I

(Resolucije, priporočila in mnenja)

MNENJA

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Mnenje Evropskega nadzornika za varstvo podatkov 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

(2008/C 101/01)

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,

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

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

SPREJEL NASLEDNJE MNENJE:

I. **UVOD**

1. Komisija je 15. marca 2007 sprejela sporočilo z naslovom „Radiofrekvenčna identifikacija (RFID) v Evropi: naslednji koraki k okviru politike“ ([1]) (v nadaljnjem besedilu „sporočilo“). Po členu 41 Uredbe (ES) št. 45/2001 je ENVP odgovoren, da institucijam in organom Skupnosti svetuje glede vseh zadev v zvezi z obdelavo osebnih podatkov. ENVP v skladu s tem členom predstavlja svoje mnenje.

2. To mnenje je treba razumeti kot odziv ENVP na sporočilo in tudi na druge ukrepe s področja RFID, ki so bili izvedeni po njegovem sprejetju. Ti drugi ukrepi, upoštevani v tem mnenju, vključujejo:

— Sklep Komisije z dne 28. junija 2007 o ustanovitvi strokovne skupine za radiofrekvenčno identifikacijo ([2]), ki je neposredna posledica sporočila. Ta skupina je poznana tudi pod imenom „skupina zainteresiranih strani za RFID“. V skladu s členom 4(4)(b) Sklepa ENVP sodeluje pri dejavnostih skupine kot opazovalec;

— Resolucijo Sveta z dne 22. marca 2007 o strategiji za varno informacijsko družbo v Evropi ([3]);

— projekt „RFID in upravljanje identitete“, ki ga je začel Evropski parlament ([4]);

([1]) COM(2007) 96 končno.
([2]) Sklep št. 467/2007/ES (UL L 176, 6.7.2007, str. 25).
([3]) UL C 68, 24.3.2007, str. 1.
([4]) Projekt „RFID in upravljanje identitete – študije primerov: od začetka razvoja do inteligentnega okolja“, ki ga je naročila služba Evropskega parlamenta za oceno znanstvenih in tehnoloških možnosti (*Scientific Technology Option Assessment* – STOA), izvedla pa skupina ETAG (*European Technology Assessment Group*). http://www.europarl.europa.eu/stoa/default_en.htm

— Mnenje št. 4/2007 o pojmu osebnih podatkov, ki ga je junija 2007 sprejela delovna skupina za varstvo podatkov iz člena 29 ([1]);

— Sporočilo Komisije Evropskemu parlamentu in Svetu o nadaljevanju delovnega programa za boljše izvajanje Direktive o varstvu podatkov ([2]) in mnenje ENVP o tem sporočilu z dne 25. julija 2007 ([3]);

— sprejetje predloga Komisije za direktivo o spremembi (med drugim) Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij ([4]).

3. ENVP pozdravlja sporočilo Komisije o RFID, saj so v njem obravnavana glavna vprašanja, ki se porajajo v zvezi z uporabo tehnologije RFID, pa tudi odločilna vprašanja, povezana z zasebnostjo in varstvom podatkov. Sporočilo temelji na doslednih in natančnih pripravah. Pred njegovo objavo je bilo izvedenih pet tematskih delavnic in spletno javno posvetovanje ([5]), ki jih je naročila Komisija.

4. ENVP se pridružuje mnenju, da bi lahko sistemi RFID igrali ključno vlogo v novi razvojni fazi informacijske družbe, ki se ponavadi imenuje tudi „internet stvari“ (*Internet of things*), prav tako pa se pridružuje tudi pomislekom, navedenim v odstavku 3.2 sporočila, da bi lahko sistemi RFID ogrozili posameznikovo zasebnost in pravico do varstva podatkov. ENVP je v letnem poročilu za leto 2005 sisteme RFID skupaj z biometrijo, inteligentnimi okolji in sistemi upravljanja identitete dejansko opredelil kot tehnološke novosti, ki naj bi pomembno vplivale na varstvo podatkov.

5. Po mnenju ENVP bodo k vključevanju tehnologij RFID v vsakdanje življenje in splošni razširjenosti teh tehnologij prispevali njihova privlačnost in pripravnost oziroma nove storitve, ki jih ponujajo, pa tudi prednosti, ki jih zagotavljajo z dobro prilagojenimi in doslednimi zaščitnimi ukrepi za varstvo podatkov.

6. Skratka: ENVP označuje RFID kot popolnoma novo tehnološko dejavnost, ki je v sporočilu Komisije upravičeno obravnavana kot začetek nove razvojne stopnje informacijske družbe.

7. S to novo tehnologijo se odpirajo pomembna vprašanja na različnih področjih, med drugim na področju varstva podatkov in zasebnosti. Mnenje ENVP je omejeno na to področje.

II. **OSREDNJA TEMA MNENJA**

8. Mnenje je zlasti osredotočeno na možne posledice tega tehnološkega razvoja za varstvo podatkov in zasebnost. Te posledice so še negotove, med drugim tudi zato, ker sta razvoj sistemov RFID in njihovo vključevanje v vsakdanje življenje v polnem zagonu in zato še zdaleč ni jasno, kje se bo ta razvoj ustavil.

9. ENVP v zvezi s tem zavzema naslednje stališče:

— Najprej je treba pojasniti praktične posledice uporabe sistemov RFID za varstvo podatkov in zasebnost.

— Nadalje je treba te posledice podrobno opredeliti v okviru obstoječega pravnega okvira za varstvo podatkov in zasebnost.

— Nazadnje ENVP obravnava vprašanje, ali te posledice zahtevajo natančnejša pravila za reševanje vprašanj varstva podatkov, ki se odpirajo z uporabo tehnologij RFID. To vprašanje je ENVP sprožil že v mnenju o sporočilu glede Direktive o varstvu podatkov, v tem mnenju pa ga bo obravnaval natančneje.

10. S tem pristopom želi ENVP doseči, da bodo pri razvoju sistemov RFID in njihovemu vključevanju v vsakdanje življenje upoštevani utemeljeni pomisleki glede varstva podatkov in zasebnosti.

III. **OBRAZLOŽITEV POSLEDIC**

Sistemi in oznake RFID

11. Navkljub dejstvu, da je – kot že rečeno – razvoj v polnem zamahu in izid negotov, je mogoče zelo dobro opisati glavne značilnosti tega razvoja glede na njegove posledice na varstvo podatkov.

([1]) Dokument WP 136, objavljen na spletni strani delovne skupine.
([2]) Sporočilo Komisije Evropskemu parlamentu in Svetu z dne 7. marca 2007 o nadaljevanju delovnega programa za boljše izvajanje Direktive o varstvu podatkov, COM(2007) 87 konč.
([3]) UL C 255, 27.10.2007, str. 1. V nadaljevanju: „mnenje o sporočilu glede Direktive o varstvu podatkov“.
([4]) Predlog direktive Evropskega parlamenta in Sveta z dne 13. novembra 2007 o spremembi Direktive 2002/22/ES o univerzalni storitvi in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 22. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju na področju varstva potrošnikov, COM (2007) 698 končno. Direktiva 2002/58/ES se v nadaljnjem besedilu imenuje „Direktiva o zasebnosti in elektronskih komunikacijah“.
([5]) http://www.rfidconsultation.eu/

12. Pri ocenjevanju tistih vidikov tehnologije RFID, ki bi lahko bili povezani z varstvom podatkov in zasebnostjo, je zelo pomembno, da se poleg samih oznak RFID preuči celotna infrastruktura RFID: tj. oznaka, čitalnik, omrežje, referenčne zbirke podatkov in zbirke podatkov, kjer so shranjeni podatki, pridobljeni s povezano oznako/čitalnikom. Kot je na kratko izpostavljeno v uvodu sporočila, pri RFID ne gre zgolj za „elektronske oznake“, zato vprašanja varstva podatkov niso omejena izključno na oznake, temveč obsegajo vse elemente celotne infrastrukture RFID. Vsi elementi dejansko prispevajo k izvajanju evropskega pravnega okvira za varstvo podatkov, ko je to potrebno. Nanje vplivajo glavni trendi v razvijajoči se informacijski družbi, kot so skoraj neomejena pasovna širina, povsod razširjene mrežne povezave in neomejena skladiščna zmogljivost.

