

Eiropas Ekonomikas un sociālo lietu komitejas atzinums par tematu "Radiofrekvenču identifikācija (RFID)"

(2007/C 256/13)

Saskaņā ar Eiropas Kopienas dibināšanas līguma 262. pantu Eiropas Komisija 2007. gada 26. februāra vēstulē lūdza Eiropas Ekonomikas un sociālo lietu komiteju izstrādāt atzinumu "Radiofrekvenču identifikācija (RFID)".

Par Komitejas dokumenta sagatavošanu atbildīgā Transporta, enerģētikas, infrastruktūras un informācijas sabiedrības specializētā nodaļa atzinumu pieņēma 2007. gada 19. jūnijā. Ziņotājs — Morgan kgs.

Eiropas Ekonomikas un sociālo lietu komiteja 437. plenārajā sesijā, kas notika 2007. gada 11. un 12. jūlijā (11. jūlija sēdē), ar 138 balsīm par, 1 balsi pret un 6 atturoties, pieņēma šo atzinumu.

1. Secinājumi un ieteikumi

1.1 Radiofrekvenču identifikācija (RFID) ir nozīmīga tehnoloģija, kas laika gaitā kļūs īpaši svarīga. Tās pašreizējie un turpmākie lietojumi paver iespēju būtiski uzlabot daudzus uzņēmējdarbības procesus gan publiskajā, gan privātajā sektorā un sniegt ievērojamu labumu gan fiziskām personām, gan uzņēmumiem. Tā paver arī iespējas būtiski veicināt interneta lietojumu attīstību, padarot iespējamu "lietisko internetu", kā to ir raksturojusi ANO aģentūra. Tomēr, ja netiek nodrošināta ļoti rūpīga RFID kontrole, minētā tehnoloģija var apdraudēt personu privātumu, pilsoniskās brīvības, kā arī fizisko personu un uzņēmumu drošību.

1.2 Paziņojuma pilnais nosaukums ir "Radiofrekvenču identifikācija Eiropā: ceļā uz politikas īstenošanas pasākumiem". Komisija jau ir rīkojusi plašu apspriešanu, un minētais paziņojums sagatavots, pamatojoties uz tās rezultātiem. EESK tagad ir aicināta sniegt izpētes atzinumu. Pamatojoties uz atsauksmēm par minēto paziņojumu, Komisija gada beigās publicēs ieteikumu dalībvalstīm. Likumdošanas iniciatīvas, kurām nepieciešams ilgāks laiks, tiks ierosinātas vēlāk. Tādēļ šajā atzinumā galvenā uzmanība jāvelta minētā paziņojuma saturam.

1.3 Lai palīdzētu formulēt attiecīgos ieteikumus, Komisija nolēma izveidot ieinteresēto aprindu grupu kopīgā viedokļa paušanai. EESK būtu ļoti gandarīta, ja tā varētu iepazīstināt ieinteresēto aprindu grupu ar šo atzinumu.

1.4 EESK atbalsta Komisijas ierosinātos pasākumus radiofrekvenču spektra, standartu, veselības, drošības un vides jomā. Komiteja uzsver, ka steidzami jānodrošina efektīva rūpniecības interešu pārstāvība Standartu forumā.

1.5 Tā kā ieteikumus dalībvalstīm Komisija publicēs šī gada beigās, ir pamats uzskatīt, ka tā akceptēs datu drošības un privātuma infrastruktūru tādu, kāda tā ir pašreiz. Konkrēti tas varētu izpausties tādējādi, ka katrā dalībvalstī esošās datu aizsardzības

iestādes kļūs par iestādēm, kas atbildīgas par privātumu un datu aizsardzību RFID jomā. Šis atzinums veltīts galvenokārt minētajiem jautājumiem.

1.6 Privātuma un pilsonisko brīvību jomā ar RFID saistītie apdraudējumi ir nopietni:

— RFID elektroniskos marķējumus var piestiprināt priekšmetiem un dokumentiem bez šo priekšmetu ieguvēja ziņas. Tā kā radioviļņi viegli šķērso audumus, plastmasas un citus materiālus, ir iespējams nolasīt RFID elektroniskos marķējumus, kas iešūti apģērbā vai piestiprināti priekšmetiem, kas atrodas rokassomās, iepirkumu somās vai koferos.

— Ar elektronisko izstrādājumu kodu palīdzību jebkuram priekšmetam varētu piešķirt noteiktu un vienreizēju identifikācijas (ID) numuru. Lietojot vienreizējus ID numurus, iespējams izveidot globālu priekšmetu reģistrācijas sistēmu, kurā jebkurš fizisks priekšmets tiek identificēts un piesaistīts tā pircējam vai īpašniekam tirdzniecības vai nodošanas vietā.

— RFID izvēršanai ir nepieciešams radīt liela apjoma datubāzes ar elektronisko marķējumu identifikācijas numuriem piesaistītajiem datiem. Tā kā datoru atmiņas apjoms un datu apstrādes veikspēja palielinās, minētos ierakstus var sasaistīt ar personu identifikācijas datiem.

— Elektroniskos marķējumus ir iespējams nolasīt no attāluma ar tādu nolasītāju palīdzību, kurus var neredzamā veidā izvietot gandrīz jebkurā vidē, kur uzturas cilvēki. Nolasītājus var izvietot zem grīdu seguma, iestrādāt paklājos, durvīs un plauktos, tādējādi fiziska persona var praktiski neuzzināt par to, ka tiek skenēta.

— Ja personas identitāte ir piesaistīta RFID elektroniskā marķējuma numerācijai, ir iespējama fizisku personu izsekošana vai profila izveidošana bez viņu ziņas vai piekrišanas.

