I

(Állásfoglalások, ajánlások és vélemények)

VÉLEMÉNYEK

EURÓPAI ADATVÉDELMI BIZTOS

Az Európai Adatvédelmi Biztos véleménye a Németországi Szövetségi Köztársaságnak a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló 2007/…/IB határozat végrehajtásáról szóló tanácsi határozat elfogadására irányuló kezdeményezéséről

(2008/C 89/01)

AZ EURÓPAI ADATVÉDELMI BIZTOS,

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

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

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

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

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT

I. **BEVEZETÉS**

1. A Hivatalos Lapban 2007. november 9-én megjelent a Németországi Szövetségi Köztársaságnak a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló 2007/…/IB határozat végrehajtásáról szóló tanácsi határozat elfogadására irányuló kezdeményezése ([1]) (a továbbiakban: a kezdeményezés). A kezdeményezést egy 2007. október 18-i melléklet ([2]) (a továbbiakban: a melléklet) egészíti ki, amely a 2007/…/IB határozat végrehajtására vonatkozó további részleteket tartalmaz.

2. A végrehajtó határozatra irányuló kezdeményezéssel kapcsolatban nem kérték ki az Európai Adatvédelmi Biztos tanácsát. Ezért ezt a véleményt a tanácsi határozatra irányuló, 2007. április 4-i kezdeményezésre vonatkozó véleménnyel ([3]) megegyező módon, saját kezdeményezésére közli.

3. Ha valamely tagállam az EU-Szerződés VI. címe alapján jogalkotási intézkedést kezdeményez, nem köteles ugyan kikérni az Európai Adatvédelmi Biztos tanácsát, viszont az eljárás nem is zárja ki a tanácskérés lehetőségét. Továbbá, az Európai Adatvédelmi Biztos 2007. április 4-i véleményében azt javasolta, hogy a kérdéses tanácsi határozat 34. cikke az alábbi mondattal egészüljön ki: „A Tanács az ilyen végrehajtási intézkedésekről konzultál az európai Európai Adatvédelmi Biztossal.” Az ajánlást azonban a felsorakoztatott érvek ellenére nem fogadták el, pedig a végrehajtási intézkedések ebben az esetben leggyakrabban a személyes adatok feldolgozását érintik. A Németországi Szövetségi Köztársaság mostani kezdeményezése egyértelműen igazolja a fenti érvek helytállóságát.

4. Az Európai Adatvédelmi Biztos nem von le semmilyen érdemi következtetést ebből az eredményből. Beleillik a Tanács által választott megközelítésbe, hogy a lehető legkevésbé módosítsa a kezdeményezést annak érdekében, hogy teljes mértékben biztosítsa a korábban több tagállam által aláírt Prümi Szerződés szövegével való összeegyeztethetőséget. Az Európai Adatvédelmi Biztos a vélemény további részében még tárgyalja e megközelítés demokratikus hatását.

II. **ÖSSZEFÜGGÉSEK ÉS JOGI KERET**

5. A Prümi Szerződést 2005. májusában – az EU-Szerződés keretein kívül – hét tagállam írta alá. Később további tagállamok is csatlakoztak e szerződéshez.

([1]) HL C 267., 2007.11.9., 4. o.

([2]) A melléklet a Hivatalos Lapban még nem jelent meg, de 11045/1/07 REV 1 ADD 1 sz. tanácsi dokumentumként nyilvánosan hozzáférhető.

([3]) HL C 169., 2007.7.21., 2. o.

6. A Prümi Szerződést a Szerződés 44. cikkén alapuló, 2006. december 5-én megkötött végrehajtási megállapodás egészíti ki. Ez a végrehajtási megállapodás szükséges a Prümi Szerződés működéséhez.

7. A Prümi Szerződés főbb elemei a 15 tagállam kezdeményezéséről szóló 2007/…/IB tanácsi határozat elfogadását követően – amelyről a Tanács már politikai megállapodást ért el – beépülnek az Európai Unió jogi keretébe. Az elemek beépítése már a kezdetektől fogva az EU-Szerződés részes feleinek szándéka volt, amit a Prümi Szerződés preambuluma is bizonyít.

