I

(Állásfoglalások, ajánlások és vélemények)

VÉLEMÉNYEK

EURÓPAI ADATVÉDELMI BIZTOS

Az európai adatvédelmi biztos véleménye 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

(2008/C 181/01)

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 ([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,

tekintettel az Európai Bizottságtól 2007. november 16-án kapott, a 45/2001/EK rendelet 28. cikkének (2) bekezdése szerinti véleménykérésre,

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

I. **BEVEZETŐ**

1. A Bizottság 2007. november 13-án javaslatot fogadott el többek között az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv módosításáról (a továbbiakban: javaslat, illetve javasolt módosítások). A 2002/58/EK irányelv hatályos változatára ebben a véleményben is a megszokott módon, azaz mint az elektronikus hírközlési adatvédelmi irányelvre történik hivatkozás.

([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.

2. A javaslat célja, hogy az elektronikus hírközlési ágazatban fokozza az egyének magánéletének és személyes adatainak védelmét. A javaslat nem a jelenleg hatályos elektronikus hírközlési adatvédelmi irányelv teljes átformálásával kívánja mindezt elérni, hanem annak *ad hoc* módosításaival, melyek legfőképp a biztonsági vonatkozású rendelkezések megerősítésére és a végrehajtási mechanizmusok javítására irányulnak.

3. A javaslat az öt távközlési EU-irányelv („távközlési csomag") szélesebb körű reformjának a részét képezi. A távközlési csomag felülvizsgálatára vonatkozó javaslatokkal ([1]) egyidejűleg a Bizottság javaslatot fogadott el az Európai Elektronikus Hírközlési Piacfelügyeleti Hatóság létrehozásáról ([2]) is.

4. Az ezen véleményben megfogalmazott észrevételek kizárólag az elektronikus hírközlési adatvédelmi irányelv javasolt módosításaira vonatkoznak, kivéve, ha a javasolt módosítások a távközlési csomag felülvizsgálatára vonatkozó javaslatokban foglalt fogalmakra vagy rendelkezésekre épülnek. A véleményben foglalt egyes észrevételek ezenkívül utalnak az elektronikus hírközlési adatvédelmi irányelv olyan rendelkezéseire, amelyeket a javaslat nem módosít.

5. Ez a vélemény a következő témákat tárgyalja: i. az elektronikus hírközlési adatvédelmi irányelv alkalmazási köre, különösen az érintett szolgáltatások (a 3. cikk (1) bekezdésének javasolt módosítása); ii. a biztonság sérülésének bejelentése (a 4. cikk (3) és (4) bekezdésének létrehozására irányuló javasolt módosítás); iii. a cookie-kra, kémprogramokra és hasonló eszközökre vonatkozó rendelkezések (az 5. cikk (3) bekezdésének javasolt módosítása); iv. az elektronikus hírközlési szolgáltatók és egyéb jogi személyek által kezdeményezett jogi lépések (a 13. cikk (6) bekezdésének létrehozására irányuló javasolt módosítás) és v. a jogalkalmazási rendelkezések megerősítése (a 15a. cikk létrehozására irányuló javasolt módosítás).

Konzultáció az európai adatvédelmi biztossal és szélesebb körű nyilvános konzultáció

6. A Bizottság 2007. november 16-án küldte meg a javaslatot az európai adatvédelmi biztosnak. Az európai adatvédelmi biztos a javaslat elküldését arra való felkérésnek értelmezi, hogy adjon tanácsot a közösségi intézményeknek és szerveknek a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló 45/2001/EK rendelet (a továbbiakban: 45/2001/EK rendelet) 28. cikkének (2) bekezdésében előírtak szerint.

7. A javaslat elfogadását megelőzően a Bizottság a javaslattervezetről informálisan konzultált az európai adatvédelmi biztossal, amit az szívesen vett, mivel ez lehetővé tette számára, hogy még a javaslat Bizottság általi elfogadása előtt javaslatokat tegyen a tervezettel kapcsolatban. Az európai adatvédelmi biztos örömmel látja, hogy felvetéseinek egy része megjelenik a javaslatban.

8. A javaslat elfogadását széles körű nyilvános konzultáció előzte meg, amit az európai adatvédelmi biztos nagyra értékel. A Bizottság 2006. júniusában indított nyilvános konzultációt a távközlési csomag felülvizsgálatáról szóló közleményéről, amelyben ismertette a helyzetről kialakított véleményét és módosító javaslatokat tett ([3]). A 29. cikk alapján létrehozott adatvédelmi munkacsoport – melynek az európai adatvédelmi biztos is tagja – ennek kapcsán 2006. szeptember 26-án véleményt ([4]) fogadott el, melyben a javasolt módosításokra vonatkozó álláspontja olvasható.

([1]) A távközlési irányelvek javasolt módosításait a következő javaslatok tartalmazzák: i. Javaslat – Az Európai Parlament és a Tanács irányelve az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról szóló 2002/21/EK irányelv, az elektronikus hírközlő hálózatokhoz és kapcsolódó eszközökhöz való hozzáférésről, valamint azok összekapcsolásáról szóló 2002/19/EK irányelv és az elektronikus hírközlő hálózatok és az elektronikus hírközlési szolgáltatások engedélyezéséről szóló 2002/20/EK irányelv módosításáról, 2007. november 13., COM(2007) 697 végleges; ii. Javaslat – Az Európai Parlament és a Tanács irányelve az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi együttműködésről szóló 2006/2004/EK rendelet módosításáról, 2007. november 13., COM(2007) 698 végleges.

([2]) Javaslat – Az Európai Parlament és a Tanács rendelete az Európai Elektronikus Hírközlési Piacfelügyeleti Hatóság létrehozásáról, 2007. november 13., COM(2007) 699 végleges.

([3]) Közlemény az elektronikus hírközlési hálózatokra és szolgáltatásokra vonatkozó uniós szabályozási keretről (SEC(2006) 816), elfogadás: 2006. június 29. A közleményt a Bizottság szolgálatainak munkadokumentuma egészítette ki (COM(2006) 334 végleges).

([4]) 8/2006 sz. vélemény az elektronikus hírközlésre és szolgáltatásokra vonatkozó szabályozási keret felülvizsgálatáról, különös tekintettel az elektronikus hírközlési adatvédelmi irányelvre, elfogadás: 2006. szeptember 26.

Az európai adatvédelmi biztos általános véleménye

9. Az európai adatvédelmi biztos összességében kedvezően ítéli meg a javaslatot. A biztos teljes mértékben támogatja azokat a célokat, amelyeket a Bizottság e javaslat elfogadásával megvalósítani kíván, vagyis azt, hogy az elektronikus hírközlési ágazatban javuljon az egyének magánéletének és személyes adatainak védelme. A biztos különösen örvendetesnek tartja a biztonság sérülésére vonatkozó kötelező értesítési rendszer bevezetését (az elektronikus hírközlési adatvédelmi irányelv 4. cikkének módosítása a (3) és (4) bekezdés beillesztésével). Adatfeltörés esetén az értesítés egyértelmű előnyökkel jár, hiszen növeli a szervezetek elszámoltathatóságát, a vállalatokat szigorúbb biztonsági intézkedések alkalmazására ösztönzi, és lehetővé teszi a legmegbízhatóbb adatvédelmi technológiák megtalálását. Ezen túlmenően lehetővé teszi az érintett személyek számára, hogy lépéseket tegyenek annak érdekében, hogy megvédjék magukat személyazonosságuk eltulajdonításával, illetve a személyes adataikkal való visszaélés egyéb formáival szemben.

10. A biztos más javasolt módosításokat is örvendetesnek tart, például azt, hogy a jogos érdekkel rendelkező jogi személyek jogi eljárást indíthatnak azokkal szemben, akik megsértik az elektronikus hírközlési adatvédelmi irányelv egyes rendelkezéseit (a 13. cikk módosítása a (6) bekezdés beillesztésével). Örvendetes továbbá a nemzeti szabályozó hatóságok vizsgálati jogkörének megerősítése, mivel ez alapján megvizsgálhatják, hogy egy adott adatfeldolgozás a jogszabályoknak megfelelően történik-e, valamint azonosítani tudják a jogsértőket (a 15a. cikk (3) bekezdésének beillesztése). Ahhoz, hogy érvényesüljön az egyének jogainak és szabadságainak védelme, képesnek kell lenni a személyes adatok jogellenes feldolgozásának és a magánélet megsértésének felszámolására. Éppen ezért rendkívül üdvözlendő a 15a. cikk javasolt (2) bekezdése, amely a jogsértések megszüntetésének elrendeléséhez szükséges jogkörrel ruházza fel a nemzeti szabályozó hatóságokat, melyek ezáltal a súlyosan jogellenes adatfeldolgozást azonnal le tudják állítani.

