I

(Állásfoglalások, ajánlások és vélemények)

VÉLEMÉNYEK

EURÓPAI ADATVÉDELMI BIZTOS

Az európai adatvédelmi biztos véleménye az információs társadalom iránti bizalomnak az adatok és a magánélet védelme elősegítése révén történő erősítéséről

(2010/C 280/01)

AZ EURÓPAI ADATVÉDELMI BIZTOS,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 16. cikkére,

tekintettel az Európai Unió Alapjogi Chartájára és különösen annak 7. és 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 [1],

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 [2],

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 [3] és különösen annak 41. cikkére,

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

I. **BEVEZETÉS**

1. Az információs és kommunikációs technológiák (IKT) életünk szinte valamennyi területén – a munkában, a játékban, a társasági életben és az oktatásban – rendkívüli lehetőségeket teremtenek. Nélkülözhetetlenek a mai információs gazdaság és általában a társadalom számára.

2. Az Európai Unió globális hatalom a fejlett IKT-megoldások terén, és a továbbiakban is az kíván maradni. E kihívásnak való megfelelés érdekében az Európai Bizottság várhatóan hamarosan új európai digitális menetrendet fogad el, amelyre vonatkozóan Kroes biztos asszony megerősítette, hogy prioritást jelent számára [4].

3. Az európai adatvédelmi biztos elismeri az IKT-ből fakadó előnyöket, és egyetért azzal, hogy az EU-nak minden erejével elő kell segítenie azok fejlesztését és széles körű elfogadását. Továbbá maradéktalanul támogatja Kroes és Reding biztos asszony nézeteit, amelyek szerint ezen új környezet középpontjában az egyéneknek kell állniuk [5]. Az egyéneknek tudniuk kell bízni abban, hogy az IKT képes biztonságban tartani adataikat és ellenőrizni azok felhasználását, valamint biztosnak kell lenniük abban, hogy a magánéletük és adataik védelméhez való jogukat a digitális térben tiszteletben fogják tartani. E jogok tiszteletben tartása elengedhetetlen a fogyasztói bizalom megteremtéséhez. Ez a bizalom pedig létfontosságú, ha a polgároktól új szolgáltatások támogatását várjuk [6].

[1] HL L 281., 1995.11.23., 31. o.
[2] HL L 201., 2002.7.31., 37. o.
[3] HL L 8., 2001.1.12., 1. o.

[4] Válaszok az Európai Parlament által Neelie Kroes biztos asszonyhoz a kinevezését megelőző európai parlamenti meghallgatásokkal összefüggésben intézett kérdőívre.

[5] Válaszok az Európai Parlament által Neelie Kroes biztos asszonyhoz a kinevezését megelőző európai parlamenti meghallgatásokkal összefüggésben intézett kérdőívre; Viviane Reding biztos asszony beszéde: „Európai digitális menetrend az új digitális fogyasztó számára", elhangzott az Európai Fogyasztók Szervezete (BEUC) által rendezett, „Fogyasztói adatvédelem és online marketing: piaci tendenciák és politikai perspektívák" című, több érdekelt bevonásával tartott fórumon, 2009. november 12-én.

[6] Lásd pl. a RISEPTIS „Bizalom az információs társadalom iránt" c. jelentését, amely a RISEPTIS (Kutatás és innováció az információs társadalomban érvényesülő biztonságért, adatvédelemért és megbízhatóságért) tanácsadó testületének jelentése. A következő címen érhető el: http://www.think-trust.eu/general/news-events/riseptis-report.html. Lásd még: J. B Horrigan, *Broadband Adoption and Use in America* (A széles sáv bevezetése és használata Amerikában), FCC Omnibus Broadband Initiative, OBI Working Paper, 1. sorozat.

4. Az EU az adatok és a magánélet védelme tekintetében erős jogi kerettel rendelkezik, amelynek elvei a digitális korban is teljes érvényűek. Ugyanakkor nem lehetünk teljesen elégedettek. Az IKT számos esetben új nehézségeket vet fel, amelyekkel a meglévő keret nem számol. Éppen ezért olyan intézkedésekre van szükség, amelyek biztosítják, hogy az egyéneknek az uniós jogszabályokban foglalt jogai továbbra is hatékony védelmet nyújtsanak ebben az új környezetben.

5. Ez a vélemény azokat az Európai Unió által ösztönözhető vagy megvalósítható intézkedéseket ismerteti, amelyek garantálhatják az egyének magánéletének és adatainak védelmét egy olyan globalizált világban, amelynek motorját a jövőben is a technológia jelenti majd. A vélemény jogalkotási és nem jogalkotási eszközöket egyaránt bemutat.

6. Az IKT-ról mint lehetőségeket, ugyanakkor kockázatokat is teremtő új jelenségről szóló áttekintést követően a vélemény annak szükségességét tárgyalja, hogy az adatok és a magánélet védelmét gyakorlati szinten már az új információs és kommunikációs technológiák kialakításától kezdve be kell építeni azokba (ez az ún. „beépített adatvédelem" elve). Az elvnek való kötelező megfelelés érdekében a vélemény ismerteti, hogy a „beépített adatvédelem" elvének érvényesülését legalább két különböző módon kell biztosítani az adatvédelemmel kapcsolatos jogi keretben. Először is általános, kötelező érvényű elvként beépítve azt, másodszor pedig kifejezetten az olyan IKT-val kapcsolatos területekbe belefoglalva, amelyek megfelelő technikai felépítéssel és tervezéssel enyhíthető, konkrét adatvédelmi, illetve a magánélet védelmével kapcsolatos kockázatokat jelentenek. Ezek a területek a rádiófrekvenciás azonosítás (RFID), a közösségi hálózati alkalmazások és a böngészőalkalmazások. Végül, a vélemény olyan egyéb eszközökre és elvekre irányuló javaslatokkal szolgál, amelyek célja az egyének magánéletének és adatainak védelme az IKT-ágazatban.

7. A fentiek tárgyalása során a vélemény részletesen kifejti a 29. cikk alapján létrehozott munkacsoport által a magánélet jövőjéről szóló nyilvános konzultáció keretében említett szempontokat ([1]). Továbbá felhasználja az európai adatvédelmi biztos korábbi véleményeit, például az adatvédelmi irányelv végrehajtásáról szóló 2007. július 25-i véleményt, az RFID-ről szóló 2007. december 20-i véleményt, valamint az elektronikus hírközlési adatvédelmi irányelvről szóló két véleményt ([2]).

II. AZ IKT ÚJ LEHETŐSÉGEKET KÍNÁL, UGYANAKKOR ÚJ KOCKÁZATOKAT IS JELENT

8. Az IKT-t a múlt más nagy találmányaihoz, például az elektromossághoz hasonlítják. Míg tényleges történelmi jelentőségét talán túl korai lenne megállapítani, az IKT és a fejlett országok gazdasági növekedése közötti összefüggés egyértelmű. Az IKT munkahelyeket és gazdasági előnyöket teremtett, valamint hozzájárult az általános jóléthez. Az IKT hatása nem pusztán gazdasági jellegű, mivel az innováció és a kreativitás előmozdításában is fontos szerepet játszott.

9. Ezenfelül az IKT nyomán megváltozott az emberek munkavégzésének, társasági életének és egymással való kapcsolattartásának formája. Társadalmi és gazdasági interakcióik során például egyre nagyobb mértékben veszik igénybe az IKT-t. Számos új IKT-alkalmazás áll a felhasználók rendelkezésére, ilyenek például az e-egészségügy, az e-közlekedés, az e-kormányzat, valamint a szórakozást és tanulást célzó innovatív interaktív rendszerek.

10. Ilyen előnyök fényében valamennyi európai intézmény kifejezetten elkötelezte magát az IKT mint az európai ipar versenyképességének javítása és Európa gazdasági talpraállásának felgyorsítása szempontjából szükséges eszköz támogatása mellett. Ennek megfelelően 2009 augusztusában a Bizottság elfogadta az Európa digitális versenyképességéről szóló jelentést ([3]) és nyilvános konzultációt indított az IKT fejlesztését célzó megfelelő jövőbeni stratégiákról. 2009. december 7-én a Tanács e konzultációban való közreműködésként közzétette „Az i2010 utáni stratégia – a nyitott, zöld és versenyképes tudásalapú társadalom felé" ([4]) című dokumentumot. Az

([1]) A 29. cikk alapján létrehozott munkacsoport 2009. december 1-jén elfogadott 168. sz. véleménye: A magánélet jövője, Közös hozzájárulás az Európai Bizottság által a személyes adatok védelméhez való alapvető jogra vonatkozó jogi keretről folytatott konzultációhoz.

([2]) 2007. július 25-i vélemény az adatvédelmi irányelv jobb végrehajtását célzó munkaprogram nyomon követéséről szóló, az Európai Parlamenthez és a Tanácshoz címzett bizottsági közleményről, HL C 255., 2007.10.27., 1. o.; 2007. december 20-i vélemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a Rádiófrekvenciás azonosítás (RFID) Európában: lépések egy politikai keret felé COM(2007) 96 című bizottsági közleményéről, HL C 101., 2008.4.23., 1. o.; 2008. április 10-i vélemény a többek között az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv („elektronikus hírközlési adatvédelmi irányelv") módosításáról szóló európai parlamenti és tanácsi irányelvre vonatkozó javaslatról, HL C 181., 2008.7.18., 1. o.; 2009. január 9-i második vélemény az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv felülvizsgálatáról.

([3]) Jelentés Európa digitális versenyképességéről – Az i2010-stratégia 2005–2009 közötti legfontosabb eredményei, (SEC(2009) 1060).

([4]) A Tanács következtetései: „Az i2010 utáni stratégia – a nyitott, zöld és versenyképes tudásalapú társadalom felé" (17107/09), elfogadás dátuma: 2009.12.18.

Európai Parlament a közelmúltban fogadott el egy jelentést, amelynek célja, hogy útmutatást nyújtson a Bizottságnak a digitális menetrend meghatározásához [1].

11. Az IKT fejlődését kísérő lehetőségek és előnyök új kockázatokat vonnak maguk után, különösen az egyének magánélete és személyes adataik védelme szempontjából. Az IKT gyakran a gyűjtött, rendszerezett, szűrt, továbbított vagy más módon megtartott információk tömegének növekedéséhez vezet (igen sok esetben az egyének tudtán kívül), ezért az ilyen adatokat érintő kockázatok megtöbbszöröződnek.

12. (Egyes) fogyasztási cikkeken például RFID chipek váltják fel a vonalkódokat. Az ellátási láncon belüli információáramlás javítása (és ezáltal a „biztonsági" készletek szükségességének csökkentése, pontosabb előrejelzések biztosítása stb.) révén az új rendszer elvben mind a vállalkozások, mind pedig a fogyasztók javát szolgálja. Ezzel egy időben azonban megteremti azt a nyugtalanító lehetőséget is, hogy a címkével ellátott értéktárgyakon keresztül különböző szervezetek vagy személyek különböző okokból nyomon követhetik a fogyasztókat.

13. Egy további példa a „számítási felhő", amely alapvetően az interneten tárolt fogyasztói és nem fogyasztói alkalmazási szolgáltatások nyújtását jelenti. Ezek a fényképtáraktól, naptáraktól, internetes levelezési és fogyasztói adatbázisoktól kezdve az összetettebb, üzleti jellegű szolgáltatásokig terjedhetnek. A vállalkozások és az egyének számára nyújtott előnyök egyértelműek; költségcsökkentés (a költségek növekményesek), a fizikai helyszín hiánya (az információk a világ bármely pontjáról könnyedén elérhetők), automatikus működés (nincs szükség informatikai erőforrás-ráfordításra és a szoftverek frissítésére) stb. Ugyanakkor fennáll a biztonsági rések és a hackelés veszélye, amely nagyon is valódi. Ezenfelül aggodalomra ad okot, hogy az egyének elveszítik a saját adataikhoz való hozzáférést és azok ellenőrzését.

