajo in se zavarujejo pred krajo identitete oziroma drugimi zlorabami svojih osebnih podatkov.

10. ENVP pozdravlja tudi druge spremembe predloga, kot so možnost, da lahko pravne osebe z zakonitim interesom vložijo tožbo proti kršiteljem določb direktive o zasebnosti in elektronskih komunikacijah (sprememba člena 13, doda se odstavek 6). Podobno pozitivna je tudi okrepitev preiskovalnih pooblastil nacionalnih regulativnih organov, saj bodo ti tako lahko ocenili, ali obdelovanje podatkov poteka v skladu s predpisi ali ne, ter ugotovili, kdo so kršitelji (doda se člen 15a(3)). Da bi zaščitili pravice in svoboščine posameznikov je treba nujno čim prej zaustaviti nezakonito obdelavo osebnih podatkov ter preprečiti kršitve zasebnosti. Predlagani novi člen 15a(2), na podlagi katerega bodo nacionalni regulativni organi pooblaščeni, da odredijo prenehanje kršitev, je zato zelo dobrodošel, saj jim bo omogočil, da takoj zaustavijo nezakonito obdelavo podatkov.

11. Zasnova predloga in večina predlaganih sprememb je v skladu s stališči glede prihodnje politike na področju varstva osebnih podatkov, izraženih v prejšnjih mnenjih ENVP, na primer v mnenju v zvezi z izvajanjem direktive o varstvu podatkov ([1]). Podlaga omenjeni zasnovi je med drugim prepričanje, da nova načela v zvezi z varstvom podatkov sicer niso potrebna, vendar nove tehnologije, kot sta internet in radiofrekvenčna identifikacija (RFID), glede vprašanj na tem področju zahtevajo bolj specifična pravila; treba bi bilo oblikovati tudi orodja za uveljavljanje zakonodaje o varstvu podatkov in zagotavljanje njene učinkovitosti, ki bi pravnim osebam omogočala ukrepanje zaradi kršitev pri varstvu podatkov, osebe, pristojne za obdelavo podatkov, pa zavezalo k obveščanju o kršitvah.

12. ENVP kljub splošnemu pozitivnemu vtisu obžaluje, da predlog ni zasnovan bolj daljnosežno. Izvajanje določb direktive o zasebnosti in elektronskih komunikacijah in temeljita analiza predmeta od leta 2003 kažeta, da so nekatere določbe zelo nejasne, kar povzroča probleme s skladnostjo in pravno varnostjo. Eden od takih primerov je vprašanje, v kakšni meri navedena direktiva zajema tudi poljavne ponudnike elektronskih komunikacijskih storitev. Upati je bilo, da bo Komisija pri reševanju nekaterih odprtih vprašanj izkoristila pregled telekomunikacijskega svežnja in zlasti direktive o zasebnosti in elektronskih komunikacijah. Predlog poleg tega glede novih vprašanj, kot je vzpostavitev sistema obveznega obveščanja o kršitvah varnosti, ponuja samo delno rešitev, saj med organizacije, za katere velja obvezno obveščanje o kršitvah varnosti, ne vključi subjektov, ki obdelujejo zelo občutljive podatke, kot so na primer spletne banke ali spletni ponudniki zdravstvenih storitev. ENVP ta pristop obžaluje.

13. ENVP upa, da bo zakonodajalec pri sprejemanju tega predloga v zakonodajnem postopku upošteval pripombe in predloge iz tega mnenja glede reševanja vprašanj, ki v predlogu Komisije niso obravnavana.

([1]) Mnenje evropskega nadzornika za varstvo podatkov z dne 25. julija 2007 o Sporočilu Komisije Evropskemu parlamentu in Svetu o nadaljevanju delovnega programa za boljše izvajanje direktive o varstvu podatkov (UL C 255, 27.10.2007, str. 1).

II. ANALIZA PREDLOGA

II.1 Področje uporabe direktive o zasebnosti in elektronskih komunikacijah, zlasti zadevnih storitev

14. Ključno vprašanje v zvezi z veljavno direktivo o zasebnosti in elektronskih komunikacijah se nanaša na področje uporabe. Predlog si v nekaterih delih prizadeva opredeliti in razjasniti področje uporabe direktive, zlasti zadevne storitve; te so navedene v oddelku (i). Žal pa s predlaganimi spremembami ne bodo rešeni vsi obstoječi problemi. Kot je navedeno v oddelku (ii) v nadaljevanju, cilj sprememb namreč ni razširitev področja uporabe direktive na elektronske komunikacijske storitve v zasebnih omrežjih.

15. V členu 3 direktive o zasebnosti in elektronskih komunikacijah so opisane storitve, ki jih zajema direktiva, tj. storitve, za katere veljajo obveznosti, določene v direktivi: „*Ta direktiva se uporabi za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih (…)*“.

16. Storitve, na katere se nanaša direktiva o zasebnosti in elektronskih komunikacijah, so torej storitve ponudnikov javno dostopnih elektronskih komunikacijskih storitev v javnih omrežjih (PPECS). PPECS so opredeljeni v členu 2(c) okvirne direktive ([1]), javna komunikacijska omrežja pa v členu 2(d) okvirne direktive ([2]). Med dejavnosti PPECS štejemo zagotavljanje dostopa do interneta, prenos informacij prek elektronskih omrežij, povezave mobilne in fiksne telefonije itd.

(i) *Predlagana sprememba člena 3 direktive o zasebnosti in elektronskih komunikacijah: zadevne storitve naj bi vključevale tudi javna komunikacijska omrežja, ki podpirajo naprave za zbiranje podatkov in identifikacijo*

17. Predlog spreminja člen 3 direktive o zasebnosti in elektronskih komunikacijah tako, da javna elektronska komunikacijska omrežja vključujejo „*javna komunikacijska omrežja, ki podpirajo naprave za zbiranje podatkov, in identifikacijske naprave*“. V uvodni izjavi 28 je pojasnjeno, da morajo za razvoj aplikacij, s katerimi se zbirajo informacije, vključno z osebnimi podatki, in ki uporabljajo radijske frekvence, kot je RFID, veljati določbe direktive o zasebnosti in elektronskih komunikacijah, in sicer ko so te aplikacije priključene na javna komunikacijska omrežja ali storitve oziroma ko uporabljajo tovrstna omrežja ali storitve.

18. ENVP meni, da je ta določba pozitivna, saj je iz nje jasno razvidno, da na področje uporabe direktive o zasebnosti in elektronskih komunikacijah sodijo številne aplikacije RFID; s tem v zvezi je torej nekaj manj negotovosti, popolnoma pa se izognemo nesporazumom in napačni razlagi predpisov.

