Az európai adatvédelmi biztos második véleménye az elektronikus hírközlési ágazatban a személyes adatok kezeléséről és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK irányelv (elektronikus hírközlési adatvédelmi irányelv) felülvizsgálatáról

(2009/C 128/04)

AZ EURÓPAI ADATVÉDELMI BIZTOS,

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

tekintettel az Európai Unió alapjogi chartájára, és különösen annak 8. cikkére,

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

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

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

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

I. **BEVEZETÉS**

Háttér

1. Az Európai Bizottság 2007. november 13-án elfogadta a többek között az elektronikus hírközlési adatvédelmi irányelv módosításáról szóló javaslatot ([1]) (a továbbiakban: a javaslat vagy a bizottsági javaslat). Az európai adatvédelmi biztos 2008. április 10-én elfogadta a bizottsági javaslatról szóló véleményét, melyben ajánlásokat fogalmazott meg a javaslat javítására, megkísérelve hozzájárulni annak biztosításához, hogy a javasolt változtatások az egyének személyes adatainak lehető legjobb védelmét eredményezzék (a továbbiakban: az európai adatvédelmi biztos első véleménye) ([2]).

2. Az európai adatvédelmi biztos üdvözölte a biztonság megsértéséről való kötelező értesítés rendszerének létrehozására irányuló bizottsági javaslatot, mely rendszer kötelezné a vállalatokat, hogy értesítsék az egyéneket személyes adataik veszélybe kerülése esetén. Továbbá örvendetesnek tartotta a jogi személyek (pl. fogyasztói szervezetek és internetszolgáltatók) számára azt lehetővé tevő új rendelkezéseket, hogy a kéretlen elektronikus levelek küldői ellen lépéseket tegyenek a spam elleni küzdelem meglévő eszközeinek további kiegészítése érdekében.

3. Az Európai Parlament első olvasatát megelőző parlamenti megbeszélések során az európai adatvédelmi biztos további véleménnyel szolgált az egyetemes szolgáltatási irányelv ([3]) és az elektronikus hírközlési adatvédelmi irányelv felülvizsgálatával kapcsolatban illetékes európai parlamenti bizottságok által készített jelentéstervezetek kapcsán felmerülő válogatott kérdésekre vonatkozó észrevételei megtétele formájában (a továbbiakban: észrevételek) ([4]). Az észrevételek elsődlegesen a forgalmi adatok feldolgozásához és a szellemi tulajdonjog védelméhez kapcsolódó kérdéseket tárgyalták.

4. Az Európai Parlament (a továbbiakban: EP) 2008. szeptember 24-én elfogadta az elektronikus hírközlési adatvédelmi irányelvre vonatkozó jogalkotási állásfoglalást ([5]) (a továbbiakban: első olvasat). Az európai adatvédelmi biztos pozitívan fogadott többet az EP azon módosításai közül, melyek az európai adatvédelmi biztos fent említett véleményét és észrevételeit követően kerültek elfogadásra. A fontos változtatások között szerepelt az információs társadalommal összefüggő szolgáltatások nyújtóinak (azaz az interneten működő vállalatoknak) a biztonság megsértéséről való kötelező értesítés hatálya alá vonása. Az európai adatvédelmi biztos szintén üdvözölte azon módosítást, mely a jogi és természetes személyek számára lehetőséget ad arra, hogy bíróság előtt jogi eljárást indíthassanak az elektronikus hírközlési adatvédelmi irányelv bármely rendelkezésének megsértése miatt (és nem csak a spamre vonatkozó rendelkezések megsértése miatt, ahogyan az

([1]) Az elektronikus hírközlési adatvédelmi irányelv felülvizsgálata egy tágabb felülvizsgálati folyamat része, melynek célja egy uniós hírközlési hatóság létrehozása, valamint a 2002/21/EK, 2002/19/EK, 2002/20/EK, 2002/22/EK és 2002/58/EK irányelvek és a 2006/2004/EK rendelet felülvizsgálata (a továbbiakban együttesen: a hírközlési csomag felülvizsgálata).

([2]) Az európai adatvédelmi biztos 2008. április 10-i 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 irányelvre vonatkozó javaslatról, HL C 181., 2008.7.18., 1. o.

([3]) Az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv (Egyetemes szolgáltatási irányelv) (HL L 108., 2002.4.24., 51.o.).

([4]) Az európai adatvédelmi biztosnak az IMCO által a 2002/22/EK (egyetemes szolgáltatási) irányelv és a 2002/58/EK (elektronikus hírközlési adatvédelmi) irányelv felülvizsgálatáról készített jelentés kapcsán felmerülő válogatott kérdésekről szóló észrevételei, 2008. szeptember 2-án. A következő címen érhető el: www.edps.europa.eu

([5]) Az Európai Parlament 2008. szeptember 24-i jogalkotási állásfoglalása 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 szóló európai parlamenti és tanácsi irányelvjavaslatról (COM(2007)0698 – C6-0420/2007 – 2007/0248(COD)).

eredetileg a bizottsági javaslatban szerepelt). A Parlament első olvasatát követte a módosított elektronikus hírközlési adatvédelmi irányelvjavaslat Bizottság általi elfogadása (a továbbiakban: módosított javaslat) ([6]).

5. A Tanács 2008. november 27-én politikai megállapodásra jutott a hírközlési csomaggal – benne az elektronikus hírközlési adatvédelmi irányelvvel – kapcsolatos szabályok felülvizsgálatáról, melyek a Tanács közös álláspontját alkotják (a továbbiakban: közös álláspont) ([7]). A közös álláspontról az Európai Közösséget létrehozó szerződés 251. cikke (2) bekezdésének értelmében értesítést kap az EP, ami a javaslat EP általi módosításait vonhatja maga után.

A Tanács álláspontjára vonatkozó általános vélemények

6. A Tanács a javaslat lényegi elemeit módosította, és az EP által elfogadott módosítások közül sokat nem fogadott el. Bár a közös álláspont természetesen pozitív elemeket is tartalmaz, az európai adatvédelmi biztos a szöveg egészét tekintve aggódik annak tartalma miatt, különösen azért, mert a közös álláspont nem emel be egyet sem az EP által, a módosított javaslatban vagy az európai adatvédelmi biztos és az európai adatvédelmi hatóságok részéről a 29. cikk alapján létrehozott munkacsoporton keresztül közzétett véleményekben ([8]) javasolt pozitív módosítások közül.

7. Épp ellenkezőleg, számos esetben törölték, vagy lényeges mértékben enyhítették a módosított javaslatnak és az EP módosításainak azon rendelkezéseit, amelyek biztosítékokat nyújtanak a polgároknak. Ez azt eredményezte, hogy az egyének számára a közös álláspontban biztosított védelem szintje lényegesen alacsonyabb lett. Az európai adatvédelmi biztos ezen okok miatt teszi most közzé második véleményét abban a reményben, hogy amint az elektronikus hírközlési adatvédelmi irányelv a jogalkotási folyamatban előrehalad, új módosítások kerülnek elfogadásra, melyek helyreállítják az adatvédelmi biztosítékokat.

8. E második vélemény néhány alapvető aggodalomra összpontosít, és nem foglalkozik újra az európai adatvédelmi biztos első véleményében vagy az észrevételekben foglalt valamennyi ponttal, amelyek mind továbbra is érvényesek. E vélemény különösen az alábbi kérdéseket tárgyalja:

— A biztonság megsértéséről való értesítésekkel kapcsolatos rendelkezések;

— Az elektronikus hírközlési adatvédelmi irányelv magán- és nyilvánosan elérhető hálózatokra való alkalmazásának köre;

— A biztonsági célú forgalmiadat-feldolgozás;

— A jogi személyek lehetősége arra, hogy bírósághoz forduljanak az elektronikus hírközlési adatvédelmi irányelv rendelkezésének megsértése miatt.

9. A fenti kérdések megválaszolása során e vélemény elemzi a Tanács közös álláspontját, és összehasonlítja azt az EP első olvasatával és a Bizottság módosított javaslatával. A vélemény ajánlásokat tartalmaz, melyek célja az elektronikus hírközlési adatvédelmi irányelv rendelkezéseinek egyszerűsítése és annak biztosítása, hogy az irányelv továbbra is megfelelően garantálja az egyének magánéletének és személyes adatainak védelmét.

II. A BIZTONSÁG MEGSÉRTÉSÉRŐL VALÓ ÉRTESÍTÉSEKKEL KAPCSOLATOS RENDELKEZÉSEK

10. Az európai adatvédelmi biztos támogatja a biztonság megsértéséről való értesítés rendszerét, melynek keretében a hatóságok és az egyének értesítést kapnak személyes adataik feltörése esetén ([9]). A biztonság megsértéséről való értesítések segíthetik az egyént abban, hogy megtegye az adatok veszélyeztetéséből eredő bármely potenciális kár enyhítésére irányuló lépéseket. Továbbá a biztonság megsértéséről való értesítés kötelezettsége arra fogja ösztönözni a vállalatokat, hogy javítsanak felelősségi körükbe tartozó személyes adatokkal kapcsolatos adatbiztonságukon és fokozzák elszámoltathatóságukat.

11. A Bizottság módosított javaslata, az Európai Parlament első olvasata és a Tanács közös álláspontja a jelenleg mérlegelés álló, a biztonság megsértéséről való értesítéssel kapcsolatos három eltérő megközelítést képviseli. Mindhárom megközelítésben vannak pozitív elemek. Azonban az európai adatvédelmi biztos úgy véli, mindhárom megközelítésen van javítanivaló, és azt javasolja, hogy a biztonság megsértéséről való értesítés rendszerének elfogadásához vezető végső lépések mérlegelése során az alábbi ajánlások kerüljenek figyelembevételre.

([6]) Módosított 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, Brüsszel, 2008.11.6., COM(2008) 723 végleges.

([7]) Elérhető a Tanács nyilvános weboldalán.

([8]) A magánélet védelméről és az elektronikus hírközlésről szóló 2002/58/EK irányelv (elektronikus hírközlési adatvédelmi irányelv) felülvizsgálatáról szóló 2/2008 vélemény, mely a 29. cikk alapján létrehozott munkacsoport weboldalán érhető el.

([9]) A vélemény a „veszélyeztetés” szóval a biztonságnak a személyes adatokat érintő bármely olyan megsértésére hivatkozik, mely továbbított, tárolt vagy más módon feldolgozott személyes adatok véletlen vagy törvénytelen megsemmisítése, elvesztése, módosítása, engedély nélküli feltárása vagy azokhoz való engedély nélküli hozzáférés eredménye.

12. A biztonság megsértéséről való értesítéssel kapcsolatos három rendszer elemzése során öt döntő fontosságú szempontot kell figyelembe venni: *(i)* a biztonság megsértésének meghatározása; *(ii)* az értesítési kötelezettség körébe tartozó alanyok („lefedett alanyok"); *(iii)* az értesítési kötelezettséget keletkeztető szabvány; *(iv)* az annak meghatározásáért felelős alany meghatározása, hogy a biztonság megsértésének egy adott esete kimeríti-e vagy sem a szabványosított feltételeket, és *(v)* az értesítés címzettjei.