11. A javaslatban követett megközelítés és a javasolt módosítások többsége összhangban áll a jövőbeli adatvédelmi politikára vonatkozó elképzelésekkel, amelyeket az európai adatvédelmi biztos korábbi véleményeiben, például az adatvédelmi irányelv végrehajtásáról szóló véleményében ([1]) körvonalazott. A megközelítés alapja többek között az a nézet, hogy bár új adatvédelmi elvek nem szükségesek, szükség van azonban részletesebb szabályokra az új technológiák – például az Internet, a rádiófrekvenciás azonosítás (RFID) stb. – által felvetett adatvédelmi kérdések kezeléséhez, továbbá olyan eszközökre, amelyek hozzájárulnak az adatvédelmi jogszabályok érvényesítéséhez és eredményessé tételéhez, például azáltal, hogy e jogszabályok alapján a jogalanyok eljárást kezdeményezhetnek az adatvédelmi előírások megsértése esetén, valamint hogy az adatkezelők kötelesek bejelentést tenni a biztonság sérüléséről.

12. A javaslatban követett megközelítés összességében kedvező megítélése ellenére az európai adatvédelmi biztos sajnálja, hogy a javaslat a lehetségesnél kevésbé célratörő. Ismert, hogy az elektronikus hírközlési adatvédelmi irányelv rendelkezéseinek 2003 óta tartó alkalmazása, valamint a témáról készített alapos elemzés is azt mutatta, hogy az irányelv egyes rendelkezései meglehetősen homályosak, ami jogbizonytalanságot és nehéz betarthatóságot okoz. Nem egyértelmű például, hogy az elektronikus hírközlési szolgáltatásokat nyújtó, félig állami szolgáltatókra milyen mértékben vonatkozik az irányelv. Egyes nyitott problémák megoldása érdekében a Bizottság meríthetett volna a távközlési csomag, különösen az elektronikus hírközlési adatvédelmi irányelv felülvizsgálatának eredményeiből. Ezenfelül a javaslat az újabb kérdések – többek között a biztonság sérülésére vonatkozó kötelező értesítési rendszer kialakítása – terén csak részleges megoldásokat kínál, mivel a biztonság sérülésének bejelentésére kötelezett szervezetek körébe nem vonja be az olyan szervezeteket, amelyek rendkívül érzékeny adattípusokat dolgoznak fel, mint például az online működő bankokat vagy egészségügyi szolgáltatókat. Az európai adatvédelmi biztos sajnálatosnak tartja ezt a megközelítést.

13. A biztos reméli, hogy a jogalkotási folyamat során a jogalkotó figyelembe veszi a javaslatra vonatkozóan e véleményben tett észrevételeket és javaslatokat, és kitér azokra a kérdésekre, amelyek a bizottsági javaslatból kimaradtak.

([1]) Az európai adatvédelmi biztos 2007. július 25-i véleménye 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.).

II. A JAVASLAT ELEMZÉSE

II.1. Az elektronikus hírközlési adatvédelmi irányelv alkalmazási köre, különös tekintettel az érintett szolgáltatásokra

14. A hatályos elektronikus hírközlési adatvédelmi irányelvvel kapcsolatban az egyik legfőbb kérdés az alkalmazási köre. A javaslat egyes elemei kísérletet tesznek a javaslat alkalmazási körének meghatározására és pontosítására, különösen az irányelv hatálya alá tartozó szolgáltatások tekintetében; ezt az alábbi i. alpont tárgyalja. Sajnálatos módon a javasolt módosítások nem nyújtanak megoldást a fennálló problémák mindegyikére. A lenti ii. alpontban leírtaknak megfelelően a módosítások sajnos nem terjesztik ki az irányelv alkalmazási körét a magánhálózatokban nyújtott elektronikus hírközlési szolgáltatásokra.

15. Az elektronikus hírközlési adatvédelmi irányelv 3. cikke megadja az érintett szolgáltatások körét, vagyis azt, hogy az irányelvben előírt kötelezettségek mely szolgáltatásokra vonatkoznak: „*Ezt az irányelvet (…) a nyilvánosan elérhető hírközlési szolgáltatások nyilvános hírközlő hálózaton történő nyújtásával összefüggő személyes adatok kezelésére kell alkalmazni*.”.

16. Az elektronikus hírközlési adatvédelmi irányelv hatálya alá tartozó szolgáltatások körébe tehát a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyilvános hálózaton keresztül nyújtó szolgáltatók („PPECS”) tartoznak. A PPECS fogalmát a keretirányelv ([1]) 2. cikkének c) pontja határozza meg. A nyilvános hírközlő hálózat fogalmát a keretirányelv 2. cikkének d) pontja határozza meg ([2]). PPECS-k által végzett tevékenység például az internet-hozzáférést nyújtó szolgáltatás, az elektronikus hírközlő hálózaton való adattovábbítás, a mobil- és telefonhálózatokra való csatlakozás stb.

i. *Az elektronikus hírközlési adatvédelmi irányelv 3. cikkére vonatkozó javasolt módosítás: Az érintett szolgáltatások körébe tartozzanak bele az adatgyűjtést és az azonosító eszközöket támogató nyilvános hírközlő hálózatok*

17. A javaslat annyiban módosítja az elektronikus hírközlési adatvédelmi irányelv 3. cikkét, hogy kimondja, hogy a nyilvános elektronikus hírközlő hálózatok körébe beletartoznak „*az adatgyűjtést és az azonosító eszközöket támogató nyilvános hírközlő hálózatok*”. A (28) preambulumbekezdés szerint az adatgyűjtésre, többek között személyes adatok gyűjtésére alkalmas, rádiófrekvencián alapuló alkalmazások – mint például a rádiófrekvenciás azonosítók – kifejlesztése az elektronikus hírközlési adatvédelmi irányelv hatálya alá kell hogy tartozzon, amennyiben ezek az alkalmazások nyilvános hírközlő hálózatokra kapcsolódnak, illetve nyilvános hírközlési szolgáltatásokat vesznek igénybe.

18. Az európai adatvédelmi biztos kedvezően ítéli meg ezt a rendelkezést, mivel az világossá teszi, hogy számos RFID-alkalmazás az elektronikus hírközlési adatvédelmi irányelv hatálya alá tartozik, ezáltal csökkenti az ehhez kapcsolódó bizonytalanságot, valamint határozottan megszünteti a jogszabályok félreértésének vagy félreértelmezésének lehetőségét.

19. A hatályos elektronikus hírközlési adatvédelmi irányelv 3. cikke értelmében már jelenleg is az irányelv hatálya alá tartoznak bizonyos RFID-alkalmazások. Ennek több összefüggő oka is van. Először is, az RFID-alkalmazások beletartoznak az elektronikus hírközlési szolgáltatások fogalmába. Másodsorban, ezeket az alkalmazásokat elektronikus hírközlő hálózatokon keresztül működtetik annyiban, hogy az alkalmazásokat olyan átviteli rendszer támogatja, amely a jeleket vezeték nélküli módon továbbítja.

([1]) Az Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról (HL L 108., 2002.4.24., 33. o.). A keretirányelv meghatározza, hogy mi értendő elektronikus hírközlő szolgáltatáson, nevezetesen: i. „elektronikus hírközlési szolgáltatás”: olyan, általában díjazás ellenében nyújtott szolgáltatás, amely hálózaton történő jelátvitelből áll, beleértve a műsorterjesztő hálózatokon nyújtott távközlési szolgáltatásokat és átviteli szolgáltatásokat is. ii. Az elektronikus hírközlési szolgáltatások fogalmába nem tartozik bele az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások segítségével történő tartalomszolgáltatás. iii. A szolgáltatásnyújtás hálózat létrehozását, üzemeltetését, ellenőrzését, illetve rendelkezésre bocsátását jelenti. iv. Az elektronikus hírközlési szolgáltatások körébe nem tartoznak bele az e-kereskedelmi irányelvben szolgáltatás(ok)ként meghatározott, információs társadalommal összefüggő szolgáltatások, vagyis az általában térítés ellenében, elektronikus úton, a szolgáltatást igénybe vevő egyéni kérelmére nyújtott távszolgáltatások.