14. Az IKT-alkalmazásokat használó egyéb területeken is bebizonyosodott, hogy az előnyök és a kockázatok együtt járnak. Vegyük például az e-egészségügyet, amely fokozhatja a hatékonyságot, csökkentheti a költségeket, növelheti a hozzáférést és általánosságban javíthatja az egészségügyi szolgáltatások minőségét. Ugyanakkor gyakran felveti azt a problémát, jogszerű-e az e-egészségügyi adatok másodlagos felhasználása, és bármely esetleges másodlagos felhasználás esetén szükségessé teszi a felhasználás céljának körültekintő elemzését [2]. Továbbá az elektronikus egészségügyi nyilvántartások használatának elterjedésével a rendszerek maguk is botrányok tárgyává váltak, amelyek során az elektronikus egészségügyi nyilvántartások feltörésének számos esete lepleződött le.

15. Összefoglalva, feltehetően a megfelelő vizsgálatok elvégzését és a szükséges intézkedések alkalmazását követően is számolni kell bizonyos szintű fennmaradó kockázattal. A kockázatoktól mentes helyzet irreális elképzelés lenne. Az alábbiakban tárgyaltak szerint azonban lehet és kell is olyan intézkedéseket végrehajtani, amelyek megfelelő szintre szorítják az ilyen kockázatok mértékét.

III. A BEÉPÍTETT ADATVÉDELEM MINT AZ IKT IRÁNTI FOGYASZTÓI BIZALOM MEGTEREMTÉSÉNEK FŐ ESZKÖZE

16. Az IKT lehetséges előnyeit a gyakorlatban csak akkor élvezhetjük, ha azok bizalmat szülnek, más szóval, ha tulajdonságaik és az általuk nyújtott előnyök révén biztosítani tudják a fogyasztók abbéli hajlandóságát, hogy igénybe vegyék az IKT-t. Ez a bizalom csak akkor alakul ki, ha az IKT megbízható, biztonságos, az egyének ellenőrzése alatt áll, valamint garantálja személyes adataik és magánéletük védelmét.

17. A fent bemutatott gyakori kockázatok és hibák, különösen, ha azok a személyes adatokkal való visszaélést vagy azok megsértését vonják maguk után és ezáltal feltárják az egyes személyek magánéletét, feltehetően veszélyeztetni fogják a fogyasztók információs társadalomba vetett bizalmát. Ez komoly kockázatot jelenthet az IKT fejlődésére és az általa biztosított előnyökre nézve.

18. A magánélet és az adatok védelmére vonatkozó ezen kockázatokra azonban nem jelenthet megoldást az IKT felszámolása, kizárása, illetve használatának vagy népszerűsítésének megtagadása. Ez nem kivitelezhető és nem is reális elképzelés; megakadályozná, hogy a fogyasztók élvezzék az IKT előnyeit, és összességében súlyosan korlátozná az elérhető előnyök körét.

19. Az európai adatvédelmi biztos úgy véli, kedvezőbb megoldás, ha az IKT tervezése és kialakítása során tiszteletben tartják a magánélet és az adatok védelmét. Éppen ezért létfontosságú, hogy a magánélet és az adatok védelmét a technológia teljes életciklusába beépítsék, a legkorábbi tervezési szakasztól kezdve a végső üzembe helyezésig, felhasználásig, majd ártalmatlanításig. Ezt az elvet általában a „beépített adatvédelem" névvel illetik, és a későbbiekben részletesebben is szó lesz róla.

20. A beépített adatvédelem a konkrét esettől vagy alkalmazástól függően különböző intézkedéseket jelenthet. Bizonyos esetekben például szükségessé teheti a személyes adatok eltávolítását/csökkentését, illetve a felesleges és/vagy nem kívánatos feldolgozás megelőzését. Más esetekben olyan eszközök rendelkezésre bocsátását kívánhatja meg, amelyek révén a felhasználók fokozottabb ellenőrzést gyakorolhatnak személyes adataik felett. Az

[1] Jelentés az Európa számára kialakítandó új digitális menetrendről: az i2010-től a digital.eu-ig (2009/2225 (INI), elfogadás dátuma: 2010.3.18.

[2] Például a kezelések nyújtása céljából gyűjtött egészségügyi információk értékesítése vagy felhasználása körültekintő értékelést kíván meg, mivel ezek nem használhatók kórházi taglétesítmények helyszínének kiválasztásához, járóbeteg-ellátást nyújtó sebészeti rendelőintézetek létrehozásához, illetve pénzügyi következményekkel járó jövőbeni tevékenységek más módon történő tervezéséhez.

ilyen intézkedéseket az előírások és/vagy bevált gyakorlatok meghatározásakor mérlegelni kell. Ugyanígy beépíthetők az információs és kommunikációs rendszerek struktúrájába vagy a személyes adatokat feldolgozó egységek szerkezeti felépítésébe.

III.1. **A különböző IKT-környezetekben alkalmazható beépített adatvédelmi elv és azok hatásai**

21. Számos különböző IKT-környezetben van szükség a beépített adatvédelem elvére. Az egészségügyi ágazat például jelentős mértékben támaszkodik az IKT-infrastruktúrákra, amelyek gyakran a páciensek egészségügyi adatainak központi tárolását kívánják meg. A beépített adatvédelem elvének az egészségügyi ágazatban történő alkalmazása esetén meg kell vizsgálni a különböző intézkedések megfelelőségét; ilyenek lehetnek például a központilag tárolt adatok mennyiségének minimalizálása vagy jegyzék formájában történő korlátozása, titkosítási eszközök használata, hozzáférés biztosítása szigorúan a szükségesség elve alapján, a továbbiakban szükségtelen adatok anonimizálása stb.

22. Hasonlóképpen, a gépjárművel és annak környezetével különböző okokból és céllal kommunikáló közlekedési rendszereket egyre inkább alapértelmezés szerint is fejlett IKT-alkalmazásokkal látják el. Egyre több gépkocsiba szerelnek például új IKT-funkciókat (GPS, GSM, érzékelőhálózat stb.), amelyek nem csupán azok helyzetét, de műszaki állapotukat is valós időben jelzik. Ezen információk alapján például a meglévő útadórendszer felváltható egy újabb, használaton alapuló útdíjjal. A beépített adatvédelemnek az ilyen rendszerek struktúrájára való alkalmazása esetén arra kell törekedni, hogy a lehető legkevesebb személyes adat feldolgozására és továbbítására legyen szükség ([1]). Ennek az elvnek megfelelően a központosított rendszereknél kívánatosabbak az olyan decentralizált vagy félig decentralizált struktúrák, amelyek korlátozzák a helyzeti adatoknak egy központi cél felé történő továbbítását.

23. A fenti példák azt szemléltetik, hogy ha az információs és kommunikációs technológiákat a beépített adatvédelem elvével összhangban alakítják ki, a magánélet és az adatok védelmére jelentett kockázatok jelentős mértékben csökkenthetők.

III.2. **A beépített adatvédelem elvét alkalmazó IKT elégtelen igénybevétele**

24. Fontos kérdés, hogy a gazdasági szolgáltatóknak, az IKT-gyártóknak/-szolgáltatóknak és az adatkezelőknek érdekében áll-e a beépített adatvédelem elvének népszerűsítése és az IKT területén történő alkalmazása. Ebben az összefüggésben lényeges a beépített adatvédelem iránti felhasználói igény felmérése is.

25. 2007-ben a Bizottság közleményt adott ki, amelyben felszólította a vállalkozásokat, hogy innovációs erőforrásaik felhasználásával hozzanak létre és alkalmazzanak a magánélet védelmét erősítő technológiákat (PET), aminek révén a fejlesztési ciklus kezdetétől fogva javítható a magánélet és a személyes adatok védelme ([2]).

26. Az ez idáig rendelkezésre álló adatok azonban azt mutatják, hogy sem az IKT-gyártók, sem pedig az adatkezelők (sem a magán-, sem pedig a közszférában) nem jártak sikerrel a beépített adatvédelem elvének következetes végrehajtása vagy népszerűsítése terén. Különböző okokat említettek, többek között a gazdasági ösztönzők vagy az intézményi támogatás hiányát, az elégtelen keresletet stb ([3]).

27. Ezzel párhuzamosan a beépített adatvédelem iránti felhasználói igény meglehetősen alacsony volt. Az IKT-termékek és -szolgáltatások felhasználói jogosan feltételezhetik, hogy magánéletük és személyes adataik a gyakorlatban biztonságban vannak, amikor pedig számos esetben nem ez a helyzet. Bizonyos esetekben egyszerűen nincsenek abban a helyzetben, hogy megtegyék a saját vagy mások személyes adatainak védelméhez szükséges biztonsági intézkedéseket. Ennek sokszor az az oka, hogy egyáltalán vagy részben nincsenek tudatában a kockázatoknak. Általánosságban véve például a fiatalok nem törődnek a személyes információk közösségi oldalakon történő közzétételével járó kockázatokkal, és gyakran figyelmen kívül hagyják az adatvédelmi beállításokat. Más felhasználók, bár tudatában vannak ezeknek a veszélyeknek, esetleg nem rendelkeznek a biztonsági, például az internetkapcsolat védelmét szolgáló technológiák alkalmazásához szükséges műszaki szakértelemmel, vagy nem tudják, hogyan módosítsák úgy böngészőbeállításaikat, hogy minimalizálhassák a böngészési tevékenységük nyomon követése alapján történő profilalkotást.

28. Mindezek ellenére a magánélet és a személyes adatok védelmét érintő kockázatok nagyon is valóságosak. Ha a magánélet és az adatok védelmét nem vesszük már a

([1]) Lásd az európai adatvédelmi biztos 2009. július 22-i véleményét az intelligens közlekedési rendszerek alkalmazásának európai bevezetésére vonatkozó cselekvési tervről szóló bizottsági közleményről és az azt kísérő, az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keret megállapításáról szóló európai parlamenti és tanácsi irányelvre vonatkozó javaslatról, amely a következő címen érhető el: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

([2]) A Bizottság 2007.5.2-i COM(2007) 228 végleges közleménye az Európai Parlamentnek és a Tanácsnak az adatvédelemnek a magánélet védelmét erősítő technológiák által történő ösztönzéséről.

([3]) Tanulmány a magánélet védelmét erősítő technológiák (PET) gazdasági előnyeiről, jls/2008/D4/036.

kezdetektől figyelembe, gyakran túl késő és gazdasági szempontból túlságosan bonyolult a rendszerek javítása, valamint késő lesz ahhoz, hogy a már okozott károkat helyreállítsák. Az adatokkal való visszaélések számának az elmúlt években tapasztalható növekedése tökéletesen szemlélteti ezt a problémát, és megerősíti a beépített adatvédelem szükségességét.

29. A fentiekből egyértelműen az következik, hogy a személyes adatok feldolgozását célzó IKT-technológiák gyártóinak és szolgáltatóinak az adatkezelőkkel közösen felelősséget kell vállalniuk azért, hogy ezeket a technológiákat adat- és magánélet-védelmi garanciák beépítésével alakítsák ki. Ez sok esetben azt jelentené, hogy tervezéskor alapértelmezés szerint kellene biztosítani az adatvédelmi beállításokat.