Učinek sistemov in oznak RFID

13. Ne glede na potrebo po širšem pristopu, ki je bila poudarjena v prejšnjem odstavku, obstaja več razlogov, ki upravičujejo, da se najprej v ospredje postavi uporaba RFID pri označevanju potrošniških izdelkov, kot npr. v maloprodaji. Najbolj očiten razlog je predvidena povečana uporaba RFID, ki se bo – kot se zdi – vsesplošno razširila. V nasprotju z drugimi aplikacijami RFID z manjšo ali omejeno uporabo bi lahko označevanje izdelkov osvojilo množični trg. Že sedaj je mnogo potrošniških izdelkov opremljenih z oznako RFID. S tem je povezano dejstvo, da bo takšna uporaba vplivala na ogromno število posameznikov, katerih osebni podatki se bodo najverjetneje obdelovali vsakokrat, ko bodo kupili izdelek, v katerega je vgrajena oznaka RFID.

14. Posebno pozornost je treba nameniti posledicam označevanja RFID za lastnike zadevnih izdelkov. Sistemi RFID bi lahko povečali razsežnosti odnosa med izdelkom in njegovim lastnikom. Ko se ta odnos razširi, je mogoče za namene prihodnjih poslov lastnika „skenirati“ in razvrstiti kot „kupca z nizkim proračunom“ ali „vabljivo tarčo“; pretirano enoznačno določanje (*one-on-one attribution* ([1])) bi lahko povzročilo samodejno „kaznovanje“ za določeno vrsto obnašanja (obveznost recikliranja, odpadki itd.). Škodljive samodejne odločitve ne bi smele vplivati na posameznika. Zaradi te zmogljivosti RFID se povečuje nevarnost, da bi se v informacijski družbi začelo uveljavljati sprejemanje samodejnih odločitev in izrabljanje tehnologije za upravljanje vedenja posameznikov.

15. Podatki, shranjeni v oznaki RFID ali pridobljeni z njo, so lahko osebni podatki, kot so opredeljeni v členu 2 Direktive o varstvu podatkov. Na primer pametne kartice, ki se uporabljajo za potovanje, lahko vsebujejo identifikacijske podatke in tudi podatke o nedavnih potovanjih imetnika. Če bi želel brezvesten posameznik slediti določeni osebi, bi zadostovala strateška namestitev čitalnikov, ki bi zagotovili informacije o gibanju imetnika kartice, s čimer bi se kršila njegova pravica do zasebnosti in varstva osebnih podatkov.

16. Podobne grožnje zasebnosti bi bile možne, tudi če podatki, shranjeni v oznaki RFID, ne bi vsebovali imen posameznikov. Oznake RFID vsebujejo posebne identifikatorje, ki pripadajo potrošniškim izdelkom: če ima vsaka oznaka poseben identifikator, se lahko takšna identifikacija uporablja za nadzorovanje. Za ponazoritev: če nekdo nosi uro z vgrajeno oznako RFID, ki vsebuje identifikacijsko številko, bi se lahko ta uporabila kot poseben identifikator za imetnika ure, čeprav njegova identiteta ni znana. Glede na to, kako se informacije uporabljajo – in v povezavi s samo uro ali posameznikom – bi se lahko Direktiva uporabljala ali pa tudi ne. Uporabljala bi se, denimo, če se pridobijo informacije o položaju posameznika, za katere je verjetno, da se bodo uporabile za nadzorovanje njegovega vedenja, ali npr. za diferenciacijo cen, zavrnitev dostopa ali neželeno izpostavljenost javnosti.

17. Zato je hkrati z aplikacijami RFID nujno treba zagotoviti potrebne tehnične ukrepe, ki bodo karseda zmanjšali tveganje za nenamerno razkritje informacij. Ti ukrepi lahko vključujejo zahtevo, da je treba takšno tveganje preprečiti že pri načrtovanju infrastrukture in zlasti oznak RFID. Z oznakami RFID se lahko na primer uporabi ukaz *kill*, ki omogoči njihovo deaktiviranje. Ta možnost bo natančneje obravnavana v poglavju IV tega mnenja.

18. Ker sistemi RFID omogočajo sledenje izdelkom po prodaji, se odpirajo nova vprašanja v okviru razprave o zasebnosti. Pri analizi njihovega učinka bo treba upoštevati dva elementa, in sicer: v kolikšni meri je izdelek namenjen osebni rabi ter mobilnost izdelka ([2]).

19. Obvezno analizo tveganja je mogoče dopolniti tudi z življenjskim ciklom izdelka, ki prispeva h kvantitativni presoji možnih groženj zasebnosti. Ob upoštevanju dejstva, da oznake ni mogoče deaktivirati, je mogoče s sledenjem končnemu izdelku z dolgim življenjskim ciklom zbrati več podatkov o lastniku izdelka in natančneje oblikovati njegov profil. Po drugi strani lahko izdelek s kratkim življenjskim ciklom, kot je pločevinka sodavice, od faze proizvodnje do faze recikliranja predstavlja manjše tveganje in bi lahko zato potreboval manj stroge ukrepe kot izdelek z veliko daljšim življenjskim ciklom.

([1]) Dr. Sarah Spiekermann, direktorica berlinskega raziskovalnega središča o internetni ekonomiji, delavnica o RFID in vseprisotni informatizaciji, ki jo je organiziral TACD (*Trans Atlantic Consumer Dialogue*), 13. marca 2007.

([2]) Dara J. Glasser, Kenneth W. Goodman in Norman G. Einspruch, *Chips, tags and scanners: Ethical challenges for radio frequency identification, Ethics and Information Technology*, Zvezek 9, št. 2, 2007.

Vprašanja zasebnosti in varstva podatkov pri uporabi sistemov RFID

20. Za boljše razumevanje posledic sistemov RFID za zasebnost in varstvo podatkov je treba opredeliti pet temeljnih vprašanj na tem področju.

21. Prvo vprašanje zadeva identifikacijo posameznika, na katerega se nanašajo osebni podatki. Pred več kot 60 leti je bila oznaka RFID namenjena prepoznavanju prijatelja oziroma sovražnika (*Identify Friend or Foe*). Ne le, da lahko danes sistemi RFID prepoznajo splošne elemente predmeta, temveč lahko privedejo tudi do identifikacije posameznika, kar pa je treba storiti tako, da se spoštujejo načela varstva podatkov.

