I

(Állásfoglalások, ajánlások és vélemények)

VÉLEMÉNYEK

EURÓPAI ADATVÉDELMI BIZTOS

Az európai adatvédelmi biztos véleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának címzett, Rádiófrekvenciás azonosítás (RFID) Európában: lépések egy politikai keret felé COM(2007) 96 című bizottsági közleményéről

(2008/C 101/01)

AZ EURÓPAI ADATVÉDELMI BIZTOS,

tekintettel az Európai Közösséget létrehozó szerződésre, és különösen annak 286. cikkére,

tekintettel az Európai Unió Alapjogi Chartájára, és különösen annak 8. cikkére,

tekintettel a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelvre,

tekintettel az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelvre,

tekintettel a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 45/2001/EK európai parlamenti és tanácsi rendeletre, és különösen annak 41. cikkére,

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

I. **BEVEZETÉS**

1. 2007. március 15-én a Bizottság elfogadta a Rádiófrekvenciás azonosítás (RFID) Európában: lépések egy politikai keret felé ([1]) című közleményt (a továbbiakban: közlemény). A 45/2001/EK rendelet 41. cikke alapján az európai adatvédelmi biztos feladata, hogy a személyes adatok feldolgozásával kapcsolatos minden ügyben tanácsokkal lássa el a közösségi intézményeket és szerveket. E cikkel összhangban az európai adatvédelmi biztos benyújtja véleményét.

2. Ez a vélemény az európai adatvédelmi biztos által a közleményre, valamint az RFID területén a közlemény elfogadása óta hozott intézkedésekre adott válasznak tekintendő. Ezek az egyéb, a vélemény kialakításánál figyelembe vett jelentős intézkedések az alábbiak:

– A közlemény közvetlen következményeként a rádiófrekvenciás azonosítással foglalkozó szakértői csoport létrehozásáról szóló, 2007. június 28-i bizottsági határozat ([2]). Ez a csoport úgy is ismeretes, mint az RFID-ben érdekeltek csoportja. A határozat 4. cikke (4) bekezdésének b) pontjával összhangban az európai adatvédelmi biztos megfigyelőként vesz részt a csoport működésében.

– A biztonságos európai információs társadalomra irányuló stratégiáról szóló, 2007. március 22-i tanácsi állásfoglalás ([3]).

– Az Európai Parlament által kezdeményezett ([4]) „Rádiófrekvenciás azonosítás és személyazonosság-kezelés” nevű projekt.

([1]) COM(2007) 96 végleges.
([2]) A 467/2007/EK határozat (HL L 176., 2007.7.6., 25. o.).
([3]) HL C 68., 2007.3.24., 1. o.
([4]) A „Rádiófrekvenciás azonosítás és személyazonosság-kezelés – esettanulmányok az intelligens környezet kialakításának élvonalából” című, a Parlament tudományos és technológiai alternatívák értékelésével foglalkozó egysége (STOA) által megrendelt és az Európai Technológiaértékelő Csoport (ETAG) által megvalósított projekt, http://www.europarl.europa.eu/stoa/default_en.htm

– A 29. cikk szerinti munkacsoport 2007. júniusában elfogadott, a személyes adatok fogalmáról szóló 4/2007. sz. véleménye ([1]).

– Az adatvédelmi irányelv jobb végrehajtását célzó munkaprogram nyomon követéséről szóló, az Európai Parlamenthez és a Tanácshoz címzett bizottsági közlemény ([2]) és az európai adatvédelmi biztos 2007. július 25-i véleménye a közleményről ([3]).

– A (többek között) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelvet módosító irányelv-javaslat elfogadása a Bizottság által ([4]).

3. Az európai adatvédelmi biztos üdvözli a Bizottság rádiófrekvenciás azonosításról szóló közleményét, mivel az foglalkozik az RFID elterjedésével kapcsolatban felmerülő főbb témákkal, továbbá olyan lényeges kérdésekre is kitér, mint a magánélet védelme és az adatvédelem. Ez a közlemény következetes és szigorú előkészítő munkálatokon alapul. Öt tematikus munkaértekezlet és egy, a Bizottság által kezdeményezett nyilvános online konzultáció ([5]) előzte meg ezt a közleményt.

4. Az európai adatvédelmi biztos egyetért azzal a nézettel, hogy az RFID-rendszerek döntő szerepet játszhatnak a rendszerint a „tárgyak internete"-ként emlegetett információs társadalom fejlődésében, továbbá teljes mértékben osztja a közlemény 3.2. bekezdésében szereplő aggodalmakat, miszerint az RFID-rendszerek veszélyeztethetik az egyéneknek a magánélet védelméhez és az adatvédelemhez való jogát. 2005. évi jelentésében az európai adatvédelmi biztos kifejtette, hogy az RFID, a biometrikus azonosítók, a környezetintelligens környezetek és a személyazonosság-kezelő rendszerek olyan technológiai fejlesztések, melyek várhatóan nagy hatással lesznek az adatvédelemre.

5. Az európai adatvédelmi biztos szerint az RFID-rendszerek jövőbeni meghonosodása és széles körű elterjedése nem csak könnyű kezelhetőségüknek vagy az általuk nyújtott szolgáltatásoknak köszönhető majd, hanem a testre szabott és következetes adatvédelmi biztosítékok jótékony hatásainak is.

6. Összegzés: az európai adatvédelmi biztos az RFID-et teljesen új technológiai fejlesztésnek tekinti, melyet a Bizottság közleménye jogosan nevezett az információs társadalom új fejlődési szakasza kezdetének.

7. Ez a fejlesztés fontos kérdéseket vet fel különböző területeken, melyek közül az egyik az adatvédelem és a magánélet védelme. Az európai adatvédelmi biztos véleménye csak erre a területre vonatkozik.

II. A VÉLEMÉNY KÖZPONTI ELEME

8. A vélemény központi elemei a fenti fejlesztések által az adatvédelemre és a magánélet védelmére gyakorolt lehetséges következmények. Ezek a következmények jelenleg bizonytalanok, mivel az RFID-rendszerek fejlesztése és meghonosodása jelenleg is folyamatban van, és egyáltalán nem világos, hogy ezek a fejlemények hova vezetnek.

9. E tekintetben az európai adatvédelmi biztos a következő megfontolásokat alkalmazza:

– Először is fel kell tárni az RFID-rendszerek elterjedése által az adatvédelemre és a magánélet védelmére gyakorolt tényleges következményeket.

– Másodszor az adatvédelemre és a magánélet védelmére vonatkozó meglévő jogi keretekkel összefüggésben pontosítani kell ezeket a következményeket.

– Harmadszor az európai adatvédelmi biztos felteszi a kérdést, hogy ezek a következmények igényelnek-e külön szabályokat, melyek lehetővé teszik az RFID-technológiák használata által felvetett adatvédelmi kérdések megválaszolását. Ezt a témát az európai adatvédelmi biztos már felvetette az adatvédelmi irányelvről szóló bizottsági közleményre adott véleményében, e véleményében pedig bővebben kifejti.

10. A fenti megfontolásokat alkalmazva az európai adatvédelmi biztos annak előmozdítására törekszik, hogy az RFID-rendszerek fejlődése és meghonosodása során az indokolt adatvédelmi és a magánélet védelmére vonatkozó aggályokat figyelembe vegyék.

III. A KÖVETKEZMÉNYEK TISZTÁZÁSA

RFID-rendszerek és -címkék

11. Annak ellenére, hogy – mint korábban említésre került – a fejlesztések jelenleg is folynak és a végkifejlet bizonytalan, a fejlemények adatvédelemre gyakorolt következményeinek főbb jellemzői igen jól meghatározhatók.