19. Nekatere aplikacije RFID so že zajete v sedanjem členu 3 direktive o zasebnosti in elektronskih komunikacijah. Razlogov za to je več. Kot prvo se za aplikacije RFID uporablja opredelitev elektronskih komunikacijskih storitev. Drugič, zagotavljajo se prek elektronskega komunikacijskega omrežja, kolikor jih podpirajo prenosni sistemi, ki omogočajo brezžični prenos signalov. Tretjič, omrežje je lahko javno ali zasebno. Če je omrežje javno, se aplikacije RFID štejejo za „zadevne storitve“ in sodijo na področje

([1]) Direktiva 2002/21/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (UL L 108, 24.4.2002, str. 33). Okvirna direktiva razmejuje pojem elektronska komunikacijska storitev, in sicer takole: (i) „Elektronska komunikacijska storitev“ pomeni storitev, ki se navadno opravlja za plačilo in je sestavljena iz prenosa signalov po omrežjih ter vključuje telekomunikacijske storitve in storitve prenosa po omrežjih. (ii) Storitve, s katerimi se vsebine zagotavljajo po elektronskih komunikacijskih omrežjih z uporabo elektronskih komunikacijskih storitev, so izvzete iz opredelitve elektronskih komunikacijskih storitev. (iii) Zagotovitev storitev pomeni vzpostavitev, obratovanje, upravljanje ali zagotavljanje dostopnosti omrežja. (iv) Elektronske komunikacijske storitve ne vključujejo storitev informacijske družbe, ki so kot storitve opredeljene v direktivi o elektronskem poslovanju in se običajno opravijo za plačilo, na daljavo, v elektronski obliki in na zahtevo prejemnika storitev.

([2]) Javno komunikacijsko omrežje pomeni elektronsko komunikacijsko omrežje, ki se v celoti ali pretežno uporablja za izvajanje javnosti dostopnih elektronskih komunikacijskih storitev.

uporabe direktive o zasebnosti in elektronskih komunikacijah. S predlagano spremembo pa ne bo o tem nobenega dvoma več, kar bo omogočilo večjo pravno varnost.

20. ENVP je v svojem prejšnjem mnenju o RFID ([1]) sicer poudaril, da s to določbo še ni izključeno, da v zvezi z RFID ne bodo potrebni dodatni pravni instrumenti. Toda takšne ukrepe bi bilo treba sprejeti v drugem sklopu in ne v okviru tega predloga.

(ii) *Potreba po vključitvi elektronskih komunikacijskih storitev v zasebna ali polzasebna omrežja*

21. ENVP je z opisano pojasnitvijo zadovoljen, obžaluje pa, da v predlogu ni obravnavano tudi vprašanje vedno manj jasnega razlikovanja med zasebnimi in javnimi omrežji. Poleg tega z obžalovanjem ugotavlja, da v opredelitev storitev, ki jih zajema direktiva o zasebnosti in elektronskih komunikacijah, niso bila vključena tudi zasebna omrežja. Člen 3(1) navedene direktive se v sedanji obliki uporablja samo za *elektronske komunikacijske storitve v javnih omrežjih*.

22. ENVP ugotavlja, da gre pri storitvah v vedno večji meri za kombinacijo zasebnih in javnih storitev. Vzemimo za primer univerze, ki na tisoče študentom omogočajo uporabo interneta in elektronske pošte. Jasno je, da je mogoče prek teh poljavnih (ali polzasebnih) omrežij posegati v zasebnost posameznikov, zato bi morala za tovrstne storitve veljati ista pravila kot za izključno javna omrežja. Na varstvo podatkov in zasebnost uporabnikov poleg tega vplivajo tudi zasebna omrežja, na primer na delovnem mestu, kjer delodajalci omogočajo delojemalcem dostop do interneta, v hotelih oziroma stanovanjih, kjer lastniki svojim gostom oziroma najemnikom nudijo dostop do telefona in elektronske pošte, ali pa v spletnih kavarnah; področje uporabe direktive o zasebnosti in elektronskih komunikacijah bi zato moralo zajemati tudi ta omrežja.

23. V skladu s sodno prakso nekaterih držav članic za elektronske komunikacijske storitve v zasebnih omrežjih že veljajo iste obveznosti kot za storitve, opravljene v javnih omrežjih ([2]). Kot so ugotovili organi za varstvo podatkov, nemška zakonodaja določa, da se lahko podjetje, ki dovoljuje uporabo zasebne elektronske pošte na službenih računalnikih, šteje za izvajalca javnih telekomunikacijskih storitev, zato se tudi zanj uporabljajo določbe direktive o zasebnosti in elektronskih komunikacijah.

24. Če povzamemo: zaradi rastočega pomena mešanih (zasebnih/javnih) in zasebnih omrežij v vsakdanjem življenju ter s tem povezanega vedno večjega tveganja za osebne podatke in zasebnost je upravičeno, da se za te storitve uporabljajo ista pravila kot za javne elektronske komunikacijske storitve. ENVP zato meni, da bi morali področje uporabe navedene direktive spremeniti tako, da bi vključevalo tudi takšne vrste zasebnih storitev; tako meni tudi Delovna skupina iz člena 29 ([3]).

II.2 **Obveščanje o kršitvah varnosti: sprememba člena 4**

25. Členu 4 direktive o zasebnosti in elektronskih komunikacijah sta dodana dva nova odstavka (3 in 4), ki določata obveznost glede obveščanja o kršitvah varnosti. Ponudniki javno dostopnih elektronskih komunikacijskih storitev (PPECS) morajo v skladu s členom 4(3) po eni strani v primeru kršitve varnosti, ki povzroči naključno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani v zvezi z zagotavljanjem elektronskih komunikacijskih storitev (s skupnim izrazom „ogrožanje podatkov"), o tem nemudoma obvestiti nacionalne regulativne organe, po drugi strani pa morajo PPECS obvestiti tudi svoje stranke.

([1]) Mnenje z dne 20. decembra 2007 o Sporočilu Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij – Radiofrekvenčna identifikacija (RFID) v Evropi: naslednji koraki k okviru politike, COM(2007) 96.

([2]) Pariško prizivno sodišče je na primer v sodbi *BNP Paribas* proti *World Press Online* z dne 4. februarja 2005 ugotovilo, da med ponudniki komercialnega dostopa do interneta in delodajalci, ki svojim zaposlenim omogočajo dostop do interneta, ni nobene razlike.