— Ļoti iespējams, ka dzīvosim pasaulē, kurā RFID nolasītāji veido visaptverošu globālu tīklu. Šādam tīklam nebūtu nepieciešams, lai nolasītāji atrastos pilnīgi visur. Sastrēgumu novēršanai paredzētā maksas sistēma Londonā spēj izsekot visām automašīnām, kuras iebrauc Londonas centrālajā daļā, ar samērā nedaudzu stratēģiski izvietotu kameru palīdzību. Līdzīgā veidā ir iespējams izveidot stratēģiski izvietotu RFID nolasītāju tīklu. To nedrīkst pieļaut.

1.7 Minētie apdraudējumi liek izdarīt šādus secinājumus:

— RFID lietotājiem jāinformē sabiedrība par īstenotajiem pasākumiem un praksi, un attiecīgās datubāzes, kurās apkopota personīgā informācija, nedrīkst būt slepenas.

— Fiziskām personām ir tiesības zināt, vai uz mazumtirdzniecībā pārdotajām precēm ir RFID elektroniskais marķējums vai nolasītāji. Visām iesaistītajām pusēm jābūt informētām par ikvienu elektroniskā marķējuma lasījumu, kas notiek mazumtirdzniecības vidē.

— RFID lietotājiem jāinformē par elektroniskā marķējuma un nolasītāju lietošanas nolūkiem. Informācijas vākšana būtu jāierobežo līdz tādām apjomam, kāds ir nepieciešams norādītajam nolūkam.

— RFID lietotāji atbild par tehnoloģijas ieviešanu un izmantošanu saskaņā ar attiecīgajiem normatīvajiem aktiem un pamatnostādnēm datu aizsardzības jomā. Tie ir atbildīgi arī par sistēmas un tās datubāzes drošību un integritāti.

1.8 Nav skaidrs, kā šos principus īstenot praksē. Būtu ļoti labi, ja katrs uzņēmums, kas iesaistīts darījumos, kas vieno uzņēmējdarbības veicējus un gala patērētājus, t.i., mazumtirgotāji, biļešu un ieejas karšu sagatavotāji, piekļūšanas kontroles dienesti, kā arī transporta pakalpojumu sniedzēji klientiem sniegtu garantiju (klientu hartas formā), ka minētie principi tiks ievēroti. Šādas hartas koncepcijā varētu iekļaut visus 4.5. punktā minētos labas prakses principus datu aizsardzības jomā. Līdztekus tam EESK ierosina šādas pamatnostādes:

a) būtu jāaizliedz komersantiem uzspiest klientiem vai piespiest tos pieņemt aktīvus vai neaktīvus elektroniskos marķējumus izstrādājumos, kurus tie iegādājas. Piemēram, elektronisko marķējumu varētu piestiprināt iepakojumam vai varētu izmantot noņemamu elektronisko marķējumu, kā tas tiek darīts ar cenu norādēm;

b) klientiem būtu jānodrošina iespēja brīvi noņemt vai atspējot savā valdījumā esošu priekšmetu elektronisko marķējumu;

c) RFID tehnoloģiju principā nedrīkstētu izmantot fizisku personu izsekošanai. Cilvēku izsekošana, izmantojot, piemēram, apģērbu, preces, biļetes vai citus priekšmetus, ir nepieļaujama;

d) RFID nekādā gadījumā nedrīkstētu izmantot veidā, kas varētu likvidēt vai mazināt anonimitāti;

e) atbildīgajai iestādei būtu skaidri jānorāda, ka c) un d) punktā minētās iespējas ir pieļaujamas tikai izņēmuma gadījumos un atbildīgā iestāde par tām iepriekš ir oficiāli jāinformē.

1.9 Varētu apsvērt noteiktus izņēmumus attiecībā uz iepriekš minētajām pamatnostādnēm gadījumos, kad

— privātpersonas izmanto iespēju saglabāt aktivizētu elektronisko marķējumu savu personīgo ērtību labad;

— privātpersonas piekrīt, ka tiek izsekotas kritiskā vidē, piemēram, paaugstinātas drošības publiskās un privātās iestādēs un ēkās;

— privātpersonas izvēlas izmantot lietojumus, kas noteiks to atrašanās vietu un tās identificēs tādā pat veidā, kā tas jau notiek ar mobilo tālruni, ATM karšu, interneta adresu palīdzību u.tml.

Par jebkuriem šāda veida izņēmumiem būtu jāinformē atbildīgā iestāde.

1.10 RFID tehnoloģija nav nevainojama, un tās iespējas vēl nav pilnībā apzinātas. No vienas puses, tā var sniegt neiedomājamus labumus mūsu tehnoloģiski attīstītajai civilizācijai, bet, no otras puses, tā var radīt līdz šim nepieredzētu apdraudējumu privātamam un brīvībai. EESK uzskata, ka RFID lietojumi būtu jāizstrādā saskaņā ar stingru ētikas kodeksu attiecībā uz privātuma, brīvības un datu drošības ievērošanu, taču lietojumu attīstība būtu jāturpina ar nosacījumu, ka tiek nodrošinātas nepieciešamās garantijas.

1.11 Tātad, atļaujot RFID lietojumus, būtu jānodrošina, lai to izmantošana būtu pilnībā pārredzama jebkurai no iesaistītajām pusēm. Lietojumi, kas paredzēti darbībām ar precēm, kopumā ir pieņemami. Tādi lietojumi, kas ir saistīti ar cilvēku marķēšanu, kopumā nav pieņemami, izņemot vidēs, kur viņi uzturas īslaicīgi. Lietojumi, kuri uzrāda cilvēku saikni ar precēm, var būt pieņemami tirdzniecības nolūkos. Lietojumi, kuri identificē cilvēkus, izmantojot preces, ko viņi ir iegādājušies, principā nav pieļaujami. Turklāt daži lietojumi ir nepieļaujami brīvā sabiedrībā, un tos nedrīkstētu atļaut nekādā gadījumā. Komisijas ieteikumā dalībvalstīm vislielākā uzmanība jāvelta obligātajai prasībai nodrošināt privātumu un anonimitāti.

