I

(Resolucije, priporočila in mnenja)

MNENJA

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Mnenje Evropskega nadzornika za varstvo podatkov o krepitvi zaupanja v informacijsko družbo s spodbujanjem varstva podatkov in zasebnosti

(2010/C 280/01)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 16 Pogodbe,

ob upoštevanju Listine Evropske unije o temeljnih pravicah ter zlasti členov 7 in 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 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 ([3]) ter zlasti člena 41 Uredbe –

SPREJEL NASLEDNJE MNENJE:

I. UVOD

1. Informacijske in komunikacijske tehnologije (IKT) dajejo izjemne možnosti na skoraj vseh področjih našega življenja – pri delu, igri, socializaciji in izobraževanju. So bistvenega pomena za sodobno informacijsko gospodarstvo in družbo na splošno.

2. Evropska unija je svetovna sila na področju naprednih IKT in je odločena to tudi ostati. Za uspešen odgovor na ta izziv se pričakuje, da bo Evropska komisija kmalu sprejela nov evropski program za digitalne tehnologije, ki ga je komisarka Kroesova potrdila kot svojo prednostno nalogo ([4]).

3. Evropski nadzornik za varstvo podatkov (ENVP) priznava koristi, ki izhajajo iz IKT, in se strinja, da bi morala EU storiti vse, kar je v njeni moči, da spodbudi njihov razvoj in široko sprejetje. Prav tako v celoti podpira stališči komisark Kroesove in Redingove, da morajo biti posamezniki v središču tega novega okolja ([5]). Posamezniki morajo imeti možnost, da se zanesejo na zmožnost IKT, da te ohranjajo varnost njihovih informacij in da bo uporaba teh informacij nadzorovana, in biti prepričani, da se bodo v digitalnem prostoru spoštovale njihove pravice do zasebnosti in varstva podatkov. Spoštovanje teh pravic je bistveno za zaupanje potrošnikov. Tako zaupanje pa je ključnega pomena, če želimo, da državljani sprejmejo nove storitve ([6]).

([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.

([4]) Odgovori na vprašalnik Evropskega parlamenta za komisarko Neelie Kroes v okviru zaslišanj v Evropskem parlamentu, ki so potekala pred imenovanjem komisarke.

([5]) Odgovori na vprašalnik Evropskega parlamenta za komisarko Neelie Kroes v okviru zaslišanj v Evropskem parlamentu, ki so potekala pred imenovanjem komisarke; govor komisarke Viviane Reding z naslovom „Evropski program za digitalne tehnologije za novega potrošnika digitalnih tehnologij“ (*A European Digital Agenda for the New Digital Consumer*) na forumu več zainteresiranih strani, ki ga je BEUC organiziral na temo „Zasebnost potrošnikov in spletno trženje: tržne usmeritve in politične perspektive“ (*Consumer Privacy and Online Marketing: Market Trends and Policy Perspectives*), Bruselj, 12. novembra 2009.

([6]) Glej na primer poročilo RISEPTIS, „Zaupanje v informacijsko družbo“ (*Trust in the Information Society*), poročilo svetovalnega odbora, RISEPTIS (Raziskave in inovacije v zvezi z varnostjo, zasebnostjo in zaupanjem v informacijsko družbo). Na voljo na spletnem naslovu http://www.think-trust.eu/general/news-events/riseptis-report.html Glej tudi: J. B Horrigan, *Broadband Adoption and Use in America*, FCC Omnibus Broadband Initiative, OBI Working Paper Series No 1.

4. EU ima trden pravni okvir za varstvo podatkov/zasebnosti, katerega načela ostajajo v digitalni dobi popolnoma veljavna. Vendar ne smemo počivati na lovorikah. IKT v številnih primerih zbujajo nove skrbi, ki se v sedanjem okviru ne obravnavajo. Zato je treba ukrepati za zagotovitev, da bodo posamezne pravice iz zakonodaje EU še naprej zagotavljale učinkovito varstvo v tem novem okolju.

5. V tem mnenju so obravnavani ukrepi, ki bi jih Evropska unija lahko spodbujala ali izvajala za zagotavljanje zasebnosti in varstva podatkov posameznikov v globaliziranem svetu, ki bo še naprej temeljil na tehnološkem napredku. Obravnavani so zakonodajni in nezakonodajni instrumenti.

6. Po pregledu IKT kot novega razvoja, ki ustvarja priložnosti in tveganja, se v mnenju obravnava potreba po praktični vključitvi varstva podatkov in zasebnosti od samega začetka novih informacijskih in komunikacijskih tehnologij (ki se imenuje načelo „vgrajene zasebnosti“, angl. „privacy by design“). Za prilagoditev skladnosti temu načelu se v mnenju obravnava potreba po vključitvi načela „vgrajene zasebnosti“ v pravni okvir za varstvo podatkov na vsaj dva različna načina. Prvič, treba ga je vključiti kot splošno zavezujoče načelo in, drugič, treba ga je vključiti na posebna področja IKT, na katerih obstajajo posebna tveganja v zvezi z varstvom podatkov/zasebnostjo, ki bi jih bilo mogoče ublažiti z ustrezno tehnično strukturo in načrtovanjem. Ta področja so radiofrekvenčna identifikacija (RFID), aplikacije socialnih omrežij in brskalniške aplikacije. Ne nazadnje so v mnenju predstavljeni predlogi glede drugih orodij in načel, katerih namen je varstvo zasebnosti in podatkov posameznikov v sektorju IKT.

7. Pri obravnavi zgoraj navedenega so v mnenju podrobneje predstavljene nekatere točke, ki jih je k javnemu posvetovanju o prihodnosti zasebnosti prispevala Delovna skupina iz člena 29 ([1]). Mnenje poleg tega temelji na predhodnih mnenjih ENVP, kot so mnenje z dne 25. julija 2007 o izvajanju direktive o varstvu podatkov, Mnenje z dne 20. decembra 2007 o radiofrekvenčni identifikaciji (RFID) in dve mnenji o direktivi o e-zasebnosti ([2]).

II. IKT PONUJAJO NOVE PRILOŽNOSTI, VENDAR POVZROČAJO TUDI NOVA TVEGANJA

8. IKT se primerja z drugimi pomembnimi izumi, kot je elektrika. Čeprav je morda prezgodaj za oceno njihovega dejanskega zgodovinskega vpliva, je povezava med IKT in gospodarsko rastjo v razvitih državah jasna. IKT so ustvarile nova delovna mesta, prinesle gospodarske koristi in prispevale k splošni blaginji. Njihov vpliv presega zgolj gospodarski vidik, saj imajo te tehnologije pomembno vlogo pri spodbujanju inovativnosti in ustvarjalnosti.

9. Poleg tega so IKT spremenile način dela, druženja in interakcije ljudi. Ljudje na primer vse bolj uporabljajo IKT za socialne stike in gospodarske povezave. Posamezniki lahko uporabljajo veliko novih aplikacij IKT, kot so e-zdravstvo, e-promet, e-uprava in inovativni interaktivni sistemi za zabavo in učenje.

10. Vse evropske institucije so zaradi takih koristi izrazile zavezanost k podpori IKT kot nujnega orodja za izboljšanje konkurenčnosti evropske industrije in pospešitev oživitve evropskega gospodarstva. Komisija je avgusta 2009 sprejela Poročilo o digitalni konkurenčnosti Evrope ([3]) in začela javno posvetovanje o ustreznih prihodnjih strategijah za spodbujanje IKT. Svet je 7. decembra 2009 predstavil prispevek k temu posvetovanju z naslovom „Obdobje po strategiji i2010 – v smeri odprte, okolju prijazne in konkurenčne družbe znanja“ ([4]).

([1]) Mnenje št. 168 Delovne skupine iz člena 29 z naslovom „Prihodnost zasebnosti: skupni prispevek k posvetovanju Evropske komisije o pravnem okviru za temeljno pravico do varstva osebnih podatkov“, sprejeto 1. decembra 2009.

([2]) Mnenje 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; Mnenje z dne 20. decembra 2007 o sporočilu Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij z naslovom „Radiofrekvenčna identifikacija (RFID) v Evropi: naslednji koraki k okviru politike“ (COM(2007) 96), UL C 101, 23.4.2008, str. 1; Mnenje z dne 10. aprila 2008 o predlogu direktive, med drugim o spremembi Direktive 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; drugo mnenje z dne 9. januarja 2009 o pregledu Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij.

([3]) Poročilo o digitalni konkurenčnosti Evrope – Glavni dosežki strategije i2010 v obdobju 2005–2009 (SEC(2009) 1060).

([4]) Sklepi Sveta „Obdobje po strategiji i2010 – v smeri odprte, okolju prijazne in konkurenčne družbe znanja“ (17107/09), sprejeti 18. decembra 2009.

Evropski parlament je pred kratkim sprejel poročilo za usmerjanje Komisije pri določitvi digitalne agende ([1]).

11. Priložnosti in koristi, ki spremljajo razvoj IKT, prinašajo nova tveganja, zlasti glede zasebnosti in varstva osebnih podatkov posameznikov. IKT pogosto vodijo k bistvenemu povečanju (zelo pogosto na načine, ki jih posamezniki ne opazijo) števila informacij, ki se zbirajo, razvrščajo, filtrirajo, prenašajo ali kako drugače hranijo, zato se tveganja v zvezi s takimi podatki množijo.

12. Na primer, čipi RFID nadomeščajo črtne kode na (nekaterih) potrošniških izdelkih. Novi sistem naj bi z izboljšanjem informacijskega toka v dobavni verigi (s čimer se zmanjša potreba po „varnostnih“ zalogah, zagotavljajo natančnejše napovedi itd.) koristil podjetjem in potrošnikom. Hkrati pa to prinaša skrb zbujajočo možnost, da bi različni subjekti posameznikom za različne namene sledili prek označenih osebnih predmetov.

13. Drug primer je „računalništvo v oblaku“, ki je v bistvu zagotavljanje gostiteljskih potrošniških in nepotrošniških aplikacijskih storitev prek interneta. Te segajo od fototek, koledarjev, spletne pošte in podatkovnih zbirk o potrošnikih do bolj zapletenih poslovnih storitev. Koristi za podjetja in posameznike so jasne: znižanje stroškov (stroški naraščajo), lokacija ni pomembna (lahek dostop do informacij kjer koli na svetu), avtomatizacija (ni potrebe po namenskih virih IT in posodabljanju programske opreme) itd. Hkrati so nevarnosti varnostnih težav in vdorov v računalniške sisteme zelo resnične. Prav tako obstaja zaskrbljenost, da bi izgubili dostop do lastnih podatkov in nadzor nad njimi.