8. A tanácsi határozat elfogadásához vezető jogalkotási eljárás során a cél már nem a nagy horderejű kérdések megvitatása, hanem a Prümi Szerződés vívmányaira vonatkozó megállapodás volt. Ez a cél azért is vált egyre fontosabbá, mert a jogalkotási eljárás ideje alatt több tagállamban is folytatódott a Szerződés megerősítésének folyamata, és a Szerződés hatályba lépett.

III. A VÉLEMÉNY TÁRGYA ÉS KÖZPONTI KÉRDÉSE

9. Ez a vélemény a végrehajtási szabályokról szóló tanácsi határozattervezetre összpontosít. Az Európai Adatvédelmi Biztosnak a prümi kezdeményezésről szóló tanácsi határozatra vonatkozó véleményében szereplő megállapítások továbbra is érvényesek, és e helyen nem ismételjük meg azokat, kivéve, ha ez azon kérdések kiemeléséhez szükséges, amelyekkel a jogalkotó a végrehajtási szabályok révén még foglalkozhat.

10. Ezzel összefüggésben hangsúlyozni kell, hogy a végrehajtási szabályok sajátos jelentőséggel bírnak, ugyanis – egyes adminisztratív és technikai rendelkezések mellett – a rendszernek és működésének alapvető vonatkozásait és eszközeit határozzák meg. A végrehajtási szabályok 1. fejezete például a Prümről szóló tanácsi határozatban használt kifejezések fogalommeghatározásait tartalmazza. A végrehajtási szabályok ezenkívül közös rendelkezéseket állapítanak meg az adatcserére vonatkozóan (2. fejezet), és meghatározzák a DNS-adatok (3. fejezet), a daktiloszkópiai adatok (4. fejezet), és a gépjármű-nyilvántartási adatok (5. fejezet) cseréjének konkrét jellemzőit. A 6. fejezet záró rendelkezései további, kézikönyvekben szereplő végrehajtási szabályok elfogadására, valamint a határozat alkalmazásának értékelésére vonatkozó fontos rendelkezéseket tartalmaznak.

11. Ezenkívül a melléklet vizsgálatára is sor kerül, amilyen mértékben hozzájárul, vagy hozzá kell járulnia a javasolt rendszer jellemzőinek és az adatalanyok számára nyújtandó biztosítékoknak a meghatározásához.

IV. ÁLTALÁNOS SZEMPONTOK

Korlátozott mozgástér

12. Az Európai Adatvédelmi Biztos megállapítja, hogy a Prümi Egyezmény tekintetében már létező, hatályos végrehajtási szabályok előreláthatólag ebben az esetben is erőteljesen csökkentik a Tanács valóságos mozgásterét. A kezdeményezés (3) preambulumbekezdése és 18. cikke egyaránt megállapítja, hogy a végrehajtási határozat és a kézikönyvek is a Prümi Egyezmény adminisztratív és technikai végrehajtásával kapcsolatos, 2006. december 5-én elfogadott végrehajtási rendelkezéseken alapulnak. Ennek alapján, a jelenlegi kezdeményezés értelmében mind a 27 tagállamnak a Prümi Egyezményt aláíró 7 tagállam által kijelölt utat kell követnie.

13. Ez a megközelítés gátolja a valóban átlátható és demokratikus jogalkotási folyamatot, ugyanis jelentős mértékben hátráltatja a széles körű vita megtartásának lehetőségét, és az Európai Parlament jogalkotói szerepének, valamint a többi intézmény – köztük az Európai Adatvédelmi Biztos – tanácsadói szerepének tényleges figyelembevételét. Az Európai Adatvédelmi Biztos a kezdeményezésnek és mellékletének nyílt megvitatását ajánlja, mégpedig valamennyi intézményi szereplő valóságos hozzájárulásával, és az Európai Parlament teljes körű társjogalkotói szerepének érvényesítésével, amely szerepet a december 13-án, Lisszabonban aláírt reformszerződés hatályba lépését követően e területen biztosítani fog számára.