2. Kas ir RFID un kāda ir tās nozīme?

2.1 RFID ir tehnoloģija, ar kuru iespējams nodrošināt automātisku identifikāciju un datu ieguvu, izmantojot radiofrekvences. Tehnoloģijas galvenās iezīmes ir šādas: ar elektronisku marķējumu jebkuram objektam, dzīvniekam vai pat cilvēkam iespējams piesaistīt identifikācijas numuru un cita veida informāciju, kā arī, izmantojot bezvadu ierīci, nolasīt minēto informāciju.

2.2 Elektroniskie marķējumi sastāv no elektroniskas shēmas datu glabāšanai un antenas, kura nodrošina datu pārraidi ar radioviļņu palīdzību. RFID nolasītājs pārlūko elektroniskajā marķējumā glabāto informāciju. Nolasītājam pārraidot radioviļņus, notiek visu attiecīgajā diapazonā esošo elektronisko marķējumu savstarpēja komunikācija. Nolasītāja vadība un informācijas apkopošana un filtrēšana tiek nodrošināta ar attiecīgas programmatūras palīdzību.

2.3 Ir pieejamas dažādu veidu RFID sistēmas. Elektroniskie marķējumi var būt aktīvi vai pasīvi. Aktīvajos marķējumos ietilpst borta akumulators iekšējo shēmu barošanai un radioviļņu ģenerēšanai, lai varētu nodrošināt pārraidi arī bez RFID nolasītāja klātbūtnes. Pasīvo marķējumu barošana notiek, izmantojot nolasītāja pārraidītos radioviļņu enerģiju, un tiem nav sava strāvas avota. Elektroniskie marķējumi var būt "tikai lasošie" un "lasošie-rakstošie". "Tikai lasošie" elektronisko marķējumu ražošana ir lētāka, un tos izmanto vairumā lietojumu.

2.4 RFID sistēmas diapazons ir atkarīgs no radiofrekvences, nolasītāja jaudas un starp elektronisko marķējumu un nolasītāju esošā materiāla. Pasīvajām sistēmām tas var būt līdz dažiem metriem, bet aktīvajām sistēmām — lielāks par 100 metriem.

2.5 RFID ir zemākais posms bezvadu tehnoloģiju hierarhijā. Pēc signāla veiktajiem attālumiem augšējo pozīciju tajā ieņem satelītkomunikāciju sistēmas, piemēram, GPS. Tām seko plaša pārklājuma mobilo tālrunu tehnoloģijas, piemēram, GSM un GPRS, īsāka diapazona signāli ēku iekšienē, piemēram, Wi-Fi, personālie tīkli, piemēram *Bluetooth*, un visbeidzot — RFID. Katra no minētajām tehnoloģijām ir diskrēta un autonoma, tādējādi, piemēram, nepastāv risks, ka RFID elektroniskos marķējumus varētu nolasīt ar satelītsistēmu palīdzību. Tomēr ir iespējama datu pārraide starp dažādajām sistēmām, piemēram, ar mobilo tālrunu palīdzību.

2.6 Daži piemēri, kas liecina par RFID lietojuma iespējamajām priekšrocībām:

- fiziskām personām tas var nozīmēt drošību (piemēram, pārtikas nekaitīgums, veselības aprūpe, viltošanas novēršana), ērtības (īsākas rindas norēķinu vietās, labāka bagāžas apstrāde lidostās, automatizēti maksājumi) un uzlabota pacientu aprūpe, īpaši — hronisko slimību, piemēram, demences gadījumā;
- sagaidāms, ka transporta nozarē RFID paaugstinās efektivitāti, drošību un pakalpojumu kvalitāti pasažieru un preču pārvadājumos;
- veselības aprūpes jomā RFID spētu paaugstināt aprūpes kvalitāti un pacientu drošību, kā arī nodrošināt medikamentu atbilstības un loģistikas jomas izaugsmi. Notiek darbs, lai RFID elektronisko marķējumu ieviestu uz atsevišķiem medikamentiem;

— mazumtirdzniecībā tas varētu palīdzēt samazināt piegāžu nepietiekamību, krājumu apjomu un zādzību skaitu;

— daudzās nozarēs, kurās ir izplatīti viltojumi, ar RFID palīdzību varētu efektīvāk izņemt no apgrozības neatļautas preces un novērst to iekļūšanu piegādes ķēdē;

— RFID marķējums var arī veicināt ražojumu detaļu un izejvielu šķirošanas un pārstrādes procesu veikspējas uzlabošanu, kam būtu pozitīvi rezultāti atkritumu apsaimniekošanas un ilgtspējīgas attīstības jomā.

2.7 Daudzi RFID lietojumu aspekti atspoguļojas grāmatu aprītē. Iespiesto grāmatu sarežģītā numerācija rada ievērojamas ar loģistiku saistītas problēmas izdevējiem, izplatītājiem, bibliotēkām un mazumtirgotājiem. Papildus piegādes ķēdes loģistikai ir nepieciešams pārraudzīt grāmatu apriti pēc novietošanas plauktos, lai tās varētu viegli atrast un pārvietot. Turklāt bibliotēkām ir nepieciešams kontrolēt grāmatu izsniegšanas ciklu, savukārt pircējiem ir grūtības sekot savu grāmatu atrašanās vietai. RFID marķējums uz grāmatām var sniegt risinājumu visām šīm problēmām. Analogiski grāmatu izsniegšanai bibliotēkās ir iespējami arī citi lietojumi, kas saistīti ar priekšmetu aprites cikliem vai iznomāšanu.

2.8 Ar minēto tehnoloģiju saistītos apdraudējumus raksturo izvilks no IBM patenta pieteikuma (20020615758), kas datēts ar 2002. gada novembri. Tas attiecas uz personu identifikāciju un izsekošanu ar RFID elektroniskā marķējuma palīdzību.