A Bizottság, a Tanács és az EP megközelítésének áttekintése

13. Az Európai Parlament, a Bizottság és a Tanács mind másmás megközelítést képvisel a biztonság megsértéséről való értesítéssel kapcsolatban. Az EP első olvasatában módosította a biztonság megsértéséről való értesítésnek a Bizottság javaslatában foglalt eredeti rendszerét ([10]). Az EP megközelítésében az értesítési kötelezettség nemcsak a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtóira vonatkozik, hanem az információs társadalommal összefüggő szolgáltatás nyújtóira („PPECS-ek" és „ISSP-k") is. Továbbá e megközelítés alapján a személyes adatok valamennyi adatvédelmi jogsértéséről értesíteni kellene a nemzeti szabályozó hatóságot vagy az illetékes hatóságokat (a továbbiakban együttesen: a hatóságok). Ha a hatóságok úgy döntenek, hogy a biztonság komoly megsértéséről van szó, megkívánnák a PPECS-ektől és az ISSP-ktől, hogy haladéktalanul értesítsék az érintett személyt. A rövidesen bekövetkező veszélyt és közvetlen fenyegetést jelentő adatvédelmi jogsértések esetében a PPECS-ek és az ISSP-k a hatóságok értesítése előtt értesítenék az egyéneket, és nem várnák meg a szabályozói döntést. A fogyasztók értesítésének kötelezettsége alóli kivétel körébe tartoznak azon alanyok, melyek igazolni tudják a hatóságok felé, hogy „*megfelelő technikai védelmi intézkedések kerültek alkalmazásra*", melyek értelmezhetetlenné teszik az adatokat a hozzáférésre engedéllyel nem rendelkező bármely személy számára.

14. A Tanács megközelítésében az előfizetők és a hatóságok részére is biztosítani kell az értesítést, de csak olyan esetekben, amikor a *lefedett alany* úgy ítéli meg, hogy a biztonság megsértése *komolyan veszélyezteti* az előfizető magánéletét (azaz személyazonosság eltulajdonítása vagy azzal való visszaélés, fizikai sérülés, jelentős megalázás vagy hírnévnek való ártás).

15. A Bizottság módosított javaslata megtartja a hatóságoknak a valamennyi jogsértésről való értesítésére vonatkozó – az EP által elfogadott – kötelezettséget. Azonban az EP megközelítésével ellentétben a módosított javaslat tartalmaz egy kivételt az értesítési kötelezettség alól az olyan érintett egyének esetében, melyekkel kapcsolatban a PPEC igazolni tudja az illetékes hatóság számára, hogy *(i)* „*ésszerű alapon nem valószínű*" kár (pl. gazdasági veszteség, társadalmi kár vagy személyazonosság-eltulajdonítás) bekövetkezése a biztonság megsértésének eredményeként, vagy *(ii)* „*megfelelő technikai védelmi intézkedések*" kerültek alkalmazásra az adatvédelmi jogsértés által érintett adatok esetében. A Bizottság javaslata így az egyéni értesítésekhez kötődő káralapú elemzést is tartalmaz.

16. Fontos megjegyezni, hogy az EP ([11]) és a Bizottság megközelítésében végső soron a *hatóságok* feladata annak eldöntése, hogy a biztonság megsértése súlyos-e, illetve hogy ésszerű alapon valószínű-e, hogy kárt okoz. A Tanács megközelítése szerint ezzel ellentétben a döntés az *érintett alanyokra* hárul.

17. A Tanács és a Bizottság javaslata csak a PPECS-ekre vonatkozik, az (EP megközelítésében szereplő) ISSP-kre nem.

A biztonság megsértésének meghatározása

18. Az európai adatvédelmi biztos üdvözli, hogy a három jogalkotási javaslatban a biztonság megsértésének meghatározása megegyezik: „*A biztonság olyan megsértése […] amely […] továbbított, tárolt vagy más módon feldolgozott személyes adatok véletlen vagy jogellenes megsemmisítését, elveszítését, módosítását, jogosulatlan felfedését vagy az azokhoz való jogosulatlan hozzáférést eredményezi […]*" ([12]).

19. Amint alább részletesebben leírásra kerül, ez a meghatározás abban a tekintetben örvendetes, hogy elég tág ahhoz, hogy az összes olyan releváns helyzetet magába foglalja, melyek indokolttá teszik a biztonság megsértéséről való értesítést.

20. Először, a meghatározás kiterjed az olyan esetekre, mikor egy harmadik fél *jogosulatlanul fért hozzá* személyes adatokhoz, mint pl. amikor egy személyes adatokat tároló szervert feltörnek és ilyen információkhoz férnek hozzá.

21. Másodszor, e meghatározás az olyan helyzetekre szintén kiterjed, melyekben személyes adatok elveszítésére, felfedésére került sor, míg a jogosulatlan hozzáférés tényét még bizonyítani kell. Ez nem terjedne ki az olyan helyzetekre, amikor a személyes adatok elveszhettek (pl. CD-ROM-ok, USB-meghajtók vagy más hordozható eszközök esete), vagy nyilvánosan hozzáférhetővé váltak a rendes felhasználók számára (pl. az alkalmazottak adatait tartalmazó fájl figyelmetlenségből az interneten keresztül egy nyilvánosan elérhető helyen átmenetileg hozzáférhetővé vált). Minthogy sok esetben nem lesz arra utaló bizonyíték, hogy az ilyen adatok egy adott időpontban egy jogosulatlan harmadik fél által hozzáférhetőek-e, illetve felhasználhatóak-e vagy sem, megfelelőnek tűnik kiterjeszteni a meghatározás körét ezen esetekre. Az európai adatvédelmi biztos ezért e meghatározás megtartását javasolja. Az európai adatvédelmi biztos ezenfelül a biztonság megsértésére vonatkozóan az elektronikus hírközlési adatvédelmi irányelv 2. cikkében szereplő meghatározásnak a beillesztését javasolja, mivel ez jobban összhangban lenne az irányelv átfogó felépítésével és fokozná az érthetőséget.

([10]) Különösen a 187., 124–127., valamint a 27., 21. és a 32. számú EP-módosítás foglalkozik ezzel a kérdéssel.

([11]) Kivéve a rövidesen bekövetkező és közvetlen veszély esetét, mikor is a lefedett alanyoknak először a fogyasztókat kell értesíteniük.

([12]) A közös álláspont és a módosított javaslat 2. cikkének i) pontja, és az EP első olvasata 3. cikkének (3) bekezdése.

Azon alanyok, akikre az értesítési kötelezettségnek ki kell terjednie

22. Az EP megközelítésében az értesítési kötelezettség a PPECS-ekre és az ISSP-kre is vonatkozik. A Tanács és a Bizottság rendszereiben azonban csak a PPECS-ek – így a hírközlési vállalatok és az internetszolgáltatók – lesznek kötelesek értesíteni az egyéneket a biztonság megsértésének a személyes adataik veszélyeztetéséhez vezető eseteiről. A más ágazatokat – pl. az online bankokat, az internetes kereskedőket, az online egészségügyi szolgáltatókat és másokat – nem terheli ez a kötelezettség. A fent kifejtett okokból az európai adatvédelmi biztos úgy ítéli meg, hogy közpolitikai szempontból alapvető annak biztosítása, hogy az értesítési kötelezettség vonatkozzon az információs társadalommal összefüggő szolgáltatásokra, amelyek magukban foglalják az online vállalkozásokat, az online bankokat, az online egészségügyi szolgáltatókat stb.

23. Először is, az európai adatvédelmi biztos megjegyzi, hogy jóllehet a hírközlési vállalatok biztonsága minden bizonnyal ki van téve értesítési kötelezettséget indokolttá tévő sérüléseknek, ugyanez igaz a másfajta társaságokra/szolgáltatókra is. Az internetes kereskedők, online bankok, online gyógyszertárak biztonságát éppúgy megsérthetik, mint a hírközlési társaságokét, ha nem még inkább. A kockázatok mérlegelése ezért nem szól amellett, hogy a biztonság megsértéséről való értesítés kötelezettsége a PPECS-ekre korlátozódjék. A tágabb megközelítés szükségességét igazolja más országok tapasztalata is. Így például az Egyesült Államokban szinte minden (ezidáig több mint 40) állam olyan törvényeket hozott a biztonság megsértéséről való értesítés tekintetében, amelyek alkalmazási köre szélesebb, nem csupán a PPECS-ekre terjed ki, hanem minden, az elkért személyes adatokat tároló intézményre is.

24. Másodszor, ha a PPECS-ek által rendszeresen feldolgozott személyes adatok típusainak megsértése hatással lehet az egyén magánéletére, ugyanez igaz, ha nem mindjárt fokozottabban is, az ISSP-k által feldolgozott személyes információk típusaira. A bankok és más pénzügyi intézmények természetesen birtokában lehetnek szigorúan bizalmas információknak (pl. a bankszámlára vonatkozó részletek), amelyek felfedése lehetővé tenné azoknak a személyazonossággal való visszaélésre történő felhasználását. Hasonlóképpen a fokozottan érzékeny egészségügyi információknak az online egészségügyi szolgáltatások általi felfedése különösen is ártalmas lehet az egyénekre nézve. Ezért a személyes adatok azon típusai, amelyek veszélybe kerülhetnek, ugyancsak a biztonsági megsértéséről való értesítés szélesebb körű, legalább az ISSP-kre kiterjedő alkalmazását kívánják meg.

25. A cikk alkalmazási körének kiterjesztésével szemben felvetődtek egyes jogi kérdések, így például a követelmény által érintett intézményekkel kapcsolatban. Mindenekelőtt az, hogy az elektronikus hírközlési adatvédelmi irányelv hatálya csupán a PPECS-ekre vonatkozik, akadályként merült fel azelőtt, hogy az értesítési kötelezettséget az ISSP-kre is alkalmazzák.

26. E tekintetben az európai adatvédelmi biztos emlékeztetni kíván az alábbiakra: i. Semmiféle jogi akadálya nincsen annak, hogy az irányelv bizonyos rendelkezéseinek hatályát a PPECS-eken kívül kiterjesszék más szereplőkre is. A közösségi jogalkotó e tekintetben teljes körű mérlegelési jogkörrel rendelkezik. ii. Más példák is vannak a meglévő elektronikus hírközlési adatvédelmi irányelvben a PPECS-ektől eltérő intézményekre történő alkalmazásra.

27. A 13. cikk például nemcsak a PPECS-ekre vonatkozik, hanem minden olyan társaságra is, amely – előzetes beleegyezést igénylő – nem kívánt tájékoztatást küld. Továbbá az elektronikus hírközlési adatvédelmi irányelv 5. cikkének (3) bekezdése, amely tiltja többek között az előfizető vagy felhasználó végberendezésében történő adattárolást, például a „cookie”-kat, nemcsak a PPECS-ekre nézve kötelező, hanem bárkire, aki az egyén végberendezésében való információtárolást vagy az ott tárolt információkhoz való hozzáférést kísérel meg. Továbbá a jelen jogalkotási folyamatban a Bizottság még azt is javasolta, hogy az 5. cikk (3) bekezdésének alkalmazási köre terjedjen ki azokra az esetekre is, amikor hasonló technológiákat („cookie”-k, kémprogramok) nemcsak elektronikus hírközlési rendszereken keresztül közvetítenek, hanem bármely más lehetséges módon (az internetről történő letöltéseken vagy külső adattároló eszközökön – például CD-ROM-okon, USB-kulcsokon, flash drive-okon stb. – keresztül történő terjesztés). Mindezek az elemek üdvözlendők és megtartandók, egyidejűleg azonban jelentős precedenseket szolgáltatnak az alkalmazási kör körül folyó jelen vitára is.