([2]) „Nyilvános hírközlő hálózat”: teljes egészében vagy nagyrészt nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtására használt elektronikus hírközlő hálózat.

Végül, a hálózat lehet akár nyilvános, akár magánhálózat is. Ha nyilvános hálózatról van szó, az RFID-alkalmazások „érintett szolgáltatásnak" tekintendők, és az elektronikus hírközlési adatvédelmi irányelv hatálya alá tartoznak. Mindenesetre a javasolt módosítás az eddigi kétségeket eloszlatja, és nagyobb jogbiztonságot teremt.

20. Természetesen – amint azt a biztos a rádiófrekvenciás azonosításról szóló korábbi véleményében ([1]) is kifejtette – ez a rendelkezés nem zárja ki annak lehetőségét, hogy az RFID vonatkozásában további jogi eszközök hatályba léptetése válik szükségessé. Azonban az ilyen intézkedések elfogadása nem e javaslat keretébe tartozik.

ii. *Az irányelv alkalmazási köre kiterjesztésének szükségessége a magánhálózatokban vagy félmagán hálózatokban nyújtott elektronikus hírközlési szolgáltatásokra*

21. Jóllehet az európai adatvédelmi biztos örvendetesnek tartja az irányelv hatályának fent leírt tisztázását, sajnálatosnak tartja, hogy a javaslat nem foglalkozik a magánhálózatok és nyilvános hálózatok közötti, egyre elmosódóbb különbségtétellel. A biztos sajnálatosnak tartja továbbá, hogy az elektronikus hírközlési adatvédelmi irányelv hatálya alá tartozó szolgáltatások fogalommeghatározását a javaslat nem terjeszti ki a magánhálózatokra. Az elektronikus hírközlési adatvédelmi irányelv 3. cikkének (1) bekezdése jelenleg csak *a nyilvános hálózatokon keresztül történő elektronikus hírközlési szolgáltatások*ra vonatkozik.

22. A biztos megjegyzi, hogy a mai tendencia szerint a szolgáltatások egyre inkább magán- és közszolgáltatások keverékei. Erre példa, hogy az egyetemek diákok ezrei számára teszik lehetővé az internet és e-mail használatát. Ezek a részben nyilvános (vagy részben magán-) hálózatok egyértelműen sérthetik az egyének magánéletét, és ezért az ilyen típusú szolgáltatásokra ugyanazokat a szabályokat kell alkalmazni, mint a tisztán nyilvános hálózatokra. Ezen túlmenően az olyan magánhálózatok, mint amilyeneket a munkáltatók alkalmazottaik részére internet-hozzáférés céljából vagy a hotelek és lakástulajdonosok vendégeik részére telefonálás és e-mailezés céljából biztosítanak, továbbá az internetkávézók által működtetett magánhálózatok hatással vannak a felhasználók adatainak és magánéletének védelmére, aminek következtében az elektronikus hírközlési adatvédelmi irányelv alkalmazási körét ezen hálózatokra is ki kellene terjeszteni.

23. Egyes tagállamok esetjoga már eddig is azonos kötelezettségeket rótt a magánhálózatban, illetve a nyilvános hálózatban nyújtott elektronikus hírközlési szolgáltatásokra ([2]). A német jog alapján az adatvédelmi hatóságok szintén azt a megállapítást tették, hogy ha egy cégen belül lehetővé teszik a magán e-mail használatát, akkor a céget úgy lehet tekinteni, mint amely nyilvános távközlési szolgáltatást nyújt, és amelyre ezáltal vonatkoznak az elektronikus hírközlési adatvédelmi irányelv rendelkezései.

24. Összefoglalva, a vegyes (magán/nyilvános) és magánhálózatok egyre nagyobb mindennapi jelentősége – és ezzel egyidejűleg a személyes adatok és a magánélet egyre jelentősebb veszélyeztetettsége – indokolttá teszi, hogy e szolgáltatásokra ugyanazok a szabályok vonatkozzanak, mint a nyilvános elektronikus hírközlési szolgáltatásokra. Az európai adatvédelmi biztos éppen ezért úgy véli, hogy az irányelvet módosítani kell abból a célból, hogy hatálya a magánszolgáltatásokra is kiterjedjen; ezzel a nézettel a 29. cikk alapján létrehozott munkacsoport is egyetért ([3]).

II.2. **A biztonság sérülésének bejelentése: a 4. cikk módosítása**

25. Az elektronikus hírközlési adatvédelmi irányelv 4. cikke két új, a (3) és a (4) bekezdéssel egészül ki, melyek a biztonság sérülésének bejelentési kötelezettségét állapítják meg. A 4. cikk (3) bekezdése értelmében a biztonság olyan megsértése esetén, amely a hírközlési szolgáltatások nyújtásával összefüggésben továbbított, tárolt vagy más módon feldolgozott személyes adatok véletlen vagy jogellenes megsemmisítését, elveszítését, módosítását, jogosulatlan felfedését vagy az azokhoz való jogosulatlan hozzáférést eredményezi (együttesen: az adatok sérülése), a szolgáltatónak (PPECS) kötelessége egyrészt a nemzeti szabályozó hatóságot indokolatlan késedelem nélkül értesíteni, kötelessége másrészt a fogyasztókat is értesíteni.

([1]) Az európai adatvédelmi biztos véleménye (2007. december 20.) 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" című, COM(2007) 96 bizottsági közleményről.

([2]) A Párizsi Feljebbviteli Bíróságnak a *BNP Paribas* kontra *World Press Online* ügyben hozott, 2005. február 4-i ítélete például megállapította, hogy nincs különbség azon internetszolgáltatók között, akik piaci alapon nyújtottak internet-hozzáférést, illetve az alkalmazottaik részére internet-hozzáférést biztosító munkáltatók között.

([3]) 8/2006 sz. vélemény az elektronikus hírközlésre és szolgáltatásokra vonatkozó szabályozási keret felülvizsgálatáról, különös tekintettel az elektronikus hírközlési adatvédelmi irányelvre, elfogadás: 2006. szeptember 26.

Az említett kötelezettségből fakadó előnyök

26. Az európai adatvédelmi biztos üdvözli a biztonság sérülésének kötelező bejelentését bevezető rendelkezéseket (a 4. cikk (3) és (4) bekezdése). A biztonság sérülésének bejelentése kedvező hatással van a személyes adatok és a magánélet védelmére; az Egyesült Államokban már gyűjtöttek tapasztalatokat erre vonatkozóan, hiszen ott az államok szintjén már évek óta érvényben vannak a biztonság sérülésének bejelentésére vonatkozó jogszabályok.

27. Először is, a biztonság sérülésének bejelentésére vonatkozó jogszabályok révén nő a szolgáltatók elszámoltathatósága a sérült adatok tekintetében. Az adatvédelmi politika, illetve a magánélet védelmével kapcsolatos politika keretében az elszámoltathatóság azt jelenti, hogy minden egyes szervezet felelősséggel tartozik az általa gondozott és kezelt adatokért. A bejelentési kötelezettség újbóli megerősítését jelenti egyrészt annak, hogy a sérült adatokat a szolgáltató kezelte, másrészt annak, hogy az érintett szervezett felelőssége, hogy megtegye a szükséges intézkedéseket az ilyen adatok tekintetében.

28. Másodsorban, a biztonság sérülésének bejelentési kötelezettsége olyan tényezőnek bizonyult, amely a személyes adatokat feldolgozó szervezeteket biztonsági beruházásokra ösztönzi. Valójában önmagában az a tény, hogy a biztonság sérülését nyilvánosan be kell jelenteni, arra indítja a szervezeteket, hogy szigorúbb biztonsági előírásokat alkalmazzanak a személyes adatok védelmére és az adatok sérülésének megakadályozására. A biztonság sérülésének bejelentése ezenfelül hozzájárul a legeredményesebb biztonsági megoldások és mechanizmusok megtalálásához és az azokra vonatkozó megbízható statisztikai elemzések elkészítéséhez. Az adatbiztonság sérüléséről és a legmegfelelőbb adatvédelmi technológiákról sokáig nem állt rendelkezésre kellő számú megerősített adat. Ezt a problémát könnyen orvosolhatja a biztonság sérülésének bejelentési kötelezettsége, amint ez az USA-ban is történt a biztonság sérülésének bejelentésére vonatkozó jogszabályoknak köszönhetően, mivel a bejelentések információt szolgáltatnak arról, hogy mely technológiák kedveznek jobban az adatok sérülésének ([1]).