30. Ebben az összefüggésben mérlegelnünk kell, milyen lépésekre van szükség a döntéshozók részéről ahhoz, hogy ösztönözni tudják a beépített adatvédelem elvének az IKT fejlesztése során való alkalmazását. Az első kérdés az, vajon az adatvédelemmel kapcsolatos meglévő jogi keret rendelkezései megfelelően gondoskodnak-e arról, hogy a beépített adatvédelem elvét mind az adatkezelők, mind pedig a gyártók/fejlesztők végrehajtsák. A második kérdés az, milyen intézkedésekre kerül majd sor az európai digitális menetrenddel összefüggésben annak érdekében, hogy az IKT-ágazat elnyerje a fogyasztók bizalmát.

IV. A BEÉPÍTETT ADATVÉDELEM ELVÉNEK BELEFOGLALÁSA AZ UNIÓS JOGSZABÁLYOKBA ÉS POLITIKÁKBA

IV.1. Az adatok és a magánélet védelmével kapcsolatos jelenlegi jogi keret

31. Az EU a 95/46/EK irányelv ([1]), a 2002/58/EK irányelv ([2]), valamint az Emberi Jogok Európai Bírósága ([3]) és az Európai Bíróság ítélkezési gyakorlatának formájában hatékony keretet biztosít az adatok és a magánélet védelméhez.

32. Az adatvédelmi irányelv „a személyes adatokon … végzett bármely művelet vagy műveletek összessége" (gyűjtés, tárolás, közlés stb.) esetében alkalmazandó. Az irányelv a személyes adatok feldolgozását végzők („adatkezelők") tekintetében bizonyos elveknek és kötelezettségeknek való megfelelést ír elő. Rendelkezik az egyének bizonyos jogairól, például a személyes adatokhoz való hozzáférés jogáról. Az elektronikus hírközlési adatvédelmi irányelv kifejezetten a magánéletnek az elektronikus hírközlési ágazatban megvalósuló védelmével foglalkozik ([4]).

33. A jelenlegi adatvédelmi irányelv nem ír elő kifejezetten a beépített adatvédelemre vonatkozó követelményt. Ugyanakkor olyan rendelkezéseket tartalmaz, amelyek különböző helyzetekben közvetve nagyon is megkövetelhetik a beépített adatvédelem elvének végrehajtását. Különösképpen a 17. cikk előírja, hogy a jogellenes adatfeldolgozás megelőzése érdekében az adatkezelők hajtsanak végre megfelelő technikai és szervezési intézkedéseket ([5]). A beépített adatvédelem éppen ezért igen általános módon érvényesül. Továbbá, az irányelv rendelkezései elsősorban az adatkezelőkre és a személyes adatok általuk végzett feldolgozására vonatkoznak. Nem írják elő közvetlenül, hogy az információs és kommunikációs technológiáknak összhangban kell állniuk a magánélet és az adatok védelmével, aminek az IKT-tervezőkre és -gyártókra, valamint a szabványosítás szakaszában végzett tevékenységekre is ki kellene terjedniük.

34. Az elektronikus hírközlési adatvédelmi irányelv ennél nyíltabban fogalmaz. A 14. cikk (3) bekezdése előírja, hogy „Szükség esetén intézkedések fogadhatók el annak biztosítására, hogy a végberendezések konstrukciója olyan legyen, amely az 1999/5/EK irányelvvel, valamint az információtechnológia és a távközlés terén történő szabványosításról szóló, 1986. december 22-i 87/95/EGK tanácsi határozattal összhangban összeegyeztethető a felhasználóknak a személyes adataik védelmére és felhasználása ellenőrzésére vonatkozó jogával." E rendelkezést azonban korábban még sohasem alkalmazták ([6]).

35. Noha a két irányelv fenti rendelkezései elősegítik a beépített adatvédelem *ösztönzését*, a gyakorlatban nem bizonyultak elégségesnek ahhoz, hogy *biztosítani* tudják az adatvédelem beépítését az IKT-ba.

36. A fenti helyzet eredményeképpen a jog nem kellően pontosan követeli meg, hogy az IKT-t a beépített adatvédelem elvével összhangban alakítsák ki. Továbbá az

([1]) Az Európai Parlament és a Tanács 95/46/EK irányelve (a továbbiakban: adatvédelmi irányelv).

([2]) Az Európai Parlament és a Tanács 2009/136/EK irányelve (a továbbiakban: elektronikus hírközlési adatvédelmi irányelv).

([3]) Az emberi jogok és alapvető szabadságok védelméről szóló, 1950. november 4-én Rómában elfogadott európai egyezmény 8. cikkében szereplő legfontosabb elemek és feltételek értelmezése a különböző területek vonatkozásában.

([4]) A Lisszaboni Szerződés a magánélet és a személyes adatok védelme tiszteletben tartásának az EU Alapjogi Chartájának 7. és 8. cikkében önálló alapvető jogként történő elismerése révén megerősítette ezt a védelmet. Az EU Alapjogi Chartája a Lisszaboni Szerződés hatálybalépésétől kezdve jogilag kötelező érvénnyel bír.

([5]) A 17. cikk a következőképpen szól: „A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő végrehajtsa a megfelelő technikai és szervezési intézkedéseket a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében, különösen, ha a feldolgozás közben az adatokat hálózaton keresztül továbbítják, továbbá a feldolgozás minden más jogellenes formája ellen." A 46. preambulumbekezdés ezt kiegészítve a következőt mondja: „mivel az érintettek jogainak és szabadságainak védelme a személyes adatok feldolgozása tekintetében megkívánja, hogy megfelelő műszaki és szervezeti intézkedéseket hozzanak mind az adatfeldolgozó rendszer megtervezésekor, mind az adatfeldolgozás időpontjában, különösen a biztonság fenntartása, és ezáltal az engedély nélküli adatfeldolgozás megelőzése érdekében."

([6]) A Bizottság bejelentette, hogy az 1999/5/EK irányelv 2010 végén történő módosítását tervezi.

adatvédelmi hatóságok nem rendelkeznek a beépített adatvédelem alkalmazásának biztosításához szükséges megfelelő hatáskörrel. Ez alacsony hatékonysághoz vezet. Az adatvédelmi hatóságok például szankciókat foganatosíthatnak az egyének által benyújtott hozzáférési kérelmekre adott válasz elmulasztása esetén, és jogukban áll előírni bizonyos intézkedések végrehajtását a jogellenes adatfeldolgozás megelőzése céljából. Ugyanakkor nem minden esetben kellően egyértelmű, hogy hatáskörükön belül megkövetelhetik-e, hogy egy adott rendszert olyan módon alakítsanak ki, amely elősegíti az egyének adatvédelemmel kapcsolatos jogainak biztosítását ([1]). A meglévő jogi rendelkezések alapján például nem világos, vajon előírható-e, hogy egy információs rendszer struktúráját úgy kell megtervezni, hogy az megkönnyítse az egyének hozzáférési kérelmeire adott vállalati válaszadást, aminek köszönhetően e kérelmeket automatikusan és gyorsabban lehetne kezelni. Továbbá a technológia létrehozását és üzembe helyezését követő későbbi módosítási kísérletek megoldások olyan egyvelegét eredményezhetik, amelyek nem működnek maradéktalanul, valamint komoly gazdasági terhet jelentenek.

37. Az európai adatvédelmi biztos véleménye szerint, amelyet a 29. cikk alapján létrehozott munkacsoport is oszt ([2]), a jelenlegi jogi keretben foglaltnál nyíltabbá tehető a beépített adatvédelem elvének támogatása.

IV.2. **A beépített adatvédelem elvének különböző szinteken történő alkalmazása**

38. A fentiek fényében az európai adatvédelmi biztos négy intézkedés meghozatalát javasolja a Bizottságnak.

a) Tegyen javaslatot egy, a beépített adatvédelemre vonatkozó általános rendelkezésnek az adatvédelemmel kapcsolatos jogi keretbe történő beépítésére.

b) Ezt az általános rendelkezést olyan konkrét rendelkezések formájában dolgozza ki, amelyek révén a különböző ágazatok részére konkrét jogi eszközök javasolhatók. Az adatvédelmi irányelv 17. cikke (és más meglévő jogszabályok) alapján előfordulhat, hogy ezek a konkrét rendelkezések már jelenleg is részét képezik egyes jogi eszközöknek.

c) Vezérelvként foglalja bele a beépített adatvédelem elvét az európai digitális menetrendbe.

d) Vezesse be a beépített adatvédelem elvét más (elsősorban nem jogszabályi) európai uniós kezdeményezésekbe is.

A beépített adatvédelemre vonatkozó általános rendelkezés

39. Az európai adatvédelmi biztos azt javasolja, hogy a beépített adatvédelem elvét egyértelműen és nyíltan foglalják bele az adatvédelemmel kapcsolatos jelenlegi jogszabályi keretbe. Ez megerősítené és nyilvánvalóbbá tenné a beépített adatvédelem elvét és kötelezővé tenné annak hatékony végrehajtását, valamint megerősített jogalapot biztosítana a végrehajtásért felelős hatóságok számára ahhoz, hogy megköveteljék annak tényleges gyakorlati alkalmazását. A fent ismertetett tényeket figyelembe véve ez különösen szükséges, nem csupán azért, mert maga az elv a bizalom megnyerésének fontos eszköze, hanem azért, is, mert arra ösztönzi az érdekelteket, hogy végrehajtsák a beépített adatvédelmet és erősítsék a meglévő jogi keretben biztosított garanciákat.

40. Ez a javaslat a 29. cikk alapján létrehozott munkacsoport ajánlását veszi alapul, amely szerint a „beépített adatvédelem" elvét általános elvként bele kell foglalni az adatvédelemmel kapcsolatos jogi keretbe, különösképpen az adatvédelmi irányelvbe. A 29. cikk alapján létrehozott munkacsoport szerint: „Az elvnek a technológiatervezők és -gyártók, valamint az IKT-k beszerzése és használata mellett döntő adatkezelők részére egyaránt kötelező erejűnek kell lennie. Kötelezni kell őket arra, hogy már az információtechnológiai eljárások és rendszerek tervezési szakaszában figyelembe vegyék a technológiai adatvédelem szempontját. Az ilyen rendszerek vagy szolgáltatások nyújtóinak, valamint az adatkezelőknek bizonyítaniuk kell, hogy e követelményeknek való megfeleléshez szükséges valamennyi intézkedést megtették."

41. Az európai adatvédelmi biztos üdvözli Viviane Redingnek a beépített adatvédelemmel kapcsolatos támogatását, amelyről az adatvédelmi irányelv felülvizsgálatának bejelentésével összefüggésben nyilatkozott ([3]).

42. Ezzel elérkeztünk a jogszabály tartalmához. Mindenekelőtt, a beépített adatvédelem általános elvének technológiai szempontból semlegesnek kell lennie. Az elv nem irányulhat a technológia szabályozására, tehát nem írhat elő konkrét technológiai megoldásokat. Ehelyett arról kell rendelkeznie, hogy a létező magánélet- és adatvédelmi

([1]) Lásd az Egyesült Királyság informatikai biztosa hivatalának „Beépített adatvédelem" című, 2008 novemberében megjelent jelentését.

([2]) Lásd a 29. cikk alapján létrehozott munkacsoport 2009. december 1-jén elfogadott 168. sz. véleményét: A magánélet jövője, Közös hozzájárulás az Európai Bizottság által a személyes adatok védelméhez való alapvető jogra vonatkozó jogi keretről folytatott konzultációhoz.

([3]) A beépített adatvédelem elve egyaránt szolgálja a polgárok és a vállalkozások javát. A beépített adatvédelem hatékonyabb védelmet biztosít majd az egyének számára, valamint bizalmat teremt az új szolgáltatások és termékek iránt, ami pedig kedvező hatást gyakorol a gazdaságra. Vannak már biztató példák, de sok még a tennivaló. Programbeszéd a 2010. január 28-i Adatvédelmi napon, Európai Parlament, Brüsszel.

elveket be kell építeni az információs és kommunikációs rendszerekbe és megoldásokba. Ez lehetővé tenné az érdekeltek, a gyártók, az adatkezelők és az adatvédelmi hatóságok számára, hogy eseti alapon értelmezzék az elv jelentését. Másodszor, az elvnek való megfelelést a szabványok és a struktúrák tervezésétől kezdve az adatkezelők által történő végrehajtásukig valamennyi szakaszban kötelezővé kell tenni.