28. Továbbá a jelenlegi jogalkotási folyamatban a Bizottság és az Európai Parlament, valamint természetesen a Tanács javaslatot tett egy új, az alábbiakban tárgyalandó bekezdésre (6. cikk (6a) bekezdés), amely a PPECS-ektől eltérő intézményekre vonatkozik.

29. Végezetül pedig, figyelembe véve a biztonság megsértéséről való értesítés kötelezettségéből származó átfogó pozitívumokat, az állampolgárok nagy valószínűséggel nemcsak akkor várják el e tájékoztatást, ha személyes adataik a PPECS-ek révén kerülnek veszélybe, hanem akkor is, ha ISSP-k révén. Az állampolgárok várakozásai nem teljesülhetnek, ha például nem kapnak értesítést, amikor egy online bank elveszítette a bankszámlájukra vonatkozó információkat.

30. Összefoglalva: az európai adatvédelmi biztos meggyőződése, hogy a biztonság megsértéséről való értesítés előnyeinek teljes körű kiaknázása csak akkor érhető el jobban, ha az alkalmazási kör mind a PPECS-ekre, mind az ISSP-kre kiterjed.

Az értesítési kötelezettséget keletkeztető szabvány

31. Az értesítés keletkeztetése tekintetében – amint az az alábbiakban bővebben kifejtésre kerül – az európai adatvédelmi biztos úgy véli, hogy a három javasolt szabvány közül a legalkalmasabb a módosított javaslat *„ésszerű alapon valószínű, hogy kárt okozhat”* megfogalmazása. Mindazonáltal fontos biztosítani, hogy a „kárt okoz” kellőképpen tág jelentésű legyen ahhoz, hogy lefedje az egyének magánéletére vagy jogos érdekeire nézve negatív hatások minden releváns esetét. Máskülönben ajánlatos lenne új szabványt kialakítani, amelynek értelmében kötelező az értesítés, *„amennyiben a sérülés ésszerű alapon valószínű, hogy káros hatással lehet egyénekre”*.

32. Az előző szakaszban vázoltaknak megfelelően a feltételek, amelyek között biztosítani kell az egyének értesítését (az úgynevezett „kiváltó ok” vagy „szabvány”), eltérnek az EP, a Bizottság és a Parlament megközelítésében. Az értesítések mennyisége, amelyeket az egyének kapnak, természetesen nagy mértékben függ majd az értesítési kötelezettséget keletkeztető feltétel vagy szabvány meghatározásától.

33. A Tanács és a Bizottság rendszereiben akkor kell értesítést küldeni, ha a biztonság megsértése *„az előfizető magánéletének komoly megsértését”* jelenti (Tanács), és ha *„a biztonság megsértésének eredményeként ésszerű alapon valószínű, hogy a fogyasztói érdek kárt szenved”* (Bizottság). Az EP rendszerében a magánszemélyek értesítésének kötelezettségét kiváltó ok *„a biztonság megsértésének súlyossága”* (vagyis akkor kell értesíteni az egyéneket, ha a biztonság megsértését súlyosnak ítélik meg). E küszöb alatt nem szükséges az értesítés ([13]).

34. Az európai adatvédelmi biztos megérti, hogy ha személyes adatok veszélybe kerülnek, lehet azzal érvelni, hogy azoknak az egyéneknek, akikhez ezek az adatok tartoznak, minden körülmények között joguk van tudni erről az eseményről. Mindazonáltal nagyon is mérlegelendő, hogy ez megfelelő megoldás-e más érdekek és megfontolások fényében.

35. A javaslatok közt szerepelt, hogy túl sok értesítéshez és „értesítési fásultsághoz” vezethet, ha az értesítésküldési kötelezettség minden olyan esetre vonatkozik – vagyis mindenféle korlátozás nélkül –, amikor személyes adatok veszélybe kerültek, és ez közönyt eredményezhet. Amint az alábbiakban bővebben kifejtésre kerül, az európai adatvédelmi biztos ezt fontos érvnek tartja, ugyanakkor viszont hangsúlyozni kívánja azon aggodalmát, hogy a túlzott mennyiségű értesítés az információbiztonsági gyakorlatok széles körű kudarcát jelezheti.

36. A fentebb említettekkel összhangban, az európai adatvédelmi biztos tudatában van a túlzott mennyiségű értesítés lehetséges negatív következményeinek, és segíteni kíván annak biztosításában, hogy a biztonság megsértéséről való értesítésekkel kapcsolatban elfogadott jogi keret ne ezt eredményezze. Ha az egyének gyakran kapnának értesítéseket még azokról az esetekről is, amelyeknek nincs kedvezőtlen, káros vagy veszélyes hatása, az értesítés egyik legfontosabb célkitűzése csorbulna, hiszen az egyének paradox módon éppen akkor nem vennék figyelembe az értesítéseket, amikor viszont ténylegesen lépéseket kellene tenniük saját védelmük érdekében. Ezért fontos megtalálni a helyes egyensúlyt az értelmes tájékoztatásban, hiszen ha az egyén nem reagál a kapott értesítésekre, jelentős mértékben csökken az értesítési rendszerek hatékonysága.

37. Annak érdekében, hogy olyan megfelelő szabvány kerüljön elfogadásra, amely nem vezet túlzott mennyiségű értesítéshez, az értesítési kötelezettséget keletkeztető feltétel mérlegelése mellett figyelembe kell venni más tényezőket is, például a biztonság megsértése fogalmának meghatározását, valamint az értesítési kötelezettség hatálya alá tartozó információt. E tekintetben az európai adatvédelmi biztos megjegyzi, hogy a három javasolt megközelítésben – tekintettel a biztonság megsértésének fentebb tárgyalt tág definíciójára – nagy lehet az értesítések mennyisége. A túlzott mennyiségű értesítéssel kapcsolatos aggodalmakat erősíti az is, hogy a biztonság megsértése fogalmának meghatározása a személyes adatok minden típusára kiterjed. Azzal együtt, hogy az európai adatvédelmi biztos ezt tartja helyes megközelítésnek (mely nem korlátozza az értesítési kötelezettség alá tartozó személyes adatok típusát), szemben más megközelítésekkel, mint például az Egyesült Államok törvényeivel, ahol a követelmények az információ érzékeny voltára összpontosítanak, ugyanakkor ezt a tényezőt sem szabad figyelmen kívül hagyni.

38. A fentiek értelmében, valamint a különböző változók együttes figyelembevételével az európai adatvédelmi biztos helyénvalónak tartja egy küszöb vagy szabványosított szint beillesztését, amely alatt nem kötelező az értesítés.

39. Úgy tűnik, a javasolt szabványok – azaz ha a biztonság megsértése „komoly *kockázatot jelent a magánéletre*” vagy *„ésszerű alapon valószínű, hogy kárt okoz*” – mindegyike magában foglalja például a társadalmi vagy az egyén hírnevét ért kárt és a gazdasági veszteséget. Ezek a szabványok például foglalkoznának a nem nyilvános azonosítók – például útlevélszám – kiadása révén a személyazonosság-lopásnak való kitettség eseteivel, valamint az egyén magánéletére vonatkozó információk felfedésével. Az európai adatvédelmi biztos üdvözli ezt a megközelítést. Meggyőződése, hogy a biztonság megsértéséről való értesítés kínálta előnyöket nem lehet teljes mértékben kiaknázni, ha az értesítési rendszer csak a gazdasági kárt okozó sérülésekre vonatkozik.

([13]) Lásd a 11. lábjegyzetet, az e szabály alóli kivétel tekintetében.

40. A két javasolt szabvány közül az európai adatvédelmi biztos a bizottsági szabványt – *„ésszerű alapon valószínű, hogy kárt fog okozni*" – részesíti előnyben, mivel az megfelelőbb szintű védelmet biztosítana az egyének számára. A jogsértések sokkal nagyobb valószínűséggel minősülnek majd értesítést igénylőnek, ha *„ésszerű alapon valószínű, hogy kárt okoznak*" az egyének magánéletében, mint ha ilyen kár *„komoly veszélyét*" kell jelenteniük. Így tehát jelentősen korlátozná az értesítésköteles jogsértések számát, ha az csak az egyén magánéletére komoly veszélyt jelentő sérülésekre vonatkozna. Ha csak e sérülésekre terjedne ki, korlátlan mérlegelési jogkört biztosítana a PPECS-eknek és ISSP-knek arra vonatkozóan, hogy szükséges-e az értesítés, amennyiben sokkal egyszerűbb lenne igazolniuk azt a következtetést, hogy nem áll fenn a kár *„komoly veszélye*", mint azt, hogy *„ésszerű alapon nem valószínű*", hogy kár következik be. Miközben a túl sok értesítés egyértelműen kerülendő, kétely esetén nagyobb súllyal kell latba esnie a magánélet védelmének, és az egyéneket minimális szinten legalább akkor kellene védelmezni, amikor a biztonság megsértése ésszerű alapon valószínű, hogy kárt okoz nekik. Továbbá az *„ésszerű alapon valószínű*" megfogalmazás hatékonyabb lesz a gyakorlatban mind a lefedett alanyok, mind az illetékes hatóságok tekintetében, hiszen az esetnek és releváns összefüggéseinek a tárgyilagos értékelését követeli meg.

41. A személyes adatok biztonságának megsértése továbbá olyan kárt okozhat, amelyet nehéz számszerűsíteni és amely igen sokféle lehet. Ugyanazon adattípus felfedése ugyanis az egyén körülményeitől függően lehet, hogy jelentős károkat okoz az egyik személynek, míg a másiknak kevesebbet. Az olyan szabvány, amely előírja, hogy a kár anyagi, jelentős vagy komoly kell, hogy legyen, nem lenne megfelelő. A Tanács megközelítése például, amely előírja, hogy a biztonság megsértése *komoly* hatással kell, hogy legyen valakinek a magánéletére, nem biztosítana megfelelő védelmet az egyéneknek, amennyiben ez a szabvány megköveteli, hogy a magánéletre gyakorolt hatás „komoly" legyen. Ez ugyancsak teret enged a szubjektív értékelésnek.

42. Miközben – a fentiek értelmében – az *„ésszerű alapon valószínű, hogy kárt okoz*" megfogalmazás alkalmas szabványnak tűnik a biztonság megsértéséről való értesítéshez, az európai adatvédelmi biztost továbbra is aggodalommal tölti el, hogy ez potenciálisan nem terjed ki minden olyan helyzetre, amikor indokolt lenne az egyének értesítése, például minden olyan helyzetben, amikor ésszerű alapon valószínű az egyének magánéletére vagy más törvényes jogaira gyakorolt negatív hatás. Ezen okból megfontolandó egy olyan szabvány, amely megkövetelné az értesítést, *„ha a sérülés ésszerű alapon valószínű, hogy hátrányos befolyással van az egyének számára*".