([1]) A munkacsoport honlapján közzétett WP 136 számú dokumentum.
([2]) Az adatvédelmi irányelv jobb végrehajtását célzó munkaprogram nyomon követéséről szóló, az Európai Parlamenthez és a Tanácshoz címzett, 2007. március 7-i bizottsági közlemény, COM(2007) 87 végleges.
([3]) HL C 255., 2007.10.27., 1. o. A továbbiakban: „Az adatvédelmi irányelvről szóló közleményre adott vélemény".
([4]) Az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelvet, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelvet, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelvet és a fogyasztóvédelmi együttműködésről szóló 2006/2004/EK rendeletet módosító 2007. november 13-i európai parlamenti és tanácsi irányelvjavaslat, COM(2007) 698 végleges. A 2002/58/EK irányelv a továbbiakban: elektronikus hírközlési adatvédelmi irányelv.
([5]) http://www.rfidconsultation.eu/

12. Az RFID-technológia adatvédelmi és a magánélet védelmére vonatkozó lehetséges aspektusainak felmérése során rendkívül fontos, hogy ne az RFID-címkéket önmagukban vizsgáljuk, hanem a teljes RFID-infrastruktúrát: a címkét, a leolvasót, a hálózatot, a referencia-adatbázist és azt az adatbázist, amely a címke leolvasása során keletkezett adatokat tárolja. Mint arra a közlemény bevezetője is röviden utal, az RFID nem csak „eletronikus címkék" rendszerét jelenti, ezért az adatvédelmi kérdések nem csak a címkékre korlátozódnak, hanem a teljes RFID-infrastruktúra valamennyi részére kiterjednek. Továbbá a fenti elemek mindegyike hozzájárulhat az európai adatvédelmi jogi keret végrehajtásához, amikor az szükséges. A fenti folyamatokat erősítik a fejlődő információs társadalom főbb tendenciái, mint például a szinte korlátlan sávszélesség, a helyfüggetlen hálózati csatlakozás és a korlátlan tárhely.

Az RFID-rendszerek és -címkék hatása

13. Az előző bekezdésben kifejtett tágabb megközelítés szükségessége ellenére több okból is indokolt, hogy elsőként az RFID-nek a fogyasztási cikkek kiskereskedelmi címkézésében történő használatát vizsgáljuk meg. Nyilvánvaló ok a várakozásoknak megfelelően növekvő használat, mely láthatólag egyre szélesebb körű elterjedést eredményez. Más kevésbé elterjedt vagy korlátozott használatú RFID-alkalmazásokkal szemben az árucikkek címkézése tömegesen elterjedt piaci alkalmazássá válhat. Már most is számos fogyasztási cikk rendelkezik RFID-címkével. Ehhez kapcsolódik az a tény, hogy ez a fajta használat számos egyént érint majd, akiknek személyes adatait minden alkalommal feldolgozhatják, amikor RFID-címkével ellátott terméket vásárolnak.

14. Különös figyelmet kell fordítani az RFID-címkézésnek az árucikkek tulajdonosait érintő következményeire. Az RFID-rendszerek kitágítják az árucikk és tulajdonosa közti kapcsolatot. Ebben a kibővült kapcsolatban a tulajdonost bevizsgálhatják, és a jövőbeli tranzakciókra nézve a „kis költségvetésű" vagy „vonzó célpont" kategóriákba sorolhatják; a túlzottan merev osztályozási rendszer ([1]) bizonyos viselkedések automatikus „büntetését" vonhatja maga után (újrahasznosítási kötelezettség, hulladék, stb.). Az egyéneket nem szabad kedvezőtlen, automatizált döntések folyamatának kitenni. Az RFID-lehetőségek tovább fokozzák a veszélyt, hogy az információs társadalom közelebb kerül egy olyan helyzethez, amelyben automatizált döntések születnek, és ahol visszaélnek a technológiával az emberi viselkedés szabályozása érdekében.

15. Az RFID-címkén tárolt vagy az általa létrehozott adatok az adatvédelmi irányelv 2. cikke szerinti személyes adatnak minősülhetnek. Például az utazáshoz használt intelligens kártyák az azonosításhoz szükséges információn kívül a tulajdonos legutóbbi útjairól is tartalmazhatnak információkat. Ha egy gátlástalan egyén fel akar kutatni valakit, elegendő, hogy a stratégiailag fontos helyeken leolvasókat helyezzen el, melyek információkat szolgáltatnak a kártyatulajdonos mozgásairól, megsértve ezzel annak a magánélet és a személyes információk tiszteletben tartásához való jogát.

16. A magánélet védelmét hasonlóan fenyegeti az is, ha az RFID-címkén tárolt információ nem tartalmazza az egyének nevét. Az RFID-címkék a fogyasztási cikkekhez kapcsolódó egyedi azonosítókat tartalmaznak: ha minden címkének egyedi azonosítója van, akkor ez az azonosítás használható megfigyelési célokra. Ha például valaki egy azonosító számot tartalmazó RFID-címkével ellátott órát visel, akkor ez a szám az óra viselőjének egyedi azonosítójaként is használható, abban az esetben is, ha a személy kiléte nem ismert. Az információ felhasználásának módjától függően – és magára az órára vagy az egyénre vonatkoztatva – az irányelv vagy alkalmazható, vagy nem. Alkalmazható akkor, ha például olyan információ keletkezik az egyének tartózkodási helyéről, amelyet valószínűsíthetően viselkedésük megfigyelésére használnak fel, vagy például differenciált ár alkalmazása, hozzáférés megtagadása vagy a nyilvánosságnak való nem kívánt kitétel esetén.

17. Ebben az összefüggésben biztosítani kell, hogy az RFID-alkalmazások fel legyenek szerelve az információk nem kívánt feltárásának kockázatát minimalizáló technológiai megoldásokkal. Ezek a megoldások azt is jelenthetik, hogy az RFID-infrastruktúrát, különösen az RFID-címkéket úgy kell megtervezni, hogy az effajta végkifejlet megelőzhető legyen. Az RFID-címkéket például egy deaktiváló hatású, „kioltó paranccsal" lehetne ellátni. Ezt a lehetőséget alább, a vélemény IV. fejezetében bővebben kifejtjük.

18. Azáltal, hogy az eladási ponton túl is lehetővé válik a termékek nyomon követése, az RFID-rendszerek új kérdéseket vetnek fel a magánélet védelméről szóló vitában. Két elemet kell figyelembe venni hatásuk vizsgálata során: azt, hogy mennyire személyesnek tekinthető az árucikk, és az árucikk mobilitását ([2]).

19. A szükséges kockázatelemzésnek a tárgy élettartama is része lehet, és hozzájárulhat a magánélet védelmét veszélyeztető potenciális fenyegetés kvantitatív felméréséhez. Figyelembe véve, hogy a címke deaktiválására nem feltétlenül kerül sor, egy hosszú élettartamú késztermék több adatot gyűjthet össze a termék tulajdonosáról, és pontosabb profil kialakítását teszi lehetővé. Másrészt egy rövid élettartamú árucikk – például a fémdobozos üdítőital – a gyártástól az újrahasznosításig kisebb kockázatot jelent, ezért enyhébb intézkedéseket igényel, mint egy sokkal hosszabb élettartamú termék.

([1]) Dr. Sarah Spiekermann, az internetgazdasággal foglalkozó berlini kutatóközpont igazgatója, a Transzatlanti Fogyasztói Párbeszéd által szervezett, az RFID-ről és a helyfüggetlen számítástechnikáról szóló 2007. március 13-i munkaértekezlet.

([2]) Dara J. Glasser, Kenneth W. Goodman, Norman G. Einspruch, Chips, tags and scanners: Ethical challenges for radio frequency identification, Ethics and Information Technology, Volume 9, No 2/2007.

A magánélet és az adatok védelme az RFID-rendszerek kiépítése során

20. Az RFID-rendszerek által a magánélet védelmére és az adatvédelemre gyakorolt következmények jobb megértése érdekében öt alapvető magánélet-védelmi és biztonsági kérdést kell megkülönböztetni.

21. Az első kérdés az adatalany azonosítása. Az RFID-címke célja több mint hatvan évvel ezelőtt a közeledő „barát vagy ellenség azonosítása" volt. Ma az RFID-rendszerek nem csak egy tárgy általános elemeit képesek azonosítani, hanem végső soron lehetővé teszik egy egyén azonosítását, ezért fontos, hogy ezt az adatvédelmi szempontokkal összhangban tegyék.

