

**Az Európai Gazdasági és Szociális Bizottság véleménye – Tárgy: Rádiófrekvenciás azonosítás (RFID)**

(2007/C 256/13)

2007. február 26-i levelében az Európai Bizottság az Európai Közösséget létrehozó szerződés 262. cikke alapján felkérte az Európai Gazdasági és Szociális Bizottságot, hogy készítsen véleményt a következő tárgyban: *Rádiófrekvenciás azonosítás (RFID)*.

A bizottsági munka előkészítésével megbízott „Közlekedés, energia, infrastruktúra és információs társadalom” szekció a véleményét 2007. június 19-én elfogadta. (Előadó: Peter MORGAN.)

Az Európai Gazdasági és Szociális Bizottság a 2007. július 11-12-én tartott 437. plenáris ülésén (a július 11-i ülésnapon) 138 szavazattal 1 ellenében, 6 tartózkodás mellett elfogadta az alábbi véleményt.

**1. Következtetések és ajánlások**

1.1 A rádiófrekvenciás azonosítás (RFID) jelentős technológia, amely idővel igen fontossá válik majd. Jelenlegi és jövőbeli alkalmazásaiban benne rejlik a lehetőség, hogy a magán- és közszféra üzleti folyamatainak egész sorát pozitív irányba fejlessze, komoly előnyöket hozva az egyének és vállalkozások számára. Az internetes alkalmazások nagyarányú fejlődésének ösztönzésére is képes lehet, lehetővé téve azt, amit az ENSZ egyik szerve a „tárgyak internete” névvel illetett. Igen gondos ellenőrzés nélkül azonban az RFID a magánélet megsértésének és a polgári szabadságjogok sérülésének veszélyét is magában rejt, emellett egyének és vállalkozások biztonságát veszélyeztetheti.

1.2 A közlemény teljes címe: „Rádiófrekvenciás azonosítás (RFID) Európában: lépések egy politikai keret felé”. Az Európai Bizottság már eddig is széles körű konzultációkat folytatott; ezek szolgáltatták a közlemény alapját. Most az EGSZB-t kérték fel feltáró vélemény elkészítésére. A közleményre érkező reakciók alapján az Európai Bizottság az év végén ajánlást dolgoz majd ki a tagállamok számára. A kidolgozásukhoz hosszabb időt igénylő jogszabályok később következnek. Ennek a véleménynek így az említett ajánlás tartalmára kell koncentrálnia.

1.3 Az Európai Bizottság úgy döntött, hogy az ajánlások megfogalmazását segítő tesztcsoporthoz hoz létre az érintettek közül. Az EGSZB örömmel venné, ha lehetőséget kapna arra, hogy a jelen véleményt ismertesse az érintettek e csoportjával.

1.4 Az EGSZB támogatja az Európai Bizottság által a rádiófrekvenciák, szabványok, egészségügy, biztonság és környezetvédelem terén javasolt lépéseket. Kiemeljük, hogy sürgető szükség van a szabványokkal foglalkozó fórum munkájában való hatékony ipari részvétel kialakítására.

1.5 Mivel az Európai Bizottság ez év végén közlésezi a tagállamoknak szóló ajánlásait, feltételezhető, hogy az adatbiztonságot és a magánélet védelmét szolgáló infrastruktúrát a mai formájában fogja elfogadni. Ez mindenképp arra utal, hogy az

egy-egy tagállamokban már létező adatvédelmi szervek lesznek az RFID magánélet- és adatvédelmi kérdései terén illetékes hatóságok. E témák állnak e vélemény középpontjában.

1.6 Az RFID komoly veszélyeket jelent a magánélet védelme és a polgári szabadságjogok szempontjából:

- Az RFID-címkéket úgy lehet tárgyra és dokumentumokra helyezni, illetve ezekbe ágyazni, hogy a tárgyakat, dokumentumokat megszerző egyén nem is tud róluk. Mivel a rádióhullámok könnyen és hang nélkül áthaladnak a szöveteken, műanyagokon és egyéb anyagokon, a ruházatba varrt vagy például pénztárcában, bevásárlótáskában, bőröndben elhelyezett tárgyra rögzített RFID-címkék leolvashatók.
- Az elektronikus termékkód lehetővé tehetné, hogy a földön bármely tárgynak saját azonosítója legyen. Az egyedi azonosítószámok révén globális regisztrációs rendszer alakítható ki, amelyben minden fizikai tárgy azonosítva van, és a vásárlás vagy átruházás helyén adatkapcsolatba kerül a vásárlójával vagy tulajdonosával.
- Az RFID széles körű elterjedéséhez az egyedi címkeadatok hatalmas adatbázisait kell létrehozni. Ezek a rekordok személyazonosító adatokkal összekapcsolhatók, különösen, ahogy a számítógépek memória- és feldolgozókapacitása növekszik.
- A címkéket távolról is lehet olvasni, olyan leolvasókkal, amelyek láthatatlanul elhelyezhetők szinte minden olyan környezetben, ahol sok ember gyűlik össze. Ehhez a címkéknek nem kell szemmel is láthatóknak lenniük. Leolvasókat be lehet építeni a padlócsempékbe, bele lehet szőni a szőnyegekbe, elrejtteni az ajtónyílásokban vagy a polcokban, így az egyén gyakorlatilag nem tudhatja, mikor olvassák le.
- Ha személyazonosító adatok kapcsolódnak az RFID-címkeszámokhoz, akkor az egyéneket tudomásuk és hozzájárulásuk nélkül nyomon lehet követni, illetve profiljukat össze lehet állítani.