([3]) Mnenje 8/2006 o pregledu regulativnega okvira za elektronske komunikacije in storitve s poudarkom na direktivi o zasebnosti in elektronskih komunikacijah, sprejeto 26. septembra 2006.

Prednosti te obveznosti

26. ENVP pozitivno ocenjuje ti določbi (člen 4(3) in (4)), ki uvajata obvezno obveščanje o kršitvah varnosti. Z vidika varstva osebnih podatkov in zasebnosti je obveščanje o kršitvah pozitivno; učinki obveščanja so v Združenih državah že preizkušeni, saj je tam že nekaj let v veljavi državna zakonodaja o obveščanju glede kršitev.

27. Kot prvo, zakonodaja v zvezi z obveščanjem glede kršitev v še večji meri poudarja odgovornost PPECS v primerih ogrožanja informacij. Izraz odgovornost v okviru varstva podatkov in varstva zasebnosti pomeni, da je vsaka posamezna organizacija odgovorna za informacije, ki so ji zaupane oziroma so pod njenim nadzorom. Obveznost obveščanja ponovno potrjuje, da je po eni strani ogrožene podatke nadzoroval PPECS, po drugi pa, da je ta organizacija tista, ki je odgovorna za sprejetje ustreznih ukrepov v zvezi s takimi podatki.

28. Izkazalo pa se je tudi, da je obveznost obveščanja o kršitvah varnosti eden izmed dejavnikov, ki v organizacijah, ki obdelujejo osebne podatke, spodbuja naložbe v varnost. Preprosto dejstvo, da so organizacije dolžne javnost obvestiti o kršitvah varnosti, jih prisili k temu, da uporabljajo strožje varnostne standarde za zaščito osebnih informacij in preprečevanje kršitev. Obveščanje o kršitvah varnosti pa bo omogočilo tudi pripravo in izvedbo zanesljive statistične analize glede najučinkovitejših varnostnih rešitev in mehanizmov. Dolgo časa je vladalo pomanjkanje zanesljivih podatkov o kršitvah varnosti informacij ter najustreznejših tehnologijah za zaščito informacij. Obveznosti glede obveščanja o kršitvah varnosti so verjetno rešitev za ta problem; tako se je izkazalo pri ameriških zakonih o obveščanju glede kršitev varnosti, saj je iz obvestil razvidno, katere tehnologije omogočajo kršitve ([1]).

29. Nenazadnje pa se posamezniki zaradi obveznosti obveščanja o kršitvah varnosti bolj zavedajo tveganja, ki so mu izpostavljeni, kadar so ogroženi njihovi osebni podatki, zato jim je v pomoč pri sprejemanju ustreznih ukrepov, s katerimi tako tveganje zmanjšajo. Če so na primer ogroženi bančni podatki določenega posameznika, se ta lahko, potem ko je bil o tem obveščen, odloči za spremembo podatkov za dostop do svojega bančnega računa, in s tem komu drugemu onemogoči, da bi jih pridobil in se z njimi nezakonito okoristil (običajen izraz za to je „kraja identitete“). Če povzamemo, ta obveznost zmanjšuje verjetnost, da bi posamezniki postali žrtve kraje identitete, žrtvam pa lahko pomaga sprejeti ustrezne ukrepe za rešitev nastalega problema.

Pomanjkljivost predlagane spremembe

30. ENVP je sicer zadovoljen s sistemom obveznega obveščanja o kršitvah varnosti, ki je določen v členu 4(3) in (4), vendar se bolj zavzema za to, da bi imel ta člen širše področje uporabe in bi tako vključeval tudi ponudnike storitev informacijske družbe. Predpis bi tako zajemal tudi spletne banke, spletna podjetja, spletne ponudnike zdravstvenih storitev in druge ([2]).

31. Razlogi, s katerimi je mogoče utemeljiti obveznost obveščanja o kršitvah varnosti za ponudnike javnih elektronskih komunikacijskih storitev, tj. PPECS, veljajo tudi za druge organizacije, ki ravno tako množično obdelujejo osebne podatke, katerih razkritje bi lahko še posebej škodilo posameznikom, na katere se nanašajo osebni podatki. Mednje spadajo spletne banke, posredniki podatkov in drugi spletni ponudniki, ki obdelujejo občutljive podatke (podatke o zdravstvenem stanju, politična stališča itd.). Ogrožanje informacij, s katerimi razpolagajo spletne banke in spletna podjetja in lahko zajemajo ne le številke bančnih računov, pač pa tudi podatke s kreditnih kartic, lahko povzroči krajo identitete; v takih primerih je treba posameznike o tem nujno obvestiti, da lahko sprejmejo ustrezne/potrebne ukrepe. Nazadnje so bile omenjene spletne zdravstvene storitve, v zvezi s katerimi posamezniki morda ne utrpijo finančne škode, zato pa obstaja možnost negospodarske/moralne škode, če so ogrožene občutljive informacije.

([1]) Glej poročilo „*Security Economics and the Internal Market*“, ki so ga po naročilu agencije ENISA pripravili prof. Ross Anderson, Rainer Böhme, Richard Clayton in Tyler Moore. Poročilo si lahko ogledate na povezavi http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Storitve informacijske družbe so opredeljene v direktivi o elektronskem poslovanju kot storitve, ki se običajno opravijo za plačilo, na daljavo, v elektronski obliki in na zahtevo prejemnika storitev.

32. Z razširitvijo področja uporabe obveznosti prej opisane koristi, ki naj bi jih prinesla uvedba te obveznosti, poleg tega ne bodo omejene le na eno področje dejavnosti, tj. ponudbo javno dostopnih elektronskih komunikacijskih storitev, pač pa bodo vključevale tudi splošne storitve informacijske družbe. Z uvedbo obveznega obveščanja o kršitvah varnosti za storitve informacijske družbe, kot so storitve spletnih bank, se poveča odgovornost teh ponudnikov, hkrati pa jih bo to spodbudilo k strožjim varnostnim ukrepom, s katerimi se bodo v prihodnje izognili morebitnim kršitvam varnosti.