Az adatvédelem jogi kerete és a harmadik pillérbeli adatvédelemről szóló kerethatározat-tervezethez fűződő viszonya

14. Az adatvédelem alkalmazandó jogi kerete összetett és ingadozó. A prümi kezdeményezésének 6. fejezete valóban tartalmaz néhány biztosítékot és konkrét szabályt az adatvédelemre vonatkozóan. Ezek a konkrét szabályok azonban nem önmagukban léteznek, és megfelelő működésükhöz szükség van arra, hogy a rendőri és igazságügyi hatóságok által feldolgozott személyes adatok védelmét szolgáló teljesen kidolgozott, általános keretbe illeszkedjenek. A prümi kezdeményezésének 25. cikke jelenleg az Európa Tanács 108. sz. egyezményére hivatkozik. Az Európai Adatvédelmi Biztos azonban már többször hangsúlyozta, hogy a 108. sz. egyezményben foglalt elveket pontosítani kell, ezáltal biztosítva a magas szintű, összehangolt adatvédelmet, amely képes mind az állampolgárok jogait, mind a bűnüldözés hatékonyságát szavatolni a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben ([1]).

15. Ennek fényében a Bizottság már 2005. októberében egy általános eszközre – a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló tanácsi kerethatározat-tervezet (a továbbiakban: a harmadik pillérbeli adatvédelemről szóló kerethatározat-tervezet) – vonatkozó javaslatot terjesztett elő. Ezt a javaslatot a Tanács még mindig nem fogadta el, azaz további vitákra és lehetséges módosításokra, ezzel együtt az elfogadás és a végrehajtás további elhúzódására lehet számítani. Mostanra továbbá az is világos, hogy a kerethatározatot jelenlegi formájában csak a más tagállamokkal kicserélt személyes adatokra lehetne alkalmazni, az országon belüli adatfeldolgozásra viszont nem ([2]).

([1]) Lásd az Európai Adatvédelmi Biztos közelmúltbeli véleményét a prümi kezdeményezésről (57–76. cikk), és 2007. április 27-i harmadik véleményét a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló tanácsi kerethatározati javaslatról (14. cikk) (HL C 139., 2007.6.23., 1. o.).

([2]) A javaslat legutóbbi tervezete 16397/07 dokumentumszámon férhető hozzá a tanácsi nyilvántartásban.

16. Ezenkívül megállapítható, hogy a harmadik pillérbeli adatvédelemről szóló kerethatározat-tervezet jelenlegi megszövegezésében – bár célja a magas szintű adatvédelem biztosítása – csak minimális összehangolásról és biztosítékokról rendelkezik. Ez azt jelenti, hogy bizonyos eszközöknek – például a jelenlegi kezdeményezésnek –, amelyek fel tudták volna használni az adatvédelem átfogó, általános keretét, most saját maguknak kell a harmadik pillérbeli adatvédelemről szóló kerethatározat-tervezet hiányosságait pótolniuk.

17. Ezért az Európai Adatvédelmi Biztos egyrészt ismételten kijelenti, hogy a Prümről szóló tanácsi határozatoknak nem szabad hatályba lépniük addig, amíg a tagállamok nem hajtották végre a harmadik pillérbeli adatvédelemről szóló általános kerethatározatot. Ennek a feltételnek kifejezetten szerepelnie kellene a kezdeményezésben, és az adatcsererendszeren belüli adatvédelmi biztosítékok helyes működését is előzőleg megfelelő módon ellenőrizni kell. Ezzel összefüggésben az egyes jogi eszközök közötti kapcsolatokat is egyértelművé kell tenni, biztosítva, hogy a harmadik pillérbeli adatvédelemről szóló kerethatározat „lex generalisként" működjék, ugyanakkor lehetővé téve a prümi kezdeményezésében megállapított további konkrét garanciák és szigorúbb egyedi előírások alkalmazhatóságát ([1]).

18. Másrészt a jogalkotónak egyértelművé kellene tennie azt is, hogy a prümi kezdeményezésének 6. fejezetében megállapított, a DNS-re, ujjlenyomatokra és gépkocsi-nyilvántartásra vonatkozó konkrét adatvédelmi szabályok nemcsak ezen adatok cseréjére, hanem összegyűjtésükre, tárolásukra és országon belüli feldolgozásukra, valamint a tanácsi határozat hatálya alá tartozó egyéb személyes adatok szolgáltatására is érvényesek. Ez az egyértelműsítés összhangban lenne a prümi kezdeményezésének 24.2. cikkével, és logikusan következne a fenti típusú adatok gyűjtésére, tárolására és megosztására vonatkozó tagállami kötelezettségből.