22. Drugo vprašanje zadeva identifikacijo upravljavca(-ev). Identifikacija upravljavca, kot je opredeljen v členu 2(d) Direktive o varstvu podatkov, je lahko pri sistemih RFID težja, zato je jo je treba natančneje obravnavati. Vendar pa identifikacija upravljavca ostaja ključen korak pri določanju odgovornosti vseh zadevnih akterjev, ki bodo morali ravnati v skladu s pravnim okvirom za varstvo podatkov. Glede na možne dodatne storitve v zvezi z označenim predmetom se lahko upravljavec, ki obdeluje podatke, med življenjskim ciklom oznake večkrat zamenja.

23. Tretje vprašanje zadeva dejstvo, da je tradicionalno razlikovanje med zasebno in javno sfero vse manj pomembno. Čeprav razlikovanje med zasebno in javno sfero tudi v preteklosti ni bilo vedno popolnoma jasno, se večina ljudi zaveda mej med njima (in sivih con) ter sprejema ozaveščene ali smiselne odločitve o načinu ravnanja. Po mnenju Edwarda T. Halla ([1]) osebni prostor ponavadi pomeni fizično oddaljenost od drugih. Upravljanje zasebnosti se lahko obravnava tudi kot dinamičen proces urejanja meja zasebnosti ([2]). Zato tudi ni presenetljivo, da brezžična komunikacija z oznakami in dejstvo, da je z njo mogoče brati zunaj vidnega polja, sprožata pomisleke glede zasebnosti, saj so zabrisane tradicionalne meje in njihovo upravljanje. Obstaja bojazen, da bi lahko posameznik izgubil del nadzora ali ves nadzor nad upravljanjem razdalj, ki ga je imel do sedaj. Zato so tako zagovorniki kot tudi nasprotniki sistemov RFID ob začetku izvajanja sistemov RFID pozornost namenjali obsegu odčitavanja.

24. Četrto vprašanje je povezano z velikostjo in fizičnimi lastnostmi oznak RFID. Ker mora biti oznaka načeloma majhna in poceni, so tudi varnostni ukrepi, ki bi se lahko uporabili na tem elementu sistema RFID, že v osnovi omejeni. Dodatne varnostne zahteve so potrebne tudi zato, ker brezžično komuniciranje predstavlja večje tveganje kot komuniciranje preko žičnih povezav.

25. Peto vprašanje zadeva slabo preglednost obdelave. Sistemi RFID lahko povzročijo neopaženo zbiranje in obdelavo informacij, ki ju je mogoče uporabiti za profiliranje posameznika. To je mogoče zelo dobro ponazoriti s primerjavo sistemov RFID in mobilnih telefonov, ki je tudi najbolj pogosta. Po eni strani je bil mobilni telefon z vidika tehnologije zelo sprejemljiv, ne glede na morebitna tveganja v zvezi z vdorom v zasebnost. Lahko bi sklepali, da bodo sistemi RFID sprejeti na podoben način. Po drugi strani pa je treba poudariti, da je mobilni telefon viden predmet, ki ga končni uporabnik lahko vseeno nadzoruje, saj ga lahko izključi. Pri RFID to ni mogoče.

26. Čeprav sta – kot že omenjeno – neopaženo zbiranje in obdelava informacij lahko zakonita, je prav tako mogoče in v nekaterih okoliščinah zelo verjetno, da pride to nezakonitega zbiranja in obdelave takšnih podatkov.

27. Iz pojasnil, navedenih v tem poglavju, je mogoče sklepati, da je široka uporaba tehnologije RFID nekaj popolnoma novega in bi lahko pomembno vplivala na našo družbo in varstvo temeljnih pravic, npr. pravice do zasebnosti in pravice do varstva podatkov. RFID lahko privede do kakovostnih sprememb.

IV. **PODROBNA OPREDELITEV POSLEDIC**

Uvod

28. To poglavje je predvsem osredotočeno na učinek RFID na varstvo temeljnih pravic v naši družbi, npr. pravice do zasebnosti in varstva podatkov. Ta učinek bo opredeljen v dveh delih; najprej bo na kratko opisano, kako so te temeljne pravice zaščitene v skladu s sedanjim pravnim okvirom, nato pa bodo podrobneje obravnavane možnosti doslednega izvajanja sedanjega pravnega okvira. V mnenju o sporočilu glede Direktive o varstvu podatkov je ta cilj izražen z besedami „sedanje določbe Direktive morajo biti v celoti izvedene“.

29. Izhodišče je naslednje: tehnološke novosti, kot so sistemi RFID, nedvomno vplivajo na zahteve po učinkovitem pravnem okviru za varstvo podatkov. Potreba po učinkovitem varstvu osebnih podatkov posameznika lahko poleg tega omeji uporabo teh novih tehnologij. Gre torej za obojestranski vpliv: tehnologija vpliva na zakonodajo in obratno ([3]).

([1]) Eduard T. Hall, 1966. *The Hidden Dimension*. (1. izd.). Garden City, N.Y: Doubleday.

([2]) Altman, I. 1975 *The Environment and Social Behaviour,* Brooks/Cole Monterrey.

([3]) Glej pripombe ENVP v zvezi s sporočilom Komisije o interoperabilnosti evropskih zbirk podatkov, ki so bile marca 2006 objavljene na spletni strani ENVP.

Varstvo temeljnih pravic

30. Varstvo temeljnih pravic do zasebnosti in varstva podatkov v Evropski uniji je v prvi vrsti zagotovljeno s pravnim okvirom, ki je potreben za zaščito pravic, potrjenih v členu 8 Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin ter v členih 7 in 8 Listine Evropske unije o temeljnih pravicah. Zadeven pravni okvir za varstvo podatkov in RFID v osnovi predstavlja Direktiva 95/46/ES o varstvu podatkov ter Direktiva 2002/58/ES o zasebnosti in elektronskih komunikacijah ([1]).

31. Splošni pravni okvir za varstvo podatkov, kot je določen v Direktivi 95/46/ES, se uporablja za RFID, če so podatki, ki jih obdelujejo sistemi RFID, opredeljeni kot osebni podatki. Medtem ko se v nekaterih primerih pri aplikacijah RFID nedvomno obdelujejo osebni podatki in zato spadajo v področje uporabe Direktive o varstvu podatkov, obstajajo tudi aplikacije, pri katerih uporaba omenjene direktive ni tako očitna. Namen Mnenja št. 4/2007 delovne skupine za varstvo podatkov iz člena 29 o pojmu osebnih podatkov je prispevati k oblikovanju jasnejšega in splošno priznanega razumevanja pojma osebnih podatkov in tako zmanjšati s tem povezano negotovost ([2]).

32. V zvezi z Direktivo o zasebnosti in elektronskih komunikacijah pa je treba povedati, da zaenkrat še ni jasno, ali se ta direktiva uporablja za aplikacije RFID. Zato predlog Komisije z dne 13. novembra 2007 za spremembo te direktive vsebuje določbo, v kateri je opredeljeno, da se ta direktiva dejansko uporablja za nekatere aplikacije RFID. Vendar pa nekatere aplikacije RFID morda ne bodo zajete, saj je direktiva omejena na obdelavo osebnih podatkov v povezavi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih.

33. Varstvo osebnih podatkov lahko dopolnjuje vrsta samoregulativnih instrumentov (nezakonodajni okvir). Uporabo teh instrumentov dejavno spodbujata obe direktivi, zlasti člen 27 Direktive o varstvu podatkov, ki določa, da morajo države članice in Komisija spodbujati pripravljanje kodeksov ravnanja, katerih namen je prispevati k pravilnemu izvajanju te direktive. Poleg tega bi lahko samoregulativni instrumenti učinkovito prispevali k izvajanju varnostnih ukrepov iz člena 17 Direktive o varstvu podatkov in člena 14 Direktive o zasebnosti in elektronskih komunikacijah.