– Elképzelhető egy olyan világ, ahol az RFID-leolvasók átfogó globális hálózatot alkotnak. Egy ilyen hálózathoz nem lenne szükség arra, hogy mindenütt leolvasókat helyezzenek el. A közlekedési dugók ellen bevezetett londoni behajtásiadó-rendszer viszonylag kevés, stratégiai pontokon elhelyezett kamerával nyomon tudja követni a London központjába belépő autókat. Ugyanígy stratégiai pontokon elhelyezett RFID-címkeleolvasókból is hálózatot lehet létrehozni. Nem szabad hagyni, hogy ez megtörténjen.

1.7 E veszélyek az alábbiakat teszik szükségessé:

- Az RFID-t alkalmazóknak nyilvánosságra kell hozniuk, milyen politikát és gyakorlatot követnek, és nem lehetnek személyes jellegű információkat tartalmazó, titkos adatbázisok.
- Az egyéneknek joguk van tudni arról, ha a kiskereskedelmi környezetben RFID-címkek vagy -leolvasók találhatóak. A kiskereskedelmi környezetben végbemenő minden címkeleolvasásnak valamennyi fél számára világosnak kell lennie.
- Az RFID-t alkalmazóknak tájékoztatást kell adniuk arról, hogy milyen célra használják a címkeket és leolvasókat. Az információgyűjtést az aktuális célhoz szükséges mértékűre kell korlátozni.
- Az RFID alkalmazói felelősek a technológia telepítéséért és az adatbiztonsági jogszabályoknak és iránymutatásoknak megfelelő működésért. A rendszer és az adatbázis biztonsága és integritása is az ő felelősségi körükbe tartozik.

1.8 Hogy ezeket az elveket miként lehet a gyakorlatba átültetni, az egyelőre eldöntetlen. Az ideális az volna, ha az üzletek és fogyasztók közötti tranzakciókban érintett valamennyi üzletág, úgymint kiskereskedelem, jegykiadás, beléptetés-ellenőrzés és szállítási szolgáltatások, „vevői charta” formájában egyfajta garanciát nyújtának a vevőknek arra, hogy ezeket az elveket betartják. Fogalmi szempontból ez a charta tartalmazhatná a bevált gyakorlat valamennyi, a 4.5. pontban részletezett adatvédelmi elvét. Emellett az EGSZB a következő irányelveket javasolja:

- a) A kereskedők számára meg kell tiltani, hogy arra kényszerítsék a vevőket, hogy elfogadják, hogy az általuk vásárolt termékekben élő vagy alvó címkek legyenek. Az árcédulákhoz hasonlóan például a csomagoláshoz lehetne a címkeket rögzíteni vagy eltávolítható címkeket lehetne használni.
- b) A vevők számára lehetővé kell tenni, hogy eltávolíthassanak vagy inaktívvá tehessenek minden olyan címkét, amely a tulajdonukban lévő tárgyakon található.
- c) Az RFID-t elvben nem szabad egyének nyomon követésére használni. Emberek helyzetét nem szabad például a ruházaton, árukon, jegyeken vagy más tárgyakon keresztül nyomon követni.
- d) Az RFID-t soha nem lehet olyan módon alkalmazni, ami megszüntetheti vagy korlátozhatja az anonimitást.
- e) Az illetékes hatóságnak világos útmutatást kell adnia arról, hogy a (c) és (d) módszerek csak kivételes körülmények

között és a hatóság előzetes, hivatalos értesítése esetén engedhetők meg.

1.9 Fontolóra lehet venni bizonyos kivételeket a fenti irányelvek alól, arra az esetre, ha

- magánszemélyek választják azt a lehetőséget, hogy személyes kényelmük érdekében aktív címkeket őriznek meg;
- magánszemélyek hozzájárulásukat adják ahhoz, hogy kritikus környezetekben, például szigorú biztonságot igénylő köz- és magánlétesítményekben és -intézetekben nyomon követhessék őket;
- magánszemélyek döntenek úgy, hogy olyan alkalmazásokat használnak, amelyek révén azonosíthatók és tartózkodási helyük megállapítható ugyanolyan módon, ahogy már most is nyomon követhetők és azonosíthatók a mobiltelefonok, bankkártyák és internetcímek stb. révén;

Minden ehhez hasonló kivételről értesíteni kell az illetékes hatóságot.

1.10 Az RFID nem kiérlelt technológia, így még nem vagyunk teljesen tisztában azzal, hogy mire képes. Egyrészt hihetetlenül nagy előnyöket hozhat technológizálódott társadalmunkban, másrészt a legnagyobb technológiai jellegű veszélyt jelentheti a magánélet védelmére és a szabadságra. Az EGSZB úgy véli, hogy az RFID-alkalmazásokat a magánélet és a szabadság védelmére és az adatbiztonságra vonatkozó szigorú etikai kódex alapján kell fejleszteni, de az alkalmazásfejlesztésnek – a megfelelő biztosítékok mellett – folytatódnia kell.

1.11 Azt mondhatjuk tehát, hogy ahol engedélyezik az RFID-alkalmazásokat, a megvalósításnak minden érintett számára átláthatónak kell lennie. Az árukezelés javítására szolgáló alkalmazások általában elfogadhatók. Az emberek „felcímkezésével” járó alkalmazások rendszerint nem fogadhatók el, azon környezetek kivételével, ahol a személyek csupán átmenetileg tartózkodnak. Marketingcélokból elfogadhatók lehetnek az olyan alkalmazások, amelyek embereket árukkal kapcsolnak össze. Az olyan alkalmazások azonban, amelyek az embereket az általuk vásárolt cikkek alapján azonosítják, rendszerint elfogadhatatlanok. Emellett van némely alkalmazás, amely nem egyeztethető össze a szabad társadalommal, ezért soha nem engedélyezhető. Az Európai Bizottság tagállamoknak szóló ajánlásainak középpontjában a magánélet védelmének és az anonimitás megőrzésének alapvető igénye kell, hogy álljon.