22. A második kérdés az adatkezelő(k) azonosítása. Az RFID-rendszerek esetében az adatvédelmi irányelv 2. cikke (d) bekezdésében meghatározott adatkezelő azonosítása bonyolultabb lehet, ezért alaposabb vizsgálatot igényel. Az adatkezelő azonosítása ugyanakkor továbbra is kritikus lépés minden érintett szereplő felelősségének meghatározásában, akiknek biztosítaniuk kell az adatvédelemre vonatkozó jogi keretek betartását. A címke élettartama alatt az adatokat feldolgozó adatkezelő személye a címkével ellátott tárggyal kapcsolatban felmerülő kiegészítő szolgáltatások szerint többször is változhat.

23. A harmadik kérdés a személyes és nyilvános szféra közötti hagyományos különbségtétel. Bár a személyes és nyilvános terek közti különbségtétel a múltban nem mindig volt teljesen egyértelmű, a többség ismeri a köztük lévő határt (és a szürke területeket), és tájékozódáson alapuló vagy intuitív döntéseket hoz arról, hogy miként cselekedjen ennek megfelelően. Hall ([1]) szerint a személyes tér rendszerint a másoktól való fizikai távolságban nyilvánul meg. A magánélet védelmére hozott intézkedések a határok szabályozását szolgáló dinamikus folyamatnak is tekinthetők ([2]). Ezért nem meglepő, hogy a címkékkel való kommunikáció vezeték nélküli jellege, valamint az, hogy a látótérből kiesve is leolvashatóak, aggályos a magánélet védelme szempontjából, hiszen elmossa ezeket a hagyományos határokat és megnehezíti kezelésüket. Félő továbbá, hogy ezek az egyének részben vagy teljesen elveszthetik a távolság kezelése felett mostanáig meglévő ellenőrzésüket. Ennek megfelelően az RFID-rendszerek első alkalmazásainak leolvasási hatókörét a támogatók és az ellenzők egyaránt vizsgálták.

24. A negyedik kérdés az RFID-címkék méretével és fizikai tulajdonságaival kapcsolatos. Mivel a címkének alapvetően kicsinek és olcsónak kell lennie, az RFID-rendszer e részébe beépíthető biztonsági intézkedések meghatározás szerint korlátozottak. A kommunikáció vezeték nélküli jellege azonban nagybb kockázati szintet jelenthet a vezetékes kommunikációhoz képest, ezért további biztonsági intézkedésekre van szükség.

25. Az ötödik kérdés az átláthatóság hiánya a feldolgozás során. Az RFID-rendszerek révén észrevétlenül gyűjthetők és feldolgozhatók olyan információk, melyek segítségével feltérképezhető egy ember profilja. Ezt a következményt nagyon jól illusztrálja, ha az RFID-rendszereket a mobiltelefonhoz hasonlítjuk, ami kezd egyre gyakoribb hasonlattá válni. Egyrészt a mobiltelefon nagyon magas szintű technológiai elfogadottságnak örvend, függetlenül annak kockázatától, hogy betolakodhat az emberek magánéletébe. Megállapítható, hogy az RFID-et is ugyanúgy el fogják fogadni az emberek. Másrészt azonban hangsúlyozni kell, hogy a mobiltelefon látható tárgy, amely még mindig a végfelhasználó ellenőrzése alatt van, és ki lehet kapcsolni. Ez nem igaz az RFID-re.

26. Bár a fent említett észrevétlen információgyűjtés és -feldolgozás jogszerű lehet, az is elképzelhető, hogy bizonyos körülmények között sor kerülhet az adatok jogtalan gyűjtésére és feldolgozására.

27. Az ebben a fejezetben foglaltak indokolják az alábbi következtetést. Az RFID-technológia széleskörű használata alapvetően új, és döntő hatással lehet társadalmunkra és a társadalmunk olyan alapvető jogainak védelmére, mint a magánélet és az adatok védelme. Az RFID minőségi változást eredményezhet.

IV. A KÖVETKEZMÉNYEK MEGHATÁROZÁSA

Bevezetés

28. Ez a fejezet elsősorban az RFID-nek a társadalmunkban elfogadott alapvető jogokra, mint a magánélet védelmére és az adatvédelemre gyakorolt hatását vizsgálja. Ez két lépésben történik: az első lépés röviden leírja, hogyan történik a fenti alapvető jogok védelme a jelenlegi jogi keretek között. Második lépésként az európai adatvédelmi biztos kifejti a jelenlegi jogi keretek teljes kihasználására vonatkozó lehetőségeket. Ez a célkitűzés az adatvédelmi irányelvről szóló véleményben „az irányelv jelenlegi rendelkezései teljes körű végrehajtása"-ként fogalmazódik meg.

29. A kiindulási pont az alábbi: az RFID-rendszerekhez hasonló új technológiai fejlesztések nyilvánvaló hatással vannak a hatékony adatvédelmi jogi keretekkel szemben támasztott követelményekre. Ugyanakkor az egyének személyes adatai hatékony védelmének szükségessége is korlátozhatja ezen új technológiák használatát. A kapcsolat tehát kétoldalú: a technológia befolyásolja a jogszabályokat, a jogszabályok pedig a technológiát ([3]).

([1]) Hall, E.T.1966. The Hidden Dimension. (1st ed.). Garden City, N.Y: Doubleday.

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

([3]) Lásd az európai adatbázisok közötti kölcsönös átjárhatóságról szóló bizottsági közleményhez fűzött – az európai adatvédelmi biztos honlapján közzétett – 2006. márciusi észrevételeket.

Az alapvető jogok védelme

30. A magánélet védelméhez és az adatvédelemhez való alapvető jogok védelmét az Európai Unión belül elsősorban a jogszabályi keretek biztosítják, melyek azért szükségesek, mivel az emberi jogok és alapvető szabadságok európai egyezményének 8. cikkében és az Európai Unió Alapjogi Chartájának 7. és 8. cikkében foglalt jogokról van szó. Az adatvédelemre és RFID-re vonatkozó jogszabályi kereteket alapvetően a 95/46/EK adatvédelmi irányelv és a 2002/58/EK elektronikus hírközlési adatvédelmi irányelv tartalmazza ([1]).

31. A 95/46/EK irányelvben lefektetett általános adatvédelmi jogszabályi keretek alkalmazhatóak az RFID-re, amennyiben az RFID-rendszerek által kezelt adatok személyes adatoknak minősülnek. Míg bizonyos esetekben az RFID-alkalmazások nyilvánvalóan személyes adatokat dolgoznak fel, és vitathatatlanul az adatvédelmi irányelv hatáskörébe tartoznak, addig léteznek olyan alkalmazások is, ahol az adatvédelmi irányelv alkalmazhatósága nem ilyen egyértelmű. A 29. cikk szerinti adatvédelmi munkacsoport a személyes adatok fogalmáról szóló 4/2007 sz. véleménye a személyes adatok fogalmának világosabb és általánosan elismert meghatározására törekszik, ezáltal is csökkentve a fenti bizonytalanságot ([2]).

32. Az elektronikus hírközlési adatvédelmi irányelv tekintetében a helyzet a következő. Ma még nem világos, hogy ez az irányelv alkalmazható-e az RFID-alkalmazásokra. Ezért a Bizottság 2007. november 13-i, az irányelvet módosító javaslata olyan rendelkezést tartalmaz, amely pontosítja, hogy az irányelv alkalmazható bizonyos RFID-alkalmazások esetén. Egyéb RFID-alkalmazásokra ugyanakkor nem vonatkozik, mivel ez az irányelv a nyilvánosan elérhető hírközlési szolgáltatások nyilvános hírközlő hálózaton történő nyújtásával összefüggő személyes adatok kezelésére korlátozódik.