14. Dokazano je, da koristi in tveganja soobstajajo tudi na drugih področjih, na katerih se uporabljajo aplikacije IKT. To je mogoče ponazoriti na primeru e-zdravstva, ki lahko izboljša učinkovitost, zniža stroške, poveča dostopnost in na splošno izboljša kakovost zdravstvenih storitev. Vendar je pogosto vprašanje zakonitosti sekundarne uporabe informacij e-zdravstva, kar zahteva pazljivo analizo namenov vsake morebitne sekundarne uporabe ([2]). Poleg tega so ob vse bolj razširjeni uporabi elektronskih zdravstvenih zapisov pogosti škandali v zvezi s samimi sistemi, v katerih je bilo ugotovljenih veliko primerov vdorov v elektronske zdravstvene kartoteke.

15. Če povzamemo, določena stopnja preostalega tveganja bo verjetno obstajala še naprej, celo po izvedbi ustreznih ocen in izvedbi potrebnih ukrepov. Nično tveganje ni stvarno. Kot bo dodatno obravnavano v nadaljevanju, je mogoče in treba izvajati ukrepe za zmanjšanje takega tveganja na ustrezne ravni.

III. VGRAJENA ZASEBNOST KOT KLJUČNO ORODJE ZA PRIDOBITEV ZAUPANJA POSAMEZNIKOV V IKT

16. Mogoče koristi IKT se lahko v praksi uresničijo le, če lahko pridobijo zaupanje, ali z drugimi besedami, če lahko zagotovijo pripravljenost uporabnikov, da se zanašajo na IKT zaradi njihovih značilnosti in koristi. Tako zaupanje bo pridobljeno le, če so IKT zanesljive, varne, pod nadzorom posameznikov ter če je zagotovljeno varstvo njihovih osebnih podatkov in zaupnosti.

17. Splošno razširjena tveganja in napake, kot so tiste, opisane zgoraj, zlasti ko vključujejo zlorabo ali kršitve varnosti osebnih podatkov, ki razkrivajo zasebnost posameznikov, bodo verjetno ogrozile zaupanje uporabnikov v informacijsko družbo. To bi lahko resno ogrozilo razvoj IKT in koristi, ki bi jih lahko prinesle.

18. Vendar rešitev za odpravo teh tveganj v zvezi z zasebnostjo in varstvom podatkov ne more biti odpraviti, izključiti ali zavrniti uporabo ali spodbujanje IKT. To ne bi bilo niti izvedljivo niti stvarno; posameznikom bi preprečilo, da bi imeli koristi od IKT, in resno omejilo splošne prednosti, ki jih omogočajo te tehnologije.

19. ENVP verjame, da je bolj pozitivna rešitev načrtovati in razvijati IKT na način, ki spoštuje zasebnost in varstvo podatkov. Zato je ključnega pomena, da sta zasebnost in varstvo podatkov vključena v celoten življenjski krog tehnologije, od zelo zgodnje faze zasnove vse do njene končne uvedbe, uporabe in končne odstranitve. To se navadno imenuje „vgrajena zasebnost“, ki bo podrobneje obravnavana v nadaljevanju.

20. Vgrajena zasebnost lahko vključuje različne ukrepe, odvisno od posameznega primera ali aplikacije. V nekaterih primerih lahko na primer zahteva izločitev/omejitev osebnih podatkov ali preprečitev nepotrebne in/ali neželene obdelave. V drugih primerih lahko vključuje zagotavljanje orodij za krepitev nadzora posameznikov nad njihovimi osebnimi podatki. O takih ukrepih je treba

([1]) Poročilo o določitvi nove digitalne agende za Evropo: od i2010 k digital.eu (2009/2225 (INI), sprejeto 18. marca 2010.

([2]) Na primer, skrbno bi bilo treba proučiti, da se zdravstvene informacije, zbrane za namene zdravljenja, ne prodajajo ali uporabljajo za izbiro lokacij za pomožne klinike, ustanovitev ambulantnih kirurških centrov ali kako drugače za načrtovanje prihodnjih dejavnosti s finančnimi posledicami.

razmisliti, ko so standardi in/ali najboljše prakse opredeljeni. Prav tako jih je mogoče vključiti v strukturo informacijskih in komunikacijskih sistemov ali v strukturne organizacije subjektov, ki obdelujejo osebne podatke.

III.1. **Načelo vgrajene zasebnosti, ki se uporablja v različnih okoljih IKT, in njihov vpliv**

21. Potrebo po načelu vgrajene zasebnosti lahko najdemo v številnih različnih okoljih IKT. Na primer, zdravstveni sektor vse bolj uporablja infrastrukture IKT, ki pogosto vključujejo centralizirano hrambo informacij o zdravju bolnikov. Uporaba načela vgrajene zasebnosti v zdravstvenem sektorju bi zahtevala oceno ustreznosti različnih ukrepov, kot je možnost zmanjševanja obsega centralno shranjenih podatkov ali omejitev teh podatkov na kazalo, uporabo orodij za šifriranje, dodeljevanje pravic dostopa strogo „na podlagi potrebe po seznanitvi“, anonimizacija podatkov, ko niso več potrebni, itd.

22. Podobno prometni sistemi vse bolj delujejo s privzetimi naprednimi aplikacijami IKT, ki za različne namene in funkcije delujejo vzajemno z vozilom in njegovim okoljem. Avtomobili so na primer vse bolj opremljeni z novimi funkcionalnostmi IKT (GPS, GSM, mrežo senzorjev itd.), ki poleg njihove lokacije prikazujejo tudi tehnične razmere v realnem času. Te informacije bi bilo na primer mogoče uporabiti za nadomestitev sedanjega sistema cestne takse s cestnino glede na dejansko uporabo. Uporaba vgrajene zasebnosti pri načrtovanju strukture takih sistemov bi morala podpirati obdelavo in nadaljnji prenos kar najmanjše količine osebnih podatkov ([1]). Ob upoštevanju tega načela bi bilo primerneje kot centralizirane strukture uporabljati decentralizirane ali poldecentralizirane strukture, ki omejujejo razkritje podatkov o lokaciji na centralno točko.

23. Zgornji primeri kažejo, da se lahko tveganja v zvezi z zasebnostjo in varstvom podatkov bistveno zmanjšajo, če so informacijske in komunikacijske tehnologije zgrajene v skladu z načelom vgrajene zasebnosti.

III.2. **Nezadostna uvedba IKT, ki uporabljajo vgrajeno zasebnost**

24. Pomembno vprašanje je, ali so gospodarski subjekti, proizvajalci/ponudniki IKT in upravljavci podatkov zainteresirani za trženje in izvajanje načela vgrajene zasebnosti v IKT. V zvezi s tem je treba oceniti tudi povpraševanje uporabnikov po vgrajeni zasebnosti.

25. Komisija je leta 2007 izdala sporočilo, v katerem je podjetja pozvala, naj bodo inovativna pri oblikovanju in izvajanju tehnologij za boljše varovanje zasebnosti kot načina za izboljšanje varstva zasebnosti in osebnih podatkov od samega začetka razvojnega cikla ([2]).

26. Doslej razpoložljivi podatki pa kažejo, da niti proizvajalcem IKT niti upravljavcem podatkov (v zasebnem ali javnem sektorju) ni uspelo dosledno izvajati ali tržiti vgrajene zasebnosti. Navajajo se različni razlogi, vključno s pomanjkanjem gospodarskih spodbud ali institucionalne podpore, nezadostnim povpraševanjem itd ([3]).

27. Hkrati je povpraševanje uporabnikov po vgrajeni zasebnosti precej majhno. Uporabniki proizvodov in storitev IKT lahko upravičeno domnevajo, da so njihova zasebnost in osebni podatki dejansko zavarovani, čeprav v številnih primerih to ne drži. V nekaterih primerih preprosto ne morejo sprejeti varnostnih ukrepov, s katerimi bi zavarovali svoje osebne podatke ali osebne podatke drugih. V številnih primerih je to posledica popolnega ali celo delnega nepoznavanja tveganj. Mladi ljudje se na splošno na primer ne zavedajo tveganj za zasebnost, povezanih z objavljanjem osebnih podatkov v socialnih omrežjih, in se pogosto ne menijo za nastavitve zasebnosti. Drugi uporabniki se morda zavedajo tveganj, vendar nimajo potrebnega tehničnega znanja za uvedbo zaščitnih tehnologij, kot so tiste, ki varujejo njihovo internetno povezavo, ali za spremembo nastavitev brskalnika za zmanjšanje profiliranja na podlagi spremljanja njihovega brskanja po spletnih straneh.

28. Vendar so tveganja za varstvo zasebnosti in varstvo podatkov zelo resnična. Če se zasebnost in varstvo podatkov ne upoštevata od začetka, je pogosto prepozno in z ekonomskega vidika preveč nerodno, da bi popravili

([1]) Glej Mnenje evropskega nadzornika za varstvo podatkov z dne 22. julija 2009 o sporočilu Komisije z naslovom „Akcijski načrt za uvajanje inteligentnih prometnih sistemov v Evropi“ ter spremljajočem predlogu direktive Evropskega parlamenta in Sveta o določitvi okvira za uvajanje inteligentnih prometnih sistemov v cestnem prometu in vmesnike do drugih vrst prevoza, na voljo na spletnem naslovu: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

([2]) Sporočilo Komisije Evropskemu parlamentu in Svetu z dne 2. maja 2007 o spodbujanju varstva podatkov s tehnologijami za boljše varovanje zasebnosti (PET), COM(2007) 228 konč.

([3]) Študija o ekonomskih koristih tehnologij za boljše varovanje zasebnosti (PET), JLS/2008/D4/036.

sisteme, obenem pa prepozno za odpravo že povzročene škode. Vse večje število kršitev varnosti podatkov v zadnjih letih odlično ponazarja to težavo in krepi potrebo po vgrajeni zasebnosti.

29. Zgoraj navedeno jasno kaže, da morajo biti proizvajalci in ponudniki tehnologij IKT, načrtovanih za obdelavo osebnih podatkov, skupaj z upravljavci podatkov odgovorni, da jih načrtujejo z vgrajenimi zaščitnimi ukrepi glede varstva podatkov in zasebnosti. V številnih primerih to pomeni, da jih je treba načrtovati z nastavitvami vgrajene zasebnosti.