## 2. Mi az az RFID, és miért kell foglalkoznunk vele?

2.1 A rádiófrekvenciás azonosítás (RFID) olyan technológia, amely rádiófrekvenciák révén automatikus azonosítást és adattárolást tesz lehetővé. E technológia legkiemelkedőbb jellemzője, hogy egy elektronikus címke segítségével lehetővé teszi egy egyedi azonosító és egyéb információk hozzárendelését egy tárgyhöz, állathoz vagy akár egy személyhez is, valamint ezen információknak a leolvasását egy vezeték nélküli berendezés segítségével.

2.2 Maga a címke egy adattároló elektronikus áramkörből és egy, az adatokat rádióhullámok révén továbbító antennából áll. Az RFID-leolvasó a címkéket lekérdezve jut hozzá a tárolt információhoz. Amikor a leolvasó rádióhullámokat bocsát ki, bizonyos hatókörön belül valamennyi címke kommunikációs kapcsolatba lép vele. A leolvasó működtetéséhez, valamint az információ összegyűjtéséhez és szűréséhez szoftverre van szükség.

2.3 Különböző típusú RFID-rendszerek állnak rendelkezésre. A címkék lehetnek aktívak vagy passzívak. Az aktív címkék beépített elemet tartalmaznak a belső áramkörök működtetésére és rádióhullámok generálására. Ezek RFID-leolvasó nélkül is adni tudnak. A passzív címkéket a leolvasó által kibocsátott rádióhullám látja el energiával, saját áramellátásuk nincs. A címkék lehetnek „csak olvashatók”, illetve „olvashatók és írhatók”. A csak olvasható címkék olcsóbban előállíthatók; a legelterjedtebb alkalmazásokban ezeket használják.

2.4 Az RFID-rendszerek hatótávolsága a rádiófrekvenciától, a leolvasó teljesítményétől, valamint a címke és a leolvasó közötti anyagoktól függ; néhány méterről (passzív rendszerek esetén) akár 100 méternél nagyobb távolságig (aktív rendszereknél) terjedhet.

2.5 Az RFID a vezeték nélküli technológiák hierarchiájának alján található. Ha aszerint állítunk fel rangsort, hogy a jelek mekkora utat tesznek meg, az első helyet a műholdas kommunikációs rendszerek – ilyen például a GPS – foglalják el. Ezt a nagy területre kiterjedő mobiltelefon-technológiák, például a GSM vagy a GPRS követik, majd a rövidebb, épületen belüli hatósugarú jelekkel működők (ilyen például a Wi-Fi) következnek, majd a személyi hálózatok, például a Bluetooth, és végül a sort az RFID zárja. Minden ilyen technológia különálló és önálló, azaz nem áll fenn például annak a veszélye, hogy műholdas rendszerek leolvassák az RFID-címkéket. Az adatok azonban – például mobiltelefonokkal – így is átvihetők az egyes rendszerek között.

2.6 Néhány példa az RFID-alkalmazások potenciális előnyeire:

- az egyén számára biztonságot jelenthet (pl. élelmiszerbiztonság, egészségügyi ellátás, hamisítások kiszűrése), kényelmesebbé teheti az életet (rövidebb sorok a pénztárnál, jobb poggyászkezelés a repülőtereken, automatikus fizetés), emellett javíthatja a betegek gondozását, különösen olyan, krónikus betegségek esetén, mint a demencia;
- a közlekedésben az RFID várhatóan javítja majd a hatékonyságot, a biztonságot, illetve a személyeket és árukat érintő szolgálatok minőségét;
- az egészségügyi ellátásban az RFID növelheti az ellátás színvonalát és a betegek biztonságát, javíthatja a gyógykezelések megfelelését és logisztikáját. Az egy-egy tablettára helyezhető RFID-címkék megvalósításán jelenleg dolgoznak;

- a kiskereskedelemben az RFID segíthet csökkenteni az áruhiányt, a készletmennyiséget és a lopások számát.
- sok olyan iparágban, ahol elterjedt a hamisítás, az RFID használata segíthet annak kimutatásában, hogy hol kerülnek a szállítási láncba a jogellenesen gyártott áruk;
- az RFID-címkézés emellett javíthatja a termékek alkatrészainak és alapanyagainak válogatását és újrahasznosítását is, ami kedvező volna a hulladékkezelés és a fenntartható fejlődés szempontjából.

2.7 Az RFID használatának számos oldala jól bemutatható a könyvek életciklusa során történő alkalmazásán. A kinyomtatott könyvek, hatalmas számuk miatt, logisztikai rémálmodt jelennek a kiadók, terjesztők, könyvtárak és kiskereskedők számára. A szállítási lánc logisztikája mellett nyomon kell követni a polcra kikerült könyveket is, egyrészt hogy meg lehessen találni, másrészt hogy fel lehessen tölteni őket. Emellett a könyvtárakban is figyelemmel kell kísérni a kölcsönzési ciklust, és a könyvvásárlóknak is nehézséget okozhat saját könyveik nyomon követése. A könyveken elhelyezett RFID-címkék megoldást nyújtanak mindezen problémákra. A könyvtári könyvek ellenőrzéséhez hasonló módon történhet bármilyen más újrahasznosított vagy bérelt tárgy nyomon követése is.