([1]) V točki 59 tega mnenja je obravnavana ustreznost tretje direktive, tj. Direktive 99/5/ES Evropskega parlamenta in Sveta z dne 9. marca 1999 o radijski opremi in telekomunikacijski terminalski opremi ter medsebojnem priznavanju skladnosti te opreme (UL L 91, 7.4.1999, str. 10).

([2]) Glej med drugim str. 10 mnenja, navedenega v opombi 5.

Dosledno izvajanje obstoječega okvira

34. V mnenju o sporočilu glede Direktive o varstvu podatkov je navedenih več instrumentov, ki so na voljo za boljše izvajanje Direktive. Večina nezavezujočih instrumentov iz tega mnenja je povezana z RFID, npr. obrazložitvena sporočila ali druga sporočila, spodbujanje najboljših praks, uporaba pečatov zaupnosti in revizije varstva podatkov s strani tretjih strank. V poglavju 5 bo obravnavana možnost sprejetja posebnih pravil za RFID. Izboljšave pa so možne tudi znotraj sedanjega okvira.

Samoregulativni instrumenti

35. ENVP se strinja s Komisijo, da je v prvi fazi primerno omogočiti prostor za samoregulacijo, da bi lahko zainteresirane strani hitro vzpostavile pravno ustrezno okolje, kar bi pripomoglo k oblikovanju varnejšega pravnega okolja.

36. Komisija naj bi v posvetovanju s skupino zainteresiranih strani za RFID spodbudila in usmerjala ta proces samoregulacije. V zvezi s tem ENVP pozdravlja v sporočilu napovedano priporočilo, ki naj bi vsebovalo posebne smernice za določitev „načel, ki bi jih morali upoštevati javni organi in druge zainteresirane strani pri uporabi RFID“.

37. Sporočilo predvideva samoregulacijo v obliki kodeksa ravnanja ali kodeksa dobre prakse. Po mnenju ENVP bi bilo treba s samoregulacijo ne glede na obliko, v kateri je izražena:

— zagotoviti konkretne in praktične smernice o posameznih vrstah aplikacij RFID ter tako prispevati k skladnosti s pravnim okvirom za varstvo podatkov,

— obravnavati posebna vprašanja in težave glede varstva podatkov, ki se pojavljajo v okviru splošnih aplikacij RFID,

— prispevati k enotni in usklajeni uporabi Direktive o varstvu podatkov po vsej EU, zlasti v sektorju, za katerega je verjetno, da bo uporabljal isto vrsto aplikacij RFID v celotni EU, izvajati pa bi jo morale vse zadevne zainteresirane strani.

— Nespoštovanje bi moralo imeti negativne (verjetno finančne) posledice.

38. ENVP opozarja na področje, na katerem bo samoregulacija še posebej koristna. Za tiste aplikacije RFID, ki vključujejo obdelavo osebnih podatkov, Direktiva o varstvu podatkov upravljavcem podatkov nalaga različne obveznosti, zlasti v skladu s členom 17 (varnost obdelave) in členom 7 (obdelava podatkov je dovoljena le, če obstaja ustrezna pravna podlaga). V skladu s temi določbami morajo upravljavci podatkov na eni strani sprejeti ukrepe proti nepooblaščenemu razkritju podatkov, na drugi strani pa zagotoviti, da se obdelava, kot je razkritje informacij prek čitalnikov, kjer je to ustrezno, dovoli le s privolitvijo posameznika, na katerega se podatki nanašajo.

39. Te določbe Direktive o varstvu podatkov je mogoče razlagati kot zahtevo, da se aplikacije RFID uporabljajo na podlagi nujnih tehničnih rešitev, da se prepreči oziroma čim bolj zmanjša tveganje neželenega razkritja in zagotovi, da se obdelava ali prenos podatkov zgodi le s privolitvijo, kjer je to ustrezno. Po mnenju ENVP bosta ta obveznost (tj. uporaba nujnih tehničnih rešitev za preprečitev oziroma čim večje zmanjšanje tveganja neželenega razkritja) in njena zavezujoča narava za uporabnike aplikacij RFID še močnejša in jasnejša, če bo ta zahteva vključena v navedeni prihodnji kodeks ravnanja ali kodeks dobre prakse. Zato ENVP toplo priporoča, da se v priporočilo Komisije vključi ta razlaga Direktive o varstvu podatkov, s katero se poudari obstoj obveznosti, da je treba aplikacije RFID uporabljati na podlagi nujnih tehnoloških ukrepov za preprečitev neželenega zbiranja ali razkritja informacij.

Potreba po smernicah

40. ENVP priporoča, da Komisija v tesnem sodelovanju s strokovno skupino RFID pripravi enega ali več dokumentov, ki bodo zagotovili jasne smernice o tem, kako sedanji pravni okvir uporabiti v okolju RFID. V smernicah bi morali biti predvideni praktični načini izvajanja načel iz Direktive o varstvu podatkov in Direktive o zasebnosti in elektronskih komunikacijah. ENVP v zvezi s splošnim pristopom smernic in njihovo konkretno vsebino podaja naslednje predloge.

41. Smernice, v katerih so opredeljena načela, ki veljajo za uporabo RFID, bi morale biti ustrezno ciljno naravnane in slediti pristopu, prilagojenemu posameznim sektorjem. Z enakim pristopom za vse ne bo dosežen zastavljeni namen, in sicer zagotoviti jasen in skladen okvir. Namesto tega morajo biti smernice omejene na natančno opredeljene sektorske aplikacije RFID.

42. Poleg tega bi morale biti v smernicah predlagane praktične in učinkovite metode za razvoj *tehnik in standardov*, ki bi lahko prispevali k usklajenosti sistemov RFID s pravnim okvirom za varstvo podatkov in zagotovili, da bo načelo spoštovanja zasebnosti upoštevano že pri načrtovanju sistemov (*privacy-by-design*).

43. Pri uporabi sedanjega pravnega okvira v okolju RFID je treba posebno pozornost nameniti spoštovanju načel varstva podatkov in obveznosti, ki veljajo za upravljavce podatkov aplikacij RFID. Poseben pomen imajo naslednje obveznosti in načela:

— načelo pravice do informacij, vključno s pravico vedeti, kdaj se podatki zbirajo prek čitalnikov, in po potrebi, ali so izdelki označeni,

— pojem privolitve kot ene izmed pravnih podlag za obdelavo podatkov. Ta pojem se odraža v obveznosti o deaktivaciji oznak RFID na prodajnem mestu, razen če posameznik, na katerega se nanašajo osebni podatki, da svojo privolitev ([1]). Pravica do deaktivacije oznak RFID služi tudi zagotavljanju varnosti informacij, tj. zagotavljanju, da se podatki, ki se obdelujejo prek oznak RFID, ne razkrijejo neželenim tretjim osebam,

— pravica posameznika, da ne postane predmet škodljivih odločitev, sprejetih zgolj na podlagi samodejne obdelave določenega osebnega profila.

44. Kar zadeva pravico do informacij, bi moralo biti v smernicah določeno, da je treba posameznikom zagotoviti *informacije* v zvezi z obdelavo njihovih osebnih podatkov. Med drugim jih je predvsem treba opozoriti na *(i)* prisotnost čitalnikov in prisotnost aktiviranih oznak RFID na izdelkih ali njihovi embalaži; *(ii)* posledice prisotnosti teh čitalnikov ali oznak v smislu zbiranja podatkov in *(iii)* namene, za katere se zbirajo podatki.