30. Na podlagi navedenega je treba razmisliti, katere ukrepe morajo sprejeti oblikovalci politike za spodbujanje vgrajene zasebnosti pri razvoju IKT. Prvo vprašanje je, ali sedanji pravni okvir za varstvo podatkov vsebuje ustrezne določbe za zagotavljanje, da upravljavci podatkov in proizvajalci/razvijalci upoštevajo načelo vgrajene zasebnosti. Drugo vprašanje je, kaj je treba narediti v okviru evropskega programa za digitalne tehnologije, da bi sektor IKT pridobival zaupanje potrošnikov.

IV. VKLJUČITEV NAČELA VGRAJENE ZASEBNOSTI V ZAKONE IN POLITIKE EU

IV.1. Sedanji pravni okvir za varstvo podatkov in zasebnosti

31. EU ima vzpostavljen trden okvir za varstvo podatkov in zasebnosti v Direktivi 95/46/ES ([1]), Direktivi 2002/58/ES ([2]) ter sodni praksi Evropskega sodišča za človekove pravice ([3]) in Sodišča Evropske unije.

32. Direktiva o varstvu podatkov se uporablja za „*kakršen koli postopek ali niz postopkov, ki se izvajajo v zvezi z osebnimi podatki*“ (zbiranje, shranjevanje, razkrivanje itd.). Od tistih, ki obdelujejo osebne podatke („upravljavci podatkov“), zahteva skladnost z določenimi načeli in obveznostmi. Določa posamezne pravice, kot so pravica do dostopa do osebnih informacij. Direktiva o e-zasebnosti posebej obravnava varstvo zasebnosti v sektorju elektronskih komunikacij ([4]).

33. Veljavna direktiva o varstvu podatkov ne vključuje nobene izrecne zahteve po vgrajeni zasebnosti. Vendar vključuje določbe, s katerimi se lahko v različnih primerih posredno zahteva izvajanje načela vgrajene zasebnosti. Zlasti se s členom 17 zahteva, naj upravljavci podatkov izvajajo ustrezne tehnične in organizacijske ukrepe za preprečevanje nezakonite obdelave podatkov ([5]). Vgrajena zasebnost je zato obravnavana zelo na splošno. Poleg tega se določbe direktive nanašajo predvsem na upravljavce podatkov in njihovo obdelavo osebnih informacij. Določbe izrecno ne zahtevajo, naj bodo informacijske in komunikacijske tehnologije skladne z zahtevami po varstvu zasebnosti in podatkov, kar zahteva tudi obravnavo načrtovalcev in proizvajalcev IKT, vključno z dejavnostmi v fazi standardizacije.

34. Direktiva o e-zasebnosti je bolj izrecna. Člen 14(3) določa, da „[k]adar je potrebno, se lahko sprejmejo ukrepi, ki zagotovijo, da je terminalska oprema zgrajena na način, ki je združljiv s pravico uporabnikov do varstva in nadzora uporabe njihovih osebnih podatkov, v skladu z Direktivo 1999/5/ES in Sklepom Sveta 87/95/EGS z dne 22. decembra 1986 o standardizaciji na področju informacijske tehnike/tehnologije in komunikacij“. Vendar se ta določba ni nikoli uporabila ([6]).

35. Čeprav zgornje določbe zadevnih dveh direktiv pomagajo pri *spodbujanju* vgrajene zasebnosti, v praksi ne zadostujejo za *zagotovitev*, da je zasebnost vključena v IKT.

36. Zaradi zgoraj navedenega se z zakonodajo ne zahteva dovolj natančno, naj bodo IKT načrtovane v skladu z načelom vgrajene zasebnosti. Poleg tega organi za varstvo podatkov nimajo dovolj pristojnosti za zagotavljanje

([1]) Direktiva 95/46/ES Evropskega parlamenta in Sveta (v nadaljnjem besedilu: direktiva o varstvu podatkov).

([2]) Direktiva 2002/58/ES Evropskega parlamenta in Sveta (v nadaljnjem besedilu:direktiva o e-zasebnosti).

([3]) Razlaga glavnih elementov in pogojev iz člena 8 Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin (EKČP), sprejete v Rimu dne 4. novembra 1950, kot se uporabljajo za različna področja.

([4]) Lizbonska pogodba je okrepila tako varstvo s priznanjem spoštovanja zasebnega življenja in varstva osebnih podatkov kot ločenih temeljnih pravic v členih 7 in 8 Listine Evropske unije o temeljnih pravicah. Listina Evropske unije o temeljnih pravicah je postala zavezujoča, ko je začela veljati Lizbonska pogodba.

([5]) Člen 17 se glasi: „Države članice določijo, da mora upravljavec izvajati ustrezne tehnične in organizacijske ukrepe za zavarovanje osebnih podatkov pred slučajnim ali nezakonitim uničenjem ali slučajno izgubo, predelavo, nepooblaščenim posredovanjem ali dostopom, predvsem kadar obdelava vključuje prenos podatkov po omrežju, ter proti vsem drugim nezakonitim oblikam obdelave.“ Uvodna izjava 46 dopolnjuje ta člen z naslednjim: „ker varstvo pravic in svoboščin posameznikov, na katere se osebni podatki nanašajo, v zvezi z obdelavo osebnih podatkov zahteva, da se sprejmejo primerni tehnični in organizacijski ukrepi med načrtovanjem sistema obdelave, pa tudi med samo obdelavo, predvsem zato, da bi ohranjali varnost in tako preprečili vsako nepooblaščeno obdelavo.“

([6]) Komisija je napovedala posodobitev Direktive 1999/5/ES proti koncu leta 2010.

vključevanja vgrajene zasebnosti. To vodi k neučinkovitosti. Organi za varstvo podatkov lahko na primer naložijo kazni za neodgovarjanje na zahtevke posameznikov za dostop do podatkov in imajo pristojnost, zahtevati izvajanje nekaterih ukrepov za preprečevanje nezakonite obdelave podatkov. Vendar ni vedno dovolj jasno, ali lahko na podlagi svojih pristojnosti zahtevajo, da mora biti sistem načrtovan tako, da lajša uveljavljanje pravic do varstva podatkov posameznikov ([1]). Na primer, na podlagi veljavnih zakonskih določb ni jasno, ali je mogoče zahtevati, da naj bo zgradba informacijskega sistema načrtovana tako, da omogoča lažje odzivanje podjetij na zahteve za dostop do podatkov posameznikov, s čimer lahko take zahteve obdelujejo samodejno in hitreje. Poleg tega lahko poznejši poskusi spreminjanja tehnologije, ko je že bila razvita ali uvedena, pripeljejo do vrste najrazličnejših rešitev, ki ne delujejo v celoti, poleg tega pa so ekonomsko nerentabilne.

37. Po mnenju ENVP, ki se strinja z Delovno skupino iz člena 29 ([2]), bi bilo mogoče v sedanjem pravnem okviru izrecneje podpreti načelo vgrajene zasebnosti.

IV.2. **Vključevanje vgrajene zasebnosti na različne ravni**

38. ENVP na podlagi navedenega Komisiji priporoča, da sprejme štiri ukrepe:

(a) predlaga vključitev splošne določbe o vgrajeni zasebnosti v pravni okvir za varstvo podatkov;

(b) natančno opredeli to splošno določbo v posebnih določbah, kadar so predlagani posebni pravni instrumenti v različnih sektorjih. Te posebne določbe bi bilo mogoče že zdaj vključiti v pravne instrumente na podlagi člena 17 direktive o varstvu podatkov (in druge veljavne zakonodaje);

(c) vgrajeno zasebnost kot vodilno načelo vključi v evropski program za digitalne tehnologije;

(d) vgrajeno zasebnost kot načelo uvede v druge pobude EU (predvsem nezakonodajne).

Splošna določba o vgrajeni zasebnosti

39. ENVP predlaga nedvoumno in izrecno vključitev načela vgrajene zasebnosti v sedanji zakonodajni okvir za varstvo podatkov. Načelo vgrajene zasebnosti bi tako postalo močnejše in bolj izrecno, kar bi prispevalo k njegovemu učinkovitemu izvajanju, poleg tega pa bi dalo več legitimnosti izvršilnim organom, da zahtevajo njegovo dejansko uporabo v praksi. To je zlasti potrebno zaradi zgoraj opisanih dejstev, ne samo zaradi pomena načela samega kot orodja za spodbujanje zaupanja, temveč tudi kot spodbudo zainteresiranim stranem za izvajanje načela vgrajene zasebnosti in krepitev jamstev, ki jih določa sedanji pravni okvir.

40. Ta predlog temelji na priporočilu Delovne skupine iz člena 29 za uvedbo načela „vgrajene zasebnosti“ kot splošnega načela v pravni okvir za varstvo podatkov, zlasti v direktivo o varstvu podatkov. Po navedbah Delovne skupine iz člena 29: „To načelo mora biti zavezujoče za načrtovalce in proizvajalce tehnologije ter upravljavce podatkov, ki odločajo o nakupu in uporabi IKT. Ti bi morali upoštevati varstvo tehnoloških podatkov že v fazi načrtovanja informacijsko-tehnoloških postopkov in sistemov. Ponudniki takih sistemov ali storitev in upravljavci morajo dokazati, da so sprejeli vse potrebne ukrepe za skladnost s temi zahtevami.“

41. ENVP prav tako pozdravlja dejstvo, da je komisarka Viviane Reding v okviru napovedane revizije direktive o varstvu podatkov potrdila načelo vgrajene zasebnosti ([3]).

42. S tem preidemo na vsebino takega zakonskega urejanja. Prvo in najpomembneje je, da mora biti splošno načelo vgrajene zasebnosti tehnološko nevtralno. Namen tega načela ni zakonsko urejanje tehnologije, tj. načelo ne sme predpisovati posebnih tehničnih rešitev. Namesto tega mora določati, da se veljavna načela varstva zasebnosti in podatkov vključijo v informacijske in komunikacijske sisteme in rešitve. To bo zainteresiranim stranem, proizvajalcem, upravljavcem podatkov in organom za varstvo podatkov omogočilo, da si pomen načela razlagajo za vsak primer posebej. Drugič, skladnost z načelom

([1]) Glej poročilo Urada informacijskega pooblaščenca Združenega kraljestva z naslovom „Vgrajena zasebnost“, objavljeno novembra 2008.