2.8 A technológiában rejlő veszélyek jellegének illusztrálására íme egy kivonat az IBM 2002. novemberi, 20020615758-as számú szabadalmi bejelentéséből, amely az RFID-címkével ellátott tárgyakat használó személyek azonosítását és nyomon követését érinti:

„RFID-címkével ellátott tárgyakat használó és azokat magukkal vivő személyek azonosítására és nyomon követésére szolgáló módszer és rendszer. Az eladás helyén található termináloknál összegyűjtik a kiskereskedelmi egységben vásárló minden személy korábbi vásárlásainak adatait, és egy tranzakciós adatbázisban tárolják. Amikor RFID-címkével ellátott tárgyakat viselő vagy magával hordó személy lép be a boltba vagy más kijelölt területre, egy ott elhelyezett RFID-címkeleolvasó letapogatja a rajta lévő RFID-címkéket, és kiolvassa a bennük lévő információt. Az összegyűjtött RFID-címkeinformációkat ismert korrelációs algoritmusok révén összevetik a tranzakciós adatbázisban található tranzakciós rekordokkal. A korrelációs eredmények alapján meghatározható a személy pontos kiléte vagy bizonyos jellemzői. Ez az információ a személy boltban vagy más helyen történő mozgásának figyelésére használható fel.”

Az American Express 20050038718-as számú szabadalmi bejelentése is hasonló jellegű.

2.9 Az RFID nyilvánvalóan jóval több egyszerű elektronikus vonalkódnál. A szabadalmi bejelentés kivonata az alábbi fő különbségeket említi:

- (a) a címke nem csupán a cikk leírását tartalmazza, hanem egy egyedi cikkazonosítót is, amelynek révén azonosítható a cikk vásárlója;

- (b) a címkének nem kell fizikailag mikrocsipnek lennie: az áramköröket a legtöbb anyagra, például ruházati cikkekre közvetlenül rá lehet nyomtatni;
- (c) a címke az eladás után is aktív maradhat, így újra meg újra leolvasható;
- (d) címkeleolvasókat nemcsak az eladás helyén lehet elhelyezni, hanem bárhol, nem is feltétlenül az eladó helyiségekben;
- (e) az adatbázisok útján történő összevetés új dimenziót jelent az adatgyűjtés, a magánélet védelme és az adatbiztonság szempontjából.

2.10 Vita tárgyát képezheti, hogy a címke a kasszánál történő fizetés után is aktív maradjon-e. Egyrészt ez fenyegetést jelent a magánélet védelme szempontjából, másrészt azonban hasznos is lehet a vásárló számára. Ha például van otthon RFID-leolvasónk, az segíthet a borospincék, hűtőszekrények, ruhásszekrények és könyvtárak tartalmának rendezésében. Érthető módon tehát a választásnak az egyén kezében kell maradnia, de a technológiának és az adott alkalmazásnak is lehetővé kell tennie a számára ezt a választást.

2.11 Az RFID-nek a kiskereskedelmi termékek azonosítása mellett még igen sok egyéb alkalmazása van. Az EGSZB-nél alkalmazott személyi belépőkártya is RFID-eszköz. A londoni metróban kiterjedten alkalmazzák az RFID-kártyákat, fizetésre és beléptetésre. Nemsokára a hitelkártyákba is RFID-eszközt építenek majd a kis összegű tranzakciók PIN-kód nélküli kezeléséhez. RFID-táblákat használnak útdíjfizetési és járművezető-azonosítási alkalmazásokban. A síliftekhöz való hozzáférés néhány európai síterepen a síruha zsebében hordott RFID-lapokkal szabályozható. E vélemény előadója nap mint nap három RFID-kártyát és egy RFID-táblát használ. Kutyáját a bőr alá ültetett RFID-csip azonosítja. Az ilyen csipeket világszerte egyre elterjedtebben alkalmazzák az állatok jelölésében, hogy későbbi útjuk az élelmiszerláncban nyomon követhető legyen. Innen már nem sok választ el minket attól, hogy a kutyákhoz hasonlóan a bűnözőket és a problémás betegeket is megjelöljük.

2.12 Az EGSZB-nél alkalmazott személyazonosító kártya egy ártalmatlan RFID-eszköz. Sokkal problematikusabb a személyazonosítás akkor, ha az RFID-címkéket a munka- vagy egyenruhákba építik be, hogy az egyenruhát viselő személy mozgása a létesítmény stratégiai pontjain elhelyezett leolvasókkal folyamatosan nyomon követhető legyen. Ugyanakkor el kell ismerni, hogy ez bizonyos esetekben kívánatos lehet, például biztonsági célokból. Mindenesetre egy adott személy tartózkodási helyének nyomon követése – amennyiben nem kísérik megfelelő biztosítékok – a magánülethez való jog jelentős megsértését jelentené, amelyhez alapos indok és igen gondos ellenőrzés szükséges.

2.13 A *The Economist* című újság a jövőbeli alkalmazások bizarr előfutáraként beszámol arról, hogy a barcelonai Beach Clubban a VIP-területhez a belépőjegy a vendégek karjába beültetett mikrocsip. Ez a rizsszemnél alig nagyobb, üvege és szili-

konba ágyazott csip szolgál az emberek azonosítására belépéskor és akkor, amikor az italokért fizetnek. Helyi érzéstelelnítés mellett nővér injektálja be őket. Lényegében ezek is RFID-címkék.

### 3. A közlemény lényegi tartalma

3.1 Az RFID azért érdekes politikai szempontból, mert a benne rejlő lehetőségek révén a növekedés és a munkahelyteremtés új motorjává válhat, és így jelentős szerepet játszhat a lisszaboni stratégia megvalósításában, amennyiben az innovációs akadályok leküzdhetőek.

3.2 2006-ban az Európai Bizottság nyilvános konzultációt szervezett az RFID-ről, amely a legelső felhasználók tapasztalataiból kiindulva rámutatott a technológiával szembeni elvárásokra, ugyanakkor az állampolgárok RFID-alkalmazások iránti aggodalmaira is, amelyek között szerepel a személyek azonosítása és/vagy nyomon követése.