Konkrét jogi eszközökben szereplő rendelkezések

43. A jelenlegi és a tervezett jogi eszközöknek a jelenlegi jogi keret, illetve a fent javasolt általános rendelkezés elfogadását követően ez utóbbi rendelkezés alapján magukban kell foglalniuk a beépített adatvédelem elvét. Az intelligens közlekedési rendszerekkel kapcsolatos jelenlegi kezdeményezések szerint például a Bizottságot terheli az intézkedések, a szabványosítási kezdeményezések, az eljárások és a bevált gyakorlatok meghatározásának konkrét kezdeti felelőssége. E feladatok végrehajtása során a beépített adatvédelemnek vezérelvként kell szolgálnia.

44. Az európai adatvédelmi biztos továbbá megjegyzi, hogy a beépített adatvédelem elve szintén különleges jelentőséggel bír a szabadság, a biztonság és a jog érvényesülésének térségében, különösképpen a Stockholmi Programban előirányzott információkezelési stratégia ([1]) céljaival összefüggésben. A Stockholmi Programhoz kapcsolódó véleményében az európai adatvédelmi biztos hangsúlyozta, hogy az információcsere szerkezetének a „beépített adatvédelmen" kell alapulnia ([2]): „Ez pontosabban fogalmazva azt jelenti, hogy a közbiztonsági célokra kidolgozott információs rendszereknek mindig a »beépített adatvédelem« elvével összhangban kell elkészülniük."

45. A 29. cikk alapján létrehozott munkacsoportnak a magánélet jövőjéről szóló véleménye ([3]) még ennél is pontosabb formában írja elő, hogy a szabadság, a biztonság és a jog érvényesülésének térségében – ahol továbbra is az állami hatóságok a központi szereplők, és ahol a felügyeletet erősítő intézkedések közvetlen hatással vannak a magánélet és az adatok védelméhez való alapvető jogra – kötelezővé kell tenni a beépített adatvédelemre vonatkozó követelményeket. E követelményeknek az információs rendszerekbe történő bevezetésével a kormányok úttörő szerepet játszó vevőkként fellépve is ösztönöznék a beépített adatvédelmet.

A beépített adatvédelem mint az európai digitális menetrend vezérelve

46. Az információs és kommunikációs technológiák egyre összetettebbek, és egyre komolyabb kockázatokat jelentenek a magánélet és az adatok védelmére. Általánosságban a digitalizált információk, amelyekhez jóval egyszerűbb hozzáférni, azokat másolni vagy továbbítani, sokkal nagyobb veszélyeknek vannak kitéve, mint a papíralapú információk. Az egymással kapcsolatban álló tárgyak hálózatának térnyerésével együtt növekednek a kockázatok is. Minél nagyobbak a magánélet és az adatok védelmével kapcsolatos kockázatok, annál nagyobb lesz a hatékonyabb adat-/magánélet-védelmi garanciák iránti igény. Éppen ezért a beépített adatvédelem végrehajtását szükségessé tevő indokok az IKT-ágazatban még sürgetőbbek. Ezenkívül, a fentieknek megfelelően az egyének által az IKT iránt érzett bizalom alapvető fontosságú, ha azt szeretnénk, hogy a polgárok támogassák ezeket az új szolgáltatásokat, a magánélet és az adatok védelme pedig e bizalom legfőbb elemei.

47. A fentiek alátámasztják, hogy az IKT fejlesztésére vonatkozó stratégiának meg kell erősítenie azt az elvárást, hogy ezeket a magánélet és az adatok védelmének elképzelését beépítve, tehát a beépített adatvédelem elvét figyelembe véve tervezzék meg.

48. Éppen ezért az európai digitális menetrendnek kifejezetten támogatnia kell a beépített adatvédelem elvét mint az IKT és az online szolgáltatások iránti polgári bizalom megnyeréséhez szükséges tényezőt. A menetrendnek el kell ismernie, hogy a magánélet védelme és a bizalom együtt járnak, valamint hogy a beépített adatvédelemnek meghatározó tényezőnek kell lennie egy megbízható IKT-ágazat kialakításában.

A beépített adatvédelem mint egyéb uniós kezdeményezésekben szereplő elv

49. A beépített adatvédelem elvét a Bizottságnak vezérelvként kell alkalmaznia a különböző IKT-ágazatok, többek között az e-egészségügy, az e-közbeszerzés, az e-társadalombiztosítás, az e-tanulás stb. területén folytatott politikák, tevékenységek és kezdeményezések végrehajtásakor. E kezdeményezések többsége intézkedésként szerepel majd az európai digitális menetrendben.

50. Ez azt jelenti például, hogy a kormányzati alkalmazások hatékonyságának és korszerűbbé tételének biztosítását célzó, és ezáltal az egyének és a kormányzatok közötti interakciót lehetővé tevő kezdeményezéseknek tartalmazniuk kell azt az elvárást, hogy az alkalmazásokat a beépített adatvédelem elvével összhangban alakítsák ki és működtessék. Ugyanez vonatkozik a Bizottság azon politikáira és tevékenységeire is, amelyek a gyorsabb internetkapcsolat és a digitális tartalom biztosítására irányulnak, vagy átfogó módon szorgalmazzák a vezetékes és vezeték nélküli kommunikációt és adattovábbítást.

([1]) A stockholmi program – A polgárokat szolgáló nyitott és biztonságos Európa; jóváhagyta az Európai Tanács 2009 decemberében.

([2]) 2009. július 10-i vélemény a szabadságon, a biztonságon és a jog érvényesülésén alapuló, a polgárok szolgálatában álló térségről szóló, a Tanácshoz és az Európai Parlamenthez intézett bizottsági közleményről, HL C 276., 2009.11.17., 8. o., 60. pont.

([3]) A 29. cikk alapján létrehozott munkacsoport 2009. december 1-jén elfogadott 168. sz. véleménye: A magánélet jövője, Közös hozzájárulás az Európai Bizottság által a személyes adatok védelméhez való alapvető jogra vonatkozó jogi keretről folytatott konzultációhoz.

51. A fentiekbe értendők azok a területek is, ahol a Bizottság az olyan nagyléptékű informatikai rendszerekért felelős, mint a SIS és a VIS, valamint azok az esetek is, amelyekben a Bizottság felelőssége az ilyen rendszerek közös infrastruktúrájának fejlesztésére és karbantartására korlátozódik, mint például az Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS) esetében.

52. A beépített adatvédelem elvének pontos kialakítása az egyes konkrét ágazatoktól és helyzetektől függ. Amikor például egy adott IKT-ágazatra vonatkozóan a bizottsági kezdeményezéseket jogszabályjavaslatok kísérik, számos esetben az a megfelelő eljárás, ha ezek egyértelmű hivatkozást tartalmaznak, amelynek értelmében a beépített adatvédelem alkalmazandó az érintett IKT-alkalmazás/-rendszer tervezésekor. Ha egy adott területre vonatkozóan cselekvési terv születik, annak szisztematikusan biztosítania kell a jogi keret alkalmazását, és konkrétabban gondoskodnia kell arról, hogy a kapcsolódó IKT-technológiát a beépített adatvédelmet figyelembe véve dolgozzák ki.

53. Ami a kutatást illeti, a hetedik és az azt követő keretprogramokat olyan eszközként kell alkalmazni, amelyek a magánéletet és konkrétabban a beépített adatvédelem elvét hatékonyabban védő szabványok, IKT-technológiák és -struktúrák elemzését célzó projekteket támogatnak. Ezenfelül a beépített adatvédelmet az egyének személyes adatainak feldolgozására szolgáló átfogóbb IKT-projektek esetében is kötelezően mérlegelendő tényezőként kell előírni.

Kiemelt figyelmet igénylő területek

54. Bizonyos esetekben az egyének magánéletét és adatainak védelmét érintő különleges kockázatok vagy egyéb tényezők miatt (ágazati tiltakozás a beépített adatvédelmet tartalmazó termékek biztosításával szemben, fogyasztói kereslet stb.), akár jogalkotási, akár más eszköz keretén belül szükség lehet nyíltabb és pontosabb beépített adatvédelmi intézkedések megfogalmazására, amelyeket egy adott típusú információs és kommunikációs termékbe vagy technológiába kell beépíteni.

55. Az európai adatvédelmi biztos több olyan területet is meghatározott (RFID, közösségi oldalak és böngészőalkalmazások), amelyek véleménye szerint ebben a szakaszban megkívánják a Bizottság körültekintő mérlegelését és a fent szorgalmazott közvetlenebb beavatkozást. E három területet az alábbiakban részletesen is ismertetjük.

V. **RÁDIÓFREKVENCIÁS AZONOSÍTÁS – RFID**

56. Az RFID-címkéket tárgyakba, állatokba és személyekbe is be lehet építeni. Felhasználhatók személyes adatok, például egészségügyi információk gyűjtésére és tárolására, a személyek mozgásának nyomon követésére vagy a viselkedésükön alapuló, különböző célú profilalkotásra. Mindez az érintett személy tudomása nélkül is lehetséges ([1]).

57. Az adatvédelemre, a magánélet védelmére és a kapcsolódó etikai dimenziókra vonatkozó hatékony garanciák nélkülözhetetlenek az RFID és a tárgyak jövőbeli internete iránti közbizalom megnyerése érdekében. Csak így érvényesülhet a technológia által nyújtott számos gazdasági és társadalmi előny.

V.1. **Az adatvédelemmel kapcsolatos vonatkozó jogi keret hiányosságai**

58. Az RFID-alkalmazásokon keresztül végzett adatgyűjtés tekintetében az adatvédelmi irányelv és az elektronikus hírközlési adatvédelmi irányelv irányadó ([2]). Előírják többek között, hogy az RFID-alkalmazások használatának feltétele a megfelelő magánélet-védelmi garanciák biztosítása ([3]).

59. Ez a jogi keret azonban nem nyújt teljes körű megoldást a technológia nyomán felmerülő adatvédelmi és magánélet-védelmi problémákra. Ennek az az oka, hogy az RFID-alkalmazások esetében végrehajtandó garanciák típusa

([1]) Az RFID jelentése: rádiófrekvenciás azonosítás. A rádiófrekvenciás azonosítási technológia vagy infrastruktúra fő összetevői egy címke (vagyis mikrochip), egy leolvasó és a címkékkel és a leolvasókkal egy köztesszoftver révén összekapcsolt alkalmazás, valamint a kapott adatok feldolgozása. A címke egy adattárolásra szolgáló elektromos áramkörből és egy antennából áll, amely az adatokat rádióhullámok segítségével közvetíti. A leolvasón található egy antenna és egy dekóder, amely a rádiókapcsolattól érkező bejövő analóg információkat digitális adatokká alakítja. Ezt követően az adatok a hálózatokon keresztül adatbázisokhoz és kiszolgálókhoz továbbíthatók számítógépes feldolgozás céljára.