19. Ez a kérdés még jelentősebb, ha figyelembe vesszük, hogy a harmadik pillérbeli adatvédelemről szóló kerethatározat-tervezet hatálya a személyes adatok hazai feldolgozására valószínűleg nem fog kiterjedni. A Tanács így döntött, de egyidejűleg jelezte, hogy a jogalap e döntéstől függetlenül vonatkozhat az említett feldolgozási műveletekre is. A fentiek alapján, mivel a kérdéses kezdeményezéscsomag – a prümi kezdeményezése és annak végrehajtási szabályai – előírja bizonyos adatbázisok (például a DNS-adatbázis) létrehozásának és karbantartásának kötelezettségét, az adatgyűjtéshez és -tároláshoz kapcsolódó feldolgozási műveletekre – nevezetesen a DNS-profilok gyűjtésére és tárolására – vonatkozó biztosítékokról is rendelkeznie kell. Másrészt, ha az említett jogi eszközök alkalmazása az adatcserére korlátozódna, nem tartalmaznának a személyes adatok védelmére vonatkozó megfelelő rendelkezéseket, márpedig az EU-Szerződés 30. cikke (1) bekezdésének b) pontján alapuló bármely intézkedésre ilyen védelemnek kell vonatkoznia.

([1]) E ponttal kapcsolatban gondosan mérlegelni kell és meg kell vitatni a harmadik pillérbeli adatvédelemről szóló kerethatározat-tervezet legutóbbi változatának 27b. cikkét.

20. Az Európai Adatvédelmi Biztos felszólítja a jogalkotót, hogy az EU-Szerződés 30. cikke (1) bekezdésének b) pontjával összhangban biztosítsa, hogy a kérdéses kezdeményezés hatálybalépését megelőzően – az általános rendelkezéseket és a konkrét biztosítékokat tartalmazó különböző jogi eszközöket ötvöző – világos, hatékony és átfogó adatvédelmi jogi keret jöjjön létre.

21. Az Európai Adatvédelmi Biztos e véleményében adott esetben utalni fog azokra a kérdésekre, amelyekkel a harmadik pillérbeli adatvédelemről szóló kerethatározat-tervezetben nem, vagy nem kimerítően foglalkoztak, és amelyeket ezért a szóban forgó kezdeményezésben megállapított rendszer végrehajtásakor figyelembe kell venni.

A döntéshozatali folyamat és a végrehajtási szabályok átláthatósága

22. Az Európai Adatvédelmi Biztos hangsúlyozza, hogy az átláthatóság a döntéshozatali folyamatnak és a végrehajtási szabályoknak is fontos jellemzője. Az átláthatóságnak ezért egyrészt lehetővé kell tennie valamennyi érintett intézményi szereplő teljes körű és tényleges részvételét, másrészt elő kell segítenie a nyilvános vitát és az állampolgárok megfelelő tájékoztatását.

23. Ebben az esetben sajnos több tényező is akadályozza az átláthatóságot: nincs indokolás, amely ismertetné a tervezett intézkedések okait, hatékonyságukat és a lehetséges politikai alternatívákat; a melléklet még mindig hiányos – pl. még nem hirdették ki a Hivatalos Lapban, nem fordították le valamennyi hivatalos nyelvre, a cikkekre való hivatkozások és a terminológia gyakran pontatlan, és a DNS-adatbázisok tartalmára vonatkozó tagállami nyilatkozatok nem állnak rendelkezésre; maga a kezdeményezés nem állapít meg olyan kötelezettségeket vagy mechanizmusokat, amelyek az állampolgároknak a hozott intézkedésekről és ezek módosításairól szóló megfelelő tájékoztatását szolgálják.

24. Az Európai Adatvédelmi Biztos ezért az intézkedések átláthatóságának javítását ajánlja, mégpedig a melléklet végleges változatának mielőbbi elkészítése és olyan mechanizmusok kialakítása révén, amelyekkel az állampolgárok a rendszer jellemzőiről, saját jogaikról és ezek gyakorlásáról tájékoztathatók. A kezdeményezésben vagy a mellékletben kifejezetten rendelkezni kell erről az információs kampányról.

A rendszer mérete

25. A kérdéses kezdeményezés szorosan követi a Prümi Szerződés végrehajtási szabályait. Mindazonáltal – amint azt már a Tanács prümi kezdeményezéséről szóló véleményben is megjegyeztük (33–35. cikk) – a néhány tagállam közötti információcserére tervezett mechanizmusok nem feltétlenül alkalmasak egy jóval nagyobb méretű rendszer, azaz 27 tagállam közötti információcsere számára, ezért módosításukra lehet szükség.