3.3 A további fejlesztések és az RFID széles körű elterjedése tovább erősítheti az információs és kommunikációs technológiák (IKT) szerepét az innováció ösztönzésében és a gazdasági növekedés elősegítésében.

3.4 Ahhoz, hogy a felhasználók elfogadják ezt az új technológiát, átlátható és következetes jogi és politikai keretszabályozást kell kialakítani. Mivel az RFID-technológia lényegénél fogva határokon átnyúló, a keretszabályozásnak biztosítania kell a belső piacon belüli összhangot.

#### 3.5 Biztonság, magánélet és etika

3.5.1 Komoly aggodalmak merülnek fel arra vonatkozóan, hogy ez a mindent átható és tág lehetőségeket nyújtó technológia veszélyeztetheti a magánéletet: az RFID-technológia használható az azonosítható vagy a már azonosított személyekhez közvetlenül vagy közvetve kapcsolódó – és ezért személyes adatnak minősülő – információk gyűjtésére; az RFID-címkék személyes adatok tárolására is használhatók; az RFID-technológia személyek mozgásának nyomon követésére/visszakeresésére, vagy egy-egy személy viselkedési profiljának meghatározására is használható. Az RFID betolakodhat az emberek magánéletébe. Felhívták a figyelmet az alapvető értékek és a magánélet megsértésének lehetőségére, valamint a kiterjedtebb megfigyelés veszélyeire, különösen a munkahelyen, ahol ez diszkriminációhoz, kirekesztéshez, áldozattá váláshoz, sőt, akár a munkahely elvesztéséhez is vezethet.

3.5.2 Egyértelmű, hogy az RFID alkalmazásának társadalmilag, politikailag és etikailag is elfogadhatónak, valamint jogszerűnek kell lennie. Az RFID csak akkor válthatja valóra a benne rejlő számos gazdasági és társadalmi előnyt, ha hatékony garanciák vannak az adatvédelemre, a magánélet biztonságára és a kapcsolódó etikai szempontokra vonatkozóan, amelyek az RFID nyilvános elfogadásáról folytatott vita központjában állnak.

3.5.3 Az adatvédelemre és a magánélet védelmére vonatkozó közösségi keretszabályozást olyan stabilra tervezték, hogy az innováció ne tudja megkerülni. A személyes adatok védelméről az általános adatvédelmi irányelv<sup>(1)</sup> rendelkezik, amelyet minden technológiára alkalmazni kell, így az RFID-re is. Az általános adatvédelmi irányelvet kiegészíti az elektronikus hírközlési adatvédelmi irányelv<sup>(2)</sup>. Ezeknek az irányelveknek az értelmében a tagállamok hatóságainak biztosítaniuk kell, hogy az RFID-alkalmazások bevezetése összhangban álljon a magánélet védelmére és az adatvédelemre vonatkozó jogszabályokkal. Ezért az RFID-alkalmazások gyakorlati megvalósításához részletes útmutatás kidolgozására és ehhez kapcsolódó eljárási szabályzat összeállítására lehet szükség.

3.5.4 Ami a biztonságot illeti, az iparágak, a tagállamoknak és az Európai Bizottságnak közös erőfeszítéseket kell tennie az RFID-technológiák és -rendszerek kiterjedt alkalmazása kapcsán esetlegesen felmerülő rendszerszintű kérdések és az ezekkel összefüggő biztonsági veszélyek megértésének elmélyítésére. A fent említett kihívások megválaszolásának fontos elemeként olyan tervezési kritériumokat kell meghatározni és elfogadni, amelyek segítségével megszüntethetők a magánélettel és a biztonsággal kapcsolatos kockázatok, nemcsak a technológia, hanem a szervezetek és az üzleti folyamatok szintjén is. Ezért az RFID-rendszerek kiválasztása és az RFID-alkalmazások üzembe helyezése előtt gondosan meg kell vizsgálni a biztonsággal és a magánélet védelmével kapcsolatos kockázatok hasznait és költségeit.

3.5.5 Kétségek merültek fel az RFID-rendszer központi elemét jelentő, egyedi azonosítókat nyilvántartó adatbázisok nyilvánosságával és semlegességével, illetve az összegyűjtött adatok tárolásával és kezelésével kapcsolatban is, beleértve a harmadik fél általi felhasználást is. Márpedig ez jelentős kérdés, tekintettel arra, hogy az RFID fontos szerepet játszik az internet új fejlődési hulláma szempontjából, amelynek eredményeképpen végül intelligens készülékek és bonyolult érzékelőeszközök milliárdjai fognak összekapcsolódni egyetlen globális hálózati kommunikációs infrastruktúrává. Az internet fejlődésének ez az új szakasza a „tárgyak internete”.

3.5.6 A jövőbeli „tárgyak internetében” az identitások nyilvántartását és névadását végző rendszernek védelmet kell nyújtania az üzemzavar és a nem rendeltetésszerű használat ellen, amelyek komoly problémákat okozhatnak. El kell kerülni, hogy az adatok olyan egyedi érdekeket képviselő személyek kezébe kerüljenek, akik ezeket az adatbázisokat és rendszereket saját céljaikra használhatnák. A biztonsági, etikai és magánéletvédelmi követelményeket minden olyan érdekelt számára biztosítani kell, az egyéntől a vállalatig, akinek szenzitív kereskedelmi adatai megtalálhatóak az RFID-alapú üzleti folyamatokban.