([2]) Az elektronikus hírközlési irányelv a 3. cikkben utal az RFID-re: „Ezt az irányelvet a Közösségben a nyilvánosan elérhető hírközlési szolgáltatások nyilvános hírközlő hálózaton – az adatgyűjtést és az azonosító eszközöket támogató nyilvános hírközlő hálózatokat is beleértve – történő nyújtásával összefüggő személyes adatok kezelésére kell alkalmazni.” (Ezt az 56. preambulumbekezdés egészíti ki.) „A technológiai fejlődés adatgyűjtő és azonosító eszközökön alapuló új alkalmazások kifejlesztését teszi lehetővé, amelyek lehetnek rádiófrekvenciákat használó, vezeték nélküli eszközök is. A rádiófrekvenciás azonosításra használt eszközök (RFID) például rádiófrekvenciákat használnak az egyedileg azonosított címkékről történő adatszerzéshez, amely adatok azután a már meglévő hírközlő hálózatokon továbbíthatók. Az ilyen technológiák széles körű használata jelentős gazdasági és társadalmi előnyökkel járhat, és így hathatósan járulhat hozzá a belső piachoz, ha alkalmazásuk elfogadható a polgárok számára. Ennek elérése érdekében biztosítani kell az egyének alapvető jogainak – ideértve a magánélet és az adatvédelem tiszteletben tartásához való jogot is – védelmét. Amennyiben ezeket az eszközöket nyilvánosan hozzáférhető elektronikus hírközlő hálózatokhoz kapcsolják vagy azok alapvető infrastruktúraként elektronikus hírközlési szolgáltatásokat használnak, a 2002/58/EK irányelv (elektronikus hírközlési adatvédelmi irányelv) vonatkozó rendelkezéseit – beleértve a biztonságra, a forgalommal és az helymeghatározással kapcsolatos adatokra, valamint a titkosságra vonatkozó rendelkezéseket is – kell alkalmazni.”

([3]) Az adatvédelmi irányelv 17. cikke például kötelezően előírja a megfelelő technikai és szervezési intézkedések végrehajtását a személyes adatok véletlen vagy jogellenes megsemmisülése vagy jogosulatlan nyilvánosságra hozatala elleni védelem érdekében.

tekintetében az irányelvek nem kellően részletezettek. A létező szabályokat továbbiakkal kell kiegészíteni, amelyek konkrét garanciákat írnak elő, és különösképpen kötelezővé teszik bizonyos technikai megoldások (beépített adatvédelem) beépítését az RFID-technológiába. Ez a helyzet a személyes adatokat tároló címkék esetében, amelyeknek beépített hatástalanító paranccsal kell rendelkezniük, valamint a titkosítás használatára bizonyos típusú személyes adatokat tároló címkék esetében.

V.2. **Az önszabályozás mint első lépés**

60. 2007 márciusában a Bizottság közleményt ([1]) fogadott el, amely többek között elismerte az RFID gyakorlati végrehajtására vonatkozó részletes útmutatás szükségességét, valamint a magánéletet és a biztonságot érintő kockázatok elkerülését célzó tervezési kritériumok elfogadásának kívánatos voltát.

61. E célok elérése érdekében a Bizottság 2009 májusában ajánlást fogadott el a magánélet- és adatvédelmi elveknek az RFID-alkalmazások területén történő alkalmazásáról ([2]). Ez az RFID-alkalmazások kiskereskedelemben történő felhasználása esetén a címke hatástalanítását írja elő az árusítás helyén, kivéve, ha a fogyasztó hozzájárulását adja annak üzemben tartásához. Ez minden esetben érvényes, kivéve, ha a magánélet védelméről és az adatvédelemről készített hatásvizsgálat eredményei szerint a címkék valószínűsíthetően nem fenyegetik a magánélet és a személyes adatok védelmét, mely esetben azok az árusítóhely elhagyását követően is üzemben maradnának, hacsak a fogyasztó nem él a díjmentes hatástalanítás lehetőségével.

62. Az európai adatvédelmi biztos egyetért az önszabályozó eszközök használatára vonatkozó bizottsági megközelítéssel. Az alábbiakban ismertetettek szerint azonban elképzelhető, hogy az önszabályozás nem hozza meg a kívánt eredményt; éppen ezért felkéri a Bizottságot, hogy készüljön fel alternatív intézkedések elfogadására.

V.3. **Problematikus területek és további lehetséges intézkedések az önszabályozás kudarca esetén**

63. Az európai adatvédelmi biztost aggodalommal tölti el, hogy a kiskereskedelmi ágazatban RFID-alkalmazásokat felhasználó szervezetek esetleg figyelmen kívül hagyják, hogy az RFID-címkéket nem kívánatos harmadik felek is nyomon követhetik. Az ilyen nyomon követés feltárhatja a címkén (esetlegesen) tárolt személyes adatokat, de azt is lehetővé teheti a harmadik fél számára, hogy egy adott személyt egyszerűen a nála lévő egy vagy több címkén található egyedi azonosítók felhasználásával kövessen vagy idővel felismerjen akár az RFID-alkalmazás működési hatókörén kívül eső környezetben is. Továbbá aggodalommal tölti el, hogy az RFID-alkalmazások szolgáltatói hajlamosak lehetnek arra, hogy indokolatlanul alkalmazzák a kivételt, és az árusítás helyének elhagyását követően is üzemben tartsák a címkét.

64. Ha a fentiek megtörténnek, előfordulhat, hogy túl késő lesz az egyének adatainak és magánéletének védelmére irányuló kockázatok csökkentéséhez, amelyek addigra sérülhetnek. Ezenfelül az önszabályozás jellegéből következően a nemzeti végrehajtási hatóságok gyengébb helyzetből hívhatják fel az RFID-alkalmazásokat működtető szervezeteket bizonyos beépített adatvédelmi intézkedések alkalmazására.

65. A fentiek fényében az európai adatvédelmi biztos felszólítja a Bizottságot, készüljön fel arra, hogy a jelenlegi jogi keret hatékony végrehajtásának kudarca esetén javaslatot tegyen az RFID felhasználásával kapcsolatos fő problémákat szabályozó jogalkotási eszközökre. A Bizottság értékelése nem halasztható el indokolatlanul; a halogatás veszélyt jelent az egyénekre nézve, emellett pedig az ágazat tekintetében is éppen ellentétes hatást váltana ki, mivel túlságosan komoly jogi bizonytalanságok állnak fenn, és a meghonosodott problémák javítása várhatóan nehezebb és költségesebb lesz.

66. A szükséges javasolt intézkedések között az európai adatvédelmi biztos javasolja az árusítás helyén történő hozzájárulás lehetőségének biztosítását, amelynek értelmében az árusítás helyén a fogyasztási cikkeken található valamennyi RFID-címkét alapesetben hatástalanítanák. Nem szükséges és nem helyénvaló, hogy a Bizottság meghatározza a konkrétan alkalmazandó technológiát. Ehelyett az uniós jognak az üzemben tartáshoz való hozzájárulás megszerzésére vonatkozó jogi kötelezettséget kell előírnia, és a szolgáltatókra kell bíznia annak eldöntését, hogyan kívánják teljesíteni ezt a követelményt.

V.4. **További mérlegelendő kérdések: A tárgyak internetének irányítása**

67. Az RFID-címkék által gyűjtött információk – például termékinformációk – végül akár egy globális kommunikációs infrastruktúrahálózathoz is eljuthatnak. Ezt általában „a tárgyak interneté”-nek nevezik. Azért merülnek fel adatvédelemmel és a magánélet védelmével kapcsolatos kérdések, mert a valódi világ tárgyai RFID-címkékkel azonosíthatók, amelyek a termékinformációkon kívül személyes adatokat is tartalmazhatnak.

68. Számos nyitott kérdés merül fel azzal kapcsolatban, ki irányítja majd a címkével ellátott tárgyakkal kapcsolatos adatok tárolását. Hogyan szervezik majd ezt az adattárolást? Ki kaphat hozzáférést? 2009 júniusában a Bizottság közleményt fogadott el a tárgyak internetéről ([3]), amely nyíltan meghatározta a jelenségből fakadó lehetséges adatvédelmi és magánélet-védelmi problémákat.

([1]) A Bizottság 2007.3.15-i közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Rádiófrekvenciás azonosítás (RFID) Európában: lépések egy politikai keret felé, COM(2007) 96 végleges.

([2]) A Bizottság 2009.5.12-i ajánlása a magánélet- és adatvédelmi alapelveknek a rádiófrekvenciás azonosítás által támogatott alkalmazások területén történő alkalmazásáról (C(2009) 3200 végleges).

([3]) A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek és az Európai Gazdasági és Szociális Bizottságnak – A tárgyak internete – Cselekvési terv Európáért, 2009.6.18., COM(2009) 278 végleges.

69. Az európai adatvédelmi biztos hangsúlyozni kíván néhány, a közlemény által felvetett kérdést, amelyek véleménye szerint a tárgyak internetének fejlődésével komoly figyelemre tartanak számot. Először is, a decentralizált struktúra szükségessége javíthatja az elszámoltathatóságot, valamint az EU jogi keretének végrehajthatóságát. Másodszor, az egyéneknek a nyomon követés alóli mentességéhez való jogát a lehető legnagyobb mértékben fenn kell tartani. Más szóval csupán igen korlátozott esetekben fordulhat elő, hogy beleegyezésük nélkül nyomon követik őket az RFID-címkék révén. A beleegyezésnek kifejezettnek kell lennie. Ezt a jelenséget általában a „chipek kiiktatásá"-nak és a magánélethez való jognak nevezik. Végül, a tárgyak internetének létrehozása során a beépített adatvédelem elvét vezérelvként kell alkalmazni. Ez megkövetelné például, hogy a felhasználói irányítást biztosító beépített mechanizmusokkal rendelkező konkrét RFID-alkalmazások már alapesetben tartalmazzanak adatvédelmi beállításokat.

70. Az európai adatvédelmi biztos számít rá, hogy a Bizottság a közleményben előirányzott intézkedések megvalósítása, különösképpen a mindenütt jelen lévő információ társadalmában a magánéletről és a bizalomról szóló közlemény szövegezése során konzultálni fog vele.

VI. **KÖZÖSSÉGI HÁLÓZATOK ÉS AZ ALAPÉRTELMEZETT ADATVÉDELMI BEÁLLÍTÁSOK SZÜKSÉGESSÉGE**

71. A közösségi hálózatok manapság igazán felkapottak. Úgy tűnik, hogy népszerűségük az e-mailét is felülmúlta. Kapcsolatot teremtenek az azonos érdeklődésű és/vagy tevékenységet folytató személyek között. A tagok online profilt hozhatnak létre, és médiafájlokat, például videókat, fényképeket, zenét, valamint szakmai profiljukat is megoszthatják egymással.

72. A fiatalok rendkívül gyorsan magukévá tették a közösségépítést, és ez a tendencia folytatódik. Az elmúlt néhány évben csökkent az európai internetfelhasználók átlagéletkora: ma már a 9–10 évesek is hetente többször csatlakoznak; a 12–14 évesek naponta használják a világhálót, gyakran 1–3 órás időtartamban.

VI.1. **Közösségi hálózatok és az adatvédelemmel és a magánélet védelmével kapcsolatos vonatkozó jogi keret**

73. A közösségi hálózatok kialakulása lehetővé tette a felhasználók számára, hogy információkat töltsenek fel az internetre saját magukról és harmadik személyekről. A 29. cikk alapján létrehozott munkacsoport szerint [1] ezáltal az internetfelhasználók az adatvédelmi irányelv korábbi 2. cikke d) pontjának értelmében [2] az általuk feltöltött adatok tekintetében adatkezelőnek minősülnek. A legtöbb esetben azonban az effajta adatfeldolgozás az irányelv korábbi 3. cikkének (2) bekezdésében foglalt, háztartási tevékenységre vonatkozó kivétel kategóriájába tartozik. A közösségi hálózatok szolgáltatói ugyanakkor adatkezelőnek minősülnek, amennyiben lehetőséget nyújtanak a felhasználói adatok feldolgozására, valamint a felhasználói adatkezeléssel kapcsolatos valamennyi alapszolgáltatást (pl. regisztráció és a fiók törlése) biztosítják.