33. A személyes adatok védelmét az önszabályozási (nem jogszabályi) eszközök széles köre egészítheti ki. Ezen eszközök használata aktív támogatást élvez mindkét irányelvben, különösen az adatvédelmi irányelv 27. cikke szerint, amely előírja, hogy a tagállamoknak és a Bizottságnak bátorítania kell az irányelv megfelelő végrehajtását elősegítő magatartási kódexek kidolgozását. Ezen felül az önszabályozás eszközei hatékonyan járulhatnak hozzá az adatvédelmi irányelv 17. cikke és az elektronikus hírközlési adatvédelmi irányelv 14. cikke által előírt biztonsági intézkedések végrehajtásához.

([1]) E vélemény 59. pontja egy harmadik irányelv, a rádióberendezésekről és a távközlő végberendezésekről, valamint a megfelelőségük kölcsönös elismeréséről szóló, 1999. március 9-i 1999/5/EK európai parlamenti és tanácsi irányelv jelentőségét tárgyalja (HL L 91., 1999.4.7., 10. o.).

([2]) Lásd többek közt az ezen dokumentum 5. lábjegyzetében hivatkozott vélemény 10. oldalát.

A meglévő keretszabályozás teljes körű végrehajtása

34. Az adatvédelmi irányelvről szóló közleményről készített vélemény számos, az irányelv jobb végrehajtását szolgáló eszközt sorol fel. A vélemény nem kötelező erejű eszközeinek többsége lényeges az RFID szempontjából, mint például az értelmező közlemények és egyéb közlemények, a legjobb gyakorlatok előmozdítása, az adatvédelmi bizalompecsétek és a harmadik felek általi adatvédelmi ellenőrzések. Az RFID-re vonatkozó speciális szabályok elfogadásának lehetőségét az V. fejezetben vizsgáljuk. Ugyanakkor a jelenlegi keretszabályozáson is lehet javítani.

Az önszabályozás eszközei

35. Az európai adatvédelmi biztos egyetért a Bizottsággal abban, hogy első szakaszban helyénvaló teret hagyni az önszabályozásnak, mert ezáltal az érdekeltek gyorsan jogilag megfelelő környezetet teremthetnek, és ezzel hozzájárulhatnak egy biztonságosabb jogi környezet megteremtéséhez.

36. A Bizottság az RFID-ben érdekeltek csoportjával folytatott konzultáció alapján várhatóan ösztönözni és irányítani fogja az önszabályozás folyamatát. Ebben az összefüggésben az európai adatvédelmi biztos üdvözli a közleményben foglalt ajánlásokat, melyek várhatóan külön útmutatásokat tartalmaznak *„azon alapelvek meghatározására, amelyeket a hatóságoknak és egyéb érdekelt feleknek az RFID használata tekintetében alkalmazniuk célszerű.”*.

37. A közlemény úgy rendelkezik, hogy az önszabályozás magatartási kódexek vagy a bevált gyakorlatokról szóló kódexek formájában történik. Az európai adatvédelmi biztos szerint az önszabályozásnak formájától függetlenül az alábbiaknak kell megfelelnie:

– Konkrét és gyakorlati útmutatással kell szolgálnia bizonyos típusú RFID-alkalmazásokról és ennélfogva hozzá kell járulnia az adatvédelmi jogi kereteknek való megfeleléshez.

– Foglalkoznia kell az általános RFID-alkalmazások kapcsán felmerülő adatvédelmi kérdésekkel és problémákkal.

– Hozzá kell járulnia az adatvédelmi irányelvnek Unió-szerte egységes és összehangolt alkalmazásához, pontosan egy olyan ágazatban, amely valószínűsíthetően ugyanazokat a típusú RFID-alkalmazásokat használja az egész Unióban.

– Valamennyi érdekeltnek alkalmaznia kell. A szabályok be nem tartásának negatív (lehetőleg pénzügyi) következményekkel kell járnia.

38. Az európai adatvédelmi biztos rámutat egy olyan területre, ahol az önszabályozás különösen hasznos lehet. Az adatvédelmi irányelv különböző kötelezettségeket ró az adatkezelőkre azon RFID-alkalmazások esetén, melyek személyes adatok feldolgozását vonják maguk után, különösen a 17. cikk (az adatfeldolgozás biztonsága) és a 7. cikk (annak szükségessége, hogy adatokat csak a megfelelő jogi alapok megléte esetén lehet feldolgozni) rendelkezései értelmében. Az említett rendelkezéseknek megfelelően az adatkezelőknek egyrészt intézkedéseket kell hozniuk az adatok jogosulatlan feltárása ellen. Másrészt az adatkezelőknek biztosítaniuk kell, hogy a feldolgozás, valamint az információk leolvasók segítségével történő feltárása, amennyiben szükséges, csak azon személyek tájékoztatáson alapuló jóváhagyásával történhet, akikre az adatok vonatkoznak.

39. Az adatvédelmi irányelv szóban forgó rendelkezései értelmezhetők úgy, hogy az RFID-alkalmazásokat el kell látni a nem kívánt feltárás kockázatának megelőzéséhez vagy minimalizálásához szükséges műszaki megoldásokkal, melyek egyúttal azt is biztosítják, hogy az adatok feldolgozása vagy továbbítása, amennyiben szükséges, csak előzetes tájékoztatáson alapuló jóváhagyással történhet. Az európai adatvédelmi biztos szerint egy ilyen kötelezettség létezése (azaz a nem kívánt feltárás kockázatának megelőzéséhez vagy minimalizálásához szükséges műszaki megoldások alkalmazása) és annak kötelező jellege az RFID-alkalmazások terjesztőire nézve még erősebb és világosabb lesz, ha ezt a követelményt a fent említett, jövőbeni magatartási kódexek és a bevált gyakorlatokról szóló kódexek is tartalmazni fogják. Fenti okok miatt az európai adatvédelmi biztos határozottan javasolja, hogy a Bizottság ajánlása tartalmazza az adatvédelmi irányelv ilyenfajta értelmezését, és hangsúlyozza annak a kötelezettségnek a létezését, hogy az RFID-alkalmazásokat el kell látni az információk nem kívánt gyűjtését és feltárását megakadályozó technológiai megoldásokkal.

Az iránymutatás szükségessége

40. Az európai adatvédelmi biztos azt ajánlja, hogy a Bizottság az RFID-del foglalkozó szakértői csoporttal szorosan együttműködve állítson elő egy vagy több olyan dokumentumot, amely világos útmutatást tartalmaz a jelenlegi jogi kereteknek az RFID-környezetre történő alkalmazásáról. Az útmutatásnak gyakorlati megoldásokat kell tartalmaznia arra, hogy hogyan kell az adatvédelmi irányelvben és az elektronikus hírközlési adatvédelmi irányelvben megfogalmazott elveket betartani. Az útmutatás általános megközelítése és konkrét tartalma kapcsán az európai adatvédelmi biztos az alábbi javaslatokat teszi.

41. Az RFID-használat tekintetében alkalmazandó elveket kifejtő útmutatónak kellően összeszedettnek kell lennie, és ágazatspecifikus megközelítést kell alkalmaznia. A „mindent egy kaptafára” megközelítés nem felel meg annak a célkitűzésnek, hogy tiszta és koherens keretrendszert hozzunk létre. Az útmutatásra vonatkozó célkitűzést sokkal inkább jól meghatározott ágazati RFID-alkalmazásokra kell korlátozni.

42. Ezen kívül az útmutatásoknak gyakorlati és hatékony módszereket kell javasolniuk az olyan *technikák és szabványok* kidolgozására, melyek hozzájárulhatnak ahhoz, hogy az RFID-rendszerek megfeleljenek az adatvédelmi jogi kereteknek, és amelyek elősegítik a beépített magánélet-védelmi („privacy by design”) technológiák használatát.

43. A jelenlegi jogi keretek RFID-környezetre történő alkalmazása során különös figyelmet kell fordítani az RFID-alkalmazások adatkezelőire vonatkozó adatvédelmi elvek és kötelezettségek alkalmazására. Különösen fontosak az alábbi kötelezettségek és elvek:

– Az információhoz való jog elve, beleértve azt a jogot is, hogy tudható legyen, ha az adatgyűjtés leolvasókkal történik, és ha adott esetben a termékek címkével vannak ellátva.