3.5.7 Az RFID információs rendszer kialakítása során figyelembe kell venni a folyamatban tevékenyen részt vevő felek (például gazdasági szervezetek, közigazgatási szervek, kórházak) és a rendszernek alávetett végfelhasználók (polgárok, fogyasztók, betegek, alkalmazottak) igényeit is. Mivel a végfelhasználók általában nem vesznek részt a technológiai tervezés szakaszában, az

Európai Bizottság egy olyan alkalmazáspecifikus iránymutatás-készlet (magatartási kódex, helyes gyakorlati megoldások) kialakítását támogatja, amelyet az összes felet képviselő belső szakértői csoport dolgozna ki. 2007 végéig az Európai Bizottság ajánlást tesz közzé azon alapelvek meghatározására, amelyeket a hatóságoknak és egyéb érdekelt feleknek az RFID használata tekintetében alkalmazniuk célszerű.

3.5.8 Az Európai Bizottság ezenkívül azt is fontolóra veszi, hogy az elektronikus hírközlési adatvédelmi irányelv jövőbeli módosítási javaslatába megfelelő rendelkezéseket illesszen, és ezzel párhuzamosan a megalakítandó RFID-érdekcsoporttól, a 29. cikk szerinti adatvédelmi munkacsoporttól és egyéb érintett kezdeményezésektől – amilyen például a tudomány és az új technológiák etikájával foglalkozó európai csoport – származó információkat is figyelembe veszi. Ezek alapján az Európai Bizottság felméri az adatok és a magánélet védelmét biztosító további jogalkotási lépések szükségességét.

3.5.9 Az Európai Bizottság szorosan figyelemmel kíséri a „tárgyak internetéhez” vezető fejlődést, amelynek várhatóan az RFID is fontos eleme lesz. 2008 végén az Európai Bizottság közlése egy közleményt, amely az említett fejlemények természetét és hatásait elemzi, különös tekintettel a magánélet védelmére, a bizalom és az irányítás problematikájára. Értékelné fogja a szakpolitikai alternatívákat, beleértve további jogalkotási intézkedések lehetőségét az adatok és a magánélet védelmének biztosítása, illetve az egyéb közpolitikai célkitűzések tárgyalása céljából.

3.5.10 A biztonsági, a magánélet védelmével kapcsolatos és az etikai kérdésekre vonatkozó megjegyzések a vélemény negyedik pontjában olvashatók.

### 3.6 Az RFID-vel kapcsolatos politikák egyéb kérdései

3.6.1 A biztonság, a magánélet védelme és az etika teljes szféráján kívül az RFID a rádióspektrumra, a szabványokra, az egészségre, a biztonságra és a környezetvédelemre vonatkozó politikákkal kapcsolatos kérdéseket is felvet.

3.6.2 A spektrumhasználat feltételeinek a harmonizációja fontos a könnyű mobilitás és az alacsony költségek lehetővé tételéhez. Az Európai Bizottság nemrég határozatot (2006/808/EK) fogadott el az UHF frekvenciasávban található RFID-frekvenciákról. Ezt a kiosztást egy háromtól tíz évig terjedő időszakra elegendőnek tartják, de amennyiben szükség lenne további frekvenciákra, az Európai Bizottság cselekedni fog, él a rádióspektrum-határozat (676/2002/EK) értelmében rá ruházott hatáskörrel. Az EGSZB elfogadja ezt az álláspontot.

3.6.3 Az új nemzetközi ISO szabványok egyszerűsített elfogadása és a regionális szabványok harmonizálása alapvető fontosságú a szolgáltatások zökkenőmentes használatba vételéhez. Az érintett európai szabványügyi testületek – a CEN és az ETSI – teljes mértékben részt vesznek a folyamatban. Az Európai Bizottság felkéri e testületeket – az iparral együtt –, hogy biztosítsák azt, hogy a létrejövő szabványok megfeleljenek az európai

(1) 95/46/EK irányelv a személyes adatok feldolgozása vonatkozásában az egyének védelméről.

(2) 2002/58/EK irányelv az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről.

követelményeknek (különösen a magánélet védelmére, a biztonságra, a szellemi tulajdonjogra, valamint az engedélyezett kérdésekre vonatkozóan). Mivel az ipari szabványok és az egyéni szabadalmak gyakran egymással párhuzamosan fejlődnek, az EGSZB sürgeti az Európai Bizottságot, hogy tegyen meg mindent annak érdekében, hogy az ipar és a szabványügyi testületek gyors fellépéssel vegyék elejét annak, hogy az RFID európai alkalmazásai túlságosan függővé váljanak költséges, máshol birtokolt szellemi tulajdonoktól.

3.6.4 Ami a környezetet illeti, az RFID-eszközökre teljes mértékben vonatkozik a WEEE és a RoHS irányelv. Az egészséggel kapcsolatban az RFID-eszközök elektromágneses mezőinek (EMF) kérdése merülhet fel. Az RFID-vel kapcsolatos EMF-ek általában gyengék, így a lakosság és a munkavállalók várhatóan jóval kisebb mértékben vannak kitéve e-sugárzásnak, mint amit a hatályos szabványok megengednek. Tekintettel azonban a vezeték nélküli alkalmazások számának általános növekedésére, az Európai Bizottság felül fogja vizsgálni a jogi keretszabályozást. Az EGSZB elfogadja ezt az álláspontot.

#### 4. Megjegyzések

4.1 Mivel az Európai Bizottság ez év végén közzéteszi a tagállamoknak szóló ajánlásait, feltételezhető, hogy az adatbiztonságot és a magánélet védelmét szolgáló infrastruktúrát a mai formájában fogja elfogadni. Ez mindenekelőtt arra is utal, hogy az egyes tagállamokban már létező adatvédelmi szervek lesznek az RFID magánélet- és adatvédelmi kérdései terén illetékes hatóságok.

4.2 Közleményében az Európai Bizottság többek között kijelentette, hogy új csoportot hoz létre az érdekeltekből, és konzultál vele. Az EGSZB szeretné ismertetni ezt a véleményt a csoporttal.