([2]) Glej Mnenje št. 168 Delovne skupine iz člena 29 z naslovom „Prihodnost zasebnosti: skupni prispevek k posvetovanju Evropske komisije o pravnem okviru za temeljno pravico do varstva osebnih podatkov“, sprejeto 1. decembra 2009.

([3]) „Vgrajena zasebnost“ je načelo, ki je v interesu državljanov in podjetij. Pripeljala bo do boljšega varstva za posameznike ter zaupanja v nove storitve in proizvode, kar bo pozitivno vplivalo na gospodarstvo. Na voljo je nekaj spodbudnih primerov, vendar je dela še veliko. Programski govor na dnevu varstva podatkov 28. januarja 2010, Evropski parlament, Bruselj.

mora biti obvezna v različnih fazah, od oblikovanja standardov in načrtovanja zgradbe do njihovega izvajanja s strani upravljavca podatkov.

Določbe v posebnih pravnih instrumentih

43. Sedanji in prihodnji zakonodajni instrumenti morajo vključevati načelo vgrajene zasebnosti na podlagi sedanjega pravnega okvira, po sprejetju zgoraj predlagane splošne določbe pa tudi na podlagi te določbe. Na primer, v skladu s sedanjimi pobudami, povezanimi z inteligentnimi prometnimi sistemi, bo Komisija nosila posebno začetno odgovornost pri določitvi ukrepov, pobud za standardizacijo, postopkov in dobrih praks. Vodilno načelo pri opravljanju teh nalog mora biti vgrajena zasebnost.

44. ENVP nadalje ugotavlja, da je načelo vgrajene zasebnosti zlasti pomembno na področju svobode, varnosti in pravice, zlasti v zvezi s cilji strategije za upravljanje informacij, kot so predvideni v stockholmskem programu ([1]). ENVP je v mnenju o stockholmskem programu poudaril, da mora struktura za izmenjavo informacij temeljiti na „vgrajeni zasebnosti“ ([2]): „Natančneje to pomeni, da bi morali pri razvoju informacijskih sistemov, oblikovanih za namene javne varnosti, zmeraj upoštevati načelo vgrajene zasebnosti.“

45. V mnenju Delovne skupine iz člena 29 o prihodnosti zasebnosti ([3]) je še natančneje navedeno, da morajo biti na področju svobode, varnosti in pravice – na katerem so javni organi glavni akterji, ukrepi, ki krepijo nadzor, pa neposredno vplivajo na temeljni pravici do zasebnosti in varstva podatkov – zahteve po vgrajeni zasebnosti nujne. Vlade bi z uvedbo teh zahtev v informacijske sisteme kot prvi naročniki spodbujale tudi vgrajeno zasebnost.

Vgrajena zasebnost kot vodilno načelo v evropskem programu za digitalne tehnologije

46. Informacijske in komunikacijske tehnologije so vse bolj zapletene in vključujejo večja tveganja v zvezi z zasebnostjo in varstvom podatkov. Na splošno so digitalizirane informacije, do katerih je lažje dostopati ter jih je lažje kopirati in prenašati, izpostavljene precej večjim tveganjem od informacij v papirni obliki. Bližje bomo omrežjem medsebojno povezanih stvari, večja bodo tveganja. Večja kot so tveganja v zvezi z zasebnostjo/varnostjo podatkov, večje bo povpraševanje po okrepljenih zaščitnih ukrepih glede varstva podatkov/zasebnosti. Zato je utemeljitvam potrebe po izvajanju vgrajene zasebnosti v sektorju IKT težje nasprotovati. Poleg tega – kot je bilo navedeno zgoraj – je zaupanje posameznikov v IKT nujno, če hočemo, da državljani sprejmejo te nove storitve, pri čemer sta zasebnost in varstvo podatkov ključna elementa takega zaupanja.

47. Zgoraj navedeno poudarja, da mora strategija za razvoj IKT potrditi potrebo po tem, da se načrtuje z neločljivo povezanim elementom zasebnosti in varstva podatkov, tj. ob upoštevanju načela vgrajene zasebnosti.

48. Zato mora biti v evropskem programu za digitalne tehnologije načelo vgrajene zasebnosti izrecno potrjeno kot nujen element za zagotavljanje zaupanja državljanov v IKT in spletne storitve. V njem je treba priznati, da sta zasebnost in zaupanje neločljivo povezana ter da mora biti vgrajena zasebnost vodilna pri razvoju sektorja IKT, ki je vreden zaupanja.

Vgrajena zasebnost kot načelo v drugih pobudah EU

49. Vgrajena zasebnost mora biti za Komisijo vodilno načelo pri izvajanju politik, dejavnosti in pobud v posebnih sektorjih IKT, vključno z e-zdravstvom, e-javnimi naročili, e-socialno varnostjo, e-učenjem itd. Številne od teh pobud bodo posamezni ukrepi v evropskem programu za digitalne tehnologije.

50. To na primer pomeni, da morajo pobude za zagotavljanje, da so vladne aplikacije učinkovitejše in sodobnejše, da lahko posamezniki vzajemno delujejo z upravami, vključevati potrebo po tem, da so te aplikacije načrtovane in delujejo v skladu z načelom vgrajene zasebnosti. Enako velja za politike in dejavnosti Komisije, ki zagotavljajo hitrejši internet, digitalne vsebine ali splošno spodbujanje fiksnih in brezžičnih komunikacij ter prenosa podatkov.

([1]) Stockholmski program – odprta in varna Evropa, ki služi državljanom in jih varuje; Evropski svet ga je odobril decembra 2009.

([2]) Mnenje z dne 10. julija 2009 o sporočilu Komisije Evropskemu parlamentu in Svetu o območju svobode, varnosti in pravice za državljane, UL C 276, 17.11.2009, str. 8, točka 60.

([3]) Mnenje št. 168 Delovne skupine iz člena 29 z naslovom „Prihodnost zasebnosti: skupni prispevek k posvetovanju Evropske komisije o pravnem okviru za temeljno pravico do varstva osebnih podatkov“, sprejeto 1. decembra 2009.

51. Zgoraj navedeno vključuje tudi področja, na katerih je Komisija odgovorna za obsežne sisteme IT, kot sta SIS in VIS, ter tiste primere, v katerih je odgovornost Komisije omejena na razvoj in vzdrževanje skupne infrastrukture takega sistema, kot je evropski informacijski sistem kazenskih evidenc (ECRIS).

52. Kako se bo razvilo načelo vgrajene zasebnosti, bo odvisno od vsakega posameznega sektorja in primera. Kadar bodo pobude Komisije na primer spremljali zakonodajni predlogi o posebnem sektorju IKT, bo v številnih primerih ustrezno vključiti izrecno napotilo na pojem vgrajene zasebnosti, ki se uporablja za načrtovanje posamezne aplikacije/sistema IKT. Če so načrtovani akcijski načrti za posebno področje, morajo ti sistematično zagotoviti uporabo pravnega okvira in natančneje zajamčiti, da je ustrezna tehnologija IKT vzpostavljena ob upoštevanju vgrajene zasebnosti.

53. Kar zadeva raziskave, je treba sedmi okvirni program in naslednje programe uporabljati kot orodje za podporo projektom, katerih cilj je analiza standardov, tehnologij IKT in strukture, ki spodbujajo zasebnost in, natančneje, načelo vgrajene zasebnosti. Poleg tega mora biti vgrajena zasebnost tudi nujni element, ki ga je treba upoštevati v obsežnejših projektih IKT, katerih cilj je obdelava osebnih podatkov posameznikov.

Področja, ki zbujajo posebno skrb

54. V nekaterih primerih je zaradi posebnih tveganj za zasebnost posameznikov ali varstvo njihovih podatkov ali zaradi drugih dejavnikov (nepripravljenosti industrije, da zagotovi proizvode vgrajene zasebnosti, povpraševanja potrošnikov itd.) morda treba opredeliti izrecnejše in posebne ukrepe glede vgrajene zasebnosti ter jih vključiti v določeno vrsto informacijskih in komunikacijskih proizvodov/tehnologij, najsibo v zakonodajne instrumente ali ne.

55. ENVP je opredelil različna področja (RFID, socialno mreženje in brskalniške aplikacije), ki si po njegovem mnenju v tej fazi zaslužijo temeljit razmislek Komisije in bolj praktično ukrepanje, kot je bilo priporočeno zgoraj. Ta tri področja so nadalje obravnavana v nadaljevanju.

V. **RADIOFREKVENČNA IDENTIFIKACIJA – RFID**

56. Oddajnike RFID je mogoče vgraditi v predmete, živali in ljudi. Uporabljati jih je mogoče za zbiranje in shranjevanje osebnih podatkov, kot so zdravstvene evidence, sledenje gibanja ljudi ali profiliranje njihovega vedenja za različne namene. To je mogoče storiti, ne da se posameznik tega zaveda ([1]).

57. Učinkovita jamstva glede varstva podatkov, zasebnosti in vseh povezanih etičnih razsežnosti so ključna za zaupanje javnosti v RFID in prihodnji internet stvari. Le takrat je mogoče od te tehnologije pričakovati številne gospodarske in družbene koristi.

V.1. **Vrzeli veljavnega pravnega okvira za varstvo podatkov**

58. Direktiva o varstvu podatkov in direktiva o e-zasebnosti se uporabljata za zbiranje podatkov, ki se izvaja prek aplikacij RFID ([2]). Med drugim se z njima zahteva, naj se za upravljanje aplikacij RFID vzpostavijo ustrezni zaščitni ukrepi glede varstva zasebnosti ([3]).

59. Vendar se v tem pravnem okviru ne obravnavajo v celoti vsa vprašanja v zvezi z varstvom podatkov in zasebnosti, ki se porajajo v zvezi s to tehnologijo. Razlog je, da direktivi nista dovolj natančni glede vrste zaščitnih

([1]) RFID pomeni radiofrekvenčna identifikacija. Glavni deli radiofrekvenčne identifikacijske tehnologije *ali* infrastrukture so *oddajnik* (tj. mikročip), čitalnik in aplikacija, povezana z oddajniki in čitalniki prek vmesne programske opreme (*middleware*) za obdelavo proizvedenih podatkov. Oddajnik je sestavljen iz elektronskega vezja, ki shranjuje podatke, in antene, ki podatke sporoča prek radijskih valov. Čitalnik ima anteno in demodulator, ki prevaja vhodne analogne informacije iz radijske povezave v digitalne podatke. Informacije je nato mogoče poslati prek omrežij v podatkovne zbirke in strežnike v računalniško obdelavo.