29. Végezetül, a biztonság sérülésének bejelentése ráébreszti az egyéneket arra, hogy személyes adataik sérülése milyen kockázatokkal jár, és segít abban, hogy a kockázatok csökkentésére megtegyék a szükséges intézkedéseket. Banki adatok sérülése esetén például az erről tájékoztatott egyén dönthet úgy, hogy megváltoztatja a bankszámlájához való hozzáféréshez használt adatokat annak megakadályozása érdekében, hogy valaki ezen információkat megszerezze és jogellenes célokra felhasználja (ismert nevén: a személyazonosság eltulajdonítása). Összegezve, ez a kötelezettség csökkenti annak valószínűségét, hogy egyes személyek a személyazonosság eltulajdonításának essenek áldozatul, valamint segítheti az áldozatokat abban, hogy a probléma megoldása érdekében megtegyék a szükséges lépéseket.

A javasolt módosítás hiányossága

30. Habár az európai adatvédelmi biztos örvendetesnek tartja a biztonság sérülésének bejelentésére vonatkozóan a 4. cikk (3) és (4) bekezdésében előírt rendszert, megfelelőbbnek tartotta volna, ha annak alkalmazási köre tágabb, és az információs társadalommal összefüggő szolgáltatásokat nyújtó szolgáltatókra is kiterjed. Ez azt jelentené, hogy a jogszabály az online bankokra, online vállalkozásokra, online egészségügyi szolgáltatókra stb. is kiterjedne ([2]).

31. Azok az indokok, amelyek alapján a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyilvános hálózaton keresztül nyújtó szolgáltatók („PPECS") a biztonság sérülésének bejelentésére kötelezhetők, egyéb szervezetek esetében is fennállnak, amelyek szintén jelentős mennyiségű olyan adatot dolgoznak fel, amelyek felfedése különösen sérelmes lehet az adatalanyok szempontjából. Ilyen szervezetek az online bankok, az adatkereskedők és más olyan online szolgáltatók, amelyek érzékeny adatokat (például egészségügyi, politikai nézetekre vonatkozó adatokat stb.) dolgoznak fel. Az online bankok és online vállalkozások által tárolt adatok sérülése – mely adatok között nem csak bankszámlaszámok, hanem hitelkártya-adatok is szerepelhetnek – előidézheti a személyazonosság eltulajdonítását, amiről az egyéneket feltétlenül tájékoztatni kell annak érdekében, hogy megtehessék a szükséges intézkedéseket. Az online egészségügyi szolgáltatások esetében az egyének ha pénzügyi kárt nem is szenvednek el, de nem gazdasági jellegű kár érheti őket az érzékeny adatok sérülése következtében.

([1]) Lásd Ross Anderson, Rainer Böhme, Richard Clayton és Tyler Moore „*Security Economics and the Internal Market*" című, az ENISA rendelésére készült jelentését.A jelentés elérhető az alábbi webcímen: http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Az információs társadalommal összefüggő szolgáltatásokat nyújtó szolgáltatók az e-kereskedelmi irányelv meghatározása szerint általában térítés ellenében, elektronikus úton, a szolgáltatást igénybe vevő egyéni kérelmére távszolgáltatás(ok)at nyújtanak.

32. Továbbá, a kötelezettek körének bővítése révén a kötelezettség teljesítésétől várt fent leírt előnyök nemcsak egy tevékenységi ágazatra – a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyilvános hálózaton keresztül nyújtó szolgáltatókra – korlátozódnak, hanem általánosságban érvényesülnek az információs társadalommal összefüggő szolgáltatások területén. Amennyiben a biztonság sérülésének bejelentési kötelezettsége az információs társadalommal összefüggő szolgáltatásokra, például az online bankokra is vonatkozna, az nem csupán e gazdasági szereplők elszámoltathatóságát növelné, hanem arra is ösztönözné őket, hogy fokozzák a biztonsági intézkedéseket, és ezáltal elkerüljék a biztonság jövőbeli sérülésének lehetőségét.

33. Az elektronikus hírközlési adatvédelmi irányelv már egyéb esetekben is vonatkozik a PPECS-ektől eltérő szervezetekre, például a közlések titkosságára vonatkozó 5. cikk és a kéretlen elektronikus levelekre vonatkozó 13. cikk esetében. Ez példázza, hogy a jogalkotó a múltban azt a bölcs döntést hozta, hogy az irányelv egyes rendelkezéseinek alkalmazási körét kibővíti, mivel az szükséges és megfelelő. Az európai adatvédelmi biztos reméli, hogy a jogalkotó ma is hasonlóan érzékeny és rugalmas megközelítést alkalmaz, és a 4. cikk alkalmazási körébe bevonja az információs társadalommal összefüggő szolgáltatásokat nyújtó szolgáltatókat is. Elegendő lenne, ha e célból a 4. cikk (3) bekezdése az információs társadalommal összefüggő szolgáltatásokat nyújtó szolgáltatókra való hivatkozással egészülne ki a következők szerint: „*A biztonság olyan megsértése esetén, amely (…) eredményezi, a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyújtó szolgáltatónak* és az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltatónak *a biztonság megsértéséről (…) értesítenie kell az érintett előfizetőt és a nemzeti szabályozó hatóságot*."

34. Az európai adatvédelmi biztos véleménye szerint ez a kötelezettség és annak mind a PPECS-ekre, mind az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltatókra való alkalmazása az első lépés lehet egy olyan fejlődési folyamatban, amelyben végül általánosságban valamennyi adatkezelő részt vesz.

A biztonság sérüléséhez kapcsolódó, a komitológia keretében kezelendő kérdésekre vonatkozó külön jogi keret

35. A javaslat a biztonság sérülésének bejelentési kötelezettségével kapcsolatos számos kérdésre nem ad választ. E kérdések közé tartoznak például a bejelentés körülményei, formája és az alkalmazandó eljárások. A javaslat 4. cikkének (4) bekezdése ehelyett az ilyen határozatok elfogadását egy „komitológiai" bizottságra ([1]), nevezetesen az 1999. június 28-i tanácsi határozat szerint a keretirányelv 22. cikkével létrehozott hírközlési bizottságra hagyja. Az ilyen intézkedések elfogadására konkrétan az 1999. június 28-i tanácsi határozat 5. cikkének megfelelően kerülne sor, amely „*az alap-jogiaktusok alapvető fontosságú rendelkezéseinek alkalmazására szolgáló általános hatályú intézkedések*" tekintetében meghatározza a szabályozási bizottsági eljárás szabályait.

36. Az európai adatvédelmi biztos nem ellenzi azt, hogy valamennyi ilyen kérdést a végrehajtási jogszabályok rendezzenek. A jogszabályok komitológia révén történő elfogadása általában lerövidíti a jogalkotási folyamatot. A komitológia ezenkívül hozzájárul a harmonizáció biztosításához, ami határozottan követendő cél.

37. Tekintettel arra, hogy a végrehajtási intézkedéseknek – amint az az alábbiakban részletesebben szerepel – nagy számú fontos kérdésre kell kiterjedniük, helyénvalónak tűnik, hogy e kérdésekkel együttesen, egyetlen jogszabály keretében foglalkozzanak, ne pedig szétdarabolva, úgy, hogy egyes kérdésekre az elektronikus hírközlési adatvédelmi irányelv, míg más kérdésekre a végrehajtási jogszabályok vonatkozzanak. Üdvözlendő tehát a Bizottság azon megközelítése, hogy az ilyen jellegű határozatokat az európai adatvédelmi biztossal – és remélhetőleg más érdekeltekkel – folytatott konzultációt követően, végrehajtási jogszabályok révén fogadja el.

A végrehajtási intézkedések révén kezelendő kérdések

38. A végrehajtási intézkedések jelentősége akkor mérhető fel, ha bizonyos részletességgel ismerjük azokat a kérdéseket, amelyeket ezen intézkedések révén kell kezelni. A végrehajtási intézkedések határozhatják meg például az értesítések elküldésére vonatkozó kötelező szabályokat. Meghatározzák például, hogy mi tekintendő a biztonság sérülésének, hogy milyen feltételeknek kell teljesülniük az egyének és a hatóságok értesítése tekintetében, valamint hogy milyen határidők vonatkoznak az értesítésre.