43. Ennek az alternatív szabványnak megvan az az előnye is, hogy összhangban áll az európai uniós adatvédelmi jogszabályokkal. Az adatvédelmi irányelv ugyanis gyakran hivatkozik az adatalanyok jogaira és szabadságaira tett hátrányos befolyásra. Az adatfeldolgozási műveleteknek az adatvédelmi hatóságok felé történő bejelentésének a kötelezettségével foglalkozó 18. cikk és (49) preambulumbekezdés például felhatalmazza a tagállamokat a kötelezettség alóli mentességre azon esetekben, amikor az adatfeldolgozás *„valószínűleg nem befolyásolja hátrányosan az érintettek jogait és szabadságait*". Hasonló megfogalmazást alkalmaz a közös álláspont 16. cikkének (6) bekezdése annak érdekében, hogy lehetővé tegye a jogi személyeknek, hogy pert indíthassanak a kéretlen levelek küldőivel szemben.

44. A fentiek figyelembevételével elvárható lenne, hogy a lefedett alanyok és különösen az adatvédelmi jogszabályok érvényesítésében illetékes hatóságok jobban ismerjék a fent említett szabványt és így megkönnyítsék arra vonatkozó értékelésüket, hogy a biztonság egy adott megsértése kimeríti-e a szabványosított feltételeket.

Az annak meghatározásáért felelős alany, hogy a biztonság megsértése megfelel-e vagy sem a szabványnak

45. Az EP megközelítése szerint (az azonnali veszély eseteit kivéve) és a Bizottság módosított javaslatában a tagállami hatóságok határozhatják meg, hogy a biztonság megsértése megfelel-e vagy sem annak a szabványnak, amely kötelezettséget keletkeztet az érintett egyének értesítésére.

46. Az európai adatvédelmi biztos úgy véli, hogy egy hatóság bevonása fontos szerepet játszik a szabványnak való megfelelés meghatározásában, amennyiben – bizonyos mértékben – ez a törvény helyes alkalmazásának a biztosítéka. Ez a rendszer elejét veheti annak, hogy a társaságok a sérülést nem megfelelő módon ártalmatlannak/nem komolynak értékeljék, és így elmulasszák az értesítést, amikor az ténylegesen szükséges lenne.

47. Másrészt az európai adatvédelmi biztost aggodalommal tölti el az, hogy egy olyan rendszer, amelyben a hatóságoknak kell az értékelést elvégezniük, kevéssé gyakorlatias és nehezen alkalmazható, vagy a gyakorlatban csökkentené a hatékonyságot. Így még csökkentené is az egyének nyújtott adatvédelmi biztosítékokat.

48. Ebben a megközelítésben ugyanis az adatvédelmi hatóságokat valószínűleg elhalmozzák majd a biztonság megsértéséről való értesítések, és komoly nehézségekkel szembesülhetnek a szükséges értékelések elvégzésében. Fontos szem előtt tartani, hogy annak értékeléséhez, hogy egy jogsértés megfelel-e a szabványnak, a hatóságokhoz el kell juttatni a kellő mennyiségű, gyakran összetett műszaki természetű belső információt, amelyet azoknak igen gyorsan fel kell dolgozniuk. Figyelembe véve az értékelés nehéz voltát és azt, hogy egyes hatóságok csak korlátozott erőforrásokkal rendelkeznek, az európai adatvédelmi biztos attól tart, hogy a hatóságoknak nagyon nehéz lesz megfelelniük e kötelezettségnek, és erőforrásokat vonhatnak el más kiemelt fontosságú területektől. Ez a rendszer továbbá szükségtelen nyomást helyezhetne a hatóságokra; ha ugyanis úgy döntenek, hogy a jogsértés nem komoly, az egyének viszont mégis kárt szenvednek, a felelősség potenciálisan a hatóságokat terhelhetné.

49. Az említett nehézség még nagyobb jelentőséget kap, ha figyelembe vesszük, hogy az idő kulcsfontosságú tényező a biztonság megsértéséből származó kockázatok minimalizálásában. Hacsak a hatóságok nem képesek az értékelést nagyon rövid határidővel elvégezni, az értékelésnek a hatóságok általi elvégzéséhez szükséges többletidő növelheti az érintett egyének által elszenvedett károkat. Így előfordulhat, hogy ez a további lépés, amely azt lett volna hivatott szolgálni, hogy nagyobb védelmet biztosítson az egyének számára, paradox módon végül kevesebb védelmet kínál, mint a közvetlen értesítésen alapuló rendszerek.

50. Az európai adatvédelmi biztos az említett okból kifolyólag úgy ítéli meg, hogy jobb lenne egy olyan rendszert kidolgozni, amelyben az érintett alanyok végeznék el annak értékelését, hogy az adott jogsértés megfelel-e vagy sem a szabványnak, ahogyan arról a tanácsi megközelítés rendelkezik.

51. A lehetséges visszaélés veszélyének – például annak, hogy az alanyok elutasítják az értesítést olyan körülmények között, amelyekben arra egyértelműen szükség lenne – elkerülése érdekében azonban kulcsfontosságú beiktatni bizonyos, az alábbiakban kifejtett adatvédelmi biztosítékokat.

52. Először, a lefedett alanyokat érintő, annak eldöntésére vonatkozó kötelezettséghez, hogy kell-e értesítést küldeniük, társulnia kell egy másik kötelezettségnek, amely előírja, hogy kötelezően értesítsék a hatóságokat a szabványnak megfelelő jogsértésekről. Az érintett alanyoknak ezen esetekben tájékoztatniuk kellene a hatóságokat a biztonság megsértéséről és az értesítésre, valamint minden kiküldött értesítés tartalmára vonatkozó döntésük indokairól.

53. Másodszor, a hatóságoknak valós felügyeleti szerepet kell kapniuk. E feladatkörük gyakorlása során a hatóságok számára lehetővé kell tenni (de kötelezővé nem), hogy felderítsék a jogsértés körülményeit, és megköveteljenek bármiféle szükséges helyreállító intézkedést ([14]). Ez nemcsak az egyének értesítését kellene, hogy magában foglalja (amennyiben arra még nem került sor), hanem az arra vonatkozó jogkört is, hogy a további sérülések megelőzése érdekében lépések megtételére vonatkozó kötelezettséget rójanak ki. A hatóságoknak tényleges jogosultságokat és erőforrásokat kellene biztosítani e tekintetben, és rendelkezniük kell az annak eldöntéséhez szükséges mozgástérrel, hogy mikor reagálnak a biztonság megsértéséről való értesítésre. Más szóval, ez lehetővé tenné a hatóságok számára a szelektálást és – például – a nagy, valóban ártalmas biztonsági sérülések vizsgálatát, ellenőrizve és érvényesítve a törvényi követelményeknek való megfelelést.

54. A fentiek elérése érdekében az európai adatvédelmi biztos az elektronikus hírközlési adatvédelmi irányelvben – úgymint a 15a. cikk (3) bekezdésében – és az adatvédelmi irányelvben elismert jogkörök mellé az alábbi szöveg beillesztését javasolja: „*Ha az előfizetőt vagy az érintett személyt még nem értesítették, a sérülés természetének mérlegelése után az illetékes nemzeti hatóság kötelezheti erre a PPECS-eket vagy ISSP-ket.*”

55. Az európai adatvédelmi biztos javasolja továbbá, hogy az EP és a Tanács erősítse meg az EP által javasolt (122. módosítás, 4. cikk (1a) bekezdés), az alanyokra vonatkozó azon kötelezettséget, hogy kockázatértékelést és -azonosítást végezzenek rendszereikre és az általuk feldolgozni kívánt személyes adatokra vonatkozóan. Az alanyoknak e kötelezettség alapján testre szabott és gondos meghatározást kell adniuk azon biztonsági intézkedésekről, amelyeket eseteikben alkalmazni fognak, és amelyeknek a hatóságok rendelkezésére kell állniuk. Ha a biztonság megsértése következik be, e kötelezettség segítségére lesz majd a lefedett alanyoknak – és adott esetben felügyeleti szerepükben a hatóságoknak is – abban, hogy eldöntsék, az információ veszélyeztetése az egyénekre nézve lehet-e hátrányos befolyással vagy okozhat-e kárt.

56. Harmadszor, a lefedett alanyokat érintő, annak eldöntésére vonatkozó kötelezettséghez, hogy értesíteniük kell-e az egyéneket, társulnia kell a részletes és átfogó belső ellenőrzési nyomvonal vezetésére vonatkozó kötelezettségnek, amely leír minden bekövetkezett jogsértést és minden azzal kapcsolatos értesítést, valamint bármely, a jövőbeli jogsértések elkerülése érdekében hozott intézkedést. E belső ellenőrzési nyomvonalat a hatóságok rendelkezésére kell bocsátani felülvizsgálatra és esetleges vizsgálatokra. Ez lehetővé teszi a hatóságok számára, hogy ellássák felügyeleti szerepüket. Ezt az alábbi gondolatmenetet követő szövegezés elfogadásával lehetne elérni: „*A PPECS-knek és ISSP-knek átfogó nyilvántartást kell vezetniük, amely részletezi a bekövetkezett jogsértéseket, az azokhoz kapcsolódó műszaki információkat és a megtett ellenlépéseket. A nyilvántartásban meg kell említeni minden, az előfizetők vagy érintett egyének, valamint az illetékes nemzeti hatóságok számára kiadott értesítést, beleértve azok dátumát és tartalmát. A nyilvántartást kérésre át kell nyújtani az illetékes nemzeti hatóságnak.*”

57. E szabványnak, valamint a biztonság megsértésére vonatkozó irányelv más releváns szempontjainak – így az értesítés formájának és eljárásainak – a következetes végrehajtása érdekében természetesen helyénvaló lenne, ha a Bizottság az európai adatvédelmi biztossal, a 29. cikk szerinti munkacsoporttal és az érintett szereplőkkel folytatott konzultációt követően technikai intézkedéseket fogadna el a végrehajtásra vonatkozóan.

([14]) A 15a. cikk (3) bekezdése elismeri ezt a felügyeleti szerepet, amikor rögzíti, hogy „a tagállamok biztosítják, hogy az illetékes nemzeti hatóságok és adott esetben más nemzeti szervek rendelkezzenek az ezen irányelv értelmében elfogadott nemzeti rendelkezések nyomon követéséhez és érvényesítéséhez szükséges valamennyi vizsgálati jogkörrel és forrással, beleértve a számukra esetlegesen szükséges, vonatkozó információk megszerzésére vonatkozó hatáskört is.”