33. Obstajajo tudi primeri, v katerih se direktiva o zasebnosti in elektronskih komunikacijah že uporablja tudi za subjekte razen PPECS, npr. v členu 5 o zaupnosti sporočil in v členu 13 o neželeni elektronski pošti. To potrjuje, da je zakonodajalec v preteklosti sprejel zelo modro odločitev o tem, da se razširi področje uporabe nekaterih določb direktive o zasebnosti in elektronskih komunikacijah, saj je menil, da bi bilo to primerno in nujno. ENVP upa, da zakonodajalec tudi sedaj ne bo okleval in se bo odločil za podobno smiseln in prilagodljiv pristop ter razširil področje uporabe člena 4 in vanj vključil ponudnike storitev informacijske družbe. Zato bi zadostovalo, da se v člen 4(3) vstavi napotilo na ponudnike storitev informacijske družbe: „*V primeru kršitve varnosti, ki povzroči naključno ali …, ponudnik javno dostopnih komunikacijskih storitev in ponudnik storitev informacijske družbe zadevnega naročnika in nacionalni regulativni organ … obvestita o taki kršitvi*“.

34. ENVP meni, da je ta obveznost, ki se uporablja za PPECS in ponudnike storitev informacijske družbe, prvi korak v procesu, s katerim bi lahko uporabo obveznosti sčasoma na splošno razširili na vse osebe, odgovorne za obdelavo podatkov.

Specifični pravni okvir za kršitve varnosti, ki ga je treba preučiti po postopku v odboru

35. V predlogu niso obravnavana številna vprašanja, povezana z obveznostjo obveščanja o kršitvah varnosti. Med točkami, ki bi jih bilo treba obravnavati, so pogoji, oblika in postopki, ki se uporabljajo za obveščanje o kršitvah varnosti. Te odločitve so namesto tega v skladu s členom 4(4) predloga prepuščene t.i. komitološkemu odboru ([1]), tj. Odboru za komunikacije, ki je bil ustanovljen s členom 22 Okvirne direktive, v skladu s Sklepom Sveta z dne 28. junija 1999. Takšne ukrepe bi bilo treba torej sprejeti v skladu s členom 5 Sklepa Sveta z dne 28. junija 1999, v katerem so določena pravila glede regulativnega postopka, in sicer za „*ukrepe splošnega dosega za izvajanje bistvenih določb temeljnih aktov*“.

36. ENVP ne nasprotuje odločitvi, da bi vsa ta vprašanja obravnavali v izvedbenih predpisih. Sprejemanje zakonodaje po postopku v odboru verjetno skrajša zakonodajni postopek. Komitologija pa tudi prispeva k zagotavljanju usklajenosti, za katero si je zagotovo treba prizadevati.

37. Glede na množico vprašanj, ki jih bo treba obravnavati v izvedbenih predpisih, in njihov pomen, kot je poudarjeno v nadaljevanju, se zdi primerno, da bi vsa obravnavali skupaj v enem samem predpisu in ne vsakega posebej, tj. nekatera vprašanja v okviru direktive o zasebnosti in elektronskih komunikacijah, druga pa v izvedbenih predpisih. Odločitev Komisije, da ta vprašanja obravnava v izvedbenih predpisih, ki bodo sprejeti po posvetovanju z ENVP in, upajmo, z drugimi zainteresiranimi stranmi (glej naslednjo točko), je zato treba pozdraviti.

Vprašanja, ki jih bo treba obravnavati v izvedbenih ukrepih

38. Pomen izvedbenih ukrepov dojamemo, če dovolj natančno predvidimo vprašanja, ki jih bo treba v njih obravnavati. Z izvedbenimi ukrepi lahko dejansko določimo merila, na podlagi katerih bo treba zagotavljati obveščenost. V njih bo na primer opredeljena kršitev varnosti, pogoji, pod katerimi je treba posameznike in organe o njej obvestiti, in rok za obvestitev.

([1]) Zakonodajni postopki ES, v katere so vključeni odbori, ki jih sestavljajo predstavniki vlad držav članic na ravni uradnikov.

39. ENVP meni, da direktiva o zasebnosti in elektronskih komunikacijah, zlasti člen 4, ne bi smela določati nobenih izjem glede obveznosti obveščanja. ENVP je zato zadovoljen s pristopom Komisije v členu 4, ki določa obveznost obveščanja, vendar zanjo ne predvideva nobene izjeme, temveč omogoča, da se to in druga vprašanja obravnavajo v izvedbenih predpisih. Čeprav se ENVP zaveda argumentov, na podlagi katerih bi bile lahko nekatere izjeme glede omenjene obveznosti upravičene, pa je bolj naklonjen temu, da bi to in druga vprašanja po temeljiti in splošni razpravi o vseh zadevnih vprašanjih podrobno obravnavali v izvedbenih predpisih. Na podlagi omenjenega je zaradi kompleksnosti vprašanj, povezanih z obveznostjo obveščanja o kršitvah varnosti, vključno z morebitnimi upravičenimi izjemami ali omejitvami, potrebna enotna obravnava, tj. v enem samem predpisu, v katerem je obravnavano le to vprašanje.

Posvetovanje z ENVP in potreba po širšem posvetovanju

40. Ker bodo izvedbeni ukrepi pomembno vplivali na varstvo osebnih podatkov posameznikov, bi se morala Komisija pred njihovim sprejetjem temeljito posvetovati. ENVP je zato zadovoljen z besedilom člena 4(4) predloga, v katerem je jasno določeno, da se mora Komisija pred sprejetjem izvedbenih ukrepov posvetovati z evropskim nadzornikom za varstvo podatkov. Ti ukrepi varstva osebnih podatkov in zasebnosti posameznikov ne bodo le zadevali, temveč bodo imeli zanj pomembne posledice. Zato je pomembno pridobiti mnenje ENVP, kakor je določeno v členu 41 Uredbe (ES) št. 45/2001.

41. Poleg posvetovanja z ENVP bi bila lahko ustrezna tudi vključitev določbe, v skladu s katero bi bilo treba o osnutku izvedbenih ukrepov opraviti javno posvetovanje, s katerim bi pridobili mnenja ter spodbudili izmenjavo izkušenj in najboljših praks na tem področju. To bi ne le podjetjem, temveč tudi drugim zainteresiranim stranem, vključno z drugimi organi za varstvo podatkov in delovno skupino iz člena 29, omogočilo, da izrazijo svoje mnenje. Javno posvetovanje je toliko bolj potrebno, če upoštevamo, da se predpis sprejema po postopku v odboru z omejenim posredovanjem Evropskega parlamenta.

42. ENVP ugotavlja, da je v členu 4(4) predloga predvideno, da se Komisija pred sprejetjem izvedbenih pravil posvetuje tudi z evropskim organom za trg elektronskih komunikacij. ENVP zato pozitivno ocenjuje predvideno posvetovanje z evropskim organom za trg elektronskih komunikacij, ki bo glede vprašanj varnosti omrežij in informacij razpolagal z izkušnjami in znanjem Evropske agencije za varnost omrežij in informacij (ENISA). Morda bi bilo ustrezno, če bi do ustanovitve evropskega organa za trg elektronskih komunikacij v predlagani spremembi (člen 4(4)) kot začasno rešitev predvideli posvetovanje z agencijo ENISA.