([1]) Az Európai Közösségek olyan jogalkotási eljárásai, amelyekben a tagállamok kormányainak köztisztviselői szintű képviselőiből álló bizottságok vesznek részt.

39. Az európai adatvédelmi biztos úgy véli, hogy az elektronikus hírközlési adatvédelmi irányelvnek, és különösen 4. cikkének nem szabadna kivételt biztosítania az értesítési kötelezettség alól. A biztos örvendetesnek tartja e tekintetben a Bizottság 4. cikkben tükröződő megközelítését, mivel e cikk értesítési kötelezettséget ír elő, és az alól nem biztosít kivételt, hanem e kérdés kezelését – egyebek mellett – a végrehajtási jogszabályokra bízza. Jóllehet a biztos ismeri azokat az érveket, amelyek indokolhatnák a kötelezettség alóli kivételek biztosítását, mégis megfelelőbbnek tartja, hogy ezzel és más kérdésekkel a végrehajtási jogszabályok foglalkozzanak behatóbban, az összes érintett kérdés alapos, átfogó megvitatását követően. Amint azt a fentiekben kifejtettük, a biztonság sérülésének bejelentési kötelezettségéhez kapcsolódó kérdések összetett jellege – többek között a kivételek és korlátozások megfelelőségének kérdése – indokolja azok egységes kezelését, vagyis azt, hogy azokat egyetlen, kizárólag ennek a kérdésnek szentelt jogszabály szabályozza.

Konzultáció az európai adatvédelmi biztossal és a konzultáció kiszélesítésének szükségessége

40. Tekintettel arra, hogy a végrehajtási intézkedések milyen mértékben befolyásolják majd az egyének személyes adatainak védelmét, fontos, hogy a Bizottság ezen intézkedések elfogadását megelőzően megfelelő konzultációs folyamatot folytasson le. Az európai adatvédelmi biztos ezért örvendetesnek tartja a javaslat 4. cikkének (4) bekezdését, amely kifejezetten kimondja, hogy a végrehajtási intézkedések elfogadását megelőzően a Bizottság konzultál az európai adatvédelmi biztossal. Az említett intézkedések nem csak egyszerűen érintik, hanem jelentősen befolyásolják az egyének személyes adatainak és magánéletének védelmét. Emiatt fontos az európai adatvédelmi biztos véleményét kikérni a 45/2001/EK rendelet 41. cikkében előírtaknak megfelelően.

41. Az európai adatvédelmi biztossal való konzultáción felül helyénvaló lehet egy olyan rendelkezés beillesztése, amely szerint a tervezett végrehajtási intézkedésekről nyilvános konzultációt kell folytatni a szakvélemények megismerése, valamint a tapasztalatok és a bevált gyakorlatok megosztásának ösztönzése érdekében. Ez nem csak az ágazat számára, hanem egyéb érdekeltek – például más adatvédelmi hatóságok és a 29. cikk alapján létrehozott munkacsoport – számára is megfelelő fórumot jelentene véleményük ismertetésére. A nyilvános konzultáció szükségessége még nyilvánvalóbb, ha figyelembe vesszük, hogy a jogszabályok elfogadására a komitológia révén kerül sor, tehát az Európai Parlament beleszólási lehetősége korlátozott.

42. Az európai adatvédelmi biztos tudomásul veszi, hogy a javaslat 4. cikkének (4) bekezdése értelmében a Bizottság a végrehajtási intézkedések elfogadását megelőzően az Európai Elektronikus Hírközlési Piacfelügyeleti Hatósággal is konzultál. A biztos nagyra értékeli az említett hatósággal – mint az ENISA hálózat- és adatbiztonság terén szerzett tapasztalatának és tudásának letéteményesével – való konzultáció elvét. Célszerűnek látszik, hogy a javasolt módosítás (a 4. cikk (4) bekezdése) az Európai Elektronikus Hírközlési Piacfelügyeleti Hatóság létrehozásáig átmeneti megoldásként az ENISA-val való konzultációt írja elő.

II.3. **A cookie-kra, kémprogramokra és hasonló eszközökre vonatkozó rendelkezések: Az 5. cikk (3) bekezdésének módosítása**

43. Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése azokra a technológiákra vonatkozik, amelyek – elektronikus hírközlő hálózatokon keresztül – lehetővé teszik a felhasználók végberendezésében található adatokhoz való hozzáférést és azok tárolását. Az 5. cikk (3) bekezdésének alkalmazására példa a cookie-k ([1]) használata. További példa az olyan technológiák, mint a kémprogramok (rejtett kémprogramok) vagy a trójai falovak (üzenetekben vagy más, látszólag ártalmatlan szoftverekben elrejtett programok) használata. Az ilyen technológiák rendkívül változatos célokat szolgálnak: egyesek teljesen ártalmatlanok, sőt akár hasznosak a felhasználó szempontjából, míg mások egyértelműen ártalmasak és veszélyeztetik a biztonságot.

([1]) A cookie-kat az információs társadalommal összefüggő szolgáltatásokat nyújtó szolgáltatók (webhelyek) helyezik el a felhasználók végberendezésében, különböző célokból, például azért, hogy az egyes webhelyek felismerjék a látogatót, ha az ismételten az oldalra látogat. A gyakorlatban ha egy webhely cookie-t küld az internetfelhasználó felé, akkor a felhasználó számítógépéhez egy egyedi szám rendelődik hozzá (pl. ha egy számítógépnek az „A" webhely cookie-t küld, a számítógép „a 111-es számú cookie birtokosa" lesz). A webhely ezt a számot referenciaként őrzi. Ha a 111-es számú cookie-val rendelkező számítógép felhasználója nem törli a cookie-t tartalmazó fájlt, akkor abban az esetben, ha legközelebb ugyanarra a webhelyre látogat, a webhely képes lesz felismerni a számítógépet mint a 111-es számú cookie birtokosát. A webhely természetesen levezeti ebből, hogy az adott számítógép előzőleg már ellátogatott az oldalra. Az a mechanizmus, melynek révén a webhelyek a számítógépeket mint ismételt látogatókat fel tudják ismerni, egyszerű. Ha az oldalra látogató számítógép rendelkezik cookie-val (pl. a 111-es számú cookie-val), és ellátogat arra az oldalra, amelyik egy korábbi látogatás alkalmával a cookie-t generálta, akkor a felhasználó merevlemezén elkezdi keresni a cookie-t tartalmazó fájl számát. Ha a felhasználó böngészője olyan, cookie-t tartalmazó fájlt talál, amelynek száma megegyezik a webhely által tárolt referenciaszámmal, értesíti a webhelyet, hogy a számítógép a 111-es számú cookie-val rendelkezik.

44. Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése meghatározza azokat a feltételeket, amelyek a fent említett technológiákat is alkalmazó felhasználói végberendezésekben található adatokhoz való hozzáférésre vagy azok tárolására vonatkoznak. Az 5. cikk (3) bekezdése szerint i. az internetfelhasználókat a 95/46/EK irányelvvel összhangban egyértelműen és teljes körűen tájékoztatni kell – többek között – az adatfeldolgozás céljairól; valamint ii. az internetfelhasználók számára biztosítani kell azt a jogot, hogy visszautasítsák az ilyen adatfeldolgozást, vagyis az általuk használt végberendezésből szerzett adatok feldolgozását.

A javasolt módosításból származó előnyök

45. Az elektronikus hírközlési adatvédelmi irányelv 5. cikkének jelenlegi (3) bekezdése kizárólag olyan helyzetekre alkalmazandó, amikor a felhasználói végberendezésekben található adatokhoz való hozzáférés és azok tárolása *elektronikus hírközlő hálózatokon* keresztül történik. Ebbe beletartoznak az olyan helyzetek is, mint a cookie-k fent leírt használata, valamint egyéb technológiák, például az elektronikus hírközlő hálózatokon keresztül érkező kémprogramok használata. Azonban egyáltalán nem egyértelmű, hogy az 5. cikk (3) bekezdése alkalmazandó-e olyan helyzetekre, amikor a felhasználói végberendezésre külső adattároló eszközön lévő szoftver tölti fel a fentiekhez hasonló technológiákat (cookie-k, kémprogramok stb.). Tekintettel arra, hogy a magánélet védelmének fenyegetettsége a hírközlő csatornáktól független, szerencsétlen megoldás lenne, ha az 5. cikk (3) bekezdése kizárólag egy hírközlő csatornára korlátozódna.