45. Kot eden izmed ukrepov za zagotavljanje informacij bi bila morda primerna uporaba logotipov. Logotipi se lahko uporabijo za opozarjanje na prisotnost čitalnikov in oznak RFID, ki naj bi ostale aktivne. Vendar le z uporabo logotipov ne bo mogoče zagotoviti poštene obdelave podatkov, v okviru katere je treba posamezniku, na katerega se nanašajo osebni podatki, informacije zagotavljati na jasen in razumljiv način. Uporabo logotipov bi bilo treba obravnavati kot ukrep, ki dopolnjuje zagotavljanje podrobnejših informacij.

([1]) Za več podrobnosti glej odstavke 46–50 tega mnenja.

Temelj: načelo možnosti izbire (*opt-in*)

46. Pri vseh aplikacijah RFID bi bilo treba na prodajnem mestu nujno spoštovati in izvajati načelo možnosti izbire (*opt-in* oz. načelo predhodnega soglasja posameznika). Poprodajno posredovanje podatkov, pridobljenih z oznakami RFID, bi bilo nezakonito, razen če ima upravljavec podatkov za to ustrezno pravno podlago. Ustrezna pravna podlaga je običajno le (a) privolitev posameznika, na katerega se osebni podatki nanašajo, ali (b) dejstvo, da je razkritje nujno za zagotovitev storitve na posebno in prostovoljno zahtevo zadevnega posameznika ([1]). Obe pravni podlagi torej upoštevata načelo možnosti izbire.

47. V skladu z načelom možnosti izbire je treba oznake deaktivirati na prodajnem mestu, razen če je posameznik, ki je kupil izdelek, na katerega je pritrjena oznaka, izrazil željo, da ostane oznaka aktivna. Če posameznik uveljavi pravico do izbire in odloči, da ostane oznaka aktivna, s tem privoli k nadaljnji obdelavi njegovih podatkov, denimo k posredovanju podatkov v čitalnik ob njegovem naslednjem obisku pri upravljavcu podatkov.

48. ENVP poudarja, da je za obvladovanje vse večje raznolikosti aplikacij RFID in omogočanje novih inovativnih poslovnih modelov potreben prilagodljiv pristop. Prilagodljivost je potrebna tudi pri izvajanju načela možnosti izbire.

49. Načelo možnosti izbire je mogoče izvajati na več načinov. Namesto odstranitve oznake bi na primer lahko predvideli njeno blokado, začasno onesposobitev ali vezavo na posameznega uporabnika na podlagi modela varnostne politike, imenovanega tudi *resurrecting duckling* ([2]). V primeru oznak izdelkov s kratkim življenjskim ciklom bi se naslov oznake, ki kaže na podatke, shranjene v zbirki podatkov, lahko tudi zbrisal iz referenčne zbirke podatkov, s čimer bi preprečili nadaljnjo obdelavo dodatnih podatkov, zbranih prek te oznake.

50. Skratka, čeprav je po mnenju ENVP upoštevanje načela možnosti izbire na prodajnem mestu zakonska obveznost, ki v večini primerov obstaja že v okviru Direktive o varstvu podatkov, obstaja več dobrih razlogov za opredelitev te obveznosti v samoregulativnih instrumentih, tudi zaradi tega, da se zagotovi najprimernejši način izvajanja tega načela.V vsakem primeru pa je potrebno posebno izvajanje pri tistih aplikacijah RFID, ki ne spadajo v področje uporabe Direktive o varstvu podatkov.

([1]) Pri nekaterih aplikacijah RFID se je možno sklicevati na drugo pravno podlago, npr. člen 7(f) (zakoniti interesi, za katere si prizadeva upravljavec, ob upoštevanju ustreznih zaščitnih ukrepov).

([2]) Ime tega modela, ki sta ga razvila Frank Stajano in Ross Anderson z Univerze v Cambridgu, izhaja iz primera, „kako gosji mladič, ki se je pravkar zvalil, domneva, da je prvi premikajoči predmet, ki ga zagleda, njegova mama“.

Potreba po upoštevanju načela spoštovanja zasebnosti pri načrtovanju sistemov

51. Komisija je v sporočilu pod točko 3.2 na strani 6 potrdila zamisel o čimprejšnji natančni določitvi in sprejetju meril za načrtovanje, s čimer bi kar najbolj zmanjšali tveganja za zasebnost in varstvo podatkov. ENVP ta pristop pozdravlja. Dejansko bo sprejetje specifikacij in meril za načrtovanje, imenovanih tudi najboljše razpoložljive tehnologije (*Best Available Techniques* – BAT), učinkovito prispevalo k predpisom o varstvu podatkov in varnostnim zahtevam. Z določitvijo tehnoloških in organizacijskih meril se bo ob rednem pregledovanju okrepil vzorec, ki ga razvija Evropska unija za uskladitev zahtev na področju zasebnosti in tistih s področja varnosti.

52. Ustrezna opredelitev najboljših razpoložljivih tehnologij za sisteme RFID glede zasebnosti in varnosti bo odločilnega pomena za vzpostavitev zaupljivega okolja, ki bo spodbudilo splošno razširjenost teh tehnologij med končnimi uporabniki, pomembna pa bo tudi za konkurenčnost evropske industrije.

53. Postopek izbora najboljših razpoložljivih tehnologij za sisteme RFID bi moral temeljiti na presojah vplivov na zasebnost in varnost, v katere bo treba vložiti še veliko truda. ENVP meni, da lahko Evropska agencija za varnost omrežij in informacij (ENISA) in Skupna raziskovalna središča Evropske komisije v povezavi z zainteresiranimi stranmi v gospodarstvu prispevajo k opredelitvi najboljših praks in razvoju teh metodologij. Nemški zvezni urad za varno informacijsko tehnologijo (*Bundesamt für Sicherheit in der Informationstechnik – BSI*) je z nedavnim projektom „tehnične smernice za RFID“ dal dober primer ([3]) najboljše razpoložljive tehnologije, ki bi jo bilo treba sedaj razviti na evropski ravni.

54. Tudi standardi so lahko zelo pomembni za hitro uveljavitev načela spoštovanja zasebnosti pri načrtovanju sistemov. Komisija bi si morala zato prizadevati, da se pri razvoju mednarodnih standardov RFID sprejmejo zaščitni ukrepi za zasebnost in varstvo podatkov. Delovna skupina iz člena 29 je v delovnem dokumentu ([4]) o RFID jasno ponazorila, da lahko standardi prispevajo k razvoju sistemov RFID, pri katerem se upošteva varovanje zasebnosti.

([3]) http://www.bsi.bund.de/veranst/rfid/index.htm

([4]) Delovni dokument (WP 105) o vprašanjih varstva podatkov, povezanih s tehnologijo RFID, 19. januar 2005.

55. ENVP pozdravlja stališče, ki ga je sprejela Komisija glede raziskav in razvoja tehnologij RFID ter potrebe po zmanjšanju tveganja za zasebnost. Načelo spoštovanja zasebnosti pri načrtovanju sistemov je treba dejansko vključiti v najzgodnejšo fazo razvoja tehnologij, kar bo bolj pripomoglo k večji skladnosti tehnologij s pravnim okvirom za varstvo podatkov. Kot je na kratko predstavljeno že v letnem poročilu za leto 2006, se bo ENVP pridružil tem prizadevanjem z dajanjem mnenj in svetovanjem glede posameznih projektov 7. okvirnega programa (2007–2013).