Az értesítés címzettjei

58. Az értesítések címzettjei tekintetében az európai adatvédelmi biztos a Tanácséval szemben az EP és a Bizottság terminológiáját részesíti előnyben. Az EP ugyanis az „előfizetők" szót a „felhasználók" szóra cserélte. A Bizottság az „előfizetők" és „érintett egyének" kifejezéseket használja. Mind az EP, mind a Bizottság megfogalmazása kiterjedne nemcsak a jelenlegi előfizetőkre, hanem a korábbi előfizetőkre és harmadik felekre is, például olyan felhasználókra, akik egyes lefedett alanyokkal anélkül lépnek kapcsolatba, hogy náluk előfizetnének. Az európai adatvédelmi biztos üdvözli ezt a megközelítést, és annak megtartására kéri az EP-t és a Tanácsot.

59. Mindazonáltal a terminológia tekintetében következetlenségeket lát az EP első olvasatában, melyeket ki kell küszöbölni. Így például az „előfizetők" szó helyébe a legtöbb esetben – de nem mindig – a „felhasználók" szó lépett, más esetekben pedig a „fogyasztók". Ezt egységesíteni kellene.

III. AZ ELEKTRONIKUS HÍRKÖZLÉSI ADATVÉDELMI IRÁNYELV HATÁLYA: NYILVÁNOS ÉS MAGÁNHÁLÓZATOK

60. A jelenlegi elektronikus hírközlési adatvédelmi irányelv 3. cikkének (1) bekezdése meghatározza azokat az alanyokat, amelyekre az irányelv elsősorban vonatkozik, vagyis amelyek a nyilvános hírközlési szolgáltatások (a fentebbiekben említett PPECS-ek) nyilvános hírközlő hálózaton történő nyújtásával *összefüggésben* kezelnek személyes adatokat ([15]). PPECS-ek által végzett tevékenység például az internethozzáférést nyújtó szolgáltatás, az elektronikus hírközlő hálózaton való adattovábbítás, a mobil- és telefonhálózatokra való csatlakozás stb.

61. Az EP elfogadott egy, az eredeti bizottsági javaslat 3. cikkére vonatkozó módosítást (121. módosítás), amelynek eredményeként az elektronikus hírközlési adatvédelmi irányelv alkalmazási körét kiterjed *„a Közösségben a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyilvános és magán hírközlő hálózatokon, valamint nyilvánosan elérhető magánhálózatokon keresztül […] történő nyújtásával összefüggő személyes adatok kezelésére*" (Elektronikus hírközlési adatvédelmi irányelv, 3. cikk, (1) bekezdés). A Tanács és a Bizottság sajnálatos módon nem tudta elfogadni e javaslatot, ezért ezt az elképzelést nem építették be a közös álláspontba és a módosított javaslatba.

Az elektronikus hírközlési adatvédelmi irányelv alkalmazása a nyilvánosan elérhető magánhálózatokra

62. Az alább kifejtett okokból, valamint a konszenzus elősegítése céljából az európai adatvédelmi biztos a 121. módosítás lényegének a megtartására ösztönöz. Emellett javasolja egy olyan módosítás beillesztését, amely segít tovább tisztázni a kiszélesített hatály alá tartozó szolgáltatástípusokat.

63. A magánhálózatokat gyakran használják fel elektronikus hírközlési szolgáltatások – például internet-hozzáférés – meghatározatlan, potenciálisan nagyszámú ember számára történő nyújtására. Ez a helyzet például az internetkávézókban biztosított internet-hozzáférés és a szállodákban, éttermekben, repülőtereken, vonatokon és más, a nyilvánosság előtt nyitott intézményekben elérhető Wi-Fi-hálózatok esetében, ahol ezek a szolgáltatások gyakran más szolgások kiegészítéseként vehetők igénybe (ital, szállás stb.).

64. Valamennyi fenti példában egy hírközlési szolgáltatást – például internet-hozzáférést – tesznek elérhetővé a nyilvánosság számára, nem nyilvános hálózaton, hanem magánjellegűnek tekinthető, azaz magánhálózaton keresztül. Továbbá jóllehet a fenti esetekben a hírközlési szolgáltatásokat a nyilvánosságnak nyújtják, mivel azonban az igénybe vett hálózat típusa inkább magán- mint nyilvános hálózat, e szolgáltatások nyújtása *nyilvánvalóan* nem tartozik a teljes elektronikus hírközlési adatvédelmi irányelv, vagy legalábbis néhány cikkének hatálya alá ([16]). Ennek eredményeként nincsenek védve az egyéneknek az elektronikus hírközlési adatvédelmi irányelvben biztosított alapvető jogai, és egyenlőtlen jogi helyzet áll elő azon felhasználók számára, akik ugyanazt az internethozzáférést biztosító szolgáltatást nyilvános hírközlési eszközökön keresztül veszik igénybe, azokkal szemben, akik ezt magánhálózatokon keresztül teszik. Mindez annak ellenére van így, hogy mindezen esetekben ugyanolyan mértékben állnak fenn az egyének magánéletét és személyes adatait fenyegető veszélyek, mint amikor nyilvános hálózatokat vesznek igénybe a szolgáltatás eléréséhez. Összefoglalva tehát nem látszik *ésszerű* indok az irányelv értelmében a magánhálózatokon és a nyilvános hálózatokon keresztül nyújtott távközlési szolgáltatások közötti különbségtételre.

65. Ezért az európai adatvédelmi biztos támogatna egy olyan javaslatot, mint például az EP 121. módosítása, amelynek értelmében az elektronikus hírközlési adatvédelmi irányelv hatálya kiterjedne a nyilvánosan elérhető elektronikus hírközlési szolgáltatások *magán* hírközlő hálózaton történő nyújtásával összefüggő személyesadat-feldolgozásra is.

66. Az európai adatvédelmi biztos mindazonáltal elismeri, hogy ez a megfogalmazás előreláthatatlan és esetleg nem szándékolt következményekhez vezethet. A magánhálózatok puszta említése ugyanis úgy értelmezhető, hogy kiterjed olyan helyzetekre, amelyekre nem szándékoznak kiterjeszteni az irányelv hatályát. Így például úgy ítélhetik

([15]) *„Ezt az irányelvet […] a nyilvánosan elérhető hírközlési szolgáltatások nyilvános hírközlő hálózaton történő nyújtásával összefüggő személyes adatok kezelésére kell alkalmazni."*

([16]) Ezzel szemben azt az érvet lehetne felhozni, hogy még ha a hálózat magán jellegű is, mivel a hírközlési szolgáltatást a nyilvánosság számára nyújtják, e szolgáltatások nyújtása annak ellenére, hogy a hálózat magánhálózat, a meglévő jogi keret hatálya alá tartozik. Ugyanis Franciaországban például az alkalmazottaik számára internet-hozzáférést biztosító munkáltatók ugyanolyan elbírálás alá esnek, mint azok az internet-hozzáférést biztosító szolgáltatók, amelyek kereskedelmi alapon biztosítanak internet-hozzáférést. Ezt az értelmezést nem osztják széles körben.

meg, hogy e megfogalmazás szó szerinti vagy szigorú értelmezésben a Wi-Fi-készülékkel felszerelt otthonok ([17]) tulajdonosait – amelyek a hatókörükön (általában az otthonon) belül bárkinek lehetővé teszik a csatlakozást – ugyancsak az irányelv hatálya alá vonná; jóllehet a 121. módosítás nem ezt kívánja elérni. Ennek a hatásnak az elkerülése érdekében az európai adatvédelmi biztos a 121. módosítás olyan átfogalmazását javasolja, hogy az elektronikus hírközlési adatvédelmi irányelv alkalmazási köre kiterjedjen „*a Közösségben a nyilvánosan elérhető hírközlési szolgáltatások nyilvános vagy nyilvánosan elérhető magán hírközlő hálózaton történő nyújtásával összefüggő személyes adatok kezelésére*”.

67. Ez segítene annak tisztázásában, hogy csak a nyilvánosan hozzáférhető magánhálózatok essenek az elektronikus hírközlési adatvédelmi irányelv hatálya alá. Az elektronikus hírközlési adatvédelmi irányelvnek *csupán a nyilvánosan elérhető magánhálózatokra* (nem pedig minden magánhálózatra) történő alkalmazása meghúzza a határt, így az irányelv csak a nyilvánosság számára szándékosan *elérhetővé* tett magánhálózatokon keresztül nyújtott hírközlési szolgáltatásokra fog vonatkozni. Ez a megfogalmazás segít továbbá kiemelni, hogy a magánhálózatnak a *nagy nyilvánosság tagjai számára* való elérhetősége az a kulcstényező, amely meghatározza, hogy az irányelv vonatkozike rá (a nyilvánosan elérhető hírközlési szolgáltatásra vonatkozó előírás mellett). Más szóval: attól függetlenül, hogy a hálózat magán- vagy nyilvános hálózat-e, ha a hálózatot nyilvános hírközlési szolgáltatás – például internet-hozzáférés – nyújtása céljából szándékosan elérhetővé tették a nyilvánosság számára, még ha ez a szolgáltatás egy másik szolgáltatás kiegészítője is csupán (például szállodai ellátás), az irányelv lefedi ezt a szolgáltatás-/hálózattípust.

68. Az európai adatvédelmi biztos megjegyzi, hogy a fent támogatott elgondolás, amely szerint az elektronikus hírközlési adatvédelmi irányelv előírásait a *nyilvánosan elérhető magánhálózatokra* is alkalmazni kell, összhangban áll a több tagállamban elfogadott megközelítésekkel, ahol a hatóságok az ilyen típusú szolgáltatásokat, valamint a tisztán magánjellegű hálózatokon keresztül nyújtott szolgáltatásokat bevonták az elektronikus hírközlési adatvédelmi irányelvet végrehajtó nemzeti rendelkezések hatálya alá ([18]).

69. Az új hatályba tartozó alanyok tekintetében a jogi biztonság fokozása érdekében hasznos lehet beilleszteni az elektronikus hírközlési adatvédelmi irányelvbe egy a „nyilvánosan elérhető magánhálózatok” fogalmát meghatározó módosítást, melynek megfogalmazása lehetne a következő: „*nyilvánosan hozzáférhető magánhálózat: magánműködtetésű hálózat, melyhez a nagy nyilvánosság tagjai általában korlátozott hozzáféréssel rendelkeznek akár fizetés révén, akár más szolgáltatásokkal vagy ajánlatokkal összefüggésben, az alkalmazandó feltételek elfogadásától függően*”.

70. A gyakorlatban a fenti megközelítés azt jelentené, hogy az irányelv hatálya kiterjedne a szállodák és más, a nagyközönség számára magánhálózaton keresztül internet-hozzáférést nyújtó intézmények magánhálózataira. Ezzel szemben a tisztán magánjellegű hálózatokon keresztül nyújtott hírközlési szolgáltatások nyújtása, ahol a szolgáltatás azonosítható egyének korlátozott csoportjára korlátozódik, nem tartozna a hatálya alá. Ezért például a virtuális magánhálózatok és a Wi-Fi-vel rendelkező felhasználói otthonok nem tartoznának az irányelv hatálya alá. A tisztán vállalati hálózatokon keresztül nyújtott szolgálatok sem tartoznának a hatálya alá.