II.3 **Določbe v zvezi s piškotki, vohunsko programsko opremo in drugo podobno opremo: sprememba člena 5(3)**

43. Člen 5(3) direktive o zasebnosti in elektronskih komunikacijah se nanaša na tehnologije, ki prek elektronskih komunikacijskih omrežij omogočajo dostop do podatkov in njihovo shranjevanje v uporabnikovo terminalsko opremo. Primer za uporabo člena 5(3) so piškotki ([1]). Drugi primeri vključujejo uporabo tehnologij, kot so na primer vohunska programska oprema (skriti vohunski programi) in trojanski konji (programi, ki so skriti v sporočilih ali v drugi navidezno nenevarni programski opremi). Cilj teh tehnologij in njihovi nameni so zelo različni: medtem ko so nekateri povsem neškodljivi ali uporabniku celo koristni, so drugi dejansko zelo škodljivi in nevarni.

([1]) Piškotke v uporabnikovo terminalsko opremo nameščajo ponudniki storitev informacijske družbe za različne namene, tudi za prepoznavanje obiskovalca, ki ponovno obišče določeno spletno mesto. Če je piškotek internetnemu uporabniku poslan s spletnega mesta, se uporabnikovemu računalniku dodeli enoznačna številka (računalnik, ki je prejel piškotke s spletnega mesta A, postane „lastnik piškotka 111“). Na spletnem mestu se ta številka shrani kot referenčna številka. Če uporabnik računalnika, ki je prejel piškotek 111, datoteke s piškotkom ne zbriše, bo pri naslednjem obisku istega spletnega mesta slednje računalnik prepoznalo kot lastnika piškotka 111. Spletno mesto seveda prepozna, da ga je ta računalnik že obiskal. Mehanizem, ki spletnemu mestu omogoča, da računalnik prepozna kot ponovnega obiskovalca, je enostaven. Če so v računalniku obiskovalca spletne strani shranjeni piškotki, na primer piškotek 111, in ta računalnik obišče spletno mesto, ki je pri enem od prejšnjih obiskov ustvarilo ta piškotek, bo na trdem disku uporabnika poiskal številko datoteke s piškotkom. Če uporabnikov pregledovalnik najde datoteko s piškotkom, ki ustreza referenčni številki na spletnem mestu, obvesti spletno mesto, da je v računalniku piškotek 111.

44. Člen 5(3) direktive o zasebnosti in elektronskih komunikacijah določa pogoje, pod katerimi je med drugim z uporabo omenjenih tehnologij mogoče pridobiti dostop do podatkov ali jih shraniti v uporabnikovo terminalsko opremo. V skladu s členom 5(3) *(i)* morajo biti internetni uporabniki zlasti jasno in izčrpno obveščeni v skladu z direktivo 95/46/ES, med drugim o namenih obdelave; in *(ii)* morajo imeti internetni uporabniki možnost, da zavrnejo takšno obdelavo, tj. da so izvzeti iz obdelave podatkov, pridobljenih v njihovi terminalski opremi.

Prednosti predlagane spremembe

45. Področje uporabe sedanjega člena 5(3) direktive o zasebnosti in elektronskih komunikacijah je omejeno na primere, v katerih dostop do podatkov in njihovo shranjevanje v uporabnikovo terminalsko opremo poteka prek *elektronskih komunikacijskih omrežij*. To vključuje zgoraj opisani primer uporabe piškotkov in drugih tehnologij, kot je vohunska programska oprema, ki se prenesejo prek elektronskih komunikacijskih omrežij. Vendar sploh ni jasno, ali se člen 5(3) uporablja tudi v primerih, v katerih se podobne tehnologije (piškotki, vohunska programska oprema in podobno) razširjajo s programsko opremo, nameščeno na zunanjem nosilcu podatkov, in se prenesejo v uporabnikovo terminalsko opremo. Ker je zasebnost lahko ogrožena ne glede na komunikacijski kanal, omejitev člena 5(3) na en komunikacijski kanal ni ravno najboljša rešitev.

46. ENVP je zato zadovoljen s spremembo člena 5(3), ki zaradi črtanja navedbe „elektronskih komunikacijskih omrežij" dejansko razširja področje uporabe tega člena. Tako sta v spremenjeni različici člena 5(3) zajeta oba primera: primer, v katerem dostop do podatkov in njihovo shranjevanje v uporabnikovo terminalsko opremo poteka prek elektronskih komunikacijskih omrežij, in primer, v katerem dostop do podatkov in njihovo shranjevanje v uporabnikovo terminalsko opremo poteka prek zunanjih nosilcev shranjevanja podatkov, kot so CD-ji, CD-ROM-i, USB ključi in podobno.

Tehnično shranjevanje za omogočanje lažjega prenosa

47. Zadnji stavek člena 5(3) direktive o zasebnosti in elektronskih komunikacijah ostaja v spremenjeni različici enak. V skladu z zadnjim stavkom člena 5(3) zahteve iz prvega stavka *ne preprečujejo nobenega tehničnega shranjevanja ali dostopa izključno za namen opravljanja ali lajšanja prenosa sporočila prek elektronskega komunikacijskega omrežja ali, če je nujno potrebno, za zagotovitev storitve informacijske družbe …* Tako se obvezni pravili, določeni v prvem stavku člena 5(3) (potrebno obveščanje in možnost zavrnitve), ne bosta uporabljali, če bo edini namen dostopa do uporabnikove terminalske opreme ali shranjevanja podatkov *omogočanje lažjega* prenosa ali pa bo to nujno potrebno za zagotavljanje storitev informacijske družbe, ki jih zahteva uporabnik.

48. V direktivi pa ni navedeno, v katerih primerih je edini namen dostopa do podatkov ali njihovega shranjevanja omogočanje lažjega prenosa ali zagotavljanja podatkov. Primer, v katerem bi se ta izjema nedvomno uporabljala, je vzpostavitev internetne povezave. Za vzpostavitev internetne povezave je treba namreč pridobiti naslov IP ([1]). Računalnik končnega uporabnika bo moral ponudniku dostopa do interneta razkriti nekatere svoje podatke, v zameno pa mu bo ponudnik dostopa do interneta zagotovil naslov IP. Podatki, shranjeni v terminalski opremi končnega uporabnika, bodo tako posredovani ponudniku dostopa do interneta, ki bo uporabniku zagotovil dostop do interneta. V tem primeru ponudniku dostopa do interneta ni treba objaviti zbranih podatkov ali zagotoviti pravice do zavrnitve, kolikor je ta poseg potreben za zagotovitev storitve.