V. ALI SO POTREBNI POSEBNI ZAKONODAJNI UKREPI?

56. Samoregulacija morda ne bo zadostovala za celovito izvajanje obstoječega okvira za varstvo podatkov in zasebnosti. Tudi če izpolnjuje navedene zahteve, je njena uporaba prostovoljna, njenega neupoštevanja pa ni mogoče vedno učinkovito sankcionirati. Poleg tega bi lahko bili zavezujoči zakonodajni ukrepi potrebni tudi zato, da se zagotovi zaščita posameznikovih pravic do zasebnosti in varstva podatkov. To je še zlasti pomembno v primerih, ko samoregulativni pristop ne uspe.

57. Ključno vprašanje je določitev pravnih instrumentov, potrebnih za zagotovitev, da se aplikacije RFID učinkovito uporabljajo z nujnimi tehničnimi rešitvami za preprečitev oziroma čim večje zmanjšanje tveganja za varstvo podatkov in zasebnost ter da pristojni upravljavci sprejmejo ustrezne ukrepe za izpolnitev obveznosti, ki izhajajo iz obstoječih pravnih okvirov. S tem se sprožijo nova vprašanja:

— Ali so potrebna posebna pravila?

— Če so posebna pravila potrebna, ali se lahko sprejmejo v okviru obstoječega zakonodajnega okvira, npr. z uporabo obstoječih postopkov komitologije?

— Ali pa je potreben nov zakonodajni instrument, da se zagotovi učinkovita uporaba aplikacij RFID z vgrajenimi tehnologijami za boljše varovanje zasebnosti.

58. V tem poglavju so obravnavane možnosti uvedbe zavezujočih zakonodajnih ukrepov v okviru obstoječega zakonodajnega okvira, v poglavju VI pa bo obravnavana potreba po novem zakonodajnem instrumentu, saj gre za ločeni vprašanji.

59. Kot prvo bi bilo treba posebno pozornost nameniti določbam člena 17 Direktive 95/46/ES, člena 14(3) Direktive 2002/58/ES in člena 3(3)(c) Direktive 99/5/ES. Člen 14(3) državam članicam omogoča, da sprejmejo ukrepe, s katerimi 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 ([1]). V členu 3(3)(c) Direktive 99/5/ES je določeno, da lahko Komisija s postopkom komitologije odloči, da morajo biti aparati v določenih razredih opreme ali aparati določenih tipov skonstruirani tako, da vsebujejo zaščitne naprave za zagotavljanje zaščite osebnih podatkov in zasebnosti uporabnikov in naročnikov. Člen 3(3)(c) Direktive 99/5/ES do sedaj še ni bil uporabljen.

60. Te določbe zakonodajalca na nacionalni ravni in na ravni Skupnosti pooblaščajo, da predpiše obvezno vključitev zaščitnih ukrepov za zasebnost in varstvo podatkov v proizvodnjo sistemov RFID; to je koncept, imenovan „načelo spoštovanja zasebnosti pri načrtovanju“ ([2]). Pri tem se zahteva tudi uporaba najboljših razpoložljivih tehnologij.

61. Da bi upoštevanje načela spoštovanja zasebnosti pri načrtovanju postalo obvezno, ENVP priporoča, da Komisija uporabi mehanizem iz odstavka 3(3)(c) Direktive 99/5/ES, pri čemer naj se posvetuje s strokovno skupino RFID.

62. Kot drugo je možno opredeliti uporabo obstoječega zakonodajnega okvira za RFID s spremembami samih direktiv. Kot že rečeno, je Komisija pred kratkim predstavila predlog za spremembo Direktive o zasebnosti in elektronskih komunikacijah, ki vsebuje novo določbo v tem smislu. ENVP pozdravlja prvi dokaz, da se lahko navedena direktiva uporablja za aplikacije RFID. ENVP bo posebna vprašanja, ki izhajajo iz razmerja med Direktivo o zasebnosti in elektronskih komunikacijah ter RFID, obravnaval v mnenju o predlogu za spremembo, ki bo objavljeno v začetku leta 2008.

63. Ob upoštevanju dejstva, da Komisija v bližnji prihodnosti ([3]) ne predvideva spremembe Direktive o varstvu podatkov, so možnosti za specifikacijo v zvezi z uporabo obstoječega zakonodajnega okvira za aplikacije RFID omejene.

VI. ALI JE POTREBEN POSEBEN PRAVNI OKVIR ZA RFID?

Namere Komisije

64. V sporočilu ([4]) je poudarjen pomen varnosti in zasebnosti pri načrtovanju. Izražena je tudi potreba po vključitvi vseh zainteresiranih strani. Glavni rezultat dejavnosti Komisije bo *priporočilo za določitev načel, ki bi jih morali upoštevati javni*

([1]) In v skladu s Sklepom Sveta 87/95/EGS z dne 22. decembra 1986 o standardizaciji na področju informacijske tehnologije in telekomunikacij (UL L 36, 7.2.1987, str. 31).
([2]) Glej poglavje IV.
([3]) ENVP podpira ta pristop; glej točko 64.
([4]) Glej odstavek 4.1 Sporočila.

organi in druge zainteresirane strani pri uporabi RFID. Priporočilo bo verjetno sprejeto spomladi leta 2008. V zakonodajnih načrtih, navedenih v sporočilu, sta predvidena dva koraka. Komisija bo:

— preučila ustrezne določbe o RFID v prihodnjem predlogu za spremembo Direktive o zasebnosti in elektronskih komunikacijah. Kot že rečeno, je Komisija novembra 2007 predlagala to spremembo Direktive o zasebnosti in elektronskih komunikacijah, s katero naj bi se potrdila uporabnost direktive za aplikacije RFID ([1]), vendar v njej ni predlagana razširitev področja uporabe Direktive o zasebnosti in elektronskih komunikacijah na zasebna omrežja,

— ocenila potrebo po nadaljnjih zakonodajnih ukrepih za zagotovitev varstva podatkov in zasebnosti.

65. Na podlagi tega pristopa je mogoče pričakovati, da Komisija vsaj kratkoročno ne namerava predložiti novih posebnih zakonodajnih predlogov za zagotovitev varstva podatkov in zasebnosti na področju RFID.

Parametri za zakonodajalca

66. ENVP je v svojem mnenju o sporočilu glede Direktive o varstvu podatkov navedel nekaj usmeritev za zakonodajne dejavnosti v zvezi z obdelavo osebnih podatkov, ki jih je mogoče povzeti, kakor sledi:

— prvič, treba je upoštevati ključna načela varstva podatkov:„*Nova načela niso potrebna, jasno pa je, da obstaja potreba po upravni ureditvi, ki je po eni strani učinkovita in ustreza omreženi družbi, po drugi pa zmanjšuje administrativne stroške*“ ([2]),

— drugič, zakonodajni predlogi naj bi bili predloženi le, če je v zadostni meri dokazano, da so nujni in sorazmerni. Zaradi tega se splošni zakonodajni okvir za varstvo podatkov kratkoročno ne bi smel spremeniti,

— tretjič, družbene spremembe bi lahko privedle do oblikovanja posebnih pravnih okvirov, s katerimi bi se načela Direktive o varstvu podatkov prilagodila vprašanjem, ki izhajajo iz posebnih tehnologij, kot je RFID. Jasno je, da morata biti tudi v zvezi s tem izpolnjena pogoja nujnosti in sorazmernosti.