– A beleegyezés fogalma, amely az adatfeldolgozás egyik jogi alapját alkotja. Ez a fogalom abban a kötelezettségben nyilvánul meg, hogy az RFID-címkéket az eladási ponton deaktiválni kell, ha az adatalany nem adta beleegyezését ([1]). Az RFID-címkék deaktiválásához való jog az információ biztonságát is garantálja, azaz biztosítja, hogy az RFID-címkéken keresztül feldolgozott adatok nem jutnak nem kívánt harmadik felek tudomására.

– Az egyének joga nem képezheti ellentétes döntések tárgyát, melyek csupán egy meghatározott személyes profil automatikus feldolgozásán alapulnak.

44. Az információhoz való jog tekintetében az útmutatónak rögzítenie kell, hogy az egyéneket el kell látni a személyes adataik feldolgozására vonatkozó *információkkal*. Különösen figyelmeztetni kell őket, többek közt arra, ha i. a termékeken vagy csomagolásukon leolvasók vagy aktivált RFID-címkék vannak elhelyezve; ii. ennek a jelenlétnek az információgyűjtést érintő következményeire és iii. azokra a célokra, amelyekre a begyűjtött információt fel kívánják használni.

45. A logók használata megfelelő tájékoztató intézkedés lehet. Logókkal lehet felhívni a figyelmet a vélhetően aktív állapotban maradt leolvasók és RFID-címkék jelenlétére. Ugyanakkor a logók használata önmagában nem elég az információk tisztességes kezelésének biztosításához, aminek érdekében az adatalanyokat tiszta és érthető módon kell információkkal ellátni. A logók használatát a részletesebb információk nyújtására vonatkozó rendelkezés kiegészítő intézkedésének lehet tekinteni.

([1]) Lásd részletesebben e vélemény 46–50. bekezdéseit.

Az alap: a részvételi elv

46. A megoldásoknak valamennyi vonatkozó RFID-alkalmazás esetében kötelezően tiszteletben kell tartaniuk és alkalmazniuk kell a részvételi elvet az eladási ponton. Az RFID-címkék képessé tétele arra, hogy az eladási pont után is információt közvetítsenek, törvénytelen, kivéve, ha az adatkezelő megfelelő jogi alapokkal rendelkezik. Megfelelő jogi alapok rendszerint csak az alábbiak lehetnek: a) az adatalany beleegyezése vagy b) ha a feltárás egy szolgáltatás nyújtásához, az említett egyén kifejezett és önkéntes kérése teljesítéséhez szükséges ([1]). Mindkét jogi alap „belülmaradásnak" minősül.

47. A részvételi elv szerint a címkéket az eladási ponton deaktiválni kell, kivéve, ha a címkével ellátott terméket megvásárló egyén továbbra is aktív állapotban kívánja hagyni. Azáltal, hogy az egyén él a jogával és aktív állapotban hagyja a címkét, hozzájárul adatai további feldolgozásához, például ahhoz, hogy az adatkezelőnél tett következő látogatása során adatait továbbítsák a leolvasóhoz.

48. A növekvő számú különböző RFID-alkalmazás kezelése és az új, innovatív üzleti modellek kifejlesztésének érdekében az európai adatvédelmi biztos hangsúlyozza a rugalmas megközelítés fontosságát. A rugalmasságot garantálni kell a részvételi elv megvalósítása során.

49. A részvételi elv megvalósítására több lehetőség van. A címke eltávolításának alternatívája lehet a címke blokkolása, ideiglenes megbénítása, vagy az úgynevezett „frissen kikelt kacsa" („ressurecting duckling") modellnek nevezett ([2]) biztonságpolitikai modell alapján, a címke meghatározott felhasználók számára történő zárolása. Egy rövid élettartamú címke esetében az adatbázisban tárolt információt tartalmazó címke címét a referencia-adatbázisból is ki lehet törölni, miáltal megakadályozható a címke által gyűjtött további adatok későbbi feldolgozása.

50. Befejezésképp elmondható, hogy bár az európai adatvédelmi biztos azzal érvel, hogy az eladási ponton alkalmazott „részvételi elv" olyan jogi kötelezettség, mely a legtöbb helyzetben az adatvédelmi irányelv értelmében jelenleg is fennáll, mégis indokoltnak tartja ezen kötelezettség önszabályozó eszközök által történő pontosítását annak érdekében, hogy a fenti elv megvalósítása a legmegfelelőbb módon történjen. Különleges megvalósítási eljárásokra van szükség minden olyan RFID-alkalmazás esetében, mely az adatvédelmi irányelv hatályán kívül esik.

([1]) Bizonyos RFID-alkalmazások esetében más alapokra is lehet támaszkodni, mint például a 7. cikk f) alpontja (az adatkezelő jogos érdekei, megfelelő biztosítékok megléte esetén).

([2]) A Cambridge-i Egyetemen oktató Frank Stajano és Ross Anderson által kifejlesztett modell neve arra utal, „ahogy egy nemrég kikelt liba feltételezi, hogy az első mozgó tárgy, amit lát, az anyja".

Beépített magánélet-védelemre van szükség

51. A magánélet és az adatok védelmére leselkedő veszélyek minimalizálása érdekében a bizottsági közlemény 6. oldalának 3.2. pontja támogatja a korai tervezési kritériumok meghatározásának és elfogadásának ötletét. Az európai adatvédelmi biztos üdvözli ezt a megközelítést. A specifikációk és tervezési kritériumok elfogadása, más néven az elérhető legjobb technikák („BAT") alkalmazása hatékonyan segíti elő az adatvédelmi szabályozást és a biztonsági követelmények betartását. A technológiai és szervezési kritériumok meghatározása gyakori felülvizsgálat esetén erősíti az Európai Unió által jelenleg fejlesztés alatt álló, a biztonságra és a magánélet védelmére vonatkozó követelmények szimbiózisán alapuló modellt.

52. A magánélet védelmére és a biztonságra vonatkozó, az RFID-rendszerek terén elérhető legjobb technikák döntő jelentőségűek lesznek a megbízható környezet létrehozásának szempontjából is, mely erősíti a végfelhasználók részéről történő széles körű elfogadást, valamint az európai gazdaság versenyképességét.

53. Az RFID-rendszerek terén elérhető legjobb technikák kiválasztásának folyamatát a magánélet védelmére és a biztonságra vonatkozó hatásvizsgálatokkal kell felgyorsítani; ezen a téren további erőfeszítésekre van szükség. Az európai adatvédelmi biztos szerint az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA), valamint az Európai Bizottság Közös Kutatóközpontja az érintett gazdasági ágazatokkal karöltve hozzájárulhat a legjobb gyakorlatok meghatározásához és az ilyen eljárások kifejlesztéséhez. A Német Szövetségi Információbiztonsági Hivatal (BSI) a „Műszaki útmutató az RFID-hez" nevű projekt elindításával kiváló példákkal szolgál ([3]) az olyan elérhető legjobb technikák terén, melyeket most európai szinten kell továbbfejleszteni.

54. A szabványok is döntő szerepet játszhatnak a beépített magánélet-védelmi elv korai elfogadásában. A Bizottságnak ezért hozzá kell járulnia a magánélet és az adatok védelmére vonatkozó garanciák elfogadásához a nemzetközi RFID-szabványok kidolgozásakor. A 29. cikk szerinti munkacsoport RFID-ről szóló munkadokumentuma ([4]) világosan kifejti, hogyan járulhatnak hozzá a szabványok az RFID-rendszereknek a magánélet védelmét tiszteletben tartó fejlesztéséhez.

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

([4]) Munkadokumentum (WP 105) az RFID-technológiával kapcsolatos adatvédelmi kérdésekről, 2005. január 19.

55. Az európai adatvédelmi biztos üdvözli továbbá a Bizottságnak az RFID-technológiák kutatásával és fejlesztésével, és a magánélet védelmére leselkedő kockázatok csökkentésének szükségességével kapcsolatos álláspontját. A beépített magánélet-védelmi elvet a technológiák fejlesztésének legkorábbi szakaszában kell bevezetni, mert ezáltal jobban biztosítható az adatvédelmi jogi kereteknek való megfelelésük. Az európai adatvédelmi biztos – mint azt 2006. évi jelentésében röviden bemutatta – maga is csatlakozni fog ehhez az erőfeszítéshez azáltal, hogy esetenként véleményt és tanácsot ad a hetedik keretprogram (2007–2013) projektjeivel kapcsolatban.