46. Az európai adatvédelmi biztos ezért üdvözli az 5. cikk (3) bekezdésének módosítását, amely az „elektronikus hírközlő hálózatok"-ra való utalás eltávolításával kibővíti az 5. cikk (3) bekezdésének alkalmazási körét. Az 5. cikk (3) bekezdésének módosított változata egyaránt felöleli azokat a helyzeteket, amikor a felhasználói végberendezésekben található információkhoz való hozzáférés és az adattárolás elektronikus hírközlő hálózatokon keresztül történik, és azokat, amikor ez más külső adattároló eszközön, pl. CD-ken, CD-ROM-okon, USB-kulcsokon stb. keresztül történik.

Műszaki tárolás a továbbítás megkönnyítése céljából

47. Az elektronikus hírközlési adatvédelmi irányelv 5. cikke (3) bekezdésének utolsó mondata nem változik a módosított változatban. Az utolsó mondat alapján az 5. cikk (3) bekezdésének első mondatában foglalt követelmények nem akadályozzák *„az olyan műszaki tárolást, illetve műszaki hozzáférést, amelynek kizárólagos célja az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás vagy annak megkönnyítése, vagy amely az (…) információs társadalommal összefüggő szolgáltatás nyújtásához feltétlenül szükséges*". Ezért az 5. cikk (3) bekezdése első mondatának kötelező érvényű szabályai (a tájékoztatás szükségessége és a visszautasítás lehetősége) nem alkalmazandók, ha a felhasználó végberendezéséhez való hozzáférés vagy információtárolás egyedüli célja a továbbítás *megkönnyítése*, vagy ha az a felhasználó által kért, az információs társadalommal összefüggő szolgáltatások nyújtásához feltétlenül szükséges.

48. Az irányelv nem pontosítja, melyek azok az esetek, amikor az információhoz való hozzáférésnek vagy annak tárolásának egyedüli célja a továbbítás megkönnyítése vagy a tájékoztatás. Az egyik eset, amelyre nyilvánvalóan vonatkozik a kivétel, az internetcsatlakozás létrehozása. Az internetcsatlakozás létrehozásához ugyanis IP-címre van szükség ([1]). A végfelhasználó számítógépe kérést kap, hogy adjon meg magáról bizonyos információkat az internet-hozzáférést biztosító szolgáltatónak, ezért cserébe az internet-hozzáférést biztosító szolgáltató IP-címmel látja el az adott számítógépet. Ebben az esetben a végfelhasználó végberendezésében tárolt információ továbbításra kerül az internet-hozzáférést biztosító szolgáltató felé annak érdekében, hogy a felhasználó internet-hozzáférést kapjon. Ebben az esetben az internet-hozzáférést biztosító szolgáltató egyrészt nem köteles ezt az információgyűjtést bejelenteni, másrészt nem kell, hogy biztosítsa a visszautasítás jogát, mivel ez a szolgáltatás nyújtásához szükséges.

49. Ha az internethez való csatlakozást követően a felhasználó meg kíván tekinteni egy adott oldalt, el kell küldenie kérését a weblapot tároló szervernek. A szerver akkor fog válaszolni, ha tudja, hogy hova küldje az információt, azaz, ha ismeri a felhasználó IP-címét. Az IP-cím tárolásának módja miatt szükséges, hogy a felhasználó által megtekinteni kívánt weblap hozzáférjen az internethasználó végberendezésében tárolt információhoz. Természetesen ez a tranzakció is a kivételek közé tartozik. Indokoltnak tűnik, hogy az ilyen esetek ne tartozzanak az 5. cikk (3) bekezdésének alkalmazási körébe.

([1]) Az IP-cím (Internet Protocol) olyan egyedi cím, amelyet bizonyos elektronikus eszközök az egymással való kommunikációra használnak az Internet Protocol (IP) szabványt használó számítógépes hálózatokban – egyszerűbb szavakkal: egy számítógépes cím. Bármilyen résztvevő hálózati eszköz – routerek, kapcsolók, számítógépek, infrastruktúraszerverek (pl. NTP, DNS, DHCP, SNMP stb.), nyomtatók, internetes faxok és bizonyos telefonok – saját egyedi címmel rendelkezhet egy konkrét hálózat hatókörén belül. Néhány IP-cím a teljes internet hatókörén belül egyedinek számít, míg másoknak csak egy vállalkozás hatókörén belül kell egyedinek lennie.

50. Az európai adatvédelmi biztos indokoltnak véli, hogy a tájékoztatási kötelezettség és a visszautasítás lehetőségének biztosítása ne vonatkozzon a fentihez hasonló esetekre, amikor a műszaki tárolás vagy a felhasználó végberendezéséhez való hozzáférés kizárólag a közlésnek az elektronikus hírközlő hálózatokban való továbbításához *szükséges*. Ugyanez vonatkozik arra az esetre, ha a műszaki tárolás vagy a hozzáférés az információs társadalommal összefüggő szolgáltatás nyújtásához feltétlenül szükséges. Az európai adatvédelmi biztos szerint ugyanakkor nem kell kizárni a tájékoztatási kötelezettség és a visszautasítás lehetőségének biztosítása alól azokat a helyzeteket, amikor a műszaki tárolás vagy a hozzáférés célja pusztán a közlés továbbításának *megkönnyítése*. E cikk utolsó mondata alapján például az adatalany nem kap tájékoztatást, és nincs joga ellenezni adatainak feldolgozását, ha egy cookie összegyűjti a nyelvi preferenciájára vagy földrajzi elhelyezkedésére (pl. Belgium, Kína) vonatkozó információkat, mivel ezekről a cookie-król elmondható az is, hogy céljuk a közlés továbbításának megkönnyítése. Az európai adatvédelmi biztos tudatában van, hogy a szoftver szintjén az adatalanyoknak gyakorlatilag lehetőségük van visszautasítani vagy módosítani a cookie-k tárolását. Ugyanakkor ezt egyetlen jogi rendelkezés sem támasztja alá egyértelműen pl. azzal, hogy a fenti helyzetben hivatalosan felhatalmazza az adatalanyt jogai védelmére.

51. Ennek elkerülése érdekében az európai adatvédelmi biztos javasolja, hogy az 5. cikk (3) bekezdésének utolsó részében hajtsanak végre egy kisebb módosítást, azaz töröljék a mondatból a „megkönnyítése" szót: „*nem akadályozza az olyan műszaki tárolást, illetve műszaki hozzáférést, amelynek kizárólagos célja az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás vagy annak megkönnyítése, vagy amely az (…) információs társadalommal összefüggő szolgáltatás nyújtásához feltétlenül szükséges*".

II.4. **A nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyilvános hálózaton keresztül nyújtó szolgáltatók („PPECS") és egyéb jogi személyek által kezdeményezett jogi lépések: a 13. cikk (6) bekezdésének létrehozása**

52. A 13. cikk javasolt (6) bekezdése polgári jogorvoslatot biztosít a jogos érdekkel rendelkező magánszemélyek vagy jogi személyek számára, különösen az elektronikus hírközlési szolgáltatók számára, akiknek üzleti érdekében áll fellépni azokkal szemben, akik megsértik az elektronikus hírközlési adatvédelmi irányelv 13. cikkét. Ez a cikk foglalkozik a nem kívánt kereskedelmi tájékoztatás küldésével.

53. A javasolt módosítás lehetővé teszi, hogy például az internet-hozzáférést biztosító szolgáltatók felléphessenek a kéretlen elektronikus levelek küldőivel szemben a hálózatukkal való visszaélés miatt, és keresetet indítsanak a feladók címét hamisító vagy a feltört szervereket a kéretlen elektronikus levelek átjátszóiként (spam-relay) használó szervezetek ellen.

54. Nem világos, hogy az elektronikus hírközlési adatvédelmi irányelv feljogosítja-e a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyilvános hálózaton keresztül nyújtó szolgáltatókat („PPECS") arra, hogy pert indítsanak a kéretlen elektronikus levelek küldői ellen, és a szolgáltatók csak nagyon ritkán indítottak bírósági keresetet a tagállamok jogi szabályozásába átültetett 13. cikk megsértése miatt ([1]). Annak elismerésével, hogy az elektronikus hírközlési szolgáltatók pert indíthatnak üzleti érdekeik védelme érdekében, a javaslat megerősíti, hogy az elektronikus hírközlési adatvédelmi irányelv nem csupán az egyéni előfizetőket védi, hanem az elektronikus hírközlési szolgáltatókat is.