67. V naslednjem koraku bi bilo koristno opredeliti pričakovanja, s katerimi se sooča zakonodajalec na področju RFID:

— zakonodaja mora biti prožna in puščati dovolj prostora za inovacije in tehnološki razvoj. To bi moralo privesti do zakonodaje, ki je v zadostni meri tehnološko nevtralna,

— drugič, zakonodaja mora zagotoviti pravno varnost. To bi moralo privesti do zakonodaje, ki je dovolj specifična. Zainteresirane strani morajo natančno vedeti, na kakšen način je njihovo ravnanje zakonsko urejeno,

— tretjič, zakonodaja mora učinkovito zaščititi vse upravičene interese vseh udeleženih strani. V vsakem primeru sta v zvezi s tem potrebna uveljavljanje zakonodaje in jasna opredelitev odgovornosti: katera stran je odgovorna za katero ravnanje? ([3]) Te zahteve so še bolj pomembne, ko gre za varstvo zasebnosti in podatkov, temeljne pravice posameznika v skladu z Evropsko Konvencijo o varstvu človekovih pravic in temeljnih svoboščin ter za Listino Evropske unije o temeljnih pravicah.

Stališče ENVP

68. ENVP se zaveda, da se evropskemu zakonodajalcu ni treba odzvati na vsako tehnološko novost. Tehnološki razvoj je lahko zelo hiter, sprejetje in začetek veljavnosti zakonodaje pa zahtevata svoj čas in tako je tudi prav. Zakonodaja mora biti posledica uravnoteženega upoštevanja vseh zadevnih interesov. Kadar se kot zakonodajni instrument izbere direktiva, je potrebnega še več časa, saj je treba direktive v celoti izvajati v pravnih sistemih držav članic.

69. Vendar RFID ni zgolj še ena tehnološka novost, kakor je bilo v tem mnenju poudarjeno že večkrat. V sporočilu je RFID obravnavana kot začetek nove razvojne stopnje informacijske družbe, ki se običajno imenuje tudi „internet stvari“, oznake RFID pa bodo ključni dejavniki „inteligentnih okolij“. Ta okolja so prav tako pomemben korak v razvoju pojava, ki se pogosto imenuje „družba nadzora“ ([4]). Na tej podlagi je mogoče upravičiti sprejetje zakonodajnih ukrepov na področju RFID. RFID lahko privede do kakovostnih sprememb.

([1]) Glej predlagani novi člen 3 Direktive 2002/58.
([2]) Točka 24 mnenja o sporočilu glede Direktive o varstvu podatkov.
([3]) V skladu s terminologijo o varstvu podatkov to pomeni opredelitev „upravljavca podatkov“.
([4]) To sporočilo je bilo vključeno tudi v izjavo evropskih organov za varstvo podatkov, ki je bila sprejeta 2. novembra 2006 v Londonu in je na voljo na spletni strani ENVP: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. S tega vidika ENVP priporoča, da se preuči sprejetje (predloga) zakonodaje Skupnosti, ki bi urejala glavna vprašanja uporabe RFID v zadevnih sektorjih, v primeru da pravilno izvajanje obstoječega pravnega okvira spodleti. Tak zakonodajni ukrep je treba po njegovem začetku veljavnosti šteti za *lex specialis* v odnosu do splošnega okvira za varstvo podatkov.

71. Sprejetje tovrstnega zakonodajnega instrumenta bi imelo naslednje prednosti:

— v instrumentu bi lahko bili določeni vsebinski parametri za samoregulativne mehanizme,

— možnost sprejetja zakonodajnega instrumenta bi lahko bila učinkovita spodbuda za zainteresirane strani, da vzpostavijo samoregulativne mehanizme, s katerimi bi zagotovili ustrezno zaščito.

72. Koristno bi bilo, če bi Komisija pripravila posvetovalni dokument o prednostih in slabostih specifične zakonodaje ter o glavnih elementih takšne zakonodaje. Seveda bi lahko pozvala zainteresirane strani, da prispevajo k temu posvetovanju. Vključena bi lahko bila tudi delovna skupina iz člena 29.

Možni načini

73. Rezultat posredovanja zakonodajalca bi lahko bil prilagojen pravni okvir, sestavljen iz mešanice regulativnih instrumentov, ki opredeljujejo in dopolnjujejo obstoječi pravni okvir. Ta prilagojen pravni okvir bi moral temeljiti na priznanih načelih varstva podatkov in biti osredotočen na delitev odgovornosti in učinkovitost mehanizmov nadzora.

74. Razlog, zakaj bi lahko bila potrebna takšna posebej prilagojena zakonodaja, je povezan z dejstvom, da vse aplikacije RFID ne pomenijo tudi obdelave osebnih podatkov. Z drugimi besedami, če aplikacije RFID ne vključujejo obdelave osebnih podatkov, strani, udeležene v proizvodnji in prodaji izdelkov z oznako RFID, niso pravno zavezane k izvajanju kakršnih koli tehnoloških ukrepov, ki bi preprečili prisluškovanje ali vzpostavitev čitalnikov brez ustrezne seznanitve posameznikov. Vendar – kakor je bilo prikazano – tveganja za zasebnost, povezana z morebitnim nadzorom nad posamezniki, obstajajo tudi pri teh aplikacijah RFID, zato so potrebni enaki ukrepi za varstvo zasebnosti. Zlasti to lahko velja v primerih označevanja potrošniških izdelkov *pred* prodajnim mestom. Skratka, aplikacije RFID, pri katerih se ne obdelujejo osebni podatki, lahko vseeno ogrožajo posameznikovo zasebnost, saj omogočajo prikriti nadzor in uporabo podatkov v nedovoljene namene.

75. ENVP meni, da bi se bilo treba temu nezaželenemu izidu izogniti. Glede na to, da veljavna zakonodaja samo delno upošteva to grožnjo zasebnosti – vsaj pri aplikacijah RFID, pri katerih se ne obdelujejo osebni podatki – in glede na pomanjkljivosti nezavezujočih aktov, se zdi nujno, da se za zagotovitev zadovoljivega rezultata uvedejo obvezni zakonodajni ukrepi.

76. V vsakem primeru bi morali ti ukrepi:

— določiti uporabo načela možnosti izbire na prodajnem mestu kot natančno določeno in nedvomno zakonsko obveznost tudi za aplikacije RFID, ki ne spadajo v področje uporabe Direktive o varstvu podatkov ([1]);

— zagotoviti, da se pri aplikacijah RFID obvezno uporabljajo ustrezni tehnični elementi oziroma upošteva načelo spoštovanja zasebnosti pri načrtovanju sistemov.

VII. **VPRAŠANJE UPRAVLJANJA**

77. V sporočilu je obravnavana „temeljna čezmejna“ razsežnost sistemov RFID le v okviru notranjega trga, ENVP pa meni, da bi bilo treba to razsežnost obravnavati na bolj mednarodni ravni. Že v trgovini so sistemi RFID „čezmejni“, saj oznaka morda ne bo prenehala delovati na prodajnem mestu. Na ravni celotnega sistema RFID postanejo te tehnologije prav tako „čezmejne“, kadar pride do prenosa osebnih podatkov v tretjo državo, ker ima izdelovalec označenega izdelka, ki je del sistema RFID, sedež izven Evropske unije ([2]).