([2]) Direktiva o e-zasebnosti se sklicuje na RFID v členu 3: „Ta direktiva se uporablja za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v Skupnosti, vključno z javnimi komunikacijskimi omrežji, ki podpirajo zbiranje podatkov in identifikacijske naprave“. To dopolnjuje uvodna izjava 56: „Tehnološki napredek omogoča razvoj novih aplikacij na podlagi naprav za zbiranje podatkov in identifikacijo, ki so lahko brezkontaktne naprave, ki uporabljajo radijske frekvence. Naprave za radiofrekvenčno identifikacijo (RFID) na primer uporabljajo radijske frekvence za zajetje podatkov iz enoznačno prepoznavne oznake, ki jih je nato mogoče prenesti po obstoječih komunikacijskih omrežjih. Široka uporaba takih tehnologij lahko prinese velike gospodarske in družbene koristi ter s tem predstavlja velik prispevek k notranjemu trgu, če je njihova uporaba za državljane sprejemljiva. Da bi dosegli ta cilj, je treba zagotoviti varstvo temeljnih pravic posameznikov, vključno s pravico do zasebnosti in varstva podatkov. Če se take naprave priključi na javno dostopna elektronska komunikacijska omrežja ali če uporabljajo elektronske komunikacijske storitve kot osnovno infrastrukturo, bi se morale uporabljati ustrezne določbe Direktive 2002/58/ES (Direktiva o zasebnosti in elektronskih komunikacijah), vključno z določbami o varnosti, podatkih o prometu in lokaciji ter o zaupnosti.“

([3]) Člen 17 Direktive o varstvu podatkov na primer nalaga obveznost izvajanja ustreznih tehničnih in organizacijskih ukrepov za varstvo osebnih podatkov pred naključnim ali nezakonitim uničenjem ali nepooblaščenim razkritjem.

ukrepov, ki jih je treba izvajati v aplikacijah RFID. Veljavna pravila je treba dopolniti z dodatnimi pravili, ki nalagajo posebne varnostne ukrepe, zlasti obveznost vključevanja tehničnih rešitev (vgrajene zasebnosti) v tehnologijo RFID. To drži za oddajnike, ki hranijo osebne informacije in bi morali imeti ukaze „kill“, in uporabo kriptografije v oddajnikih za hranjenje določenih vrst osebnih informacij.

V.2. **Samourejanje kot prvi korak**

60. Komisija je marca 2007 sprejela sporočilo ([1]), v katerem je med drugim priznala potrebo po natančnih smernicah o dejanskem izvajanju tehnologije RFID in sprejetju meril za načrtovanje, s katerimi se preprečijo tveganja za zasebnost in varnost.

61. Komisija je za dosego teh ciljev maja 2009 sprejela priporočilo o izvajanju načel varstva zasebnosti in varstva podatkov v aplikacijah RFID ([2]). V njem je določeno, da je treba v aplikacijah RFID, ki se prodajajo na drobno, oddajnik deaktivirati na prodajnem mestu, razen če se posamezniki strinjajo, da je aktiviran. To se ne uporablja, če je v oceni učinka na varstvo zasebnosti in varstvo podatkov ugotovljeno, da oddajniki ne pomenijo morebitnega tveganja za zasebnost ali varstvo osebnih podatkov. V tem primeru ostanejo delujoči tudi po prodajnem mestu, razen če se posamezniki odločijo za deaktivacijo, ki je brezplačna.

62. ENVP se strinja s pristopom Komisije, ki vključuje uporabo instrumentov za samourejanje. Kot je pojasnjeno v nadaljevanju, pa je mogoče, da samourejanje ne bo imelo pričakovanih rezultatov, zato ENVP poziva Komisijo, naj bo pripravljena na sprejetje nadomestnih ukrepov.

V.3. **Področja, ki zbujajo skrb, in mogoči dodatni ukrepi v primeru neuspešnega samourejanja**

63. ENVP je zaskrbljen, da bi lahko organizacije, ki upravljajo aplikacije RFID v maloprodajnem sektorju, prezrle možnost, da lahko neželene tretje osebe spremljajo oddajnike RFID. Tako spremljanje lahko razkrije osebne podatke, shranjene v oddajniku (če podatki obstajajo), poleg tega pa lahko tretji osebi omogoči, da osebo spremlja ali prepozna v času zgolj z uporabo edinstvenih identifikatorjev v enem ali več oddajnikih, ki jih nosi posameznik, v okolju, ki je lahko celo zunaj operativnega obsega aplikacije RFID. Skrbi ga tudi, da bi se lahko upravljavci aplikacij RFID pretirano zanašali na izjeme in tako puščali, da oddajnik deluje po prodajnem mestu.

64. Če se zgodi zgoraj navedeno, bo morda prepozno za ublažitev tveganj za varstvo podatkov in zasebnost posameznikov, ki sta morda že prizadeta. Poleg tega so lahko nacionalni izvršilni organi zaradi narave samourejanja v slabšem položaju, ko od organizacij, ki upravljajo aplikacije RFID, zahtevajo uporabo posebnih ukrepov glede vgrajene zasebnosti.

65. ENVP na podlagi navedenega Komisijo poziva, naj bo pripravljena, da predlaga zakonodajne instrumente, ki urejajo glavna vprašanja uporabe RFID, če izvajanje sedanjega pravnega okvira ne bo učinkovito. Komisija ne sme neustrezno odlašati z oceno; odlašanje bi ogrozilo posameznike in negativno vplivalo na industrijo, saj so pravne negotovosti prevelike, poleg tega pa je zakoreninjene težave verjetno težje in dražje odpraviti.

66. Med ukrepi, ki jih bo morda treba predlagati, ENVP priporoča določitev načela privolitve (*opt-in*, upoštevanje privolitve posameznika za uporabo njegovih podatkov) na prodajnem mestu, v skladu s katerim bi bili vsi oddajniki RFID, nameščeni na potrošniške proizvode, na prodajnem mestu samodejno deaktivirani. Morda Komisiji ni treba ali zanjo ni primerno določiti konkretno tehnologijo, ki jo je treba uporabljati. Namesto tega je treba v zakonodaji Unije določiti zakonsko obveznost pridobitve privolitve in operaterjem omogočiti, da se sami odločijo, kako bodo izpolnili zahtevo.

V.4. **Nadaljnja vprašanja, ki jih je treba proučiti: upravljanje interneta stvari**

67. Informacije, ki jih ustvarjajo oddajniki RFID – na primer informacije o izdelkih –, je mogoče povezati v globalno omrežje komunikacijske infrastrukture. To se navadno imenuje „internet stvari“. Vprašanja v zvezi z varstvom podatkov/zasebnosti se porajajo, ker lahko predmete resničnega sveta identificirajo oddajniki RFID, ki lahko poleg informacij o proizvodih vključujejo osebne podatke.

68. Obstajajo številna odprta vprašanja o tem, kdo bo upravljal shranjevanje informacij v zvezi s predmeti, opremljenimi z oddajnikom. Kakšna bo organizacija? Kdo bo imel dostop do teh informacij? Komisija je junija 2009 sprejela sporočilo o internetu stvari ([3]), v katerem so bile izrecno opredeljene mogoče težave v zvezi z varstvom podatkov in zasebnostjo, povezane s tem pojavom.

([1]) Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij z dne 15. marca 2007 o radiofrekvenčni identifikaciji (RFID) v Evropi: naslednji koraki k okviru politike, COM(2007) 96 konč.

([2]) Priporočilo Komisije z dne 12. maja 2009 o izvajanju načel varstva zasebnosti in varstva podatkov v aplikacijah, podprtih z radiofrekvenčno identifikacijo (C(2009) 3200 konč.).

([3]) Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij z naslovom „Internet stvari – akcijski načrt za Evropo“, 18. junija 2009, COM(2009) 278 konč.

69. ENVP bi rad opozoril na nekatera vprašanja, ki so bila postavljena v tem sporočilu in si po njegovem mnenju pri razvoju interneta stvari zaslužijo veliko pozornost. Prvič, potreba po decentralizirani strukturi lahko pospešuje odgovornost in izvršljivost pravnega okvira EU. Drugič, kolikor je to mogoče, je treba ohraniti pravico posameznikov, da se jih ne sledi. Z drugimi besedami, sledenje posameznikov prek oddajnikov RFID brez njihovega soglasja je treba čim bolj omejiti. Tako soglasje mora biti izrecno. To se navadno imenuje „ko čipi obmolknejo“ in pravica, da se posameznike pusti pri miru. Ne nazadnje mora biti vodilno načelo pri načrtovanju interneta stvari načelo vgrajene zasebnosti. To bi na primer zahtevalo, da so konkretne aplikacije RFID, ki imajo vgrajene mehanizme za zagotavljanje nadzora uporabnikom, načrtovane z nastavitvami vgrajene zasebnosti.

70. ENVP pričakuje, da se bo Komisija z njim posvetovala pri vzpostavljanju ukrepov, predvidenih v navedenem sporočilu, zlasti pri pripravi osnutka sporočila o zasebnosti in zaupanju v vseobsegajočo informacijsko družbo.

VI. **SOCIALNA OMREŽJA IN POTREBA PO PRIVZETIH NASTAVITVAH ZASEBNOSTI**

71. Socialna omrežja so „pravi hit“. Zdi se, da po priljubljenosti prekašajo elektronsko pošto. Osebe povezujejo z drugimi, ki imajo podobne interese in/ali dejavnosti. Ljudje lahko objavijo svoj profil na spletu in si izmenjujejo medijske datoteke, kot so videoposnetki, fotografije, glasbene datoteke in karierne profile.

72. Mladi so hitro sprejeli socialno mreženje, ta trend pa se še nadaljuje. Povprečna starost uporabnikov interneta v Evropi se je v zadnjih nekaj letih znižala: 9- in 10-letniki se zdaj povežejo večkrat na teden, 12- do 14-letniki pa uporabljajo internet vsak dan, pogosto eno do tri ure.