4.3 Az RFID komoly veszélyeket jelent a magánélet védelmére és a polgári szabadságjogok szempontjából.

(a) Az RFID-címkéket úgy lehet tárgyra és dokumentumokra helyezni, illetve ezekbe ágyazni, hogy a tárgyakat, dokumentumokat megszerző egyén nem is tud róluk. Mivel a rádióhullámok könnyen és hang nélkül áthaladnak a szöveteken, műanyagokon és egyéb anyagokon, a ruházatba varrt vagy például pénztárcában, bevásárlótáskában, bőröndben elhelyezett tárgyra rögzített RFID-címkék leolvashatók.

(b) Az elektronikus termékkód lehetővé tehetné, hogy a Földön bármely tárgynak saját azonosítója legyen. Az egyedi azonosítószámok révén globális regisztrációs rendszer alakítható ki, amelyben minden fizikai tárgy azonosítva van, és a vásárlás vagy átruházás helyén adatkapcsolatba kerül a vásárlójával vagy tulajdonosával.

(c) Az RFID széles körű elterjedéséhez az egyedi címkeadatok hatalmas adatbázisait kell létrehozni. Ezek a rekordok személyazonosító adatokkal összekapcsolhatók, különösen, ahogy a számítógépek memória- és feldolgozókapacitása növekszik.

(d) A címkéket távolról is le lehet olvasni, olyan leolvasókkal, amelyek láthatatlanul elhelyezhetők szinte minden olyan

környezetben, ahol sok ember gyűlik össze. Ehhez a címkéknek nem kell szemmel is láthatóknak lenniük. Leolvasókat be lehet építeni a padlócsempékbe, bele lehet szőni a szőnyegekbe, elrejteti az ajtónyílásokban vagy a polcokban, így az egyén gyakorlatilag nem tudhatja, mikor olvassák le.

(e) Ha személyazonosító adatok kapcsolódnak az RFID-címkeszámokhoz, akkor az egyéneket tudomásuk és hozzájárulásuk nélkül nyomon lehet követni, illetve profiljukat össze lehet állítani.

(f) Elképzelhető egy olyan világ, ahol az RFID-leolvasók átfogó globális hálózatot alkotnak. Egy ilyen hálózathoz nem lenne szükség arra, hogy mindenütt leolvasókat helyezzenek el. A közlekedési dugók ellen bevezetett londoni behajtásiadórendszer viszonylag kevés, stratégiai pontokon elhelyezett kamerával nyomon tudja követni a London központjába belépő autókat. Ugyanígy stratégiai pontokon elhelyezett RFID-címkeleolvasókból is hálózatot lehet létrehozni. Nem szabad hagyni, hogy ez megtörténjen.

4.4 A hetedik kutatási és fejlesztési keretprogramban az Európai Bizottság már útmutatót adott az adatbiztonságot és a magánélet védelmét érintő technológiák etikus alkalmazásához (Pályázati útmutató közös projektekhez, 54. o.)<sup>(3)</sup> Az RFID nagyon jó példa arra, hogyan alakul a kapcsolat a technológia és a magánélet védelméhez fűződő jog, illetve a közvélemény erre vonatkozó elvárásai között az adatgyűjtés és -megosztás területén. A magánélet védelmének problémái minden olyan esetben felmerülnek, amikor egy vagy több személyre vonatkozó egyedi, azonosítható adatokat gyűjtenek és tárolnak digitális vagy egyéb formában. A magánélet védelmére vonatkozó problémák fő oka az adatok nyilvánosságra hozatalának nem megfelelő ellenőrzése vagy ennek hiánya lehet. Adatvédelmi problémák leggyakrabban az egészségügy, a büntetőjog, a pénzügy, a genetika és a helymeghatározás területén kialakított adatforrásokkal kapcsolatban adódnak. Az RFID esetében a helymeghatározás a lényeg.

4.5 Az adatok és a magánélet védelmére vonatkozó útmutatásában<sup>(4)</sup> az Európai Bizottság a bevált gyakorlatok nyolc alkalmazandó elvét ismertetette. Ennek értelmében arra van szükség, hogy:

- az adatokat méltányosan és törvényesen dolgozzák fel,
- korlátozott célokra dolgozzák fel,
- az adatok adekvátak, a tárgyhoz tartozók, a szükséges mértéket nem meghaladják
- és pontosak legyenek,
- tárolásuk csak a szükséges ideig történjék,
- feldolgozásuk során tartsák tiszteltben az adatalany jogait,
- biztonságosak legyenek,
- és ne adják át őket olyan országoknak, ahol nem áll rendelkezésre megfelelő védelem.

Ezek az iránymutatások teljes mértékben érvényesek az RFID-alkalmazásokkal kapcsolatos magánélet-védelmi és adatbiztonsági kérdések esetében.

<sup>(3)</sup> [http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsCallPage&call\\_id=11](http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsCallPage&call_id=11).

<sup>(4)</sup> A személyes adatok védelméről szóló 95/46/EK irányelv 6. cikke.

4.6 Az EGSZB véleménye szerint a bevált gyakorlatok alapelvei a következők:

- Az RFID-t alkalmazóknak nyilvánosságra kell hozniuk, milyen politikát és gyakorlatot követnek, és nem lehetnek személyes jellegű információkat tartalmazó, titkos adatbázisok.
- Az egyéneknek joguk van tudni arról, ha a kiskereskedelmi környezetben RFID-címkék vagy -leolvasók találhatóak. A kiskereskedelmi környezetben végbemenő minden címkeleolvasásnak valamennyi fél számára világosnak kell lennie.
- Az RFID-t alkalmazóknak tájékoztatást kell adniuk arról, hogy milyen célra használják a címkéket és leolvasókat. Az információgyűjtést az aktuális célhoz szükséges mértékűre kell korlátozni.
- Az RFID alkalmazói felelősek a technológia telepítéséért és az adatbiztonsági jogszabályoknak és iránymutatásoknak megfelelő működéssért. A rendszer és az adatbázis biztonsága és integritása is az ő felelősségi körükbe tartozik.