V. SZÜKSÉG VAN KÜLÖN JOGALKOTÁSI INTÉZKEDÉSEKRE?

56. Az önszabályozás nem minden esetben elegendő az adatvédelmi és a magánélet védelmére vonatkozó meglévő keret teljes körű megvalósításához. Még ha az önszabályozás ki is elégíti a fenti követelményeket, alkalmazása önkéntes, és be nem tartását nem minden esetben lehet hatékonyan szankcionálni. Ezenkívül további kötelező erejű jogalkotási intézkedésekre lehet szükség az egyénnek a magánélet és az adatok védelméhez való jogai védelmének biztosítása érdekében. Erre leginkább az önszabályozó-megközelítés mellőzése esetén van szükség.

57. Kulcskérdés azoknak a jogi eszközöknek a meghatározása, melyek biztosítják, hogy az RFID-alkalmazások hatékonyan el legyenek látva az adatvédelmi és a magánélet védelmére vonatkozó kockázatok megelőzéséhez vagy minimalizálásához szükséges műszaki megoldásokkal, és hogy a felelős adatkezelők megfelelő intézkedéseket hozzanak a jelenlegi jogi keretek szerint fennálló kötelezettségeik teljesítése érdekében. Ez néhány további kérdést vet fel:

– szükség van külön szabályokra?

– ha igen, ezek a szabályok elfogadhatóak a meglevő jogszabályi kereteken belül, például a meglevő komitológiai eljárások igénybevételével?

– vagy új jogalkotási aktusra van szükség annak érdekében, hogy az RFID-alkalmazások hatékonyan el legyenek látva a magánélet védelmét fokozó beépített technológiákkal?

58. Ez a fejezet a kötelező erejű jogalkotási intézkedéseknek a meglevő jogi kereteken belül történő megalkotásának lehetőségeit tárgyalja, míg a VI. fejezet – külön témaként – az új jogalkotási aktusok szükségességének kérdését vizsgálja.

59. Először is, különös figyelmet kell fordítani a 95/46/EK irányelv 17. cikkében, a 2002/58/EK irányelv 14. cikkének (3) bekezdésében és a 1999/5/EK irányelv 3. cikke (3) bekezdésének c) pontjában foglalt rendelkezésekre. A 14. cikk (3) bekezdése felhatalmazza a tagállamokat, hogy intézkedéseket fogadjanak el annak biztosítására, hogy a végberendezések konstrukciója olyan legyen, amely az 1999/5/EK irányelvvel összhangban ([1]) összeegyeztethető a felhasználóknak a személyes adataik védelmére és felhasználása ellenőrzésére vonatkozó jogával. A 1999/5/EK irányelv 3. cikke (3) bekezdésének c) pontja úgy rendelkezik, hogy a Bizottság – komitológiai eljárással – határozhat arról, hogy egyes berendezéscsoportba tartozó készülékeket vagy egyes készüléktípusokat úgy kell kialakítani, hogy tartalmazzanak biztosítékokat annak érdekében, hogy biztosítsák a felhasználó és az előfizető személyes adatainak és magánéletének a védelmét. A 1999/5/EK irányelv 3. cikke (3) bekezdésének c) pontja máig nem került alkalmazásra.

60. Ezek a rendelkezések – nemzeti és közösségi szinten – feljogosítják a jogalkotót arra, hogy előírja, hogy az RFID-rendszerek gyártása során be kell építeni a magánélet védelmére és az adatvédelemre vonatkozó biztosítékokat, a beépített magánélet-védelemként ismert koncepcióval összhangban ([2]). Felszólít továbbá az elérhető legjobb technikák alkalmazására.

61. A beépített magánélet-védelmi koncepció kötelezővé tétele érdekében az európai adatvédelmi biztos azt ajánlja, hogy a Bizottság az RFID-vel foglalkozó szakértői csoporttal konzultálva alkalmazza a 1999/5/EK irányelv 3. cikke (3) bekezdésének c) pontjában foglalt mechanizmust.

62. Másodszor, az irányelvek módosításával pontosítani lehet a meglevő jogszabályi kereteknek az RFID-re történő alkalmazását. Mint elmondtuk, a Bizottság nemrég mutatott be egy, az elektronikus hírközlési adatvédelmi irányelvet módosító javaslatot, amely e tekintetben új rendelkezést tartalmaz. Az európai adatvédelmi biztos üdvözli az irányelv RFID-alkalmazásokra való alkalmazhatóságának ezt az első megerősítését. Az európai adatvédelmi biztos a módosítási javaslatról szóló véleményében – melyet 2008 elején ad ki – foglalkozni fog az elektronikus hírközlési adatvédelmi irányelv és az RFID közötti kapcsolattal.

63. Figyelembe véve, hogy a Bizottság a közeljövőben nem tervezi az adatvédelmi irányelv módosítását ([3]), ezért csak korlátozott mértékben lehet a meglevő jogszabályi kereteknek az RFID-re történő alkalmazását pontosítani.

VI. SZÜKSÉG VAN AZ RFID-RE VONATKOZÓ KÜLÖN JOGI KERETRE?

A Bizottság szándékai

64. A közlemény ([4]) hangsúlyozza a biztonság és a beépített magánélet-védelem fontosságát. Szükséges továbbá valamennyi érdekelt részvétele. A Bizottság tevékenységének legfontosabb eredménye egy „*Ajánlás azon alapelvek*

([1]) És az információtechnológia és távközlés területén történő szabványosításról szóló, 1986. december 22-i 87/95/EGK tanácsi határozattal összhangban (HL L 36., 1987.2.7., 31. o.).
([2]) Lásd a IV. fejezetet.
([3]) Az európai adatvédelmi biztos támogatja ezt a megközelítést, lásd a 64. pontot.
([4]) Lásd a közlemény 4.1. pontját.

meghatározására, amelyeket a hatóságoknak és egyéb érdekelt feleknek az RFID használata tekintetében alkalmazniuk célszerű". Az ajánlást valószínűleg 2008 tavaszán fogják elfogadni. A közleményben említett jogalkotási törekvések két lépésből állnak. A Bizottság:

– fontolóra veszi az RFID-hez kapcsolódó megfelelő intézkedések beillesztését az elektronikus hírközlési adatvédelmi irányelvet módosító következő javaslatába. Mint említésre került, a Bizottság 2007 novemberében javasolta az elektronikus hírközlési adatvédelmi irányelv módosítását, melyben megerősítette az irányelv RFID-re való alkalmazhatóságát ([1]), de nem javasolta, hogy az elektronikus hírközlési adatvédelmi irányelv hatályát a magánhálózatokra is kiterjesszék,

– felméri az adatvédelem és a magánélet védelme érdekében szükséges további jogalkotási lépések szükségességét.

65. A fenti politika alapján várható, hogy a Bizottság – legalábbis rövid távon – nem tervezi, hogy külön új jogszabályokat javasol az RFID területén megvalósuló adatvédelem és magánélet-védelem érdekében.

A jogalkotónak szóló paraméterek

66. Az európai adatvédelmi biztos az adatvédelmi irányelvről szóló közleményre adott véleményében felsorolt néhány, a személyes adatok feldolgozásával kapcsolatos jogalkotási tevékenységet, melyek összefoglalása az alábbiakban következik:

– Először is meg kell tartani a főbb adatvédelmi elveket: „*Nincs szükség új elvekre, egyértelműen szükség van viszont egyéb olyan igazgatási intézkedésekre, amelyek egyrészt hatékonyak és megfelelnek a hálózatosított társadalom elvárásainak, másrészt a lehető legalacsonyabbra csökkentik az igazgatási költségeket*" ([2]).

– Másodszor, csak akkor kell jogalkotási javaslatokat benyújtani, ha azok szükségessége és arányossága kellő bizonyítást nyert. Ezért rövid távon nem kell megváltoztatni az általános adatvédelmi jogi keretet.