"Metode un sistēma personu identifikācijai un izsekošanai, izmantojot RFID elektronisko marķējumu uz personu nestajiem priekšmetiem. Iepriekšējie dati par pirkumiem, ko persona veikusi mazumtirdzniecības vietās, tiek apkopoti tirdzniecības termināļos un glabāti tirdzniecības operāciju datu bāzē. Kad persona, kas nēsā priekšmetu, uz kura ir RFID elektroniskais marķējums, ierodas veikalā vai citā attiecīgi aprīkotā vietā, tajā esošais RFID elektroniskā marķējuma nolasītājs skenē uz attiecīgās personas esošo elektronisko marķējumu un nolasa tajā esošo informāciju. No RFID elektroniskā marķējuma iegūtā informācija tiek korelēta ar tirdzniecības operāciju datu bāzē esošajiem ierakstiem saskaņā ar attiecīgajiem korelācijas algoritmiem. Minētās korelācijas rezultāti ļauj precīzi noteikt attiecīgās personas identitāti vai noteiktas ziņas par šo personu. Šo informāciju izmanto, lai pārraudzītu personas kustību veikalā vai citās telpās."

American Express patenta pieteikuma Nr. 20050038718 saturs ir līdzīgs.

2.9 RFID ir katrā ziņā vairāk nekā tikai elektronisks svītrkods. Izvilks no patenta pieteikuma minētās galvenās atšķirības ir šādas:

- a) elektroniskais marķējums satur ne tikai priekšmeta aprakstu, bet arī diskrētu priekšmeta identifikatoru, ar kura palīdzību var identificēt pircēju;

- b) nav nepieciešams, lai elektroniskais marķējums būtu fiziska mikroshēma. Mikroshēmas var būt uzspiestas tiešā veidā uz vairuma materiālu, piemēram, apģērba;
- c) mikroshēma spēj darboties arī pēc pārdošanas, tādējādi to var pastāvīgi nolasīt no jauna;
- d) elektroniskā marķējuma nolasītāji var atrasties ne vien tirdzniecības vietās, bet arī jebkur citur un ne tikai mazumtirgotāja telpās;
- e) korelācija ar datubāzes starpniecību ievieš jaunas dimensijas datu vākšanas, privātuma un datu drošības jomā.

2.10 Tas, vai marķējumu atstāt aktivizētu pēc norēķināšanās par precīzu mazumtirdzniecības punktu, ir strīdīgs jautājums. No vienas puses, tas ir privātuma apdraudējums. No otras puses, tas var sniegt labumu pircējam. Piemēram, iespēja izmantot RFID nolasītājus mājas apstākļos var palīdzēt organizēt vīna pagrabus, ledusskapjus, apģērba skapjus un bibliotēkas. Tādēļ būtu loģiski, ka izvēle paliek privātpersonas ziņā, taču ar attiecīgās tehnoloģijas un lietojumu palīdzību šīs izvēles iespēja būtu jānodrošina.

2.11 RFID ir daudz vairāk lietojumu iespēju nekā tikai produktu identifikācija. EESK identitātes karte ir RFID ierīce. Londonas metro sistēmā RFID kartes tiek plaši lietotas maksājumu veikšanai un piekļuves nodrošināšanai. Drīzumā kredītkartēs tiks iestrādāta RFID ierīce ar mazām summām saistītu norēķinu veikšanai bez PIN koda. RFID plāksnītes tiek izmantotas ceļu lietošanas maksas iekasēšanā un autovadītāju identifikācijai. Slēpošanas pacelēju izmantošana dažos Eiropas slēpošanas kūrortos tiek pārraudzīta, izmantojot RFID plāksnītes, kas atrodas slēpošanas kostīma kabatā. Ziņotājs, kas sagatavojis šo atzinumu, ikdienā nēsā trīs RFID kartes un vienu RFID plāksnīti. Viņa suns ir identificējams ar zemādas RFID mikroshēmas palīdzību. Šādas mikroshēmas tiek plaši ieviestas visā pasaulē dzīvnieku marķēšanai, lai nodrošinātu barības ķēdes izsekojamību. Varētu būt tikai neliels solis līdz tam, lai noziedzniekus un problemātiskus slimniekus marķētu tāpat kā suņus.

2.12 EESK izmantotās identifikācijas kartes ir "maigs" RFID lietojuma veids. Identitātes problēma kļūst būtiskāka, kad RFID marķējums tiek iestrādāts darba apģērbā vai formastērpos, un tādējādi šādā apģērbā tērptas personas var tikt pastāvīgi izsekotas ar attiecīgajās telpās uzstādītu skeneru palīdzību. Tomēr ir jāatzīst, ka noteiktos gadījumos tas ir vēlams, piemēram, drošības nolūkos. Jebkurā gadījumā privātpersonas atrašanās vietas izsekošana, ja tā nenotiek, veicot atbilstošus drošības pasākumus, ir būtiska iejaukšanās privātajā dzīvē, kam ir nepieciešams nopietns pamatojums un ļoti rūpīga kontrole.

2.13 Laikraksts *The Economist* ziņo par kuriozu gadījumu, kas ļauj spriest par RFID lietojumiem nākotnē. *Baja Beach* klubā Barselonā kā ieejas biļete VIP zonā kalpo mikroshēma, kas

implantēta pastāvīgajiem klientiem rokā. Šāda mikroshēma, kas ir nedaudz lielāka par rīsa graudu un pārklāta ar stikla un silikona apvalku, tiek izmantota, lai identificētu apmeklētājus, tiem uzturoties klubā un norēķinoties par dzērieniem. To ievada medmāsa zem vietējās anestēzijas. Būtībā tā ir RFID elektroniskais marķējums.