78. Z vidika prihodnosti je upravljanje referenčnih zbirk osebnih podatkov RFID tudi ključni vidik pri ustreznem izvajanju pravnega okvira EU za varstvo podatkov. ENVP poziva k iskanju rešitve na tem področju, saj nadaljnje ogrožanje tega pravnega okvira ni sprejemljivo.

79. Po mnenju ENVP bo vprašanje upravljanja RFID v prihodnosti eden poglavitnih izzivov, v katerega bo treba veliko vložiti. Treba bo poiskati pravi forum za pogajanja in najprimernejšo infrastrukturo za upravljanje, da se zagotovi ustrezno spoštovanje pravic do varstva podatkov tudi v mednarodnem okolju.

([1]) V poglavju IV je navedeno, da je načelo možnosti izbire na prodajnem mestu zakonska obveznost, ki obstaja že v skladu z Direktivo o varstvu podatkov.

([2]) Obveznosti glede prenosa osebnih podatkov so obravnavane v členih 25 in 26 Direktive o varstvu podatkov.

80. V zvezi s tem ENVP poziva Komisijo, naj predstavi svoja stališča glede vprašanja upravljanja, po možnosti v posvetovanju s skupino zainteresiranih strani za RFID.

VIII. **SKLEP**

81. ENVP pozdravlja sporočilo Komisije o RFID, saj so v njem obravnavana glavna vprašanja, ki se porajajo v zvezi z uporabo tehnologije RFID, pa tudi odločilna vprašanja, povezana z zasebnostjo in varstvom podatkov. Strinja se s stališčem, da bi lahko sistemi RFID igrali ključno vlogo v razvoju informacijske družbe, ki se običajno imenuje „internet stvari".

Obrazložitev posledic

82. Široka uporaba tehnologije RFID je nekaj popolnoma novega in bi lahko pomembno vplivala na našo družbo in varstvo temeljnih pravic, npr. pravice do zasebnosti in pravice do varstva podatkov. RFID lahko privede do kakovostnih sprememb.

83. Razlikovati je mogoče med petimi temeljnimi vprašanji zasebnosti in varnosti:

— identifikacija posameznika, na katerega se podatki nanašajo,

— identifikacija upravljavca(-ev) podatkov,

— tradicionalno razlikovanje med zasebno in javno sfero je vse manj pomembno,

— posledice velikosti in fizičnih lastnosti oznak RFID,

— slaba preglednost obdelave.

Podrobna opredelitev posledic

84. Splošni pravni okvir za varstvo podatkov, kot je določen v Direktivi 95/46/ES, se uporablja za RFID, če so podatki, ki jih obdelujejo sistemi RFID, opredeljeni kot osebni podatki.

85. V zvezi z Direktivo o zasebnosti in elektronskih komunikacijah: predlog Komisije z dne 13. novembra 2007 za spremembo te direktive vsebuje določbo, v kateri je opredeljeno, da se ta direktiva dejansko uporablja za nekatere aplikacije RFID. Vendar pa nekatere druge aplikacije RFID morda ne bodo zajete, saj je direktiva omejena na obdelavo osebnih podatkov v povezavi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih.

86. Varstvo osebnih podatkov lahko dopolnjuje vrsta samoregulativnih instrumentov. Primerno je omogočiti prostor za samoregulacijo pod pogojem, da:

— zagotavlja konkretne in praktične smernice o posameznih vrstah aplikacij RFID,

— obravnava posebna vprašanja in težave glede varstva podatkov, ki se pojavljajo v okviru splošnih aplikacij RFID,

— prispeva k enotni in usklajeni uporabi Direktive o varstvu podatkov po vsej EU,

— jo uporabljajo vse zadevne zainteresirane strani.

87. ENVP priporoča, da Komisija v tesnem sodelovanju s strokovno skupino RFID pripravi enega ali več dokumentov, ki bodo zagotovili jasne smernice o tem, kako uporabiti sedanji pravni okvir za RFID.

88. Smernice, v katerih so opredeljena načela, ki veljajo za uporabo RFID, bi morale biti ustrezno ciljno naravnane in upoštevati pristop, prilagojen posameznim sektorjem. V smernicah bi morale biti predlagane praktične in učinkovite metode za razvoj *tehnik in standardov*, ki bi lahko prispevali k usklajenosti sistemov RFID s pravnim okvirom za varstvo podatkov in zagotovili, da bo načelo spoštovanja zasebnosti upoštevano že pri načrtovanju sistemov (*privacy-by-design*).

89. ENVP pozdravlja pristop iz sporočila Komisije, v katerem je potrjena zamisel o čimprejšnji natančni določitvi in sprejetju meril za načrtovanje.

90. Čeprav je po mnenju ENVP upoštevanje načela možnosti izbire na prodajnem mestu zakonska obveznost, ki v večini primerov obstaja že v okviru Direktive o varstvu podatkov, bi bilo treba to obveznost opredeliti v samoregulativnih instrumentih.

Ali so potrebni posebni ukrepi?

91. Da bi upoštevanje načela spoštovanja zasebnosti pri načrtovanju postalo obvezno, ENVP priporoča, da Komisija uporabi mehanizem iz odstavka 3(3)(c) Direktive 99/5/ES, pri čemer naj se posvetuje s strokovno skupino RFID.

92. Priporoča tudi, da se preuči sprejetje (predloga) zakonodaje Skupnosti, ki bi urejala glavna vprašanja uporabe RFID v zadevnih sektorjih v primeru, da pravilno izvajanje obstoječega pravnega okvira spodleti. Tak zakonodajni ukrep je treba po njegovem začetku veljavnosti šteti za *lex specialis* v odnosu do splošnega okvira za varstvo podatkov. V tem zakonodajnem ukrepu bi morali biti upoštevani tudi pomisleki glede varstva zasebnosti in podatkov, ki se porajajo pri nekaterih RFID aplikacijah, npr. pri označevanju potrošniških izdelkov pred prodajnim mestom, ki ne vključuje nujno obdelave osebnih podatkov.

93. Komisija bi morala pripraviti posvetovalni dokument o prednostih in slabostih specifične zakonodaje ter o glavnih elementih takšne zakonodaje.

94. Rezultat posredovanja zakonodajalca bi lahko bil posebej prilagojen pravni okvir, sestavljen iz mešanice regulativnih instrumentov, ki opredeljujejo in dopolnjujejo obstoječi pravni okvir. V vsakem primeru bi morali ti ukrepi:

— določiti uporabo načela možnosti izbire na prodajnem mestu kot natančno določeno in nedvomno zakonsko obveznost tudi za aplikacije RFID, ki ne spadajo v področje uporabe Direktive o varstvu podatkov ([1]),

— zagotoviti, da se pri aplikacijah RFID obvezno uporabljajo ustrezni tehnični elementi oziroma upošteva načelo spoštovanja zasebnosti pri načrtovanju.

Upravljanje

95. ENVP poziva Komisijo, naj predstavi svoja stališča glede vprašanja upravljanja, po možnosti v posvetovanju s skupino zainteresiranih strani za RFID.

V Bruslju, 20. decembra 2007

Peter HUSTINX

Evropski nadzornik za varstvo podatkov

([1]) V poglavju IV je navedeno, da je načelo možnosti izbire na prodajnem mestu zakonska obveznost, ki obstaja že v skladu z Direktivo o varstvu podatkov.