Az elektronikus hírközlési adatvédelmi irányelv hatálya alá tartozó magánhálózatok

71. A magánhálózatok fent javasolt kizárását átmeneti intézkedésnek kell tekinteni, amely további megbeszélések tárgyát kell, hogy képezze. Figyelembe véve egyrészt a kizárólag magánkézben lévő hálózatok kizárásának a magánélet védelmére való hatásait, másrészt azt a tényt, hogy ez azon személyek tömegeit érinti, akik általában vállalati hálózatokon keresztül csatlakoznak az internetre, elképzelhető, hogy a jövőben felül kell vizsgálni ezt a kérdést. A fentiekből kifolyólag, valamint az erről a témáról folytatott vita előmozdítása érdekében az európai adatvédelmi biztos egy olyan preambulumbekezdésnek az elektronikus hírközlési adatvédelmi irányelvbe történő beillesztését javasolja, amelynek értelmében a Bizottság az európai adatvédelmi biztostól, az adatvédelmi hatóságoktól és más érintett szereplőktől származó információk alapján nyilvános konzultációt folytatna az említett irányelv minden magánhálózatra történő alkalmazásáról. A preambulumbekezdés emellett azt is kimondhatja, hogy a Bizottság a nyilvános konzultáció eredményeként benyújtja a megfelelő javaslatokat az elektronikus hírközlési adatvédelmi irányelv hatálya alá tartozó alanyok körének kiterjesztésére vagy korlátozására vonatkozóan.

72. A fentiek mellett megfelelően módosítani kell az elektronikus hírközlési adatvédelmi irányelv különböző cikkeit oly módon, hogy valamennyi működési rendelkezés a nyilvános hálózatok mellett kifejezetten hivatkozzon a nyilvánosan elérhető magánhálózatokra is.

IV. **BIZTONSÁGI CÉLÚ FORGALMIADAT-FELDOLGOZÁS**

73. Az elektronikus hírközlési adatvédelmi irányelv felülvizsgálatával kapcsolatos jogalkotási folyamat során a biztonsági szolgáltatásokat nyújtó vállalatok kijelentették, hogy az online biztonság szavatolása érdekében olyan intézkedést kell az elektronikus hírközlési adatvédelmi irányelvbe illeszteni, amely törvényesíti a forgalmi adatok gyűjtését.

([17]) Általában vezeték nélküli helyi hálózatok (LAN-ok).
([18]) Lásd a 16. lábjegyzetet.

74. Az EP ennek eredményeképpen elfogadta a 181. módosítást, amely létrehozza a 6. cikk új (6a) bekezdését, ez pedig kifejezetten engedélyezi a forgalmi adatok biztonsági célú feldolgozását: „*(6a) A 95/46/EK irányelv 7. cikke és a jelen irányelv 5. cikkén kívül egyéb rendelkezések teljesítését nem érintve, a forgalmi adatok feldolgozhatóak a hálózati és információs biztonságról való gondoskodás érdekében az adatkezelő jogos érdekéből – amint azt a Tanács és a Parlament az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról 2004. március 10-i 460/2004/EK rendeletének 4. cikk c) pontja meghatározza – közcélú elektronikus kommunikációs szolgáltatásra, közcélú vagy magán elektronikus kommunikációs hálózatra, információs társadalmi szolgáltatásra vagy ahhoz kapcsolódó terminál- és elektronikus kommunikációs berendezésekre vonatkozó technikai rendelkezések végrehajtása céljából, kivéve amennyiben az ilyen érdekeket felülírják az érintett alapvető jogaihoz és szabadságaihoz fűződő érdekek. Az ilyen feldolgozás szigorúan a biztonsági tevékenység céljai szempontjából szükséges teendőkre korlátozódik.*”

75. A Bizottság módosított javaslata elvben elfogadta ezt a módosítást, ugyanakkor az „*A 95/46/EK irányelv … nem érintve*” szövegrész törlése révén elhagyott egy kulcsfontosságú tagmondatot, amelynek célja annak biztosítása volt, hogy az irányelv egyéb rendelkezéseit betartsák. A Tanács egy újraszövegezett változatot fogadott el, amely az alábbi megfogalmazás elfogadásával még egy lépéssel tovább ment a 181. módosításban szereplő fontos védelmi és érdekkiegyenlítési eszközök meggyengítésében: „*Forgalmi adatokat az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló, 2004. március 10-i 460/2004/EK európai parlamenti és tanácsi rendelet 4. cikkének c) pontja szerinti […] hálózat- és információbiztonság garantálásához feltétlenül szükséges mértékben lehet feldolgozni.*”

76. Amint az az alábbiakban kifejtésre kerül, a 6. cikk (6a) bekezdése szükségtelen és visszaélésekre adhat okot, különösebben akkor, ha abban a formájában fogadják el, amely nem tartalmazza a fontos védelmi eszközöket, az irányelv egyéb intézkedéseinek betartására vonatkozó záradékokat és az érdekek kiegyenlítését. Az európai adatvédelmi biztos ezért azt javasolja, hogy töröljék ezt a cikket, vagy legalább azt biztosítsák, hogy az erre a kérdésre vonatkozó cikk tartalmazza az EP által elfogadott 181. módosításban szereplő különböző biztosítékokat.

A forgalmi adatok feldolgozásának jogalapja az elektronikus hírközlési szolgáltatók és más adatkezelők számára a jelenlegi adatvédelmi jogszabályok értelmében

77. Az elektronikus hírközlési adatvédelmi irányelv 6. cikke szabályozza, hogy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtók milyen mértékben végezhetik törvényesen a forgalmi adatok feldolgozását, és csak bizonyos célokra – mint például a számlázásra, kapcsolásra és marketingre – korlátozza a forgalmi adatok felhasználását. A feldolgozás csak különleges feltételek fennállásakor, a marketing esetében például az érintett személyek beleegyezésével végezhető. Emellett az adatvédelmi irányelv 7. cikkének értelmében egyéb adatkezelők, mint például az információs társadalommal összefüggő szolgáltatást nyújtók is végezhetnek forgalmiadat-feldolgozást; az említett cikk megállapítja, hogy az adatkezelők csak abban az esetben dolgozhatnak fel személyes adatokat, ha a felsorolt jogi helyzetek – amelyekre szintén jogalapként hivatkoznak – közül legalább egy teljesül.

78. Ilyen jogi helyzet szerepel például az adatvédelmi irányelv 7. cikkének a) pontjában, amely az érintett hozzájárulását írja elő. Például amennyiben egy online kereskedő reklám vagy marketinganyag küldése céljából forgalmiadat-feldolgozást kíván végezni, engedélyt kell szereznie az érintett személytől. Egy másik, a 7. cikkben szereplő jogi helyzet egyes esetekben biztonsági okokból lehetővé teszi a forgalmi adatoknak a például biztonsági szolgáltatásokat nyújtó biztonsági vállalatok általi feldolgozását. Ez a 7. cikk f) pontján alapul, amely kimondja, hogy az adatkezelő feldolgozhatja a személyez adatokat, amennyiben „*az adatfeldolgozás az adatkezelő, vagy az adatokat megkapó harmadik fél, vagy felek jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezeknél az érdekeknél magasabb rendűek az érintett […] védelmet élvező érdekei az alapvető jogok és szabadságok tekintetében.*” Az adatvédelmi irányelv nem szolgál példákkal arra vonatkozóan, hogy a személyes adatok feldolgozása mely esetekben felel meg ennek a követelménynek. Ehelyett erről az adatkezelők döntenek eseti alapon, gyakran a nemzeti adatvédelmi hatóság és más hatóságok beleegyezésével.

79. Figyelembe kell venni az adatvédelmi irányelv 7. cikke, valamint az elektronikus hírközlési adatvédelmi irányelv 6. cikkének javasolt (6a) bekezdése közötti kapcsolatot. A 6. cikk javasolt (6a) bekezdése azon konkrét körülmények egyikét írja le, amelyben a 7. cikk fent idézett f) pontjában szereplő követelmények teljesülnek. A forgalmiadat-feldolgozásnak a hálózat- és információbiztonság szavatolásának elősegítése érdekében történő engedélyezésével a 6. cikk (6a) bekezdése valóban lehetővé teszi az adatkezelő jogszerű érdekének érvényesítése céljából történő adatfeldolgozást.

80. Ahogy az az alábbiakban kifejtésre kerül, az európai adatvédelmi biztos úgy véli, hogy a 6. cikk (6a) bekezdése se nem szükséges, se nem hasznos. Jogi szempontból elvben szükségtelen megállapítani, hogy egy konkrét adatfeldolgozási tevékenység – jelen esetben a forgalmi adatok biztonsági célokból történő feldolgozása – megfelel-e vagy sem az adatvédelmi irányelv 7. cikke f) pontjának, amely esetben az érintett fél hozzájárulása a 7. cikk a) pontjából kifolyólag szükséges lehet. Amint az fentebb már szerepel, ennek megítélése általában az adatkezelőkre hárul, például végrehajtási szinten a vállalatokra, az adatvédelmi hatóságokkal konzultálva, vagy – amennyiben szükséges – a bíróságokra. Az európai adatvédelmi biztos általánosságban úgy véli, hogy a konkrét esetekben a forgalmi adatok biztonsági okokból, jogszerűen és az érintettek alapvető jogainak és szabadságainak veszélyeztetése nélkül végzett feldolgozása valószínűleg megfelel az

adatvédelmi irányelv 7. cikke f) pontjában szereplő követelményeknek, és következésképpen elvégezhető. Ezen túlmenően sem az adatvédelmi irányelvben, sem az elektronikus hírközlési adatvédelmi irányelvben nem szerepel utalás arra, hogy bizonyos fajta, a 7. cikk f) pontjában szereplő követelményeknek megfelelő adatfeldolgozási tevékenységeket ki kellene zárni vagy különleges módon kellene kezelni, és ilyen kivétel nem is bizonyult szükségesnek. Ezzel szemben, amint az fentebb már szerepelt, úgy tűnik, hogy ez a fajta tevékenység sok esetben tökéletesen megfelel a jelenlegi szövegnek. Következésképpen elvben szükségtelen ezt a megállapítást jogi rendelkezéssel megerősíteni.

A 6. cikk (6a) bekezdésének európai parlamenti, tanácsi és bizottsági változatai

81. A fenti magyarázat értelmében fontos – bár nem szükséges – kiemelni, hogy az EP által elfogadott 181. módosítás mindazonáltal bizonyos mértékben az adatvédelmi jogszabályokban megtalálható, a magánélet védelmére és az adatvédelemre vonatkozó elvek figyelembevételével került megszövegezésre. Az EP 181. módosítása tovább foglalkozhatna az adatvédelemnek és a magánélet védelmének a kérdésével, például a „konkrét esetekben" szavaknak e cikk szelektív alkalmazása érdekében való beillesztésével, vagy egy konkrét megőrzési időszak belefoglalásával.