3. Komisijas dokumenta kopsavilkums

3.1 RFID ir politikas veidotāju uzmanības lokā, jo tai ir iespēja kļūt par jaunu izaugsmes un nodarbinātības virzītājspēku, līdz ar to RFID ir ietekmīgs Lisabonas stratēģijas īstenošanas veicinātājs, ja tiktu likvidēti šķēršļi, kas kavē inovācijas procesu.

3.2 Komisija 2006. gadā rikoja RFID sabiedrisko apspriešanu, kurā, pamatojoties uz pirmo lietotāju pieredzi, noskaidroja ne tikai ar tehnoloģiju saistītās sabiedrības cerības, bet arī iedzīvotāju bažas par RFID lietojumiem, kas ļauj personas identificēt un/vai izsekot.

3.3 Turpmāka attīstība un vērienīga RFID ieviešana varētu arvien palielināt informācijas un sakaru tehnoloģiju nozīmi inovāciju veicināšanā un ekonomiskās izaugsmes sekmēšanā.

3.4 Lai jaunā tehnoloģija kļūtu lietotājiem pieņemama, ir vajadzīgs nepārprotams un iepriekš paredzams tiesiskais regulējums un politika. Tā kā RFID tehnoloģijai raksturīgas pārrobežu tehnoloģijas iezīmes, minētajiem pamatnosacījumiem jānodrošina tās vienota lietošana iekšējā tirgū.

3.5 Drošība, privātums un ētika

3.5.1 Tiek paustas lielas bažas, ka šī visaptverošā un nozīmīgā tehnoloģija varētu apdraudēt privātumu: RFID tehnoloģiju var izmantot, lai vāktu informāciju, kas ir tieši vai netieši saistīta ar identificētu vai identificējamu personu, un tādēļ uzskatāma par personas datiem; RFID marķējums var uzglabāt personas datus; RFID tehnoloģiju var izmantot, lai izsekotu cilvēku pārvietošanos vai veidotu viņu izturēšanās aprakstus. RFID var būt tehnoloģija, kas apdraud privātumu. Tiek paustas bažas par iespējamiem pamatvērtību un privātuma neaizskaramības pārkāpumiem un plašāku uzraudzību, jo īpaši darba vietā, kas kalpotu par iemeslu diskriminācijai, atstumtībai, viktimizācijai un, iespējams, darba vietas zaudēšanai.

3.5.2 RFID lietojumam neapšaubāmi jābūt sabiedriski un politiski vēlamam, ētiski pieņemamam un juridiski pieļaujamam. Virkni ekonomisku un sociālu ieguvumu RFID spēs nodrošināt tikai tad, ja ir nodrošināta datu un privātuma aizsardzība, kā arī atrisināti ar to saistītie ētiskie jautājumi, kas ir galvenais temats diskusijās par to, vai RFID tehnoloģija ir sabiedrībai pieņemama.

3.5.3 Kopienas tiesību akti par datu aizsardzību un privātumu Eiropā izstrādāti tā, lai inovācijas process to neietekmētu. Personas datu aizsardzību reglamentē vispārējā datu aizsardzības direktīva ⁽¹⁾, kuru piemēro visām tehnoloģijām, tostarp arī RFID. Vispārējo datu aizsardzības direktīvu papildina e-privātuma direktīva ⁽²⁾. Saskaņā ar minētajām direktīvām dalībvalstu iestāžu pienākums ir nodrošināt, lai RFID lietojumu ieviešana notiktu saskaņā ar tiesību aktiem par privātuma un datu aizsardzību. Tādēļ, iespējams, būtu nepieciešami detalizēti norādījumi par jauno tehnoloģiju, piemēram, RFID, ieviešanu praksē un attiecīgu rīcības kodeksu izstrāde.

3.5.4 Attiecībā uz drošību nozares pārstāvjiem, dalībvalstīm un Komisijai jāapvieno pūliņi, lai padziļinātu izpratni par sistēmiskiem jautājumiem un attiecīgiem draudiem drošībai, kas, iespējams, saistīti ar plašu RFID tehnoloģiju un sistēmu ieviešanu. Nozīmīgs aspekts, risinot iepriekš minētos jautājumus, būs tādu izstrādes kritēriju noteikšana un pieņemšana, kas novērš privātumu un drošību apdraudošos riskus, turklāt ne tikai tehnoloģiskajā, bet arī organizatoriskajā līmenī un uzņēmējdarbības procesos. Tādēļ pirms RFID sistēmu izvēles un RFID lietojumu ieviešanas rūpīgi jāizvērtē konkrēto ar drošību un privātumu saistīto risku izmaksas un guvumi no tiem.

3.5.5 Tiek paustas arī bažas par to datu bāzu atvērtību un neitralitāti, kurās saglabās informāciju par RFID pamatu veidojošiem identifikācijas numuriem, par savākto datu uzglabāšanu un apstrādi, tostarp arī par faktu, ka datus izmanto trešās personas. Šis ir būtisks aspekts, ņemot vērā, ka RFID vēsta par jaunu interneta attīstības vilni, kas, iespējams, savienos miljardiem viedierīču un sarežģītu sensoru tehnoloģiju, tādējādi veidojot globālā sakaru tīkla infrastruktūru. Šo jauno interneta attīstības posmu bieži vien dēvē par "lietisko internetu".

3.5.6 Identitātes reģistrācijas un tās norādīšanas sistēmai nākotnes "lietiskajā internetā" jābūt aizsargātai pret darbības bojājumiem vai neatļautu izmantošanu, kas varētu radīt postošas sekas. Tā nedrīkst nokļūt īpaši ieinteresētu personu rokās, kas minētās datu bāzes un identitātes izpaušanas sistēmas varētu izmantot savām vajadzībām. Drošības, ētikas un privātuma prasības jāizpilda attiecībā uz visām ieinteresētajām privātpersonām vai uzņēmumiem, kuru konfidenciālo komercinformāciju izmanto RFID iespējotos uzņēmējdarbības procesos.