55. Az európai adatvédelmi biztos üdvözli, hogy a javaslat lehetőséget teremt arra, hogy az üzleti érdekkel rendelkező elektronikus hírközlési szolgáltatók pert indítsanak a kéretlen elektronikus levelek küldői ellen. Néhány kivételes esettől eltekintve az egyéni előfizetőknek se pénzük, se motivációjuk nincsen arra, hogy ilyen jellegű bírósági keresetet indítsanak. Az internet-hozzáférést biztosító szolgáltatóknak és más PPECS-eknek mind a pénzügyi, mind a technológiai feltételek rendelkezésükre állnak ahhoz, hogy vizsgálatot indítsanak a kéretlen elektronikus levelek küldői ellen és azonosítsák az elkövetőket, ezért indokoltnak tűnik, hogy jogosultak legyenek jogi lépéseket tenni a kéretlen elektronikus levelek küldői ellen.

56. Az európai adatvédelmi biztos különösen értékeli, hogy a javasolt módosítás a kéretlen elektronikus levelek címzettjei, azaz a fogyasztók érdekeit képviselő fogyasztói szervezetek és a szakszervezetek számára is lehetővé tenné, hogy a fogyasztók nevében keresetet indítsanak. A fentiek értelmében a kéretlen elektronikus levél címzettjeként szereplő adatalany által elszenvedett kár önmagában véve rendszerint nem elegendő ahhoz, hogy ő maga keresetet indítson. Az európai adatvédelmi biztos az adatvédelmi irányelv jobb végrehajtását célzó munkaprogram nyomon követéséről szóló

([1]) Ez történt a Microsoft corporation kontra Paul McDonald t/a Bizards UK (2006 All Er (D) 153) ügyben.

véleményében ([1]) már javasolta ezt az intézkedést a magánélet és az adatok védelmének általában vett megsértése kapcsán. Az európai adatvédelmi biztos véleménye szerint a javaslat tovább is mehetett volna, és olyan csoportos kereseteket is tartalmazhatott volna, amelyek polgárok csoportjai számára teszik lehetővé, hogy a személyes adatok védelmére vonatkozó ügyekben közösen élhessenek a per lehetőségével. A kéretlen elektronikus levelek esetében, ahol számos egyén megkapja a levelet, az egyéneknek lenne lehetőségük csoportokba tömörülni és keresetet indítani a kéretlen levelek küldőivel szemben.

57. Az európai adatvédelmi biztos különösen sajnálatosnak tartja, hogy a javaslat a jogi személyek által indítandó jogi lépéseket az olyan esetekre korlátozza, ahol az irányelv 13. cikke sérül, vagyis amikor a kéretlen elektronikus levelekről szóló rendelkezést megszegik. A javasolt módosítás alapján a jogi személyek nem tehetnek jogi lépéseket az elektronikus hírközlési adatvédelmi irányelv egyéb rendelkezéseinek sérelme esetén. A jelen rendelkezés nem jogosítja fel a jogi személyeket, például a fogyasztói szervezeteket arra, hogy jogi lépéseket tegyenek azon internet-hozzáférést biztosító szolgáltatók ellen, akik több millió ügyfél személyes adatait hozzák nyilvánosságra. Az elektronikus hírközlési adatvédelmi irányelv egészének és nem csak egy adott cikkének végrehajtása nagyban javulna, ha a 13. cikk (6) bekezdésében foglalt rendelkezés általánosabb lenne, és feljogosítaná a jogi személyeket, hogy az elektronikus hírközlési adatvédelmi irányelv bármely rendelkezésének megszegése esetén jogi lépéseket tegyenek.

58. E probléma megoldása érdekében az európai adatvédelmi biztos javasolja, hogy a 13. cikk (6) bekezdését alakítsák külön cikké (14. cikk). Ezenkívül javasolja a 13. cikk (6) bekezdése megfogalmazásának kis mértékű módosítását: „*az e cikk alapján*" helyett javasolja „az ezen irányelv alapján" megfogalmazást.

II.5. **A végrehajtási rendelkezések megerősítése: a 15a. cikk beillesztése**

59. Az elektronikus hírközlési adatvédelmi irányelv nem tartalmaz kifejezett végrehajtási rendelkezéseket. Ehelyett utal az adatvédelmi irányelv ([2]) végrehajtásról szóló szakaszára. Az európai adatvédelmi biztos üdvözli a javaslat új 15a. cikkét, amely kifejezetten az ezen irányelv végrehajtásának kérdéseivel foglalkozik.

60. Először is az európai adatvédelmi biztos megjegyzi, hogy az e területen való hatékony végrehajtási politika feltételezi – a javasolt 15a. cikk (3) bekezdése alapján –, hogy a nemzeti hatóságok rendelkeznek a szükséges információk összegyűjtéséhez szükséges vizsgálati jogkörrel. Az elektronikus hírközlési adatvédelmi irányelv rendelkezései megsértésének igen gyakran elektronikus jellegű bizonyíték van, amelyet különböző számítógépeken és eszközökön vagy hálózatokban tárolhatnak. Ebben az összefüggésben fontos, hogy a végrehajtó szervek rendelkezzenek olyan vizsgálati felhatalmazással, amely lehetővé teszi a belépést, a kutatást és a lefoglalást.

61. Másodszor, az európai adatvédelmi biztos különösen üdvözli a javasolt módosítást, azaz a 15a. cikk (2) bekezdését, mely alapján a nemzeti szabályozó hatóságoknak rendelkezniük kell a tiltó határozatok meghozatalához, vagyis a jogsértés megszüntetésének elrendeléséhez szükséges jogkörrel, valamint a szükséges vizsgálati jogkörrel és a szükséges forrásokkal. A nemzeti szabályozó hatóságoknak – beleértve a nemzeti adatvédelmi hatóságokat is – rendelkezniük kell a tiltó határozatok meghozatalához szükséges jogkörrel, amely alapján a bűncselekmény elkövetői beszüntetik az elektronikus hírközlési adatvédelmi irányelvet sértő tevékenységet. A tiltó határozatok vagy a jogsértés megszüntetésének elrendeléséhez szükséges jogkör hasznos eszközök az egyének jogainak folyamatban lévő, sorozatos megsértése esetén. A tiltó határozatok nagyon hasznosak továbbá az elektronikus hírközlési adatvédelmi irányelv megszegésének megakadályozásában, pl. a nem kívánt kereskedelmi tájékoztatásról szóló 13. cikk megszegése esetén, ami természeténél fogva egy folyamatban lévő magatartás.

62. Harmadsorban, a javaslat lehetővé teszi, hogy a Bizottság technikai végrehajtási intézkedéseket hozzon a nemzeti jogszabályok végrehajtása során való hatékony, határokon átnyúló együttműködés biztosítása érdekében (javasolt módosítás: 15a. cikk (4) bekezdés). Az eddigi együttműködés példája az a bizottsági kezdeményezésen alapuló megállapodás, melynek értelmében közös eljárást alakítanak ki a határokon átnyúló, nem kívánt elektronikus levelekkel kapcsolatos panaszok kezelésére.

([1]) Az európai adatvédelmi biztos véleménye 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.).

([2]) Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról.

63. Az európai adatvédelmi biztos szerint, ha a jogszabály támogatja, hogy a szabályozók együttműködjenek a más országbeli partnerszervezetekkel, akkor ez kétségtelenül megkönnyíti majd a határokon átnyúló végrehajtást. Ezért helyénvaló, hogy a javaslat felhatalmazza a Bizottságot, hogy teremtse meg a határokon átnyúló együttműködés biztosításának feltételeit, beleértve az információk megosztására szolgáló eljárásokat is.

III. **KÖVETKEZTETÉSEK ÉS AJÁNLÁSOK**

64. Az európai adatvédelmi biztos kifejezetten üdvözli a javaslatot. A javasolt módosítások megerősítik a hírközlési ágazatban az egyének magánéletének és személyes adatainak védelmét, és mindezt egyszerűen, anélkül, hogy indokolatlan és felesleges terheket rónának a szervezetekre. Konkrétabban, az európai adatvédelmi biztos úgy véli, hogy a javasolt módosítások többségét nem kell megváltoztatni, mivel megfelelően teljesítik kitűzött céljukat. Az alább következő 69. pont felsorolja azokat a módosításokat, amelyek az európai adatvédelmi biztos reményei szerint változatlanok maradnak.