49. Če želi uporabnik, potem ko je priključen na internet, obiskati določeno spletno mesto, mora poslati zahtevo strežniku, na katerem zadevno spletno mesto gostuje. Slednji bo odgovoril, če bo vedel, kam lahko pošlje informacijo, tj. če bo poznal uporabnikov naslov IP. Zaradi načina shranjevanja tega naslova mora spletno mesto, ki ga želi uporabnik obiskati, ponovno imeti dostop do podatkov v terminalski opremi internetnega uporabnika. Seveda bi se za ta poseg prav tako uporabljala izjema. V teh primerih bi bilo ustrezno, da se zahteve iz člena 5(3) ne bi uporabljale.

([1]) Naslov IP (internetni naslov) je enoznačen naslov, ki ga uporabljajo nekatere elektronske naprave za identificiranje in komuniciranje v računalniškem omrežju, ki uporablja standard „Internet Protocol". Povedano enostavneje, gre za računalniški naslov. Vsaka mrežna naprava – tudi usmerjevalniki, stikala, računalniki, infrastrukturni strežniki (npr. NTP, DNS, DHCP, SNMP itd.), tiskalniki, internetni telefaksi in nekateri telefoni – lahko imajo svoj naslov, ki je v določenem omrežju enoznačen. Nekateri IP naslovi naj bi bili enoznačni v okviru globalnega interneta, drugi pa morajo biti enoznačni le v okviru določenega podjetja.

50. Po mnenju ENVP bi bilo ustrezno, da se iz obveznosti obveščanja in zagotavljanja pravice do zavrnitve izvzameta zgoraj opisana primera, v katerih sta tehnično shranjevanje ali dostop do uporabnikove terminalske opreme *potrebna* izključno zaradi prenosa sporočila prek elektronskega komunikacijskega omrežja. Enako velja, če sta tehnično shranjevanje ali dostop nujno potrebna za zagotavljanje storitve informacijske družbe. Vendar ENVP ne vidi potrebe po izvzetju iz obveznosti obveščanja in zagotavljanja pravice do zavrnitve v primerih, v katerih je edini namen tehničnega shranjevanja ali dostopa *omogočanje lažjega* prenosa sporočila. V skladu z zadnjim stavkom tega člena se tako lahko zgodi, da oseba ne bo obveščena in ne bo mogla zavrniti obdelave svojih podatkov, če piškotek zbira podatke o njenih jezikovnih preferencah ali o kraju, v katerem se nahaja (npr. Belgija, Kitajska), saj bi se lahko štelo, da je cilj tega piškotka omogočanje lažjega prenosa sporočila. ENVP se zaveda, da imajo na ravni programske opreme posamezniki, na katere se nanašajo osebni podatki, v praksi možnost, da zavrnejo ali prilagodijo shranjevanje piškotkov. Vendar to ni dovolj natančno določeno v nobeni zakonski določbi, v skladu s katero bi lahko zadevna oseba uradno branila svoje pravice v zgoraj omenjenih primerih.

51. Da bi preprečili takšen izid, ENVP predlaga manjšo spremembo v zadnjem delu člena 5(3), in sicer črtanje besedice „lajšanja“ v zadnjem stavku: „*ne prepreči nobenega tehničnega shranjevanja ali dostopa izključno za namen opravljanja ali lajšanja prenosa sporočila prek elektronskega komunikacijskega omrežja ali, če je nujno potrebno, za zagotovitev storitve informacijske družbe …*“.

II.4 **Spori, ki jih sprožijo ponudniki javno dostopnih elektronskih komunikacijskih storitev in pravne osebe: dodani odstavek 6 člena 13**

52. Predlagani člen 13(6) določa civilnopravna sredstva za vsako fizično ali pravno osebo z upravičenim interesom, zlasti za ponudnike elektronskih komunikacijskih storitev, ki se zaradi svojega poslovnega interesa borijo proti kršiteljem člena 13 direktive o zasebnosti in elektronskih komunikacijah. Ta člen se nanaša na pošiljanje nenaročenih reklamnih sporočil.

53. S predlagano spremembo se bodo tako ponudniki dostopa do interneta lahko borili proti pošiljateljem neželene elektronske pošte, ki zlorabljajo njihova omrežja, sprožili sodne postopke proti subjektom, ki ponarejajo naslove pošiljateljev ali vdirajo v strežnike, da bi jih lahko uporabljali za pošiljanje neželene pošte, itd.

54. V direktivi o zasebnosti in elektronskih komunikacijah ni bilo jasno določeno, ali smejo ponudniki javno dostopnih elektronskih komunikacijskih storitev sprožiti postopek proti pošiljateljem neželene elektronske pošte; v zelo redkih primerih so ponudniki javno dostopnih elektronskih komunikacijskih storitev sprožili sodni postopek zaradi kršitve člena 13, kakor je bil prenesen v zakonodajo držav članic ([1]). Ker je v predlogu direktive o zasebnosti in elektronskih komunikacijah ponudnikom elektronskih komunikacijskih storitev priznana pravica, da sprožijo sodni postopek in tako zavarujejo svoj poslovni interes, njen namen ni le varovati posameznih naročnikov, temveč tudi ponudnike elektronskih komunikacijskih storitev.

55. ENVP je zadovoljen z možnostjo, predvideno v predlogu, da lahko ponudniki elektronskih komunikacijskih storitev zaradi zaščite poslovnega interesa sprožijo sodni postopek proti pošiljateljem neželene elektronske pošte. Razen v izjemnih primerih posamezni naročniki nimajo niti dovolj denarja niti niso dovolj motivirani, da bi začeli takšen postopek. Nasprotno pa so ponudniki dostopa do interneta in drugi ponudniki javno dostopnih elektronskih komunikacijskih storitev finančno in tehnološko sposobni preiskovati neželeno elektronsko pošto in ugotavljati storilce, zato bi bilo samoumevno, da lahko proti pošiljateljem neželene elektronske pošte sprožili sodni postopek.