3.5.7 Sistēmas izstrādes laikā jāapsver gan RFID informācijas sistēmas ieviešanā iesaistīto pušu (piemēram, uzņēmējdarbības organizācijas, sabiedrības pārvaldes iestādes, slimnīcas), gan šīs sistēmas gala lietotāju (iedzīvotāji, patērētāji, pacienti, nodarbinātie) prasības. Tā kā gala lietotāji parasti nav iesaistīti tehnoloģijas izstrādē, Komisija atbalstīs lietojumiem veltīju

izstrādi (rīcības kodekss, labākās prakses), kuras izstrādās ekspertu darba grupa, kurā pārstāvētas visas iesaistītās puses. Komisija 2007. gada beigās publicēs ieteikumu noteikt principus, kuri valsts iestādēm un citām ieinteresētajām pusēm jāievēro, izmantojot RFID.

3.5.8 Komisija apsvērs arī, kuri noteikumi iekļaujami nākamajā priekšlikumā grozīt e-privātuma direktīvu, un vienlaikus ņems vērā nākamās RFID tehnoloģijās ieinteresēto aprindu darba grupas, 29. panta datu aizsardzības darba grupas un citu attiecīgo iniciatīvu, piemēram, Eiropas grupas par dabaszinātņu ētiku un jaunām tehnoloģijām ieguldījumu. Pamatojoties uz iepriekš minēto, Komisija izvērtēs, vai vajadzīgi turpmāki tiesiski pasākumi, lai nodrošinātu datu un privātuma aizsardzību.

3.5.9 Komisija rūpīgi uzraudzīs "lietiskā interneta" attīstību; kurā svarīga nozīme būs RFID tehnoloģijai. Komisija 2008. gada beigās publicēs paziņojumu, kurā analizēts minētās attīstības raksturs un ietekme, īpašu uzmanību pievēršot privātuma, uzticamības un pārvaldības jautājumiem. Komisija novērtēs iespējamo rīcību, tostarp arī iespēju ierosināt turpmākus tiesiska rakstura pasākumus, lai nodrošinātu datu aizsardzību un privātumu, kā arī sasniegtu citus politiskos mērķus.

3.5.10 Piezīmes par drošību, privātumu un ētiku ir iekļautas atzinuma 4. sadaļā.

3.6 Citi RFID politikas jautājumi

3.6.1 Līdztekus drošības, privātuma un ētikas jomai ievēribu pelna arī citi ar RFID saistīti jautājumi, tostarp radiofrekvenču spektrs, standarti, veselības, drošības un vides aspekti.

3.6.2 Svarīga nozīme ir spektra izmantošanas nosacījumu harmonizācijai, lai sekmētu mobilitāti un zemas izmaksas. Komisija nesēn pieņēma lēmumu (2006/808/EK) par RFID frekvencēm UHF joslā. Šis sadalījums tiek uzskatīts par piemērotu nākamajiem trim līdz desmit gadiem, taču, ja būs vajadzīgs papildu spektrs, Komisija attiecīgi rīkosies, izmantojot savas pilnvaras saskaņā ar radiofrekvenču spektra lēmumu (676/2002/EK). EESK atbalsta šo nostāju.

3.6.3 Lai pakalpojumus sekmīgi ieviestu, būtiska nozīme ir jaunu ISO starptautisko standartu pieņemšanai un reģionālo standartu harmonizācijai. Eiropas attiecīgās standartizācijas iestādes — Eiropas Standartizācijas komiteja (CEN) un Eiropas Elektrosakaru standartizācijas institūts (ETSI) — ir pilnībā iesaistītas. Komisija aicina minētās iestādes sadarbībā ar nozares uzņēmumiem nodrošināt starptautisko Eiropas standartu atbilstību Eiropas prasībām, jo īpaši attiecībā uz privātumu, drošību,

⁽¹⁾ Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti.

⁽²⁾ Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē.

intelektuālā īpašuma tiesībām un licencēšanu. Tā kā rūpnieciskajiem standartiem un autortiesību patentiem mēdz būt kopīga virzība, EESK aicina Komisiju darīt visu iespējamo, lai rosinātu uzņēmumus un standartizācijas iestādes rīkoties ātri, nepieļaujot, ka RFID Eiropas lietojumi varētu kļūt pārāk atkarīgi no dārgām intelektuālā īpašuma tiesībām, kas noformētas citur.

3.6.4 No vides politikas viedokļa RFID ierīces ir pilnībā pakļautas direktīvas par elektrisko un elektronisko iekārtu atkritumiem (EELIA) un direktīvas par bīstamu vielu izmantošanas ierobežošanu (RoHS) prasībām. Runājot par veselības aspektu, jānorāda, ka pastāv problēma saistībā ar RFID ierīču radītā elektromagnētiskā lauka (EML) iespējamo ietekmi. Ar RFID lietojumiem saistīto EML jauda parasti ir zema, tādēļ paredzams, ka RFID ierīču radītā EML iedarbība uz sabiedrību un darba ņēmējiem būs krietni vien mazāka nekā pieļaujamā iedarbība, kas noteikta patlaban spēkā esošajos standartos. Ņemot vērā faktu, ka kopumā palielinās bezvadu lietojumu klāsts, Komisija rūpēsies arī par attiecīgā tiesiskā regulējuma pārskatīšanu. EESK atbalsta šo nostāju.

4. Piezīmes

4.1 Tā kā ieteikumus dalībvalstīm Komisija publicēs šī gada beigās, ir pamats uzskatīt, ka tā akceptēs datu drošības un privātuma infrastruktūru tādu, kāda tā ir pašreiz. Konkrēti tas varētu izpausties tādējādi, ka katrā dalībvalstī esošās datu aizsardzības iestādes kļūs par iestādēm, kas atbildīgas par privātumu un datu aizsardzību RFID jomā.