VI.1. **Socialna omrežja ter sedanji pravni okvir za varstvo podatkov in zasebnosti**

73. Razvoj socialnih omrežij uporabnikom omogoča, da na spletu objavljajo informacije o sebi in tretjih osebah. Po navedbah Delovne skupine iz člena 29 ([1]) uporabniki interneta pri tem v zvezi s podatki, ki jih nalagajo, ([2]) delujejo kot upravljavci podatkov iz prejšnjega člena 2(d) direktive o varstvu podatkov. Vendar v večini primerov taka obdelava spada v izjemo glede domače dejavnosti iz prejšnjega člena 3(2) direktive. Hkrati službe socialnega mreženja štejejo za upravljavce podatkov, če zagotavljajo sredstva za obdelavo podatkov o uporabnikih in vse osnovne storitve v zvezi z upravljanjem uporabnikov (npr. registracijo in deaktivacijo računov).

74. V pravnem smislu to pomeni, da uporabniki interneta in službe socialnega mreženja kot „upravljavci podatkov“ nosijo v smislu člena 2(d) direktive skupno odgovornost za obdelavo osebnih podatkov, čeprav v različnem obsegu in z različnimi obveznostmi.

75. V skladu s tem morajo uporabniki vedeti in razumeti, da obdelava svojih osebnih informacij in osebnih informacij drugih spada na področje določb zakonodaje EU o varstvu podatkov, ki med drugim zahteva pridobitev privolitve tistih, katerih informacije se naložijo, in podelitev pravice do popravka, nasprotovanja itd. zadevnim osebam. Podobno morajo službe socialnega mreženja med drugim izvajati ustrezne tehnične in organizacijske ukrepe za preprečevanje nepooblaščene obdelave podatkov ob upoštevanju tveganj, ki jih prinašata obdelava in narava podatkov. To pomeni, da morajo službe socialnega mreženja zagotavljati privzete nastavitve, ki upoštevajo spoštovanje zasebnosti, vključno z nastavitvami, ki omejujejo dostop do profila na stike, ki jih uporabnik sam izbere. Pri nastavitvah mora biti potrebno tudi pritrdilno soglasje uporabnika, preden je kateri koli profil dostopen tretjim osebam, profilov z omejenim dostopom pa internetni iskalniki ne smejo najti.

76. Na žalost obstaja vrzel med zakonskimi zahtevami in dejansko skladnostjo. Čeprav se s pravnega vidika uporabniki interneta štejejo za upravljavce podatkov, ki jih zavezuje pravni okvir EU za varstvo podatkov in zasebnost, pa se uporabniki interneta v realnosti te vloge pogosto ne zavedajo. Na splošno ne razumejo najbolje, da obdelujejo osebne podatke ter da so z objavljanjem takih informacij povezana tveganja v zvezi z zasebnostjo in varstvom podatkov. Zlasti mladi objavljajo vsebine na spletu, pri tem pa podcenjujejo posledice, ki jih ima to lahko nanje in na druge, na primer pri poznejšem vpisu v izobraževalne institucije ali kandidiranju za delovno mesto.

([1]) Glej Mnenje št. 163, 5/2009 Delovne skupine iz člena 29 o spletnem socialnem mreženju, sprejeto 12. junija 2009.

([2]) „Upravljavec“ pomeni fizično ali pravno osebo, javni organ, agencijo ali kateri koli drug organ, ki sam ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov; kadar namene in sredstva obdelave določa nacionalna zakonodaja ali zakonodaja Skupnosti, lahko upravljavca ali posebna merila za njegovo imenovanje določi nacionalna zakonodaja ali zakonodaja Skupnosti.

77. Hkrati ponudniki socialnih omrežij pogosto vnaprej izberejo privzete nastavitve na podlagi zavrnitev (*opt-out*, upoštevanje zavrnitve posameznika za uporabo njegovih podatkov), s čimer povzročijo lažje razkritje osebnih informacij. Nekateri od njih omogočajo, da so profili samodejno na voljo splošnim iskalnikom. To postavlja vprašanja, ali se posamezniki dejansko strinjajo z razkritjem in ali so socialna omrežja v skladu s členom 17 direktive (opisanim zgoraj), ki od njih zahteva izvajanje ustreznih tehničnih in organizacijskih ukrepov za preprečevanje nepooblaščene obdelave.

VI.2. **Tveganja, ki jih povzročajo socialna omrežja, in predlagani ukrepi za njihovo obravnavo**

78. Zgoraj navedeno ima za posledico večje tveganje za zasebnost in varstvo podatkov posameznika. Uporabnike interneta in tiste, katerih podatki so bili naloženi, izpostavlja očitnim kršitvam njihove zasebnosti in varstva podatkov.

79. Komisija mora zato obravnavati vprašanje, kaj je treba in kaj bi bilo mogoče storiti za rešitev tega položaja. V tem mnenju ni zagotovljen celovit odgovor na to vprašanje, temveč je v njem navedenih več predlogov za nadaljnji razmislek.

Vlaganje v izobraževanje uporabnikov interneta

80. Prvi predlog je vlagati v izobraževanje uporabnikov. V zvezi s tem morajo institucije EU in nacionalni organi vlagati v izobraževanje in ozaveščanje o nevarnostih spletnih strani za socialno mreženje. GD za informacijsko družbo na primer vodi program za varnejši internet, katerega cilj je usposabljati in varovati otroke in mlade, na primer z dejavnostmi ozaveščanja ([1]). Institucije EU so pred kratkim začele izvajati kampanjo „Pomisli, preden objaviš!“ (*Think before you post*) za ozaveščanje o tveganjih izmenjave osebnih informacij z neznanci.

81. ENVP spodbuja Komisijo, da še naprej podpira tovrstne dejavnosti. Vendar morajo biti dejavni tudi sami ponudniki socialnih omrežij, saj imajo pravno in družbeno odgovornost za izobraževanje uporabnikov, kako naj varno uporabljajo njihove storitve in pri tem spoštujejo zasebnost.

82. Kot je bilo opisano zgoraj, so lahko informacije pri objavljanju na socialnih omrežjih samodejno na voljo na različne načine. Informacije so lahko na primer dane na voljo javnosti na splošno, vključno z iskalniki, ki jih lahko indeksirajo in tako omogočijo neposredne povezave do njih. Po drugi strani so lahko informacije omejene na „izbrane prijatelje“ ali shranjene kot popolnoma zasebne. Dovoljenja v zvezi s profili in uporabljena terminologija se med spletnimi stranmi seveda razlikujejo.

83. Kot je opisano zgoraj, pa zelo malo uporabnikov storitev socialnega mreženja ve, kako nadzorovati dostop do informacij, ki jih objavijo, kaj šele kako spremeniti privzete nastavitve glede zasebnosti. Nastavitve glede zasebnosti običajno ostanejo nespremenjene, ker se uporabniki ne zavedajo posledic tega, če jih ne spremenijo, ali ne vedo, kako jih spremeniti. Zato nesprememba nastavitev glede zasebnosti najpogosteje ne pomeni, da so se posamezniki za sprejetje izmenjave informacij odločili po predhodni seznanitvi. V zvezi s tem je zlasti pomembno, da tretje stranke, kot so iskalniki, ne zagotavljajo povezave do posameznih profilov ob predpostavki, da uporabniki samodejno soglašajo (ker niso spremenili nastavitev glede zasebnosti) s tem, da dajo informacije na voljo brez omejitev.

84. Čeprav lahko izobraževanje uporabnikov pomaga pri reševanju tega položaja, pa ne bo učinkovito brez sprejetja drugih ukrepov. V skladu z mnenjem Delovne skupine iz člena 29 o socialnih omrežjih morajo ponudniki socialnih omrežij ponujati brezplačne privzete nastavitve glede zasebnosti, ki upoštevajo spoštovanje zasebnosti. Tako bi se uporabniki bolje zavedali svojih dejanj, kar bi jim omogočilo boljšo odločitev, ali želijo izmenjevati informacije in s kom.

Vloga za samourejanje

85. Komisija je sklenila sporazum z dvajsetimi ponudniki socialnih omrežij, znan kot „Načela varnejšega socialnega mreženja za EU“ ([2]). Cilj tega sporazuma je izboljšati varnost mladoletnikov pri uporabi spletnih strani za socialno mreženje v Evropi. Taka načela vključujejo številne zahteve, ki izhajajo iz uporabe zgoraj opisanega pravnega okvira za varstvo podatkov, na primer zahtevo po usposabljanju uporabnikov prek orodij in tehnologije za zagotavljanje, da lahko nadzorujejo uporabo in širjenje osebnih informacij. Vključujejo tudi potrebo po samodejnem zagotavljanju nastavitev glede zasebnosti.

86. Komisija je na začetku januarja 2010 objavila ugotovitve poročila, v katerem je bilo ocenjeno izvajanje načel ([3]). ENVP je zaskrbljen, ker to poročilo kaže, da so bili nekateri ukrepi sicer sprejeti, številni drugi pa ne. V poročilu so bile na primer odkrite težave v zvezi s sporočanjem varnostnih ukrepov in orodij, ki so na voljo na spletnih

([1]) Informacije o tem programu so na voljo na spletnem naslovu: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Načela so na voljo na spletnem naslovu: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Poročilo o oceni izvajanja načel varnejših socialnih omrežij za EU je na voljo na spletnem naslovu: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

straneh. Ugotovljeno je bilo tudi, da manj kot polovica podpisnikov sporazuma omejuje dostop do profilov mladoletnikov samo na njihove prijatelje.

Potreba po obveznih nastavitvah vgrajene zasebnosti

87. V zvezi s tem je ključno vprašanje, ali so potrebni dodatni politični ukrepi za zagotavljanje, da so storitve socialnih omrežij vzpostavljene z nastavitvami vgrajene zasebnosti. Na to vprašanje je opozorila nekdanja komisarka za informacijsko družbo Viviane Reding, ki je poudarila, da je zakonodaja morda potrebna ([1]). Tudi Evropski ekonomsko-socialni odbor je navedel, da je treba poleg samourejanja zakonsko določiti minimalne standarde zaščite ([2]).

88. Kot je bilo navedeno zgoraj, je mogoče obveznost ponudnikov socialnih omrežij, da samodejno izvajajo nastavitve glede zasebnosti, posredno izpeljati iz člena 17 direktive o varstvu podatkov ([3]), ki upravljavce podatkov zavezuje k sprejemanju ustreznih tehničnih in organizacijskih ukrepov („med načrtovanjem sistema obdelave, pa tudi med samo obdelavo“) za ohranjanje varnosti in preprečevanje nepooblaščene obdelave ob upoštevanju tveganj, ki izhajajo iz obdelave in narave podatkov.