74. Jogi értelemben ez azt jelenti, hogy az internethasználók és a közösségi hálózatok szolgáltatói az irányelv 2. cikke d) pontjának alkalmazásában „adatkezelőként" közösen felelnek a személyes adatok feldolgozásáért, jóllehet különböző mértékben és különböző kötelezettségekkel.

75. Ennek megfelelően a felhasználóknak tudatában kell lenniük annak és meg kell érteniük, hogy saját és mások személyes adatainak feldolgozása nyomán az uniós adatvédelmi jogszabályok rendelkezéseinek hatálya alá tartoznak, amelyek megkövetelik többek között a feltöltött adatok tulajdonosainak tájékoztatáson alapuló hozzájárulását, valamint azt, hogy az érintettek számára biztosítsák a jogorvoslatot, az elutasítás jogát stb. Hasonlóképpen a közösségi hálózatok szolgáltatóinak többek között végre kell hajtaniuk a megfelelő technikai és szervezési intézkedéseket az engedély nélküli adatfeldolgozás megelőzése érdekében, figyelembe véve az adatfeldolgozással járó kockázatokat és az adatok jellegét. Mindez azt jelenti, hogy a közösségi hálózatok szolgáltatóinak az adatok védelmével összhangban álló beállításokat kell biztosítaniuk, többek között olyanokat, amelyek segítségével a profilhoz való hozzáférés a felhasználó által kiválasztott személyekre korlátozható. A profilok harmadik fél számára történő nyilvánossá tételét megelőzően a beállításoknál kérni kell a felhasználó megerősítő beleegyezését, és a korlátozott hozzáférésű profilokat a belső keresőmotorok számára is le kell tiltani.

76. Sajnálatos módon a jogi követelmények és a tényleges megfelelés között nagy szakadék tátong. Míg jogi értelemben véve az internetfelhasználók adatkezelőnek minősülnek, így az adatvédelemmel és a magánélet védelmével kapcsolatos uniós jogi keret kötelezi őket, a valóságban gyakran nincsenek tudatában e szerepüknek. Általában kevéssé vannak tisztában azzal, hogy személyes adatokat dolgoznak fel, és hogy az ilyen információk közzététele magánélet- és adatvédelmi kockázatokat rejt magában. Különösen a fiatalok tesznek közzé úgy tartalmakat online, hogy alábecsülik azok saját maguk és mások számára jelentett következményeit, például az oktatási intézményekbe való későbbi felvételükkel vagy állásra történő jelentkezésükkel összefüggésben.

[1] Lásd a 29. cikk alapján létrehozott munkacsoport 5/2009. sz. 163. véleményét az internetes ismeretségi hálózatokról; elfogadás dátuma: 2009. június 12.

[2] „Adatkezelő" az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely önállóan vagy másokkal együtt meghatározza a személyes adatok feldolgozásának céljait és módját; ha a célokat és módokat egy adott nemzeti vagy közösségi jogszabály határozza meg, az adatkezelőt vagy a kinevezésére vonatkozó külön szempontokat ez a nemzeti vagy közösségi jogszabály jelöli ki.

77. Ezzel egy időben a közösségi hálózatok szolgáltatói gyakran előre megadják a később letiltható alapértelmezett beállításokat, és ezáltal a személyes adatok nyilvánossá tételét ösztönzik. Egyes szolgáltatók már alapesetben engedélyezik, hogy a profilok az ismert keresőmotorok számára elérhetők legyenek. Ez felveti azt a kérdést, vajon az egyének ténylegesen hozzájárultak-e a közzétételhez, és hogy a közösségi hálózatok megfelelnek-e az irányelv (fent ismertetett) 17. cikkének, amely előírja számukra, hogy az engedély nélküli adatfeldolgozás megelőzése érdekében hajtsák végre a megfelelő technikai és szervezési intézkedéseket.

VI.2. **A közösségi hálózatok által teremtett kockázatok és a megoldásukra javasolt intézkedések**

78. A fentiek eredményeképpen az egyének magánéletének és adatainak védelmét fokozott kockázatok érik. Az internetfelhasználók és a feltöltött adatok tulajdonosai esetében fennáll magánéletük és adataik védelme súlyos megsértésének a veszélye.

79. Ebben az összefüggésben a Bizottságnak azt a kérdést kell megvizsgálnia, mit kell és mit lehet tenni e helyzet megoldása érdekében. Ez a vélemény nem nyújt átfogó választ a kérdésre, hanem további megfontolásra érdemes javaslatokkal él.

Az internetfelhasználók tájékoztatására tett erőfeszítések

80. Az első javaslat a felhasználók ismereteinek bővítésére irányul. E tekintetben az EU intézményeinek és a nemzeti hatóságoknak lépéseket kell tenniük az ismeretterjesztés, valamint a közösségépítő hálózatok nyomán felmerülő veszélyekkel kapcsolatos tudatosság növelése terén. Az Információs Társadalmi Főigazgatóság által működtetett Biztonságosabb Internet Program célja például a gyermekek és fiatalok helyzetének megerősítése és védelme többek között a tudatosságot növelő intézkedések révén ([1]). Az EU intézményei a közelmúltban indították útjára a „Gondold meg, mit töltesz fel az internetre!" elnevezésű kampányt, hogy növeljék a személyes adatok idegenekkel való megosztása által jelentett kockázatokkal kapcsolatos tudatosság mértékét.

81. Az európai adatvédelmi biztos szorgalmazza, hogy a Bizottság továbbra is támogassa az ilyen típusú tevékenységeket. Ugyanakkor a közösségi hálózatok szolgáltatóinak maguknak is aktív szerepet kell vállalniuk, mivel jogi és társadalmi felelősségük a felhasználók tájékoztatása arra vonatkozóan, hogyan használhatják szolgáltatásaikat biztonságos és az adatok védelmével összhangban álló módon.

82. A fentieknek megfelelően, amikor adatokat töltünk fel a közösségi hálózatokra, ezek az adatok alapesetben számos különböző módon elérhetőek lehetnek. Hozzáférhet például általában a nagyközönség, ideértve a keresőmotorokat, amelyek indexálhatják az információkat és közvetlenül azokra mutató hivatkozást hozhatnak létre. Más részről az információk a „kiválasztott ismerősök" körére korlátozhatók, vagy teljes mértékben titkosíthatók. A profilok engedélyezése és a terminológia természetesen oldalanként eltérő.

83. A fent ismertetettek szerint azonban csak igen kevés közösségi szolgáltatásokat használó személy van tisztában azzal, hogyan szabályozhatja az általa feltöltött információkhoz való hozzáférést, az alapértelmezett adatvédelmi beállítások módosításáról nem is beszélve. Az adatvédelmi beállításokat a legtöbb esetben változatlanul hagyják, mivel a felhasználók nincsenek tudatában annak, milyen következményekkel jár, ha nem módosítják azokat, vagy nem tudják, hogyan tehetik azt meg. Éppen ezért legtöbbször az alapértelmezett beállítások változatlanul hagyása nem jelenti azt, hogy az egyének megalapozott döntés alapján hozzájárultak az adatok megosztásához. Ebben az összefüggésben különösen fontos, hogy harmadik felek, például a keresőmotorok ne hivatkozzanak az egyéni profilokra azt feltételezve, hogy a felhasználók alapértelmezés szerint (és nem az adatvédelmi beállítások módosítása révén) hozzájárultak adataik korlátozások nélküli nyilvánosságra hozatalához.

84. Míg a felhasználói ismeretterjesztés elősegítheti a helyzet megoldását, önmagában nem elégséges. A 29. cikk alapján létrehozott munkacsoport ismeretségi hálózatokról szóló véleményében megfogalmazott ajánlása értelmében a közösségi hálózatok szolgáltatóinak a személyes adatok védelmével összhangban álló és ingyenes alapértelmezett adatvédelmi beállításokat kell kínálniuk. Ezáltal a felhasználók tudatosabban cselekednének, és megfelelőbb döntéseket hozhatnának azt illetően, meg szeretnék-e osztani adataikat, és ha igen, kivel.

Az önszabályozás szerepe

85. A Bizottság „Biztonságosabb közösségi hálózatépítési elveket az EU-nak!" néven ([2]) megállapodást kötött húsz közösségi hálózati szolgáltatóval. A megállapodás célja, hogy az európai közösségi weboldalak használata során fokozza a kiskorúak biztonságát. Az elvek között számos, a fent bemutatott adatvédelmi jogi keret alkalmazásából fakadó követelmény található. Ide tartozik többek között a felhasználók helyzetének a különböző eszközök és technológiák révén történő erősítésére vonatkozó követelmény, valamint annak biztosítása, hogy a felhasználók szabályozhassák személyes adataik felhasználását és terjesztését. Ilyen elv továbbá az adatvédelmi beállítások alapértelmezés szerint történő biztosításának szükségessége.

86. 2010 január elején a Bizottság közzétette az elvek végrehajtását értékelő jelentés eredményeit ([3]). Az európai adatvédelmi biztos aggodalmát fejezi ki azt illetően, hogy a jelentés tanúsága szerint bizonyos lépések megvalósultak, mások azonban nem. A jelentés problémákat tárt fel

([1]) A programmal kapcsolatos információk a következő címen olvashatók: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Az elvek a következő címen érhetők el: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Jelentés a „Biztonságosabb közösségi hálózatépítési elveket az EU-nak" c. dokumentum elveinek értékeléséről, amely a következő címen érhető el: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

például a weboldalakon rendelkezésre álló biztonsági intézkedésekre és eszközökre vonatkozó tájékoztatás tekintetében. Ezenfelül megállapította, hogy a megállapodás aláíróinak kevesebb mint fele korlátozza a kiskorúak profiljához való hozzáférést, hogy az kizárólag az ismerősök számára legyen elérhető.

A kötelező alapértelmezett adatvédelmi beállítások szükségessége

87. Ebben az összefüggésben a fő kérdés az, szükség van-e további szakpolitikai intézkedésekre annak biztosítása érdekében, hogy a közösségi hálózatok alapértelmezett adatvédelmi beállításokkal hozzák létre szolgáltatásaikat. A problémát Viviane Reding korábbi információs társadalomért felelős biztos vetette fel, aki rámutatott, hogy szükség lehet jogi szabályozásra ([1]). Ebben a szellemben az Európai Gazdasági és Szociális Bizottság kijelentette, hogy az önszabályozáson túl jogszabályba kell foglalni a minimális védelmi előírásokat ([2]).

88. Ahogyan fentebb megjegyeztük, a közösségi hálózatok szolgáltatóira vonatkozó követelmény, amelynek értelmében alapértelmezés szerint biztosítaniuk kell az adatvédelmi beállításokat, közvetetten az adatvédelmi irányelv 17. cikkéből ([3]) is következik, amely az adatkezelők számára előírja, hogy hozzák meg a megfelelő technikai és szervezési intézkedéseket („mind az adatfeldolgozó rendszer megtervezésekor, mind az adatfeldolgozás időpontjában") a biztonság fenntartása, és ezáltal az engedély nélküli adatfeldolgozás megelőzése érdekében, figyelembe véve az adatfeldolgozással járó kockázatokat és az adatok természetét.

89. Ez a cikk azonban ezzel kapcsolatban is túlságosan általános, és pontosításra szorul. Nem határozza meg egyértelműen, hogy a közösségi hálózatokkal összefüggésben mit ért megfelelő technikai és szervezési intézkedésen. Ennélfogva a jelen helyzetet a jogbizonytalanság jellemzi, ami mind a szabályozók, mind pedig azon személyek számára problémát jelent, akiknek magánélete és személyes adatai nem részesülnek teljes körű védelemben.