4.2 Savā paziņojumā Komisija, cita starpā, ir norādījusi ka tā izveidos jaunu ieinteresēto aprindu grupu un konsultēsies ar to. EESK vēlētos iesniegt šo atzinumu minētajai grupai.

4.3 Privātuma un pilsonisko brīvību jomā ar RFID saistītie apdraudējumi ir nopietni:

- RFID elektroniskos marķējumus var piestiprināt priekšmetiem un dokumentiem bez šo priekšmetu ieguvēja ziņas. Tā kā radioviļņi viegli šķērso audumus, plastmasas un citus materiālus, ir iespējams nolasīt RFID elektroniskos marķējumus, kas iesūti apģērbā vai piestiprināti makos, somās vai koferos esošiem priekšmetiem.
- Ar elektronisko izstrādājumu kodu palīdzību jebkuram priekšmetam varētu piešķirt noteiktu unikālu identifikācijas numuru (ID). Ar minētās ID numerācijas palīdzību var izveidot globālu sistēmu priekšmetu reģistrācijai, kurā jebkurš fizisks priekšmets tiek identificēts un piesaistīts tā pircējam vai īpašniekam tirdzniecības vai nodošanas vietā.
- RFID izvēršanai ir nepieciešams radīt liela apjoma datubāzes ar elektronisko marķējumu identifikācijas numuriem piesaistītajiem datiem. Minētos ierakstus var sasaistīt ar personu identifikācijas datiem, īpaši, ņemot vērā datoru atmiņas apjomu un datu apstrādes veikspējas palielināšanās tendences.

d) Elektroniskos marķējumus ir iespējams nolasīt no attāluma ar tādu nolasītāju palīdzību, kurus var neredzamā veidā izvietot gandrīz jebkurā vidē, kur uzturas cilvēki. Nolasītājus var izvietot zem grīdu seguma, iestrādāt paklājos, durvīs un plauktos, tādējādi fiziska persona var praktiski neuzzināt par to, ka tiek skenēta.

e) Ja personas identitāte ir piesaistīta RFID elektroniskā marķējuma numerācijai, ir iespējama fizisku personu izsekošana vai profilēšana bez viņu ziņas vai piekrišanas.

f) Var paredzēt tādu pasauli, kurā RFID nolasītāji veido visaptverošu globālu tīklu. Šādam tīklam nebūtu nepieciešams, lai nolasītāji atrastos pilnīgi visur. Sastrēgumu novēršanai paredzētā maksas sistēma Londonā spēj izsekot visām automašīnām, kuras iebrauc Londonas centrālajā daļā, ar samērā nedaudzu stratēģiski izvietotu kameru palīdzību. Līdzīgā veidā ir iespējams izveidot stratēģiski izvietotu RFID nolasītāju tīklu. To nedrīkst pieļaut.

4.4 Septītajā pētniecības un izstrādes pamatprogrammā Komisija jau ir sniegusi norādes par tehnoloģijas izmantošanas ētiskajiem aspektiem no datu drošības un privātuma viedokļa ("Rokasgrāmata pieteikumu iesniedzējiem" sadarbības projektu jomā, 54. lpp.)⁽³⁾. RFID ir lielisks piemērs tam, kā veidojas saikne starp tehnoloģiju un juridiskajām tiesībām uz to, kā arī sabiedrības vēlmēm attiecībā uz privātuma nodrošināšanu datu vākšanas un apmaiņas jomā. Privātuma problēmas pastāv visur, kur digitālā vai jebkādā citā formā ir apkopoti vai glabāti dati, kas ir unikāli identificējami attiecībā uz noteiktu personu vai personām. Nepienācīga izpaušanas kontrole vai šādas kontroles neesamība var būt iemesls privātuma problēmām. Datu privātuma aspekti visbiežāk ir saistīti ar tādām jomām kā veselība, krimināltiesības, finanses, ģenētika un atrašanās vietas noteikšana. Atrašanās vietas noteikšana ir pamatjautājums attiecībā uz RFID.

4.5 Komisija norādījumos⁽⁴⁾ par datu aizsardzības privātuma nodrošināšanu ir iekļāvusi astoņus obligātus labas prakses principus. Tie ir šādi:

- dati jāapstrādā godprātīgi un likumīgi;
- datu apstrādes nolūkiem jābūt ierobežotiem;
- datu apjomam jābūt adekvātam, samērojamam, un tas nedrīkst būt pārmērīgs;
- datiem jābūt precīziem;
- datus nedrīkst glabāt ilgāk nekā nepieciešams;
- datu apstrādē jāievēro datu subjekta tiesības;
- datiem jābūt drošiem;
- datus nedrīkst nodot valstīm, kurās nav nodrošināta pienācīga datu aizsardzība.

Šie norādījumi ir pilnībā attiecināmi uz privātuma un datu drošības aspektiem saistībā ar RFID izmantošanu.

⁽³⁾ http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsCallPage&call_id=11

⁽⁴⁾ Datu aizsardzības direktīva (95/46/EK), 6. pants.

4.6 EESK uzskata, ka labas prakses pamatprincipi ir šādi:

- RFID lietotājiem jāinformē sabiedrība par īstenotajiem pasākumiem un praksi, un attiecīgās datubāzes, kurās apkopota personīga informācija, nedrīkst būt slepenas;
- fiziskām personām ir tiesības zināt, vai uz mazumtirdzniecībā pārdotajām precēm ir RFID elektroniskais marķējums vai nolasītāji; visām iesaistītajām pusēm jābūt informētām par ikvienu elektroniskā marķējuma lasījumu, kas notiek mazumtirdzniecības vidē;
- RFID lietotājiem jāinformē par elektroniskā marķējuma un nolasītāju lietošanas nolūkiem; informācijas vākšana būtu jāierobežo līdz tādām apjomam, kāds ir nepieciešams norādītajam nolūkam;
- RFID lietotāji atbild par tehnoloģijas ieviešanu un izmantošanu saskaņā ar attiecīgajiem normatīvajiem aktiem un pamatnostādņēm datu aizsardzības jomā; tie ir atbildīgi arī par sistēmas un tās datubāzu drošību un integritāti.