89. Vendar je ta člen preveč splošen in ni dovolj specifičen, niti v tem smislu. V njem ni jasno določeno, kaj pomenijo ustrezni tehnični in organizacijski ukrepi v okviru socialnih omrežij. Zato je sedanji položaj pravno negotov, kar povzroča težave regulativnim organom in posameznikom, katerih zasebnost in osebni podatki niso v celoti zavarovani.

90. ENVP ob upoštevanju navedenega poziva Komisiji, da pripravi zakonodajo, ki bo vključevala vsaj splošno obveznost vzpostavitve obveznih nastavitev glede zasebnosti skupaj z naslednjima natančnejšima zahtevama:

(a) zagotavljati nastavitve, ki omejujejo dostop do profilov uporabnikov na stike, ki so jih uporabniki sami izbrali. V zvezi z nastavitvami je treba zahtevati tudi pritrdilno soglasje uporabnika, preden je kateri koli profil dostopen tretjim osebam;

(b) zagotavljati, da notranji/zunanji iskalniki ne morejo najti profilov z omejenim dostopom.

91. Poleg določitve obveznih nastavitev vgrajene zasebnosti ostaja vprašanje, ali bi bili morda ustrezni dodatni posebni ukrepi v zvezi z varstvom podatkov in drugi ukrepi (na primer v zvezi z varstvom mladoletnikov). To zastavlja širše vprašanje, ali bi bilo ustrezno oblikovati poseben okvir za tovrstne storitve, ki bi poleg določanja obveznih nastavitev vgrajene zasebnosti zakonsko urejal tudi druge vidike. ENVP poziva Komisijo k proučitvi tega vprašanja.

VII. **BRSKALNIŠKE NASTAVITVE VGRAJENE ZASEBNOSTI ZA ZAGOTAVLJANJE PRIVOLITVE PO PREDHODNI SEZNANITVI ZA PREJEMANJE OGLASOV**

92. Ponudniki oglaševalskih omrežij uporabljajo piškotke in druge mehanizme za spremljanje vedenja posameznih uporabnikov pri brskanju po spletnih straneh za katalogizacijo njihovih interesov in oblikovanje profilov. Te informacije se nato uporabljajo za to, da se jim pošiljajo ciljno usmerjeni oglasi ([4]).

VII.1. **Drugi izzivi in tveganja na podlagi sedanjega pravnega okvira za varstvo podatkov in zasebnosti**

93. To obdelavo zajemata direktiva o varstvu podatkov (v zvezi z osebnimi podatki) in člen 5(3) direktive o e-zasebnosti. Ta člen izrecno zahteva, da je uporabnik obveščen in ima možnost odzvati se s privolitvijo ali zavrnitvijo shranjevanja mehanizmov, kot so piškotki itd., na svoj računalnik ali drugo napravo ([5]).

94. Doslej so ponudniki oglaševalskih omrežij uporabljali brskališke nastavitve in politike glede zasebnosti, da so uporabnike obveščali in jim omogočali sprejetje ali zavrnitev piškotkov. V založniških politikah zasebnosti so

([1]) Viviane Reding, članica Evropske komisije, pristojna za informacijsko družbo in medije; Pomisli, preden objaviš! Kako zagotoviti varnejše spletne strani za socialno mreženje za otroke in najstnike? Dan varne rabe interneta, Strasbourg, 9. februarja 2010.

([2]) Mnenje Evropskega ekonomsko-socialnega odbora o vplivu spletnih strani za socialna omrežja na državljane/potrošnike, 4. novembra 2009.

([3]) Obširneje o tem tudi v točki 33 tega dokumenta.

([4]) Sledilni piškotki so majhne besedilne datoteke, ki vsebujejo edinstven identifikator. Običajno ponudniki oglaševalskih omrežij (in spletni operaterji ali založniki) shranijo piškotke na trdi disk obiskovalcev, zlasti v brskalnik internetnih uporabnikov, kadar uporabniki prvič obiščejo spletne strani, ki uporabljajo oglase, ki so del njihovega omrežja. Piškotek ponudniku oglaševalskega omrežja omogoča prepoznavo obiskovalca, ki znova obišče to spletno stran ali katero koli spletno stran, ki je partnersko povezana z oglaševalskim omrežjem. Taki večkratni obiski bodo ponudniku oglaševalskega omrežja omogočili oblikovanje profilov obiskovalcev.

([5]) Člen 5(3) direktive o e-zasebnosti je bil pred kratkim spremenjen za krepitev varstva pred prestrezanjem sporočil uporabnikov, na primer z vohunsko programsko opremo (*spyware*) in piškotki, shranjenimi na računalniku uporabnika ali drugih napravah. V skladu z novo direktivo je treba uporabnikom ponuditi boljše informacije in lažje načine nadzora nad tem, ali želijo imeti piškotke shranjene na svoji terminalski opremi.

pojasnili, kako se prejemanje piškotkov v celoti zavrne ali kako se sprejmejo za vsak primer posebej. S tem so hoteli doseči skladnost s svojo obveznostjo, da uporabnikom omogočijo pravico do zavrnitve piškotkov.

95. Čeprav bi teoretično ta metoda (prek brskalnika) lahko dejansko učinkovito zagotavljala pomembno privolitev po predhodni seznanitvi, je realnost precej drugačna. Na splošno uporabniki nimajo osnovnega znanja o zbiranju katerih koli podatkov, zlasti od tretjih oseb, vrednosti takih podatkov, njihovi uporabi, delovanju tehnologije, natančneje, kako in kje zbiranje zavrniti. Koraki, ki jih morajo narediti uporabniki za zavrnitev, se zdijo ne le zapleteni, temveč tudi pretirani (najprej morajo nastaviti brskalnik, da sprejema piškotke, nato pa izbrati možnost zavrnitve).

96. Zato zelo malo ljudi v praksi izbere možnost zavrnitve, pa ne zato, ker so sprejeli odločitev po predhodni seznanitvi o sprejetju vedenjskega oglaševanja, temveč ker ne vedo, da dejansko sprejemajo piškotke, ko ne uporabijo možnosti zavrnitve.

97. Čeprav s pravnega vidika člen 5(3) direktive o e-zasebnosti določa učinkovito pravno varstvo, pa se v praksi šteje, da uporabniki interneta soglašajo, da se spremljajo za namene pošiljanja vedenjskih oglasov, čeprav se v številnih primerih, če ne celo v večini sploh ne zavedajo, da spremljanje poteka.

98. Delovna skupina iz člena 29 pripravlja mnenje, katerega namen je pojasniti pravne zahteve za izvajanje vedenjskega oglaševanja, kar je dobrodošlo. Vendar pa razlaga sama po sebi morda ne bo zadostovala za rešitev tega položaja in bo morda Evropska unija morala sprejeti dodatne ukrepe.

VII.2. **Potreba po nadaljnjem ukrepanju, zlasti določitvi obveznih nastavitev vgrajene zasebnosti**

99. Kot je opisano zgoraj, spletni brskalniki običajno omogočajo neko raven nadzora nad nekaterimi vrstami piškotkov. Privzete nastavitve večine spletnih brskalnikov zdaj sprejemajo vse piškotke. Z drugimi besedami, brskalniki so samodejno nastavljeni tako, da sprejemajo vse piškotke, ne glede na njihov namen. Samo če uporabnik spremeni nastanitve svoje brskalniške aplikacije za zavrnitev piškotkov, kar stori zelo malo uporabnikov, kot je bilo opisano zgoraj, piškotkov ne bo prejemal. Poleg tega pri prvi namestitvi ali posodobitvi brskalniških aplikacij ni čarovnika za zasebnost.

100. Način ublažitve zgornje težave bi bil zagotavljanje brskalnikov s privzetimi nastavitvami zasebnosti. Z drugimi besedami, če bi bila na voljo nastavitev brskalnikov „zavrni piškotke tretjih strank“. Za dopolnitev tega in večjo učinkovitost bi morali brskalniki od uporabnikov zahtevati, da pri prvi namestitvi ali posodobitvi brskalnika uporabijo čarovnik za zasebnost. Potrebne so večja razčlenjenost in jasne informacije o vrstah piškotkov in koristnosti nekaterih od njih. Uporabniki, ki soglašajo, da so spremljani za prejemanje oglasnih sporočil, bodo ustrezno obveščeni in bodo morali spremeniti nastavitve brskalnika. To bi jim omogočilo boljši nadzor nad osebnimi podatki in zasebnostjo. ENVP meni, da bi bil to učinkovit način za spoštovanje in ohranjanje soglasja uporabnikov ([1]).

101. Ob upoštevanju razširjene narave težave na eni strani oziroma, drugimi besedami, števila internetnih uporabnikov, ki so trenutno spremljani na podlagi soglasja, ki je navidezno, na drugi strani pa zadevne stopnje interesa, postane potreba po dodatnih zaščitnih ukrepih bolj pereča. Izvajanje načela vgrajene zasebnosti v aplikacijah spletnih brskalnikov bi prineslo bistveno spremembo in posameznikom omogočilo nadzor nad praksami zbiranja podatkov, ki se uporabljajo za namene oglaševanja.

102. ENVP zato poziva Komisijo, naj razmisli o zakonodajnih ukrepih, ki določajo obvezne nastavitve vgrajene zasebnosti v brskalnikih in zagotavljanje ustreznih informacij.

VIII. **DRUGA NAČELA, KATERIH NAMEN JE VARSTVO ZASEBNOSTI POSAMEZNIKOV/VARSTVO PODATKOV**

103. Čeprav lahko načelo vgrajene zasebnosti bistveno izboljša varstvo osebnih podatkov in zasebnosti posameznikov, je treba za zagotavljanje zaupanja potrošnikov v IKT v zakonodaji načrtovati in izvajati dopolnilna načela. Na podlagi navedenega ENVP obravnava načelo odgovornosti in dokončno oblikovanje obveznega okvira v zvezi s kršitvami varnosti, ki se uporablja v različnih sektorjih.

VIII.1. **Načelo odgovornosti za zagotavljanje skladnosti z načelom vgrajene zasebnosti**

104. V dokumentu Delovne skupine iz člena 29 z naslovom „Prihodnost zasebnosti“ ([2]) je bila priporočena vključitev načela odgovornosti v direktivo o varstvu podatkov. To

([1]) ENVP se hkrati zaveda, da to ne bi v celoti rešilo težave, ker obstajajo piškotki, ki jih ni mogoče nadzorovati z brskalnikom, kot so tako imenovani flash piškotki. Za to bi morali razvijalci brskalnikov v različice novih brskalnikov samodejno vgraditi flash kontrole v kontrole piškotkov.