82. A 181. módosítás pozitív elemeket is tartalmaz. Megerősíti, hogy a feldolgozásnak összhangban kell lennie a személyes adatok feldolgozására vonatkozó bármely más adatvédelmi elvvel („*A 95/46/EK irányelv […] és a jelen irányelv […] rendelkezése[ine]k teljesítését nem érintve*"). Továbbá, noha a 181. módosítás megengedi a biztonsági célú forgalmiadat-feldolgozást, egyensúlyt állít fel az adatfeldolgozást végző alany érdekei és azon egyének érdekei között, akiknek az adatai feldolgozásra kerülnek, annak érdekében, hogy ilyen adatfeldolgozásra csak akkor kerülhessen sor, ha az egyének alapvető jogaira és szabadságaira vonatkozó érdekeket nem írják felül az adatfeldolgozást végző alany érdekei („*kivéve amennyiben az ilyen érdekeket felülírják az érintett alapvető jogaihoz és szabadságaihoz fűződő érdekek*"). E követelmény abból a szempontból lényeges, hogy lehetőséget ad a forgalmi adatok konkrét esetekben való feldolgozására; azonban nem engedi, hogy egy alany tömeges forgalmiadat-feldolgozást végezzen.

83. A módosítás újraszövegezett tanácsi változata dicséretre méltó elemeket tartalmaz, mint például a „*feltétlenül szükséges*" terminus megtartása, mely kiemeli e cikk alkalmazási körének korlátozottságát. Azonban a tanácsi változatból kimaradnak az adatvédelemre és a magánélet védelmére vonatkozó, fent említett biztosítékok. Noha elvben az általános adatvédelmi rendelkezések érvényesek tekintet nélkül arra, hogy vajon minden esetben történik-e rájuk való konkrét hivatkozás, a 6. cikk (6a) bekezdésének tanácsi verzióját mindazonáltal úgy lehet értelmezni, mintha teljes döntési jogot adna a forgalmi adatok feldolgozására anélkül, hogy az adatvédelemre és a magánélet védelmére vonatkozó bármely olyan biztosítéktól tenné függővé, mely valamennyi adatfeldolgozásra alkalmazandó. Ezért azzal lehet érvelni, hogy anélkül lehet forgalmi adatokat gyűjteni, tárolni és tovább felhasználni, hogy meg kellene felelni az olyan adatvédelmi elveknek és konkrét kötelezettségeknek, melyek egyébként a felelős felekre vonatkoznak, mint például a méltányos és törvényes feldolgozás kötelezettségének és az adatok titkos és biztonságos kezelésének. Továbbá – mivel nem történik hivatkozás az adatok tárolásának határidejét megszabó, érvényes adatvédelmi elvekre vagy konkrét határidőkre a cikken belül – a tanácsi változatot úgy lehet értelmezni, hogy lehetőséget ad forgalmi adatok biztonsági célú, határozatlan időre szóló gyűjtésére és feldolgozására.

84. Ezenfelül a szöveg egyes helyein a Tanács gyengítette a magánélet védelmével kapcsolatos biztonsági intézkedéseket azzal, hogy potenciálisan általánosabb megfogalmazást használt. Például kimaradt *az adatkezelő jogos érdekeire* való hivatkozás, ami kétséget ébreszt azt illetően, hogy mely típusú alanyok számára hasznos ez a kivétel. Kulcsfontosságú annak az elkerülése, hogy bármely felhasználó vagy alany számára lehetővé tegyük, hogy éljen e módosítással.

85. Az EP és a Tanács friss tapasztalatai azt mutatják, hogy nehéz jogilag meghatározni a biztonsági célú adatfeldolgozás törvényesen való elvégzésének mértékét és feltételeit. Nem valószínű, hogy bármely meglévő vagy jövőbeli cikk megszüntetné a kivétel túlzottan tág körű alkalmazásából fakadó nyilvánvaló kockázatokat. Ez nem jelenti azt, hogy ilyen feldolgozásra semmilyen körülmények között sem kerülhet sor. Azonban azt, hogy sor kerülhet-e rá és milyen mértékben, végrehajtási szinten jobban fel lehet mérni. Az ilyen feldolgozást végezni kívánó alanyoknak az adatvédelmi hatóságokkal – és esetleg a 29. cikk alapján létrehozott munkacsoporttal – meg kell vitatni az alkalmazási kört és a feltételeket. A másik megoldás az lenne, ha az elektronikus hírközlési adatvédelmi irányelv tartalmazna egy cikket, mely – az adatvédelmi hatóságok kifejezett engedélyétől függően – lehetőséget ad a forgalmi adatok biztonsági célú feldolgozására.

86. Figyelembe véve egyrészt a kockázatot, melyet a 6. cikk (6a) bekezdése jelent az egyének adatvédelemhez fűződő és a magánélet védelmére vonatkozó alapvető joga tekintetében, másrészt a tényt, hogy – amint e véleményben kifejtésre kerül – jogi szempontból e cikk szükségtelen, az európai adatvédelmi biztos arra a következtetésre jutott, hogy a legjobb eredmény az lenne, ha a javasolt 6. cikk (6a) bekezdése teljes egészében törlésre kerülne.

87. Amennyiben a 6. cikk (6a) bekezdésének jelenlegi változata mentén – és az európai adatvédelmi biztos ajánlása ellenében – bármely szöveg elfogadásra kerül, annak mindenesetre tartalmaznia kell a fent tárgyalt adatvédelmi biztosítékokat. Ezenfelül megfelelően integrálni kell a 6. cikk meglévő struktúrájába, lehetőség szerint új (2a) bekezdésként.

V. A JOGI SZEMÉLYEK LEHETŐSÉGE ARRA, HOGY BÍRÓSÁGI ELJÁRÁST INDÍTHASSANAK AZ ELEKTRONIKUS ADATVÉDELMI IRÁNYELV RENDELKEZÉSEINEK MEGSÉRTÉSE MIATT

88. Az EP elfogadta a 133. módosítást, mely lehetőséget ad az internetszolgáltatóknak és más jogi személyeknek – így fogyasztói szervezeteknek – arra, hogy bírósági eljárást indíthassanak az elektronikus adatvédelmi irányelv bármely rendelkezésének megsértése miatt ([19]). Sajnos ezt sem a Bizottság, sem a Tanács nem fogadta el. Az európai adatvédelmi biztos úgy véli, hogy e módosítás igen pozitív, és megtartását javasolja.

89. Ahhoz, hogy e módosítás fontosságát felmérjük, el kell fogadnunk, hogy a magánélet védelmének és az adatvédelemnek a területén az egy személyt ért kár egyénenként véve általában önmagában nem elegendő ahhoz, hogy az adott személy bírósági eljárást indíthasson. Az egyének általában egyedül nem fordulnak bírósághoz azzal, hogy valakitől kéretlen üzeneteket kaptak, vagy hogy egy nyilvántartásban tévesen szerepelnek. E módosítás lehetővé tenné a fogyasztók közös érdekvédelmét biztosító fogyasztói szervezeteknek és szakszervezeteknek, hogy nevükben jogi eljárást indítsanak a bíróság előtt. Az érvényesítési mechanizmusok nagyobb változatossága valószínűleg szintén magasabb szintű megfelelést ösztönözne, és ezért az elektronikus adatvédelmi irányelv rendelkezéseinek hatékony alkalmazása érdekében áll.

90. Néhány tagállam jogalkotásában található olyan példa, mely már most előirányozza a csoportos jogorvoslat lehetőségét annak érdekében, hogy a fogyasztóknak vagy érdekcsoportoknak lehetővé tegye, hogy a kárt okozó féltől kártérítést igényeljenek.

91. Ezenfelül egyes tagállamok kompenzációs jogszabályai ([20]) feljogosítják a fogyasztókat, érdekcsoportokat arra, hogy (az *érintett versenytárson* felül) a jogsértés elkövetőjével szemben jogi eljárást indítsanak. E megközelítés azon a megfontoláson alapul, hogy a versenyjogot megsértő vállalatok valószínűleg hasznot húznak a jogsértésből, mivel a csak jelentéktelen kárt elszenvedő fogyasztók általában vonakodnak ügyükkel a bírósághoz fordulni. E megfontolás értelemszerűen az adatvédelemnek és a magánélet védelmének a területére is vonatkozik.

92. Ami még fontosabb – amint fent említésre került: lehetővé tenni az olyan jogalanyok számára, mint pl. a fogyasztói szervezetek és a PPECS-ek, hogy jogi eljárást indítsanak, erősíti a fogyasztók helyzetét és elősegíti az adatvédelmi jogszabályoknak való általános megfelelést. Amennyiben a jogsértő vállalatok számára nagyobb a per kockázata, valószínűleg többet fordítanak majd az adatvédelmi jogszabályoknak való megfelelésre, aminek következtében a magánélet és a fogyasztók védelme hosszú távon erősödni fog. Mindezen indokok alapján az európai adatvédelmi biztos felkéri az EP-t és a Tanácsot, hogy fogadjon el egy olyan rendelkezést, mely lehetőséget ad a jogalanyoknak, hogy bíróság előtt jogi eljárást indíthassanak az elektronikus adatvédelmi irányelv bármely rendelkezésének megsértése miatt.

VI. KÖVETKEZTETÉS

93. A Tanács közös álláspontja, az EP első olvasata és a Bizottság módosított javaslata eltérő mértékben olyan pozitív elemeket tartalmaz, melyek erősíthetik az egyének magánéletének és személyes adatainak védelmét.

94. Azonban az európai adatvédelmi biztos úgy véli, hogy lehetőség van a javításra, különösen a tanácsi közös álláspont esetében, mely sajnos nem tartotta meg az EP néhány olyan módosítását, melynek célja az egyének magánéletére és személyes adataira vonatkozó védelem biztosítása. Az európai adatvédelmi biztos sürgeti az EP-t és a Tanácsot, hogy állítsák helyre az EP első olvasatában szereplő, a magánélet védelmével kapcsolatos biztosítékokat.

95. Az európai adatvédelmi biztos tovább úgy véli, hogy az irányelv néhány rendelkezését megfelelő lenne egyszerűsíteni. Ez különösen igaz a biztonság megsértésére vonatkozó rendelkezések esetében, mivel az európai adatvédelmi biztos úgy véli, hogy a biztonság megsértéséről való értesítésben rejlő lehetőségeket akkor lehet a legjobban kiaknázni, ha a jogi keret már kezdettől fogva helyes alapokon nyugszik. Az európai adatvédelmi biztos végül úgy gondolja, hogy az irányelv néhány rendelkezésének megfogalmazását megfelelő lenne javítani és pontosítani.

96. A fentiek alapján az európai adatvédelmi biztos sürgeti az EP-t és a Tanácsot, hogy fokozza az elektronikus adatvédelmi irányelv néhány rendelkezésének javítása és pontosításra érdekében tett erőfeszítéseit, miközben ismét vezesse be a szövegbe az EP első olvasatban elfogadott azon módosításait, melyek célja az adatvédelem és a magánélet védelme megfelelő szintjének biztosítása. E célból az alábbi 97–100. pontok összegzik az érintett kérdéseket, valamint ajánlásokat és szövegezési javaslatokat tartalmaznak. Az európai adatvédelmi biztos felkéri az összes érintett felet, hogy ezeket vegye figyelembe az elektronikus adatvédelmi irányelv végső elfogadásához vezető folyamat során.