4.7 Šo principu īstenošana praksē ir strīdīgs jautājums. Būtu ļoti labi, ja katrs uzņēmums, kas iesaistīts darījumos, kas vieno uzņēmējdarbības veicējus un gala patērētājus, t.i., mazumtirgotāji, biļešu un ieejas karšu sagatavotāji, piekļūšanas kontroles dienesti, kā arī transporta pakalpojumu sniedzēji klientiem sniegtu garantiju (klientu hartas formā), ka minētie principi tiks ievēroti. Šādas hartas koncepcijā varētu iekļaut visus 4.5. punktā minētos labas prakses principus datu aizsardzības jomā. Līdztekus tam EESK ierosina šādas pamatnostādnes:

- a) būtu jāaizliedz komersantiem uzspiest klientiem vai piespiest tos pieņemt aktīvus vai neaktīvus elektroniskos marķējumus izstrādājumos, kurus tie iegādājas. Piemēram, elektronisko marķējumu varētu piestiprināt iepakojumam vai varētu izmantot noņemamu elektronisko marķējumu, kā tas tiek darīts ar cenu norādēm;
- b) būtu jānodrošina iespēja klientiem brīvi noņemt vai atiešpot savā valdījumā esošu priekšmetu elektronisko marķējumu;
- c) RFID principā nedrīkstētu izmantot fizisku personu izsekošanai. Cilvēku izsekošana, izmantojot, piemēram, apģērbu, preces, biļetes vai citus priekšmetus, ir nepieļaujama;
- d) RFID nekādā gadījumā nedrīkstētu izmantotu veidā, kas varētu likvidēt vai mazināt anonimitāti;
- e) atbildīgajai iestādei būtu skaidri jānorāda, ka c) un d) punktā minētās iespējas ir pieļaujamas tikai izņēmuma gadījumos un atbildīgā iestāde par tām iepriekš ir oficiāli jāinformē.

Briselē, 2007. gada 11. jūlijā

4.8 Varētu apsvērt noteiktus izņēmumus attiecībā uz iepriekš minētajām pamatnostādņēm gadījumos, kad

- privātpersonas izmanto iespēju saglabāt aktivizētu elektronisko marķējumu savu personīgo ērtību labad;
- privātpersonas piekrīt, ka tiek izsekotas kritiskā vidē, piemēram, paaugstinātas drošības publiskās un privātās iestādēs un ēkās;
- privātpersonas izvēlas izmantot lietojumus, kas noteiks to atrašanās vietu un tās identificēs tādā pat veidā, kā tas jau notiek ar mobilo tālruni, ATM karšu, interneta adresu palīdzību u.tml.;

Par jebkuriem šāda veida izņēmumiem būtu jāinformē atbildīgā iestāde.

4.9 Vispārēju izņēmumu varētu attiecināt uz tādu lietojumu veidu kā cilvēku vai preču izsekošana vidēs, kur attiecīgie cilvēki vai preces atrodas īslaicīgi. Gaisa transporta jomā bagāžu varētu elektroniski marķēt reģistrācijas brīdī, lai uzlabotu bagāžas apstrādes drošību un noteiktību, savukārt pasažierus varētu elektroniski marķēt, lai uzlabotu un paātrinātu nokļūšanu līdz lidmašīnām un drošības procedūras. Vēl viens lietojumu veids varētu būt pacientu elektroniska marķēšana pēc uzņemšanas slimnīcā operāciju veikšanai. Šāda lietojumu kategorija varētu būt pieņemama ar nosacījumu, ka marķējums pēc attiecīgā pagaidu lietojuma tiek likvidēts.

4.10 RFID tehnoloģija nav nevainojama, un tās iespējas vēl nav pilnībā apzinātas. No vienas puses, tā var sniegt neiedomājamus labumus mūsu tehnoloģiski attīstītajai civilizācijai, bet, no otras puses, tā var radīt līdz šim nepieredzētu apdraudējumu privātumam un brīvībai. EESK uzskata, ka RFID lietojumi būtu jāizstrādā saskaņā ar stingru ētikas kodeksu attiecībā uz privātuma, brīvības un datu drošības ievērošanu, taču lietojumu attīstība būtu jāturpina ar nosacījumu, ka tiek nodrošinātas nepieciešamās garantijas.

4.11 Tātad, atļaujot RFID lietojumus, būtu jānodrošina, lai to izmantošana būtu pilnībā pārredzama jebkurai no iesaistītajām pusēm. Lietojumi, kas paredzēti darbībām ar precēm, kopumā ir pieņemami. Tādi lietojumi, kas ir saistīti ar cilvēku marķēšanu, kopumā nav pieņemami, izņemot vidēs, kur viņi uzturas īslaicīgi. Lietojumi, kuri norāda cilvēku saikni ar precēm, var būt pieņemami tirdzniecības nolūkos. Lietojumi, kuri identificē cilvēkus, izmantojot preces, ko viņi ir iegādājušies, principā ir nepieņemami. Turklāt daži lietojumi ir nepieļaujami brīvā sabiedrībā, un tos nedrīkstētu atļaut nekādā gadījumā. Komisijas ieteikumā dalībvalstīm vislielākā uzmanība jāvelta obligātajai prasībai nodrošināt privātumu un anonimitāti.

Eiropas Ekonomikas un sociālo lietu komitejas
priekšsēdētājs
Dimitris DIMITRIADIS