26. A kisebb méretű rendszer mind a bűnüldözés, mind az érintett személyek személyes adatainak védelmével kapcsolatos kockázatok felügyelete tekintetében valóban kedvez a résztvevő tagállamok közötti szorosabb kapcsolatoknak. A nagyobb rendszer esetében más a helyzet, ugyanis az adatok gyűjtésével, tárolásával és feldolgozásával kapcsolatos – különös tekintettel a DNS-profilokra és az ujjlenyomatokra – országos gyakorlatok és jogi szabályozások jelentős mértékben eltérnek. Ezenkívül a különböző nyelvek és különböző jogi fogalmak használata is befolyásolhatja az eltérő jogi hagyományokkal rendelkező országok közötti adatcsere pontosságát. Az Európai Adatvédelmi Biztos ezért felkéri a jogalkotót, hogy a szóban forgó kezdeményezés további megvitatásakor megfelelően vegye figyelembe a rendszer méretét, és gondoskodjon arról, hogy a résztvevő tagállamok számának növekedése ne vonja maga után a hatékonyság csökkenését. Különösen, a végrehajtási szabályokban a nyelvi különbségeket is figyelembe vevő, egyedi adatközlési formátumokat kell megállapítani, és az adatcsere pontosságát folyamatosan felügyelni kell.

Az adatvédelmi hatóságok bevonása

27. A kezdeményezésben el kell ismerni a független felügyeleti hatóságok által a jelentős méretű, határokon átnyúló adatcsere tekintetében játszott fontos szerepet, és lehetővé kell tenni számukra feladataik hatékony elvégzését.

28. Először is, a jelenlegi jogi keret nem rendelkezik arról, hogy az illetékes felügyeleti hatóságokkal konzultációt kellene folytatni, vagy azokat be kellene vonni az alábbiakba: a végrehajtási szabályok és a mellékletek módosítása (a kezdeményezés 18. cikke), az adatvédelmi szabályok tagállami végrehajtása (20. cikk) vagy az adatcsere értékelése (21. cikk). Rendkívül sajnálatos például, hogy a melléklet IV. fejezete, amely részletesen megállapítja a végrehajtás értékelésének szabályait, egyáltalán nem említi meg az illetékes adatvédelmi hatóságokat. Az Európai Adatvédelmi Biztos azt ajánlja, hogy a fenti cikkek kifejezetten ismerjék el az ilyen hatóságok alapvető tanácsadói szerepét.

29. Másodszor, a kezdeményezésnek biztosítania kell, hogy a tagállamok (pótlólagos) forrásokat nyújtsanak az adatvédelmi hatóságoknak, amelyek a tervezett rendszer végrehajtásából eredő felügyeleti feladataik ellátásához szükségesek.

30. Harmadszor, a kezdeményezésnek rendelkeznie kell arról, hogy az illetékes adatvédelmi hatóságok rendszeres uniós szintű találkozót tartsanak tevékenységük összehangolása és az említett eszközök harmonizált alkalmazása céljából. Ez a lehetőséget kifejezetten szerepeltetni kell a kezdeményezésben, amennyiben a harmadik pillérbeli adatvédelemről szóló kerethatározat nem hozza létre az adatvédelmi hatóságok uniós szintű általánosabb fórumát.

V. **KONKRÉT KÉRDÉSEK**

Fogalommeghatározások

31. A kezdeményezés 2. cikke több fogalommeghatározást tartalmaz, amelyek részben tükrözik a tanácsi határozatban szereplő meghatározásokat. Először is hangsúlyozni szükséges, hogy a kezdeményezés 2. cikkének fogalommeghatározásai nem fedik pontosan a tanácsi határozatban – különösen annak 24. cikkében – található meghatározásokat. A jogalkotónak a végrehajtási problémák megelőzésére összhangba kell hoznia a két szöveg megfogalmazását.