4.7 Hogy ezeket az elveket miként lehet a gyakorlatba átültetni, az egyelőre eldöntetlen. Az ideális az volna, ha az üzletek és fogyasztók közötti tranzakciókban érintett valamennyi üzletág, úgymint kiskereskedelem, jegykiadás, beléptetés-ellenőrzés és szállítási szolgáltatások, „vevői charta” formájában egyfajta garanciát nyújtanának a vevőknek arra, hogy ezeket az elveket betartják. Fogalmi szempontból ez a charta tartalmazhatná a bevált gyakorlat valamennyi, a 4.5. pontban részletezett adatvédelmi elvét. Emellett az EGSZB a következő irányelveket javasolja:

- a) A kereskedők számára meg kell tiltani, hogy arra kényszerítsék a vevőket, hogy elfogadják, hogy az általuk vásárolt termékekben élő vagy alvó címkék legyenek. Az árcédulákhoz hasonlóan például a csomagoláshoz lehetne a címkéket rögzíteni, vagy eltávolítható címkéket lehetne használni.
- b) A vevők számára lehetővé kell tenni, hogy eltávolíthassanak vagy inaktívvá tehessenek minden olyan címkét, amely a tulajdonukban lévő tárgyakon található.
- c) Az RFID-t elvben nem szabad egyének nyomon követésére használni. Emberek helyzetét nem szabad például a ruházatokon, árukon, jegyeken vagy más tárgyakon keresztül nyomon követni.
- d) Az RFID-t soha nem szabad olyan módon alkalmazni, ami megszüntetheti vagy korlátozhatja az anonimitást.
- e) Az illetékes hatóságnak világos útmutatást kell adnia arról, hogy a (c) és (d) módszerek csak kivételes körülmények között és a hatóság előzetes, hivatalos értesítése esetén engedhetők meg.

4.8 Fontolóra lehet venni bizonyos kivételeket a fenti irányelvek alól, arra az esetre, ha

- magánszemélyek választják azt a lehetőséget, hogy személyes kényelmük érdekében aktív címkéket őrizzenek meg;

- magánszemélyek hozzájárulásukat adják ahhoz, hogy kritikus környezetekben, például szigorú biztonságot igénylő köz- és magánlétesítményekben és -intézetekben nyomon követhessék őket;
- magánszemélyek döntenek úgy, hogy olyan alkalmazásokat használjanak, amelyek révén azonosíthatók, és tartózkodási helyük megállapítható ugyanolyan módon, ahogy már most is nyomon követhető és azonosítható a mobiltelefonok, bankkártyák és internetcímekek stb. révén;

Minden ehhez hasonló kivételről értesíteni kell az illetékes hatóságot.

4.9 Az emberek vagy áruk nyomon követésével járó alkalmazásokra olyan környezetek esetében lehetne általános mentességet adni, ahol a személyek vagy áruk csupán átmenetileg tartózkodnak. A légi közlekedésben a csomagokat az utasfelvétel (check-in) során a csomagkezelés biztonságának javítása érdekében lehetne címkével ellátni, az utasokra pedig azért lehetne címkét elhelyezni, hogy ezzel is hozzá lehessen járulni a járatok pontos indulásához, és gyorsabbak legyenek a biztonsági eljárások. Egy másik szóba jöhető alkalmazás a műtét céljából kórházi felvételre felvett betegek nyomon követése lehetne. Ez a fajta alkalmazás akkor fogadható el, ha az említett átmeneti műveletek végén a címkéket minden kétséget kizáróan megsemmisítik.

4.10 Az RFID nem kérielt technológia, így még nem vagyunk teljesen tisztában azzal, hogy mire képes. Egyrészt hihetetlenül nagy előnyöket hozhat technológizálódott társadalomban, másrészt soha nem látott mértékű technológiai jellegű veszélyt jelenthet a magánélet védelmére és a szabadságra. Az EGSZB úgy véli, hogy az RFID-alkalmazásokat a magánélet és a szabadság védelmére és az adatbiztonságra vonatkozó szigorú etikai kódex alapján kell fejleszteni, de az alkalmazásfejlesztésnek – a megfelelő biztosítékok mellett – folytatódnia kell.

4.11 Azt mondhatjuk tehát, hogy ahol engedélyezik az RFID-alkalmazásokat, a megvalósításnak minden érintett számára átláthatónak kell lennie. Az árukezelés javítására szolgáló alkalmazások általában elfogadhatók. Az emberek „felcímkezésével” járó alkalmazások rendszerint nem fogadhatók el, azon környezetek kivételével, ahol a személyek csupán átmenetileg tartózkodnak. Marketingcélokból elfogadhatók lehetnek az olyan alkalmazások, amelyek embereket árukkal kapcsolnak össze. Az olyan alkalmazások azonban, amelyek az embereket az általuk vásárolt cikkek alapján azonosítják, rendszerint elfogadhatatlanok. Emellett van némely alkalmazás, amely nem egyeztethető össze a szabad társadalommal, ezért soha nem engedélyezhető. Az Európai Bizottság tagállamoknak szóló ajánlásainak középpontjában a magánélet védelmének és az anonimitás megőrzésének alapvető igénye kell, hogy álljon.

Kelt Brüsszelben, 2007. július 11-én.

az Európai Gazdasági és Szociális Bizottság  
elnöke

Dimitris DIMITRIADIS