56. ENVP je predlagani spremembi zlasti naklonjen, če bi lahko tudi potrošniške organizacije in sindikati, ki zastopajo interese potrošnikov, prejemnikov neželene elektronske pošte, v njihovem imenu sprožili sodni postopek. Kot je bilo že povedano, škoda, povzročena posamezniku, na katerega se nanašajo osebni podatki, in hkrati prejemniku neželene elektronske pošte, v posameznem primeru ponavadi ni dovolj za uvedbo sodnega postopka. Dejansko je ENVP v mnenju o nadaljevanju delovnega programa

([1]) Omenimo lahko zadevo Microsoft corporation *proti* Paulu McDonaldu t/a Bizards UK (2006 All Er (D) 153).

za boljše izvajanje direktive o varstvu podatkov ([1]) ta ukrep načeloma že predlagal za kršitve zasebnosti in varstva podatkov. Po mnenju ENVP bi bil lahko predlog daljnosežnejši in bi lahko predvidel skupinske tožbe, kar bi državljanom v zadevah v zvezi z varstvom osebnih podatkov omogočilo, da lahko skupaj nastopijo pred sodiščem. V primerih, ko številni posamezniki prejemajo neželeno elektronsko pošto, bi se lahko skupine posameznikov povezale in proti pošiljateljem neželene elektronske pošte na sodišču vložile skupinsko tožbo.

57. ENVP zlasti obžaluje, da je v skladu s predlogom možnost, da pravne osebe sprožijo sodni postopek, omejena na primere kršitve člena 13 direktive, tj. na primere kršitve določbe o nenaročenih e-sporočilih. V skladu s predlagano spremembo pravne osebe tako ne bi mogle sprožiti postopka zaradi kršitve drugih določb direktive o zasebnosti in elektronskih komunikacijah. Določba v sedanji obliki namreč pravni osebi, na primer potrošniški organizaciji, ne omogoča, da sproži postopek proti ponudniku dostopa do interneta, ki je razkril osebne podatke milijonov potrošnikov. Izvajanje celotne direktive o zasebnosti in elektronskih komunikacijah, ne le zadevnega člena, bi se bistveno izboljšalo, če bi bila določba člena 13(6) splošna in bi lahko pravne osebe sprožile sodni postopek zaradi kršitve katere koli določbe te direktive.

58. Da bi rešili ta problem, ENVP predlaga preoblikovanje člena 13(6) v ločen člen (člen 14). Besedilo člena 13(6) pa bi morali zato nekoliko spremeniti: „*na podlagi tega člena*“ bi morali nadomestiti z „*na podlagi te direktive*“.

II.5 **Okrepljene določbe o nadzoru izvajanja direktive: dodani člen 15a**

59. V direktivi o zasebnosti in elektronskih komunikacijah ni izrecnih določb o nadzoru njenega izvajanja. Namesto teh je v njej napotilo na zadevni oddelek direktive o varstvu podatkov ([2]). ENVP je zadovoljen z besedilom novega člena 15a predloga, ki izrecno ureja vprašanje nadzora izvajanja te direktive.

60. ENVP ugotavlja, da je za učinkovit nadzor izvajanja na tem področju v skladu s predlaganim členom 15a(3) nacionalnim organom treba zagotoviti preiskovalna pooblastila za pridobivanje potrebnih informacij. Zelo pogosto bodo dokazi o kršitvah določb direktive o zasebnosti in elektronskih komunikacijah predloženi v elektronski obliki in shranjeni v različnih računalnikih, napravah ali omrežjih. Zato je pomembno, da bodo imeli organi nadzora možnost pridobiti nalog za preiskavo, na podlagi katerega bodo pooblaščeni za dostop, preiskave in zaseg.

61. ENVP je zlasti zadovoljen s predlagano spremembo člena 15a(2), v skladu s katero morajo biti nacionalni regulativni organi pooblaščeni, da odredijo prepoved, tj. zahtevajo prenehanje kršitve, ter imajo na voljo potrebna preiskovalna pooblastila in sredstva. Nacionalni regulativni organi, tudi nacionalni organi za varstvo podatkov, bi morali biti pooblaščeni, da odredijo prepoved in kršiteljem onemogočijo nadaljevanje dejavnosti, ki je v nasprotju z direktivo o zasebnosti in elektronskih komunikacijah. Prepoved ali pooblastilo, s katerim se odredi prenehanje kršitve, je koristno orodje v primeru ponavljajočega se ravnanja, ki povzroča kršitev pravic posameznikov. Prepovedi bodo zelo uporabne pri preprečevanju kršitev direktive o zasebnosti in elektronskih komunikacijah, na primer kršitve člena 13 o nenaročenih komercialnih sporočilih, pri katerih gre že po naravi za ponavljajoče se ravnanje.

62. Predlog Komisiji tudi omogoča, da za zagotavljanje učinkovitega čezmejnega sodelovanja pri nadzoru nad izvajanjem nacionalne zakonodaje uvede tehnične izvedbene ukrepe (predlagana sprememba v členu 15a(4)). Pri dosedanjem sodelovanju je bil na pobudo Komisije dosežen dogovor o skupnem postopku za obravnavanje čezmejnih pritožb v zvezi z neželeno elektronsko pošto.

([1]) Mnenje evropskega nadzornika za varstvo podatkov o Sporočilu Komisije Evropskemu parlamentu in Svetu o nadaljevanju delovnega programa za boljše izvajanje direktive o varstvu podatkov (UL C 255, 27.10.2007, str. 1).

([2]) Direktiva 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov.

63. ENVP meni, da predpis nedvomno prispeva k lažjemu čezmejnemu izvajanju svojih določb, če podpira sodelovanje med regulativnimi organi in podobnimi organi v drugih državah. Zato je ustrezno, da je v predlogu predvidena možnost, na podlagi katere bo lahko Komisija ustvarjala pogoje za zagotavljanje čezmejnega sodelovanja, vključno s postopki za izmenjavo informacij.

III. **ZAKLJUČKI IN PRIPOROČILA**

64. ENVP je predlogu v celoti naklonjen. Predlagane spremembe bodo okrepile varstvo zasebnosti posameznikov in njihovih podatkov na področju elektronskih komunikacij; to bo doseženo z blagim pristopom ter brez neupravičenih in nepotrebnih obremenitev za organizacije. Natančneje, ENVP meni, da predlaganih sprememb v glavnem ne bi smeli spreminjati, če ustrezajo svojemu namenu. V točki 69 so naštete spremembe, za katere ENVP upa, da bodo ostale nespremenjene.