A biztonság megsértése

97. Az Európai Parlament, a Bizottság és a Tanács mind másmás megközelítést képvisel a biztonság megsértéséről való értesítéssel kapcsolatban. A három modell között többek között az alábbiak tekintetében van eltérés: az értesítési kötelezettség körébe tartozó alanyok, az értesítést keletkeztető szabvány vagy feltétel, az értesítésre jogosult adatalanyok stb. Szükséges, hogy az EP és a Tanács mindent tegyen meg annak érdekében, hogy szilárd jogi keretet dolgozzon ki a biztonság megsértésével kapcsolatban. E célból az EP-re és a Tanácsra az alábbi feladatok hárulnak:

([19]) Az EP első olvasata, 13. cikk (6) bekezdés.

([20]) Lásd például a tisztességtelen versenyről szóló német jogszabályt (UWG 8. cikk).

— A biztonság megsértésére vonatkozóan az EP, a Tanács és a Bizottság szövegében szereplő meghatározás *megtartása*, mivel az elég tág ahhoz, hogy az összes olyan releváns helyzetet magába foglalja, melyek feljogosítanak a biztonság megsértéséről való értesítésre

— A javasolt értesítési kötelezettség által lefedett alanyok körére vonatkozóan az információs társadalommal összefüggő szolgáltatások nyújtóira való *kiterjesztés*. Az internetes kereskedők, online bankok, online gyógyszertárak biztonságát éppúgy meg lehet sérteni, mint a hírközlési társaságokét, ha nem még inkább. A polgárok elvárják, hogy ne csak akkor kapjanak értesítést, ha az internetszolgáltató biztonságát sértik meg, hanem különösen akkor is, amikor ez az online bankjaikkal és online gyógyszertáraikkal történik.

— Az értesítés keletkeztetését tekintve a módosított javaslat „*ésszerű alapon valószínű, hogy kárt okoz*" szabványosított feltétele olyan megfelelő szabály, mely a rendszer funkcionalitását biztosítja. Mindazonáltal fontos biztosítani, hogy a „kárt okoz" kellőképpen tág jelentésű legyen ahhoz, hogy lefedje az egyének magánéletére vagy jogos érdekeire nézve negatív hatások minden releváns esetét. Máskülönben ajánlatos lenne új szabványt kialakítani, amelynek értelmében kötelező az értesítés, „*amennyiben a biztonság megsértése ésszerű alapon valószínű, hogy hátrányos befolyással van az egyének számára*". A Tanács megközelítése, amely előírja, hogy a sérülés *komoly* hatással kell, hogy legyen valakinek a magánéletére, nem biztosítana megfelelő védelmet az egyéneknek, amennyiben ez a szabvány megköveteli, hogy a magánéletre gyakorolt hatás „komoly" legyen. Ez ugyancsak teret enged a szubjektív értékelésnek.

— Míg a hatóság arra irányuló szerepe, hogy meghatározza, hogy vajon egy érintett alany köteles-e értesíteni az egyéneket, bizonyára pozitív hatással bír, gyakorlatban nehezen megvalósítható és nehezen alkalmazható, valamint más fontos prioritásoktól vonhat el forrásokat. Amennyiben a hatóságok nem képesek rendkívül gyors reagálásra, az európai adatvédelmi biztos attól tart, hogy egy ilyen rendszer az egyének védelmén még gyengíthet is, és indokolatlan terhet róhat a hatóságokra. Tehát egészében véve az európai adatvédelmi biztos olyan rendszer *létrehozását* javasolja, melyben az érintett alanyok feladata, hogy felmérjék, értesítési kötelezettségük fennáll-e.

— Annak érdekében, hogy a hatóságok a lefedett alanyok által az értesítési kötelezettségükkel kapcsolatban elvégzett értékeléseket felügyelhessék, az alábbi biztosítékokat kell *megvalósítani*:

  — *Annak biztosítása*, hogy az ilyen alanyok a biztonság megsértésének minden olyan esetéről kötelesek legyenek értesíteni a hatóságokat, melyek megfelelnek a kellő szabványnak.

  — Felügyeleti szerep *biztosítása* a hatóságok számára, mely lehetővé teszi, hogy a hatékonyság érdekében szelektíven járjanak el. A fentiek elérése érdekében az alábbi szöveget kell beilleszteni: „*Ha az előfizetőt vagy az érintett személyt még nem értesítették, a sérülés természetének mérlegelése után az illetékes nemzeti hatóság kötelezheti erre a PPECS-eket vagy ISSP-ket.*"

  — Új rendelkezés *elfogadása*, mely szerint a alanyok kötelesek részletes és átfogó belső ellenőrzési nyomvonalat vezetni. Ezt az alábbi szövegezés elfogadásával lehetne elérni: „*A PPECS-eknek és ISSP-knek átfogó nyilvántartást kell vezetniük, amely részletezi a biztonság megsértésének bekövetkezett eseteit, az azokhoz kapcsolódó műszaki információkat és a megtett ellenlépéseket. A nyilvántartásban meg kell említeni minden, az előfizetők vagy érintett egyének, valamint az illetékes nemzeti hatóságok számára kiadott értesítést, beleértve azok dátumát és tartalmát. A nyilvántartást kérésre át kell nyújtani az illetékes nemzeti hatóságnak.*"

— A biztonság megsértésére vonatkozó keret következetes végrehajtása érdekében annak *lehetővé tétele* a Bizottság számára, hogy az európai adatvédelmi biztossal, a 29. cikk alapján létrehozott munkacsoporttal és más érdekeltekkel folytatott konzultációt követően technikai végrehajtó intézkedéseket fogadjon el.

— Az értesítendő egyének tekintetében a Bizottság vagy az EP „érintett egyének" vagy „érintett felhasználók" terminust *kell használni*, mivel ez az összes olyan egyénre kiterjed, akinek adatai veszélybe kerültek.

Nyilvánosan elérhető magánhálózatok

98. Az elektronikus hírközlési szolgáltatásokat gyakran nem nyilvános, hanem magánhálózatokon (pl. hotelekben, repülőtereken hozzáférhető Wi-Fi-hálózatokon) bocsátják a nyilvánosság rendelkezésére, melyekre az irányelv nyilvánvalóan nem vonatkozik. Az EP elfogadta az irányelv alkalmazási körét annak érdekében bővítő 121. módosítást (3. cikk), hogy kiterjedjen a nyilvános és magán távközlési hálózatokra, valamint a nyilvánosan elérhető magánhálózatokra. E célból az EP-re és a Tanácsra az alábbi feladatok hárulnak:

— A 121. módosítás lényegének *megtartása*, azonban *átszövegezése* annak érdekében, hogy az elektronikus hírközlési adatvédelmi irányelv hatálya csak „*a Közösségben a nyilvánosan elérhető hírközlési szolgáltatások nyilvános vagy nyilvánosan elérhető magán hírközlő hálózaton történő nyújtásával összefüggő személyes adatok kezelésére*" terjedjen ki. A teljes egészében magánműködtetésű hálózatok (a nyilvánosan elérhető magánhálózatokkal ellentétben) nem tartoznának kifejezetten az alkalmazási körbe.

— Ennek megfelelően a működtetési rendelkezések annak érdekében való *módosítása*, hogy a nyilvános hálózatok mellet kifejezett említést tegyenek a nyilvánosan elérhető magánhálózatokra is.

— Az alábbi fogalommeghatározást tartalmazó módosítás *beillesztése*: *„nyilvánosan elérhető magánhálózat: magánműködtetésű hálózat, melyhez a nagy nyilvánosság tagjai általában korlátozott hozzáféréssel rendelkeznek akár fizetés révén, akár más szolgáltatásokkal vagy ajánlatokkal összefüggésben, az alkalmazandó feltételek elfogadásától függően”*. Ez az új alkalmazási kör által lefedett alanyok tekintetében nagyobb jogi biztonságot nyújt.

— Új preambulumbekezdés *elfogadása*, mely szerint a Bizottság nyilvános konzultációt folytat az elektronikus hírközlési adatvédelmi irányelvnek a magánhálózatokra való alkalmazásáról, az európai adatvédelmi biztos, a 29. cikk alapján létrehozott bizottság és más érdekeltek részvételével. A preambulumbekezdés azt is kimondaná, hogy a Bizottság a nyilvános konzultáció eredményeként benyújtja a megfelelő javaslatokat az elektronikus hírközlési adatvédelmi irányelv hatálya alá tartozó alanyok körének kiterjesztésére vagy korlátozására vonatkozóan.

Biztonsági célú forgalmiadat-feldolgozás

99. Az EP az első olvasatban elfogadta a 181. Módosítást (6. cikk (6a) bekezdés), mely engedélyt ad a biztonsági célú forgalmiadat-feldolgozásra. A Tanács közös álláspontja új változatot fogadott el, mely a magánélet védelmére vonatkozó biztosítékok közül többet meggyengített. E tekintetben az európai adatvédelmi biztos azt javasolja, hogy az EP és a Tanács:

— Teljes egészében *vesse el* ezt a cikket, mivel nincs rá szükség, és a vele való visszaélés esetén veszélybe sodorja az egyének adatainak és magánéletének védelmét.

— A másik lehetőség az, hogy amennyiben a 6. cikk (6a) bekezdése jelenlegi verziójának valamely változata kerül elfogadásra, abba *foglalja bele* az e véleményben kifejtett (az EP módosításában foglaltakhoz hasonló) adatvédelmi biztosítékokat.

Bírósági eljárások az elektronikus hírközlési adatvédelmi irányelv megsértése esetén

100. A Parlament elfogadta a 133. módosítást (13. cikk (6) bekezdés), mely lehetőséget ad a jogalanyoknak arra, hogy bírósági eljárást indítsanak az irányelv bármely rendelkezésének megsértése esetén. Sajnos ezt a Tanács nem tartotta meg. A Tanács és az EP feladata, hogy:

— *Hagyja jóvá* azt a rendelkezést, mely lehetőséget ad a jogalanyoknak (mint pl. a fogyasztói és kereskedelmi szervezeteknek) arra, bírósági eljárást indíthassanak az elektronikus adatvédelmi irányelv bármely rendelkezésének megsértése miatt (és ne csak a spamre vonatkozó rendelkezések megsértése miatt, ahogy a közös álláspont és a módosított javaslat jelenlegi megközelítésében szerepel). Az érvényesítési mechanizmusok nagyobb választéka előmozdítja az elektronikus adatvédelmi irányelvben foglalt rendelkezések egészének való magasabb szintű megfelelést és e rendelkezések hatékonyabb alkalmazását.

Szembenézés a kihívásokkal

101. Az összes fenti kérdésben az EP-nek és a Tanácsnak képesnek kell lennie olyan megfelelő szabályok és rendelkezések kidolgozására, melyek gyakorlatban megvalósíthatóak, funkcionálisak és tiszteletben tartják az egyéneknek a magánélet védelmére és az adatvédelemre vonatkozó jogait. Az európai adatvédelmi biztos reméli, hogy az érintett felek mindent megtesznek e feladat megoldása érdekében, és hogy e vélemény segítséget nyújt munkájukban.

Kelt Brüsszelben, 2009. január 9-én.

Peter HUSTINX

európai adatvédelmi biztos