90. A fentiek fényében az európai adatvédelmi biztos szorgalmazza, hogy a Bizottság készítsen olyan jogszabályt, amely minimális követelményként tartalmazza az adatvédelmi beállítások kötelező biztosítására vonatkozó általános előírást, és ezt pontosabb követelményekkel egészíti ki:

a) olyan beállítások biztosítása, amelyek révén a felhasználói profilhoz való hozzáférés a felhasználó saját, általa kiválasztott ismerőseire korlátozható. A profil harmadik felek számára történő nyilvánossá tételét megelőzően a beállításoknál kérni kell a felhasználó megerősítő hozzájárulását.

b) annak előírása, hogy a korlátozott hozzáférésű profilokat a belső és a külső keresőmotorok számára is le kell tiltani.

91. Az alapértelmezett beállítások révén kötelezően biztosítandó adatvédelem mellett továbbra is kérdés, nem lennének-e szükségesek további konkrét adatvédelmi és egyéb intézkedések (például a kiskorúak védelmére vonatkozóan). Ez azt az átfogóbb kérdést is felveti, vajon megfelelő lenne-e az ilyen szolgáltatásokra vonatkozó speciális keret létrehozása, amely a kötelező adatvédelmi beállítások előírásán túl egyéb szempontokat is szabályozna. Az európai adatvédelmi biztos arra kéri a Bizottságot, hogy mérlegelje a kérdést.

VII. ALAPÉRTELMEZETT ADATVÉDELMI BÖNGÉSZŐBEÁLLÍTÁSOK A HIRDETÉSEK FOGADÁSÁRA VONATKOZÓ, TÁJÉKOZTATÁSON ALAPULÓ HOZZÁJÁRULÁS BIZTOSÍTÁSA ÉRDEKÉBEN

92. A hirdetési hálózatok szolgáltatói cookie-k és más eszközök használatával követik nyomon a felhasználók internetes böngészési szokásait annak érdekében, hogy rendszerezzék érdeklődési területeiket és profilokat alkossanak. Ezeket az információkat ezt követően arra használják, hogy célzott hirdetéseket juttassanak el hozzájuk ([4]).

VII.1. Fennmaradó kihívások és kockázatok az adatok és a magánélet védelmével kapcsolatos jelenlegi jogi keretben

93. Az ilyen típusú adatfeldolgozásról (személyes adatok érintettsége esetén) az adatvédelmi irányelv, valamint az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése rendelkezik. Az említett cikk kifejezetten előírja, hogy a felhasználót tájékoztatni kell, és lehetőséget kell biztosítani számára ahhoz, hogy a cookie-hoz hasonló eszközöknek a számítógépén vagy más készülékén történő tárolásához hozzájárulhasson vagy azt elutasíthassa ([5]).

94. Ez idáig a hirdetési hálózatok szolgáltatói a böngészőbeállításokon és az adatvédelmi irányelveken keresztül tájékoztatták a felhasználókat, és tették lehetővé számukra a cookie-k elfogadását vagy elutasítását. A megjelenítők

([1]) Viviane Reding, az Európai Bizottság információs társadalomért és médiáért felelős biztosa, Gondold meg, mit töltesz fel az internetre! Hogyan tehetők biztonságosabbá a közösségi weboldalak a gyermekek és a tinédzserek számára? A biztonságosabb internet napja, Strasbourg, 2010. február 9.

([2]) Az Európa Gazdasági és Szociális Bizottság véleménye a közösségi weboldalaknak a polgárokra/fogyasztókra gyakorolt hatásairól, 2009. november 4.

([3]) Lásd még bővebben e dokumentum 33. pontját.

([4]) A követési cookie-k egyedi azonosítót tartalmazó, kisméretű szövegfájlok. Általában a hirdetési hálózatok szolgáltatói (csakúgy, mint a webhelyek működtetői vagy a megjelenítők) cookie-kat helyeznek el a látogatók számítógépének merevlemezén, elsősorban az internetfelhasználók böngészőjében, amikor a felhasználók először nyitnak meg olyan oldalakat, amelyeken az ő hálózatukhoz tartozó hirdetések jelennek meg. A cookie lehetővé teszi a hirdetési szolgáltatónak, hogy felismerjen egy korábbi felhasználót, ha az visszatér a webhelyre vagy ellátogat a hirdetési hálózat bármely partnerwebhelyére. Az ilyen ismételt látogatások alapján a hirdetési hálózat szolgáltatója megalkothatja a látogató profilját.

([5]) Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdését a közelmúltban módosították, hogy megerősítsék a felhasználói közlések – például – a felhasználó számítógépén vagy más készülékén tárolt kémszoftverekkel vagy cookie-kal történő megfigyelésével szembeni védelmet. Az új irányelv értelmében a felhasználóknak megfelelőbb tájékoztatást kell nyújtani, és egyszerűbb módon kell biztosítani számukra, hogy beállíthassák, szeretnéke, hogy cookie-kat tároljanak végberendezésükön.

adatvédelmi irányelveiben ismertették, hogyan lehet teljes körűen letiltani a cookie-k fogadását, illetve eseti alapon elfogadni azokat. Mindezzel igyekeztek eleget tenni azon kötelezettségüknek, hogy biztosítsák a felhasználók számára a cookie-k elutasítását.

95. Míg elméletben ez a módszer (a böngészőn keresztül) valóban hatékony módon biztosítja a tartalmas és tájékoztatáson alapuló hozzájárulást, a valóság egészen más. A felhasználók általában nincsenek tisztában az adatgyűjtéssel kapcsolatos alapvető fogalmakkal, még kevésbé, ha az adatok harmadik féltől származnak, nem ismerik ezeknek az adatoknak az értékét, felhasználását, a technológia működését és pontosabban azt, hogyan és hol lehet letiltani azt. A letiltáshoz szükséges lépések a jelek szerint nem csupán bonyolultak, de túlzók is (a felhasználónak először be kell állítania a cookie-k elfogadását, majd ezután választhatja a letiltást).

96. Ennek eredményeképpen a gyakorlatban igen kevesen élnek a letiltás lehetőségével, nem azért, mert tájékoztatáson alapuló döntést hoztak arra vonatkozóan, hogy elfogadják a viselkedésalapú hirdetést, hanem azért, mert nem ismerik fel, hogy a letiltás elmulasztásával tulajdonképpen beleegyeznek abba.

97. Éppen ezért, míg jogi értelemben véve az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése hatékony jogi védelmet nyújt, addig a gyakorlatban úgy ítélik meg, hogy az internetfelhasználók hozzájárultak a viselkedésalapú hirdetések küldése céljából történő nyomon követéshez, pedig sok, ha nem a legtöbb esetben egyáltalán nincs tudomásuk a nyomon követésről.

98. A 29. cikk alapján létrehozott munkacsoport jelenleg véleményt készít, amelynek célja a viselkedésalapú hirdetési tevékenységben való részvételre vonatkozó jogi követelmények tisztázása, ami üdvözlendő. A jogértelmezés azonban önmagában feltehetően nem lesz elégendő e helyzet megoldásához, és az Európai Unió részéről további intézkedésekre lehet szükség.

VII.2. **A további fellépés szükségessége, nevezetesen a kötelező adatvédelem biztosítása az alapértelmezett beállítások segítségével**

99. A fenti leírásnak megfelelően az internetes böngészők bizonyos típusú cookie-k esetén jellemzően biztosítanak valamilyen szintű ellenőrzést. Alapértelmezett beállítás szerint jelenleg a legtöbb internetes böngésző valamennyi cookie-t elfogadja. Ez azt jelenti, hogy a böngészők alapértelmezett beállítás szerint minden cookie-t elfogadnak, függetlenül azok céljától. A felhasználó csak úgy állíthatja le a cookie-k fogadását, ha böngészőalkalmazása beállításainak módosításával letiltja a cookie-kat, amit, ahogyan az a fentiekből látható, nagyon kevesen tesznek meg. Ezenfelül a böngészőalkalmazások első telepített verziójában vagy frissítésében nem található adatvédelmi varázsló.

100. A fenti probléma enyhítésének egyik módja lehetne, ha a böngészőkben alapértelmezés szerint az adatok védelmét biztosító beállításokat adnák meg. Más szóval az, ha alapvetően a „harmadik féltől származó cookie-k letiltása” beállítást tartalmaznák. Ennek kiegészítéseként és a fokozott hatékonyság érdekében a böngésző annak első telepítésekor vagy frissítésekor kérhetné a felhasználókat, hogy kövessék végig egy adatvédelmi varázsló lépéseit. Részletesebb és egyértelműbb tájékoztatásra van szükség a cookie-k típusairól és bizonyos típusok hasznos jellegéről. Azokat a felhasználókat, akik szívesen engedélyezik a nyomon követést hirdetések fogadása céljából, megfelelő módon értesítenék, és meg kellene változtatniuk böngészőbeállításaikat. Így fokozottabb ellenőrzést gyakorolhatnának személyes adataik és magánéletük felett. Az európai adatvédelmi biztos véleménye szerint ez hatékony módja lenne a felhasználói hozzájárulás tiszteletben tartásának és megszerzésének ([1]).

101. Figyelembe véve egy részről, hogy a probléma széles körben tapasztalható, tehát jelenleg is számos internetfelhasználót követnek nyomon feltételezett hozzájárulás alapján, más részről pedig azt, milyen mértékű érdekek forognak kockán, egyre sürgetőbbé válik a további garanciák szükségessége. A beépített adatvédelem elvének érvényesítése az internetes böngészőalkalmazásokban drámai különbséget jelentene a tekintetben, hogy ellenőrzést biztosítana az egyéneknek a hirdetési célú adatgyűjtési gyakorlatok felett.

102. Ezen okokból az európai adatvédelmi biztos szorgalmazza, hogy a Bizottság mérlegeljen olyan jogszabályi intézkedéseket, amelyek a böngészőkben megkövetelik az alapértelmezett beállítások révén kötelezően biztosított adatvédelmet és a kapcsolódó tájékoztatásnyújtást.

VIII. **AZ EGYÉNEK MAGÁNÉLETÉNEK/ADATAINAK VÉDELMÉT CÉLZÓ TOVÁBBI ELVEK**

103. Míg a beépített adatvédelem elvében nagy lehetőségek rejlenek az egyének személyes adatai és magánélete védelmének tekintetében, az IKT iránti fogyasztói bizalom biztosítása érdekében kiegészítő elveket kell kidolgozni, és azokat jogszabályba kell foglalni. Ennek fényében az európai adatvédelmi biztos az elszámoltathatóság elvét és egy biztonsági jogsértésekre vonatkozó, valamennyi ágazatban egyaránt alkalmazandó kötelező keret kidolgozását javasolja.

VIII.1. **Az elszámoltathatóság elve a beépített adatvédelem elvének való megfelelés biztosítása érdekében**

104. A 29. cikk alapján létrehozott munkacsoport „A magánélet jövője” című dokumentumában ([2]) ajánlásként szerepel az elszámoltathatóság elvének az adatvédelmi

([1]) Ezzel egy időben az európai adatvédelmi biztos tisztában van vele, hogy ez nem oldja meg maradéktalanul a problémát, amennyiben vannak olyan cookie-k, például az ún. flash-cookie-k, amelyek a böngészőn keresztül nem szabályozhatók. Ilyen esetekre a böngészők fejlesztőinek az új böngészőverziókban alapértelmezés szerint biztosítaniuk kellene egy flash-szabályozót is a cookie-k ellenőrzési beállításai között.