65. Čeprav ENVP predlog na splošno ocenjuje pozitivno, meni, da bi morali nekatere spremembe izboljšati ter s tem zagotoviti učinkovito varstvo osebnih podatkov in zasebnosti posameznikov. To še zlasti velja za določbe o obveščanju o kršitvah varnosti in za določbe o sodnih postopkih, ki jih sprožijo ponudniki elektronskih komunikacijskih storitev zaradi kršitve določb o neželeni elektronski pošti. Poleg tega ENVP obžaluje, da v predlogu niso obravnavana nekatera vprašanja, ki tudi v sedanji direktivi o zasebnosti in elektronskih komunikacijah niso ustrezno urejena; s tem pri tem pregledu niso izkoristili možnosti rešitve odprtih vprašanj.

66. V mnenju so za oba problema, tj. vprašanja, ki v predlogu niso ustrezno preučena, in tista, ki v njem sploh niso obravnavana, predlagane nekatere rešitve. V točkah 67 in 68 so povzeti problemi in predlagano ustrezno besedilo. ENVP zakonodajalca poziva, da jih upošteva pri sprejemanju tega predloga v zakonodajnem postopku.

67. ENVP se odločno zavzema za preoblikovanje naslednjih sprememb, vsebovanih v predlogu:

(i) **Obveščanje o kršitvah varnosti.** Kot je navedeno, se predlagana sprememba z dodanim *členom 4(4)* uporablja za ponudnike javno dostopnih elektronskih komunikacijskih storitev v javnih omrežjih (ponudniki internetnih storitev in mrežni operaterji), ki morajo svoje regulativne organe in potrošnike obveščati o kršitvah varnosti. ENVP to obveznost v celoti podpira. Meni pa, da bi se morala obveznost uporabljati tudi za ponudnike storitev informacijske družbe, ki pogosto obdelujejo občutljive osebne podatke. Tako bi morale to obveznost izpolnjevati tudi spletne banke in zavarovalnice ter spletni ponudniki zdravstvenih storitev, prav tako pa bi morala veljati za vsako spletno podjetje.

ENVP zato predlaga, da se v člen 4(3) vstavi napotilo na ponudnike storitev informacijske družbe: „*V primeru kršitve varnosti … ponudnik javno dostopnih komunikacijskih storitev in ponudnik storitev informacijske družbe zadevnega naročnika in nacionalni regulativni organ … obvestita o taki kršitvi*“.

(ii) **Sodni postopki, ki jih sprožijo ponudniki javno dostopnih elektronskih komunikacijskih storitev v javnih omrežjih.** Kot je navedeno, predlagana sprememba z dodanim *členom 13(6)* zagotavlja civilnopravna sredstva, ki fizičnim ali pravnim osebam, zlasti ponudnikom elektronskih komunikacijskih storitev, omogočajo, da ukrepajo proti kršitvam člena 13 direktive o zasebnosti in elektronskih komunikacijah, ki se nanaša na neželeno elektronsko pošto. ENVP je z določbo zadovoljen. Vendar ne razume, zakaj bi morala biti ta možnost omejena na kršitve člena 13. Zato predlaga, da bi imele pravne osebe možnost, da sprožijo sodni postopek zaradi kršitve katere koli določbe direktive o zasebnosti in elektronskih komunikacijah.

Da bi bilo to možno, ENVP predlaga preoblikovanje člena 13(6) v ločen člen (člen 14). Besedilo člena 13(6) bi morali zato nekoliko spremeniti: „*na podlagi tega člena*“ bi morali nadomestiti z „*na podlagi te direktive*“.

68. Področje uporabe direktive o zasebnosti in elektronskih komunikacijah, ki je trenutno omejeno na ponudnike javno dostopnih elektronskih komunikacijskih omrežij, je eno od najbolj zaskrbljujočih vprašanj, ki v tem predlogu ni obravnavano. ENVP meni, da je treba direktivo spremeniti ter razširiti njeno področje uporabe in tako zagotoviti, da bi se uporabljala tudi za ponudnike elektronskih komunikacijskih storitev v mešanih (javno-zasebnih) in zasebnih omrežjih.

69. ENVP se odločno zavzema, da bi naslednje spremembe ostala nespremenjene:

(i) **RFID.** Predlagana sprememba *člena 3*, v skladu s katero elektronska komunikacijska omrežja vključujejo *„javna komunikacijska omrežja, ki podpirajo zbiranje podatkov in identifikacijske naprave"*, je popolnoma ustrezna. Ta določba je povsem nedvoumna, saj je iz nje jasno razvidno, da morajo številne aplikacije RFID izpolnjevati zahteve direktive o zasebnosti in elektronskih komunikacijah, s čimer je odpravljena določena pravna negotovost.

(ii) **Piškotki/vohunska programska oprema.** Predlagana sprememba *člena 5(3)* je dobrodošla, saj se bo obveznost obveščanja in zagotavljanja pravice, da se shranjevanje piškotkov/vohunske programske opreme v uporabnikovi terminalski opremi zavrne, uporabljala tudi pri njihovem nameščanju prek zunanjih nosilcev podatkov, kot so na primer CD-ROM-i in USB ključi. Vendar ENVP predlaga manjšo spremembo v zadnjem delu člena 5(3), in sicer črtanje besedice „lajšanja".

(iii) **Izbira postopka v odboru s posvetovanjem z ENVP in pogoji/omejitve v zvezi z obveznostjo obveščanja.** Predlagana sprememba z dodanim členom 4(4) o obveščanju o kršitvah varnosti določa, da se odločitev o kompleksnih vprašanjih v zvezi s pogoji/obliko/postopki sistema za obveščanje o kršitvah varnosti po pridobitvi mnenja ENVP sprejme po postopku v odboru. ENVP odločno podpira enoten pristop. Zakonodaja o obveščanju o kršitvah varnosti je poglavje zase in jo je treba obravnavati po natančni razpravi in analizi.

V zvezi s tem so nekatere zainteresirane strani zahtevale, da se pripravijo izjeme glede obveznega obveščanja o kršitvah varnosti iz člena 4(4). ENVP temu odločno nasprotuje. Bolj se zavzema za to, da bi po podrobni razpravi temeljito analizirali predmet in način obveščanja ter primere, v katerih je mogoče skrajšati ali nekoliko omejiti njegovo vsebino.

(iv) **Nadzor nad izvajanjem.** V predlagani spremembi z dodanim *členom 15a* je veliko koristnih elementov, ki bi jih bilo treba ohraniti zaradi zagotavljanja dejanskega upoštevanja pravil; med drugim sta to razširitev preiskovalnih pooblastil nacionalnih regulativnih organov (člen 15a(3)) in uvedba pooblastil, s katerimi bi lahko nacionalni regulativni organi odrejali prenehanje kršitev.

V Bruslju, 10. aprila 2008

Peter HUSTINX

Evropski nadzornik za varstvo podatkov