– Harmadszor, a társadalom fejlődésében végbemenő változások sajátos jogi kereteket eredményezhetnek az adatvédelmi irányelv alapelveinek bizonyos technológiák, pl. az RFID által felvetett kérdésekre való alkalmazása érdekében. Világos, hogy a szükségesség és arányosság feltételeinek ebben az esetben is teljesülniük kell.

67. Következő lépésként érdemes meghatározni azokat az elvárásokat, melyekkel a jogalkotónak az RFID területén szembe kell néznie:

– A jogi szabályozásnak rugalmasnak kell lennie, és teret kell hagynia az innovációnak és a technológiai fejlődésnek. Ez olyan jogi szabályozást kíván, amely technológiai szempontból kellőképpen semleges.

– Másodszor, a jogi szabályozásnak jogbiztonságot kell teremtenie. Ez olyan jogi szabályozást kíván, amely kellőképpen konkrét. Az érdekelteknek pontosan tudniuk kell, milyen szabályozások vonatkoznak viselkedésükre.

– Harmadszor, a jogi szabályozásnak hatékonyan kell védenie minden kockán forgó, jogos érdeket. Ez minden esetben a jogi szabályozás megerősítését és a felelősségi körök világos meghatározását vonja maga után: melyik fél felel melyik viselkedésért ([3])? Ezek a követelmények még fontosabbak azokban az esetekben, ahol a magánélet védelme és az adatvédelem forog kockán, melyek az emberi jogok és alapvető szabadságok védelméről szóló európai egyezményben és az Európai Unió Alapjogi Chartájában foglalt alapvető jogok.

Az európai adatvédelmi biztos véleménye

68. Az európai adatvédelmi biztos számára világos, hogy nem minden technológiai fejlődés kívánja meg az európai jogalkotó reakcióját. A technológiai fejlődés gyorsan halad, míg egy jogszabály elfogadása és hatálybalépése időt vesz igénybe és időt kell, hogy vegyen igénybe. A jogi szabályozásnak valamennyi kockán forgó érdek egyenlő mérlegelésén kell alapulnia. Ha a választott jogi eszköz az irányelv, akkor még több időre van szükség, mivel az irányelveket maradéktalanul át kell ültetni a tagállamok jogrendszerébe.

69. Ugyanakkor az RFID több mint egy a sok technológiai fejlesztés közül, mint azt e vélemény több helyütt hangsúlyozza. A közlemény az RFID-ét az információs társadalom új fejlődési szakasza kezdetének nevezi, melyet gyakran a „tárgyak internete"-ként emlegetnek; az RFID-címkék kulcsszerepet fognak betölteni a környezetintelligens környezetek kialakításában. Ezek a környezetek fontos lépései az úgynevezett „bekamerázott társadalom" kialakulásának ([4]). Ezek figyelembevételével az RFID területén végzett jogalkotási tevékenység indokolt lehet. Az RFID minőségi változást eredményezhet.

([1]) Lásd a 2002/58/EK irányelv javasolt új 3. cikkét.
([2]) Az adatvédelmi irányelvről szóló közleményre adott vélemény 24. pontja.
([3]) Az adatvédelmi terminológia szempontjából ez az „adatkezelő" azonosítását vonja maga után.
([4]) Ez az üzenet megismétlődik az európai adatvédelmi hatóságok által 2006. november 2-án Londonban elfogadott nyilatkozatban, amely megtalálható az európai adatvédelmi biztos honlapján: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. E tekintetben az európai adatvédelmi biztos a vonatkozó ágazatokban történő RFID-használat fő kérdéseit szabályozó közösségi jogszabály (javaslat) elfogadásának megfontolását javasolja abban az esetben, ha a meglévő jogi keret megfelelő alkalmazása nem lehetséges. Ezt a jogalkotási aktust hatálybalépése után az általános adatvédelmi kerettel szemben *lex specialis*-nak kell tekinteni.

71. Egy ilyen jogalkotási aktus elfogadása az alábbi előnyökkel járna:

– Az eszköz meghatározhatja az önszabályozási mechanizmus lényeges paramétereit.

– A jogalkotási aktus elfogadásának perspektívája hatékonyan ösztönözheti az érdekelteket, hogy megfelelő védelmet nyújtó önszabályozó mechanizmusokat állítsanak fel.

72. A gyakorlatiasabb megoldás érdekében a Bizottság felkérhető arra, hogy készítsen konzultációs dokumentumot a speciális jogi szabályozás mellett és ellen szóló érvekről és a jogi szabályozás főbb elemeiről. Természetesen az érdekelteket fel lehet kérni a konzultációban való részvételre. Hasonlóképp a 29. cikk alapján létrehozott munkacsoportot is be lehet vonni.

Lehetséges módozatok

73. A jogalkotó beavatkozása testreszabott jogi keretet hozhat létre, mely a jelenlegi jogi keretet pontosító és kiegészítő szabályozó eszközök kombinációjából épül fel. Ennek a testreszabott jogi keretnek az adatvédelem ismert elvein kell alapulnia, és a felelősségek megosztására és az ellenőrzési mechanizmusok hatékonyságára kell összpontosítania.

74. Az ilyen testreszabott jogi szabályozás esetleges szükségességének sajátos oka, hogy nem minden RFID-alkalmazás vonja maga után a személyes adatok feldolgozását. Más szóval ha az RFID-alkalmazások nem járnak a személyes adatok feldolgozásával, az RFID-vel felszerelt termékek gyártásában és eladásában részt vevő felek jogilag nem kötelesek semmilyen technológiai intézkedést alkalmazni, amely megakadályozná a leolvasóknak az egyének megfelelő tájékoztatása nélkül történő lehallgatását vagy elhelyezését. Mint bebizonyítottuk, az egyének lehetséges megfigyeléséből adódó, a magánélet védelmét veszélyeztető kockázatok az ilyen RFID-alkalmazások esetén is léteznek, és ezért ugyanazok a magánélet védelmére szolgáló garanciák szükségesek. Pontosabban ez az eset állhat fenn a fogyasztási cikkeknek az eladási pont *előtt* történő felcímkézése esetén. Összefoglalva, a személyes adatokat nem feldolgozó RFID-alkalmazások továbbra is veszélyeztethetik az egyén magánéletének védelmét azáltal, hogy lehetővé teszik a burkolt megfigyelést és az információ elfogadhatatlan célokra történő felhasználását.

75. Az európai adatvédelmi biztos úgy ítéli meg, hogy ezt a nemkívánatos következményt el kell kerülni. Mivel a jelenlegi jogi szabályozás részben – legalábbis a személyes adatokat nem feldolgozó RFID-alkalmazások esetén – nem tudja megakadályozni ezt a magánélet védelmére irányuló fenyegetést, és figyelembe véve a nem kötelező erejű jogi eszközök hiányosságait, kiegészítő jogalkotási intézkedések használata tűnik szükségesnek a kielégítő eredmény érdekében.

76. Ezeknek az intézkedéseknek minden esetben:

– le kell fektetniük az eladási ponton alkalmazott részvételi elvet, mint pontos és tagadhatatlan jogi kötelezettséget az adatvédelmi irányelv hatályán kívül eső RFID-alkalmazások esetén is ([1]),

– biztosítaniuk kell az RFID-alkalmazásoknak a megfelelő műszaki jellemzőkkel vagy a beépített magánélet-védelemmel való kötelező ellátását.

VII. AZ IRÁNYÍTÁS KÉRDÉSE

77. Bár az RFID-rendszerek „lényegüknél fogva határokon átnyúló” dimenzióját a közlemény csak a belső piacra vonatkoztatja, az európai adatvédelmi biztos úgy gondolja, hogy ezt a dimenziót nemzetközibb szinten kell megragadni. Egy üzletben az RFID-rendszerek már most is „határokon átnyúlók”, mivel a címke aktivitása túlnyúlik az eladási ponton. Az egész RFID-rendszer szintjén ezek a technológiák akkor is „határokon átnyúlóvá” válnak, amikor személyes adatok harmadik országba történő továbbítására kerül sor, mivel az RFID-rendszerbe tartozó felcímkézett árucikk gyártójának székhelye az Európai Unión kívül van ([2]).