65. A javaslat általánosan kedvező fogadtatása ellenére az európai adatvédelmi biztos úgy gondolja, hogy néhány módosítást javítani kellene annak érdekében, hogy hatékonyan járuljanak hozzá az egyének személyes adatainak és magánéletének megfelelő védelméhez. Ez különösen igaz a biztonság sérülésének bejelentésére és azokra, akik az elektronikus hírközlési szolgáltatók által a nem kívánt elektronikus levelekkel kapcsolatos rendelkezések megsértése miatt kezdeményezett jogi lépésekkel foglalkoznak. Ezen kívül az európai adatvédelmi biztos sajnálatosnak tartja, hogy a javaslat nem old meg néhány, a jelenlegi elektronikus hírközlési adatvédelmi irányelvben nem megfelelően kezelt kérdést, ezáltal elszalasztja annak lehetőségét, hogy ez a felülvizsgálat megoldja a lezáratlan problémákat.

66. E két probléma – a javaslatban nem megfelelően kezelt kérdések és azok, amelyekkel a javaslat egyáltalán nem foglalkozik – megoldása érdekében ez a vélemény néhány szövegezési javaslatot terjeszt elő. A 67. és 68. pontok összefoglalják a problémákat, és konkrét megfogalmazást javasolnak. Az európai adatvédelmi biztos felszólítja a jogalkotót, hogy vegye figyelembe ezeket a javaslatnak a jogalkotási folyamaton való átfutása során.

67. A javaslatban foglalt azon módosítások, amelyek esetében az európai adatvédelmi biztos erősen támogatja a változtatást, az alábbiak:

i. **A biztonság sérülésének bejelentése**: Mint fentebb olvasható, a 4. *cikk (4) bekezdésének* javasolt beillesztése a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyilvános hálózaton keresztül nyújtó szolgáltatókra (internetszolgáltatókra, hálózatüzemeltetőkre) alkalmazandó, akik kötelesek értesíteni a nemzeti szabályozó hatóságokat és ügyfeleiket a biztonság sérüléséről. Az európai adatvédelmi biztos teljes mértékben támogatja ezt a kötelezettséget. Az európai adatvédelmi biztos ugyanakkor úgy találja, hogy ezt a kötelezettséget az információs társadalommal összefüggő szolgáltatásokat nyújtó szolgáltatókra is ki kell terjeszteni, hiszen ezek gyakran érzékeny személyes információkat dolgoznak fel. Ezért az online bankoknak és biztosítóknak, az online egészségügyi szolgáltatóknak és bármilyen egyéb online vállalkozásnak is be kellene tartania ezt a kötelezettséget.

E célból az európai adatvédelmi biztos azt javasolja, hogy a 4. cikk (3) bekezdése az információs társadalommal összefüggő szolgáltatásokat nyújtó szolgáltatókra való hivatkozással egészüljön ki a következők szerint: „*A biztonság olyan megsértése esetén (…) a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyújtó szolgáltatónak* és az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltatónak *a biztonság megsértéséről (…) értesítenie kell az érintett előfizetőt és a nemzeti szabályozó hatóságot*”.

ii. **A nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyilvános hálózaton keresztül nyújtó szolgáltatók által kezdeményezett jogi lépések**: Mint fentebb olvasható, a *13. cikk (6) bekezdésének* beillesztésére vonatkozó módosítás polgári jogorvoslatot biztosít a magán- vagy jogi személyek számára, különösen az elektronikus hírközlési szolgáltatók számára, hogy fellépjenek azokkal szemben, akik megsértik az elektronikus hírközlési adatvédelmi irányelvnek a kéretlen elektronikus levelekről szóló 13. cikkét. Az európai adatvédelmi biztos elégedett ezzel a rendelkezéssel. Az európai adatvédelmi biztos ugyanakkor nem érti, miért kellene ezt az új jogosultságot a 13. cikk megsértésének eseteire korlátozni. Az európai adatvédelmi biztos azt javasolja, hogy a jogi személyeket fel kell hatalmazni arra, hogy jogi lépéseket tegyenek az elektronikus hírközlési adatvédelmi irányelv bármely rendelkezésének megsértése esetén.

Fentiek elérése érdekében az európai adatvédelmi biztos javasolja, hogy a 13. cikk (6) bekezdését alakítsák külön cikké (14. cikk). Ezenkívül javasolja a 13. cikk (6) bekezdése megfogalmazásának kis mértékű módosítását: „*az e cikk alapján*” helyett javasolja „az ezen irányelv alapján” megfogalmazást.

68. Az elektronikus hírközlési adatvédelmi irányelv alkalmazási köre, amely jelenleg a nyilvános elektronikus hírközlési hálózatok szolgáltatóira korlátozódik, egyike a legaggasztóbb kérdéseknek, amelyekkel a javaslat nem foglalkozik. Az európai adatvédelmi biztos szerint az irányelvet módosítani kellene annak érdekében, hogy alkalmazási köre a vegyes (magán/nyilvános) és a magánkézben levő elektronikus hírközlési hálózatok szolgáltatóira is kiterjedjen.

69. Azon módosítások, amelyek esetében az európai adatvédelmi biztos erősen támogatja, hogy változatlanok maradjanak, az alábbiak:

i. **Rádiófrekvenciás azonosítás (RFID)**: A *3. cikk* javasolt módosítása, mely alapján az elektronikus hírközlő hálózatok körébe *„az adatgyűjtést és az azonosító eszközöket támogató nyilvános hírközlő hálózatok*" beletartoznak, teljesen kielégítő. Ez a rendelkezés különösen üdvözlendő, hiszen tisztázza, hogy számos rádiófrekvenciás alkalmazásnak meg kell felelnie az elektronikus hírközlési adatvédelmi irányelvben foglaltaknak, s ezáltal eloszlatja az ezzel kapcsolatos jogi bizonytalanságokat.

ii. **Cookie-k/kémszoftverek**: Az *5. cikk (3) bekezdésének* javasolt módosítása üdvözlendő, mivel ennek eredményeképp a végberendezésen tárolt cookie-król/kémszoftverekről szóló tájékoztatási kötelezettség és az elutasítás jogának biztosítására vonatkozó kötelezettség akkor is alkalmazandó, ha ezek az eszközök elhelyezése külső adattároló eszközökön, pl. CD-ROM-okon, USB-kulcsokon stb. keresztül történik. Az európai adatvédelmi biztos ugyanakkor azt javasolja, hogy az 5. cikk (3) bekezdésének utolsó részében hajtsanak végre egy kisebb módosítást, azaz töröljék a mondatból a „megkönnyítése" szót.

iii. **Komitológia választása az európai adatvédelmi biztossal folytatott konzultációt követően és a tájékoztatási kötelezettség feltételei/korlátozásai**: A 4. cikk (4) bekezdésének beillesztésére irányuló, a biztonság sérülésének bejelentésére vonatkozó módosítás alapján az európai adatvédelmi biztos véleményének meghallgatása után, komitológia keretében születik a biztonság sérülésének bejelentésére kialakított rendszer körülményeit/formátumát/eljárásait érintő összetett kérdésekkel kapcsolatos határozat. Az európai adatvédelmi biztos határozottan támogatja ezt az egységes megközelítést. A biztonság sérülésének bejelentésére vonatkozó jogi szabályozás önálló téma, amelyről gondos vita és elemzés után kell dönteni.

Ehhez kapcsolódik néhány érdekelt az irányú kérése, hogy a 4. cikk (4) bekezdésében kivételeket állapítsanak meg a biztonság sérülésének bejelentésére vonatkozóan. Az európai adatvédelmi biztos határozottan ellenzi ezt a megközelítést. Ehelyett azt támogatja, hogy a megfelelő vita lefolytatása után holisztikusan elemezzék a bejelentés általános tárgyát, módját, hogy mely esetekben lehet a bejelentést rövidíteni vagy valamilyen módon korlátozni.

iv. **Végrehajtás**: A *15a. cikk* beillesztésére irányuló javasolt módosítás számos olyan megtartandó elemet tartalmaz, amelyek hozzájárulnak a hatékony megfelelés biztosításához, beleértve a nemzeti szabályozó hatóságok vizsgálati jogkörének megerősítését (15a. cikk (3) bekezdés) és a nemzeti szabályozó hatóságoknak a jogsértés megszüntetésének elrendeléséhez szükséges jogkörrel való felruházását.

Kelt Brüsszelben, 2008. április 10-én.

Peter HUSTINX

Európai Adatvédelmi Biztos