([2]) A 29. cikk alapján létrehozott munkacsoport 2009. december 1-jén elfogadott 168. sz. véleménye: A magánélet jövője, Közös hozzájárulás az Európai Bizottság által a személyes adatok védelméhez való alapvető jogra vonatkozó jogi keretről folytatott konzultációhoz.

irányelvbe történő beépítése. Ez az elv, amelyet egyes multinacionális adatvédelmi eszközök [1] is elismernek, előírja a szervezetek számára, hogy a létező jogszabályoknak való megfelelés érdekében hajtsanak végre bizonyos folyamatokat, valamint dolgozzanak ki a jogszabálynak, illetve más kötelező érvényű eszközöknek való megfelelés vizsgálatára és kimutatására alkalmas módszereket.

105. Az európai adatvédelmi biztos teljes mértékben támogatja a 29. cikk alapján létrehozott munkacsoport ajánlását. Úgy ítéli meg, hogy ez az elv fokozottan releváns az adatvédelmi elvek és kötelezettségek hatékony alkalmazásának elősegítése szempontjából. Az elszámoltathatóság értelmében az adatkezelőknek bizonyítaniuk kell, hogy életbe léptették a vonatkozó adatvédelmi jogszabályoknak való megfeleléshez szükséges intézkedéseket. Ez várhatóan hozzájárul majd a beépített adatvédelemnek az IKT-technológiákban történő hatékony alkalmazásához, mivel az elv különösen alkalmas az elszámoltathatóság kimutatására.

106. Az elszámoltathatóság méréséhez és kimutatásához az adatkezelők használhatnak belső eljárásokat és fordulhatnak harmadik félhez is, aki könyvvizsgálatot vagy másfajta ellenőrzést és vizsgálatot végezhet, majd ezek alapján értékelheti a teljesítményt. Ebben az összefüggésben az európai adatvédelmi biztos felszólítja a Bizottságot, hogy mérlegelje, vajon az elszámoltathatóság általános elvén túl hasznos lenne-e jogszabályban előírni konkrét elszámoltathatósági intézkedéseket is, például a magánélet védelméről és az adatvédelemről készített hatásvizsgálatot, és ha igen, milyen körülmények esetén.

VIII.2. **Biztonsági jogsértés: a jogi keret kidolgozása**

107. Az elektronikus hírközlési adatvédelmi irányelv elmúlt évi módosítása bevezette azt a követelményt, hogy az érintett egyéneket, valamint az illetékes nemzeti hatóságokat értesíteni kell az adatok megsértéséről. Az adatok megsértése általános meghatározás szerint olyan jogsértés, amely a valamely szolgáltatással összefüggésben továbbított, tárolt vagy más módon feldolgozott személyes adatok megsemmisítését, elveszítését, felfedését stb. eredményezi. Az érintett személyt akkor kell értesíteni, ha az adatok megsértése valószínűleg hátrányosan befolyásolja személyes adatait vagy magánéletét. Ez akkor fordulhat elő, ha a jogsértés a személyazonossággal való visszaélést, durva sértést vagy hírnévrontást von maga után. Az illetékes hatóságokat valamennyi adatsértési eset alkalmával értesíteni kell, függetlenül attól, hogy az az egyénre nézve kockázatot jelent-e.

A biztonság megsértésével kapcsolatos kötelezettségek alkalmazása valamennyi ágazatban

108. Sajnálatos módon ez a kötelezettség csak a nyilvánosan elérhető hírközlési szolgáltatások szolgáltatóira, például telefonszolgáltatókra, internetszolgáltatókra, e-mailszolgáltatókra stb. vonatkozik. Az európai adatvédelmi biztos felszólítja a Bizottságot, hogy tegyen javaslatot a biztonsági jogsértések valamennyi ágazatban történő alkalmazására. Az említett keret tartalmát illetően az európai adatvédelmi biztos úgy ítéli meg, hogy a biztonság megsértésével kapcsolatos, az elektronikus hírközlési adatvédelmi irányelvben elfogadott jogi keret megfelelő egyensúlyt teremt az egyének jogai, ideértve személyes adataikhoz és a magánélethez való jogukat is, valamint az érintett felek számára előírt kötelezettségek között. Ez a keret ugyanakkor tényleges erővel bír, mivel tartalmas végrehajtó rendelkezések támasztják alá, amelyek a megfelelés elmulasztása esetén kellő hatáskörrel ruházzák fel a hatóságokat a vizsgálat és a szankciók tekintetében.

109. Ennek megfelelően az európai adatvédelmi biztos szorgalmazza, hogy a Bizottság fogadjon el egy olyan jogszabályjavaslatot, amely – szükség esetén a megfelelő módosításokkal – valamennyi ágazatban előírja e keret alkalmazását. A javaslat továbbá biztosítaná, hogy valamennyi ágazaton belül azonos szabványok és eljárások érvényesüljenek.

Az elektronikus hírközlési adatvédelmi irányelvben foglalt jogi keret kiegészítése komitológiai eljárás révén

110. A felülvizsgált elektronikus hírközlési adatvédelmi irányelv felhatalmazza a Bizottságot, hogy komitológiai eljárás során műszaki végrehajtási intézkedéseket, vagyis részletes intézkedéseket fogadjon el a biztonsági jogsértésekkel kapcsolatos tájékoztatásra vonatkozóan [2]. A felhatalmazást az indokolja, hogy ezáltal biztosítható a biztonsági jogsértések jogi keretének következetes végrehajtása és alkalmazása. A következetes végrehajtás eredményeképpen az egyének az egész Közösségben ugyanolyan magas szintű védelmet élvezhetnek majd, és az érintett szervezeteket nem terhelik eltérő tájékoztatási követelmények.

111. Az elektronikus hírközlési adatvédelmi irányelvet 2009 novemberében fogadták el. A jelek szerint semmi nem indokolja a műszaki végrehajtási intézkedések elfogadását célzó munka további halogatását. Az európai adatvédelmi biztos két szemináriumot szervezett, amelyek célja az adatsértésekre vonatkozó értesítésekkel kapcsolatos tapasztalatok összegyűjtése és megosztása volt. E gyakorlat eredményeit másokkal is örömmel megosztaná, és nagy várakozással tekint a Bizottsággal, illetve más érdekeltekkel történő, az adatsértések átfogó jogi keretének pontosítását célzó együttműködés elébe.

112. Az európai adatvédelmi biztos szorgalmazza, hogy a Bizottság rövid időn belül tegye meg a szükséges lépéseket. A műszaki végrehajtási intézkedések elfogadását megelőzően széles körű konzultációt kell szerveznie, amelyben az Európai Hálózat- és Információbiztonsági Ügynökség, az európai adatvédelmi biztos és a 29. cikk alapján létrehozott munkacsoport véleményét is ki kell kérnie. Továbbá a konzultációba más „érdekelt feleket” is be kell vonnia, különösen annak érdekében, hogy tájékozódjon az e cikk végrehajtását javító, rendelkezésre álló legjobb gazdasági és technikai megoldásokról.

[1] Az OECD 1980. évi ajánlása a magánélet védelmét és a személyes adatok határátlépő áramlását szabályozó irányelvekre; Madridi Adatvédelmi Nyilatkozat: Globális adatvédelmi szabványok egy globális világ számára, 2009. november 3.

[2] A komitológiai eljárás során a műszaki végrehajtási intézkedéseket a Bizottság által elnökölt, a tagállamok képviselőiből álló bizottság fogadja el. Az elektronikus hírközlési adatvédelmi irányelv esetében az úgynevezett ellenőrzéssel történő szabályozási eljárás alkalmazandó, ami azt jelenti, hogy az Európai Parlament, valamint a Tanács tiltakozhat a Bizottság által javasolt intézkedések ellen. A részletekért lásd: http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **KÖVETKEZTETÉSEK**

113. Megállapítást nyert, hogy az információs és kommunikációs technológiák megjelenését és sikeres alkalmazását érintő legfőbb probléma a bizalom, illetve annak hiánya. Ha az emberek nem bíznak az IKT-ban, ezek a technológiák kudarcra vannak ítélve. Az IKT iránti bizalom különböző tényezőktől függ; az egyik meghatározó tényező annak biztosítása, hogy az ilyen technológiák ne ássák alá az egyének magánélethez és személyes adataik védelméhez való alapvető jogát.

114. Az adatvédelemmel és a magánélet védelmével kapcsolatos jogi keret további erősítése érdekében, amelynek elvei az információs társadalomban is maradéktalanul érvényesek, az európai adatvédelmi biztos azt javasolja, hogy a Bizottság a jogalkotás és a döntéshozatal különböző szintjein alkalmazza a beépített adatvédelem elvét.

115. Az alábbi négy intézkedési lehetőséget javasolja a Bizottság számára:

a) Tegyen javaslatot egy, a beépített adatvédelemre vonatkozó általános rendelkezésnek az adatvédelemmel kapcsolatos jogi keretbe történő beépítésére. E rendelkezésnek technológiasemlegesnek kell lennie, és a megfelelést különböző szinteken kötelezővé kell tenni;

b) Ezt az általános rendelkezést olyan konkrét rendelkezések formájában dolgozza ki, amelyek révén a különböző ágazatok részére konkrét jogi eszközök javasolhatók. Az adatvédelmi irányelv (és más meglévő jogszabályok) alapján előfordulhat, hogy ezek a konkrét rendelkezések már jelenleg is részét képezik egyes jogi eszközöknek.

c) Vezérelvként foglalja bele a beépített adatvédelem elvét az európai digitális menetrendbe;

d) Vezesse be a beépített adatvédelem elvét más (elsősorban nem jogszabályi) európai uniós kezdeményezésekbe is.

116. Az európai adatvédelmi biztos három kijelölt IKT-területen azt javasolja, hogy a Bizottság vizsgálja meg, szükség van-e olyan javaslatok kidolgozására, amelyek különleges módon alkalmazzák a beépített adatvédelem elvét:

a) Az RFID-t illetően tegyen javaslatot az RFID felhasználásával kapcsolatos fő problémák szabályozására abban az esetben, ha a létező jogi keret önszabályozás útján történő hatékony végrehajtása kudarcot vall. Különösképpen biztosítsa az árusítás helyén történő hozzájárulás lehetőségét, amelynek értelmében az árusítás helyén a fogyasztási cikkeken található valamennyi RFID-címkét alapesetben hatástalanítanák;

b) A közösségi hálózatokat illetően készítsen olyan jogszabályt, amely minimális követelményként tartalmazza az adatvédelmi beállítások kötelező biztosítására vonatkozó általános előírást, és azt pontosabb követelményekkel egészíti ki a felhasználói profilokhoz való hozzáférésnek a felhasználó saját, általa kiválasztott ismerőseire történő korlátozására vonatkozóan, valamint előírva, hogy a korlátozott hozzáférésű profilokat a belső és a külső keresőmotorok számára is le kell tiltani;

c) A célzott hirdetési tevékenységgel kapcsolatban mérlegelje olyan jogszabály kidolgozását, amely engedélyezi, hogy a böngészőbeállítások alapesetben elutasítsák a harmadik féltől származó cookie-kat, valamint megköveteljék a felhasználótól, hogy a böngésző első telepítésekor vagy frissítésekor végigkövesse egy adatvédelmi varázsló lépéseit.

117. Végül, az európai adatvédelmi biztos javasolja, hogy a Bizottság:

a) mérlegelje az elszámoltathatóság elvének a meglévő adatvédelmi irányelvben történő alkalmazását; és

b) dolgozzon ki olyan szabályzati és eljárási keretet, amelynek alapján végrehajthatók az elektronikus hírközlési adatvédelmi irányelv biztonsági jogsértésekkel kapcsolatos tájékoztatásra vonatkozó rendelkezései, és általánosságban valamennyi adatkezelőre terjessze ki ezek hatályát.

Kelt Brüsszelben, 2010. március 18-án.

Peter HUSTINX

európai adatvédelmi biztos