([2]) Mnenje št. 168 Delovne skupine iz člena 29 z naslovom „Prihodnost zasebnosti: skupni prispevek k posvetovanju Evropske komisije o pravnem okviru za temeljno pravico do varstva osebnih podatkov“, sprejeto 1. decembra 2009.

načelo, ki je priznano v nekaterih večnacionalnih instrumentih za varstvo podatkov ([1]), od organizacij zahteva izvajanje postopkov za dosego skladnosti z veljavno zakonodajo ter vzpostavitev metod ocenjevanja in dokazovanja skladnosti z zakonodajo in drugimi zavezujočimi instrumenti.

105. ENVP v celoti podpira priporočilo Delovne skupine iz člena 29. Po njegovem mnenju bo to načelo zelo pomembno za spodbujanje učinkovite uporabe načel in obveznosti v zvezi z varstvom podatkov. Upravljavci podatkov morajo v skladu z načelom odgovornosti dokazati, da so vzpostavili mehanizem, potreben za dosego skladnosti z veljavno zakonodajo o varstvu podatkov. To bo verjetno prispevalo k učinkovitemu izvajanju vgrajene zasebnosti v tehnologijah IKT kot nadvse primernega elementa za dokazovanje odgovornosti.

106. Upravljavci podatkov bi za merjenje in dokazovanje odgovornosti lahko uporabljali notranje postopke, tretje osebe, ki lahko opravljajo revizije ali druge vrste pregledov in preverjanj, pa lahko posledično dodelijo pečate ali nagrade. ENVP v zvezi s tem poziva Komisijo k razmisleku, ali bi bilo poleg splošnega načela odgovornosti koristno zakonsko zahtevati sprejetje posebnih ukrepov glede odgovornosti, kot je potreba po pripravi ocen učinka glede zasebnosti in varstva podatkov, ter v katerih okoliščinah.

VIII.2. **Kršitve varnosti: dokončno oblikovanje pravnega okvira**

107. Z lanskimi spremembami direktive o e-zasebnosti je bila uvedena zahteva o sporočanju kršitev varnosti podatkov prizadetim posameznikom in ustreznim organom. Kršitev varnosti podatkov je na splošno opredeljena kot katera koli kršitev varnosti, ki povzroči uničenje, izgubo, razkritje itd. osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani v zvezi z zagotavljanjem storitev. Obveščanje posameznikov bo potrebno, če je verjetno, da bo kršitev varnosti podatkov škodljivo vplivala na njihove osebne podatke ali zasebnost. To se lahko zgodi v primeru, kadar lahko kršitev pripelje do kraje identitete ali resnega ponižanja ali škodovanja ugledu. Obveščanje ustreznih organov bo potrebno za vsako kršitev varnosti podatkov, ne glede na to, ali obstaja tveganje za posameznike.

Obveznosti glede kršitev varnosti med sektorji

108. Na žalost se ta obveznost uporablja samo za ponudnike javno dostopnih elektronskih komunikacijskih storitev, kot so telefonske družbe, ponudniki internetnega dostopa, ponudniki spletne pošte itd. ENVP poziva Komisijo, naj predloži predloge o kršitvah varnosti, ki se bodo uporabljali med sektorji. V zvezi z vsebino takega okvira ENVP meni, da pravni okvir za kršitve varnosti, sprejet v direktivi o e-zasebnosti, vzpostavlja ustrezno ravnovesje med varstvom pravic posameznikov, vključno z njihovimi pravicami do varstva osebnih podatkov in zasebnosti, in obveznostmi za zadevne subjekte. Hkrati je to okvir s pravimi „zobmi“, saj ga podpirajo pomembne izvedbene določbe, ki organom dajejo zadostne pristojnosti za preiskave in sankcije v primeru neskladnosti.

109. ENVP v skladu s tem Komisijo poziva, naj sprejme zakonodajni predlog, v skladu s katerim bi se ta okvir uporabljal v vseh sektorjih, po potrebi z ustreznimi prilagoditvami. Poleg tega bi to zagotavljalo, da se med sektorji uporabljajo isti standardi in postopki.

Dokončno oblikovanje pravnega okvira iz direktive o e-zasebnosti na podlagi komitološkega postopka

110. Spremenjena direktiva o e-zasebnosti pooblašča Komisijo, da sprejema tehnične izvedbene ukrepe, tj. podrobne ukrepe o obveščanju o kršitvah varnosti, na podlagi komitološkega postopka ([2]). To pooblastilo je upravičeno zaradi zagotavljanja doslednega izvajanja in uporabe pravnega okvira za kršitve varnosti. Dosledno izvajanje zagotavlja, da posamezniki v vsej Skupnosti uživajo enako visoko raven varstva in da zadevnim subjektom niso naložene različne zahteve glede obveščanja.

111. Direktiva o e-zasebnosti je bila sprejeta novembra 2009. Zdi se, da ni nobenega razloga, ki bi upravičeval odložitev začetka dela, katerega cilj je sprejetje tehničnih izvedbenih ukrepov. ENVP je organiziral dva seminarja za izmenjavo in zbiranje izkušenj v zvezi z obveščanjem o kršitvah varnosti podatkov. Z veseljem bo izmenjeval rezultate te dejavnosti ter se veseli sodelovanja s Komisijo in drugimi zainteresiranimi stranmi pri prilagajanju splošnega pravnega okvira za kršitve varnosti podatkov.

112. ENVP poziva Komisijo k hitremu sprejetju potrebnih ukrepov. Komisija mora pred sprejetjem tehničnih izvedbenih ukrepov izvesti obširno posvetovanje, v okviru katerega se mora posvetovati z Evropsko agencijo za varnost omrežij in informacij (ENISA), evropskim nadzornikom za varstvo podatkov in Delovno skupino iz člena 29. Poleg tega je treba v posvetovanje vključiti tudi druge „zadevne zainteresirane strani“, zlasti zato, da bi bila obveščena o najboljših razpoložljivih tehničnih in gospodarskih sredstvih za izvajanje.

([1]) Smernice OECD o varovanju zasebnosti in čezmejnem prenosu osebnih podatkov iz leta 1980; Madridska deklaracija o zasebnosti o globalnih standardih zasebnosti za globaliziran svet z dne 3. novembra 2009.

([2]) Komitologija vključuje sprejetje tehničnih izvedbenih ukrepov prek odbora predstavnikov držav članic, ki mu predseduje Komisija. Za direktivo o e-zasebnosti se uporablja tako imenovani regulativni postopek s pregledom, kar pomeni, da lahko Evropski parlament in Svet nasprotujeta ukrepom, ki jih predlaga Komisija. Za dodatne informacije glej spletno stran: http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **SKLEPNE UGOTOVITVE**

113. Zaupanje ali bolje rečeno pomanjkanje zaupanja je bilo opredeljeno kot temeljno vprašanje pri pojavu in uspešni uvedbi informacijskih in komunikacijskih tehnologij. Če ljudje IKT ne zaupajo, bodo te tehnologije verjetno neuspešne. Zaupanje v IKT je odvisno od različnih dejavnikov: od katerih je ključni zagotavljanje, da take tehnologije ne spodkopavajo temeljne pravice posameznikov do zasebnosti in varstva osebnih podatkov.

114. Za nadaljnjo krepitev pravnega okvira za varstvo podatkov/zasebnosti, katerega načela ostajajo popolnoma veljavna v informacijski družbi, ENVP Komisiji predlaga, naj vgrajeno zasebnost vključi v zakonodajo in oblikovanje politike na različnih ravneh.

115. Komisiji priporoča, naj sprejme štiri ukrepe:

(a) predlaga vključitev splošne določbe o vgrajeni zasebnosti v pravni okvir za varstvo podatkov. Ta določba mora biti tehnološko nevtralna, skladnost pa mora biti obvezna v različnih fazah;

(b) natančno opredeli to splošno določbo v posebnih določbah, kadar so predlagani posebni pravni instrumenti v različnih sektorjih. Te posebne določbe bi bilo mogoče že zdaj vključiti v pravne instrumente na podlagi člena 17 direktive o varstvu podatkov (in druge veljavne zakonodaje);

(c) vgrajeno zasebnost kot vodilno načelo vključi v evropski program za digitalne tehnologije;

(d) vgrajeno zasebnost kot načelo uvede v druge pobude EU (predvsem nezakonodajne).

116. ENVP na treh določenih področjih IKT priporoča Komisiji, naj oceni potrebo po oblikovanju predlogov za izvajanje načela vgrajene zasebnosti na posebne načine:

(a) v zvezi z RFID – predlagati zakonodajne ukrepe, ki urejajo glavna vprašanja uporabe RFID v primeru, če izvajanje sedanjega pravnega okvira prek samourejanja ne bo učinkovito. Zlasti določiti načelo privolitve (opt-in) na prodajnem mestu, v skladu s katerim bi bili vsi oddajniki RFID, nameščeni na potrošniške proizvode, na prodajnem mestu samodejno deaktivirani;

(b) v zvezi z socialnimi omrežji – pripraviti zakonodajo, ki bo vključevala vsaj splošno obveznost vzpostavitve obveznih nastavitev glede zasebnosti skupaj z natančnejšimi zahtevami o omejitvi dostopa do uporabniških profilov na stike, ki jih je uporabnik sam izbral, in določitvi, da notranji/zunanji iskalniki ne morejo najti profilov z omejenim dostopom;

(c) v zvezi s ciljno usmerjenim oglaševanjem – razmisliti o zakonodaji, ki določa, da nastavitve brskalnikov samodejno zavračajo piškotke tretjih oseb, in od uporabnikov zahtevati, da pri prvi namestitvi ali posodobitvi brskalnika uporabijo čarovnika za zasebnost.

117. Ne nazadnje ENVP Komisiji predlaga, naj:

(a) razmisli o izvajanju načela odgovornosti v veljavni direktivi o varstvu podatkov ter

(b) pripravi okvir pravil in postopkov za izvajanje določb o uradnem obveščanju o kršitvah varnosti iz direktive o e-zasebnosti ter jih razširi, da se na splošno uporabljajo za vse upravljavce podatkov.

V Bruslju, 18. marca 2010

Peter HUSTINX

evropski nadzornik za varstvo podatkov