78. Távlati szempontból az RFID-azonosítókat tartalmazó referencia-adatbázisok kezelése szintén kritikus tényező az európai adatvédelmi jogi keret megfelelő megerősítése tekintetében. Az európai adatvédelmi biztos megoldást sürget, mivel e keret további veszélyeztetése nem lenne elfogadható.

79. Az európai adatvédelmi biztos úgy látja, hogy az RFID-irányítás kérdése fontos kihívás, amely jelentős befektetést igényel. Meg kell találni a megfelelő tárgyalási fórumot és a legmegfelelőbb irányítási infrastruktúrát annak érdekében, hogy az adatvédelmi jogokat ténylegesen tiszteletben tartsák ezekben a nemzetközi környezetekben.

([1]) A IV. fejezet úgy érvelt, hogy az eladási ponton alkalmazott részvételi elv az adatvédelmi irányelv értelmében már létező jogi kötelezettség.

([2]) A személyes adatok továbbítására vonatkozó kötelezettségekkel az adatvédelmi irányelv 25. és 26. cikke foglalkozik.

80. E tekintetben az európai adatvédelmi biztos felszólítja a Bizottságot, hogy nyújtsa be – lehetőleg az RFID-ben érdekeltek csoportjával konzultálva kialakított – véleményét az irányítás kérdéséről.

VIII. **KÖVETKEZTETÉS**

81. Az európai adatvédelmi biztos üdvözli a Bizottság rádiófrekvenciás azonosításról szóló közleményét, mivel foglalkozik az RFID elterjedésével kapcsolatban felmerülő főbb témákkal, továbbá olyan lényeges kérdésekre is kitér, mint a magánélet védelme és az adatvédelem. Egyetért azzal a véleménnyel, hogy az RFID-rendszerek döntő szerepet játszhatnak a rendszerint a „tárgyak internete"-ként emlegetett információs társadalom fejlődésében.

A következmények tisztázása

82. Az RFID-technológia széles körű használata alapvetően új, és döntő hatással lehet társadalmunkra és a társadalmunk olyan alapvető jogainak védelmére, mint a magánélet és az adatok védelme. Az RFID minőségi változást eredményezhet.

83. Öt alapvető kérdést lehet megkülönböztetni a magánélet védelme és a biztonság témájában:

– Az adatalany azonosítása.

– Az adatkezelő(k) azonosítása.

– A személyes és nyilvános szféra közötti hagyományos különbségtétel jelentőségének csökkenése.

– Az RFID-címkék méretére és fizikai tulajdonságaira vonatkozó következmények.

– Az átláthatóság hiánya a feldolgozás során.

A következmények pontosítása

84. A 95/46/EK irányelvben lefektetett általános adatvédelmi jogszabályi keretek alkalmazhatóak az RFID-re, mivel az RFID-rendszerek által feldolgozott adatok személyes adatoknak minősülnek.

85. Ami az elektronikus hírközlési adatvédelmi irányelvet illeti: az irányelvet módosító, 2007. november 13-i bizottsági javaslat olyan rendelkezést tartalmaz, amely előírja, hogy az irányelvet bizonyos RFID-alkalmazások esetén alkalmazni kell. Bizonyos más RFID-alkalmazásokra ugyanakkor nem vonatkozik, mivel ez az irányelv a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyilvános hírközlő hálózaton történő nyújtásával összefüggő személyesadat-feldolgozásra korlátozódik.

86. A személyes adatok védelmét az önszabályozási eszközök széles köre egészítheti ki. Helyénvaló teret hagyni az ilyen jellegű önszabályozásnak, amennyiben:

– konkrét és gyakorlati útmutatással szolgál az RFID-alkalmazások bizonyos típusaihoz,

– foglalkozik az általános RFID-alkalmazások kapcsán felmerülő konkrét adatvédelmi kérdésekkel és problémákkal,

– hozzájárul az adatvédelmi irányelv Unió-szerte egységes és összehangolt alkalmazásához,

– valamennyi érdekelt alkalmazza.

87. Az európai adatvédelmi biztos azt ajánlja, hogy a Bizottság az RFID-vel foglalkozó szakértői csoporttal szorosan együttműködve állítson elő egy vagy több olyan dokumentumot, amely világos útmutatásokat tartalmaz e jogszabályi kereteknek az RFID-környezetre történő alkalmazásáról.

88. Az RFID-használat tekintetében alkalmazandó elveket kifejtő útmutatónak kellően összeszedettnek kell lennie, és ágazatspecifikus megközelítést kell alkalmaznia. Gyakorlati és hatékony módszereket kell javasolnia az olyan *technikák és szabványok* kidolgozására, melyek hozzájárulhatnak ahhoz, hogy az RFID-rendszerek megfeleljenek az adatvédelmi jogszabályi kereteknek, és amelyek elősegítik a beépített magánélet-védelmi koncepcióra épülő technológiák használatát.

89. Az európai adatvédelmi biztos üdvözli, hogy a Bizottság közleménye támogatja a korai tervezési kritériumok meghatározásának és elfogadásának ötletét.

90. Bár az európai adatvédelmi biztos úgy véli, hogy az eladási ponton alkalmazott „részvételi elv" olyan jogi kötelezettség, amely az adatvédelmi irányelv értelmében már most is létezik, ezt a kötelezettséget az önszabályozási eszközökben pontosítani kell.

Szükség van külön intézkedésekre?

91. A beépített magánélet-védelmi koncepció kötelezővé tétele érdekében az európai adatvédelmi biztos azt ajánlja, hogy a Bizottság az RFID-vel foglalkozó szakértői csoporttal konzultálva alkalmazza a 1999/5/EK irányelv 3. cikke (3) bekezdésének c) pontjában foglalt mechanizmust.

92. Az európai adatvédelmi biztos a vonatkozó ágazatokban történő RFID-használat fő kérdéseit szabályozó közösségi jogszabály (javaslat) elfogadásának megfontolását javasolja abban az esetben, ha a meglévő jogi keret megfelelő alkalmazása nem lehetséges. Ezt a jogalkotási aktust hatálybalépése után az általános adatvédelmi kerettel szemben *lex specialis*-nak kell tekinteni. Ez a jogalkotási intézkedés megválaszolja a bizonyos RFID-alkalmazások kapcsán felmerülő, a magánélet és az adatok védelméhez fűződő aggályokat, mint például a fogyasztási cikkeknek az eladási pont előtt történő felcímkézése, amely nem feltétlenül jár a személyes adatok feldolgozásával.

93. A Bizottságnak konzultációs dokumentumot kell készítenie a külön szabályozás mellett és ellen szóló érvekről és a jogi szabályozás főbb elemeiről.

94. A jogalkotó beavatkozása testreszabott jogi keretet hozhat létre, mely a jelenlegi jogi keretet pontosító és kiegészítő szabályozó eszközök kombinációjából épül fel. Ezeknek az intézkedéseknek minden esetben:

– le kell fektetniük az eladási ponton alkalmazott részvételi elvet, mint pontos és tagadhatatlan jogi kötelezettséget az adatvédelmi irányelv hatályán kívül eső RFID-alkalmazások esetén is ([1]),

– biztosítaniuk kell az RFID-alkalmazásoknak a megfelelő műszaki jellemzőkkel vagy a beépített magánélet-védelemmel való kötelező ellátását.

Az irányítás kérdése

95. Az európai adatvédelmi biztos felszólítja a Bizottságot, hogy nyújtsa be – lehetőleg az RFID-ben érdekeltek csoportjával konzultálva kialakított – véleményét az irányítás kérdéséről.

Kelt Brüsszelben, 2007. december 20-án.

Peter HUSTINX

európai adatvédelmi biztos

([1]) A IV. fejezet úgy érvelt, hogy az eladási ponton alkalmazott részvételi elv az adatvédelmi irányelv értelmében már létező jogi kötelezettség.