32. Másodszor, az Európai Adatvédelmi Biztos, amint azt már a prümi kezdeményezéséről szóló véleményében is kifejtette, sajnálja, hogy hiányzik a személyes adatokra vonatkozó pontos fogalommeghatározás (41–43. pont). Ennek hiánya a végrehajtási szabályok esetében még sajnálatosabb, ugyanis ezek javaslatakor már egyértelművé vált, hogy a harmadik pillérbeli adatvédelemről szóló kerethatározat-tervezet nem fog vonatkozni a személyes adatok – különösen a DNS-profilok – országos gyűjtésére és feldolgozására. Az Európai Adatvédelmi Biztos ezért ismételten felszólítja a jogalkotót, hogy szerepeltesse a személyes adatok világos és mindent magában foglaló meghatározását.

33. Ennek fényében a végrehajtási rendelkezésekben egyértelművé kell tenni az adatvédelmi szabályoknak az azonosítatlan – vagyis még azonosított személyhez hozzá nem rendelt – DNS-profilokra való alkalmazhatóságát. Ezeket az adatokat valójában a megfelelő személyekhez való hozzárendelésük céljával gyűjtik, cserélik és kísérlik meg azonosításukat. Ezért, mivel a rendszer célja a személyek azonosítása, és az érintett adatok elvben csak ideiglenesen „azonosítatlanok", a személyes adatokkal kapcsolatos rendelkezések és biztosítékok többségének, ha nem összességének, vonatkoznia kell rájuk ([1]).

34. Ezenkívül, a „DNS nem kódoló szakaszának" fogalommeghatározásával kapcsolatban (2. cikk e) pontja) az Európai Adatvédelmi Biztos ismételten emlékeztet ([2]) arra, hogy a tudomány fejlődésével bizonyos kromoszómaszakaszok esetleg majd több információt nyújthatnak egy szervezet örökletes tulajdonságairól. Ezért a „DNS nem kódoló szakaszára" vonatkozó meghatározást rugalmasan kell megfogalmazni, és annak tartalmaznia kell azt a kitételt, amelynek értelmében tilos azon DNS-markereket felhasználni, amelyek a tudomány fejlődése következtében konkrét örökletes tulajdonságokról nyújthatnak információt ([3]).

([1]) Az adatvédelmi szabályoknak a DNS-profilokra való alkalmazhatóságával kapcsolatban lásd a 29. cikk alapján létrehozott munkacsoport 2007. június 20-i 4/2007. sz. véleményét a személyes adatok koncepciójáról, WP136., 8–9. o. ugyanebben a véleményben szó van egy hasonlóságot mutató esetről, az adatvédelmi szabályoknak a dinamikus IP-címekre való alkalmazhatóságáról is, 16–17. o.

([2]) Lásd még az Európai Adatvédelmi Biztos 2006. február 28-i véleményét a hozzáférhetőség elve alapján történő információcseréről szóló tanácsi kerethatározati javaslatról (COM(2005) 490 végleges), 58–60. o. (HL C 116., 2006.5.17.).

([3]) Ezzel kapcsolatban lásd még a DNS-vizsgálatok eredményeinek cseréjéről szóló, 2001. június 25-i tanácsi állásfoglalás I. mellékletét (HL C 187., 2001.7.3., 1. o.).

Az automatizált keresések és összehasonlítások pontossága

35. A kezdeményezés 8. cikke olyan módon szabályozza a DNS-profilok automatizált keresését és összehasonlítását, hogy előírja, automatikus értesítést *„csak akkor kell küldeni az egyezésről, ha az automatizált keresés vagy összehasonlítás a lókuszok egy meghatározott minimuma esetében egyezést eredményezett”*. Ezt a minimumot a melléklet I. fejezete határozza meg: minden tagállam biztosítja, hogy a rendelkezésre bocsátott DNS-profilok a 7 uniós „standard” lókusz közül legalább 6-ot tartalmazzanak (a melléklet I. fejezetének 1.1. pontja); a kérelmező és a kért DNS-profilban egyaránt megtalálható lókuszok értékeit kell összehasonlítani (1.2. pont); egyezésnek számít, ha az összehasonlított lókuszok valamennyi értéke egyezik („pontos egyezés”), vagy ha legfeljebb egy érték különbözik („közeli egyezés”); mind a pontos egyezéseket, mind a közeli egyezéseket jelenteni kell (1.3. pont).

36. A mechanizmussal kapcsolatban az Európai Adatvédelmi Biztos megjegyzi, hogy a pontos összepárosítás lényeges feltétel. Minél több lókusz egyezik, annál kisebb az összehasonlított DNS-profilok téves összepárosításának valószínűsége. Az Európai Unióban jelenleg országonként eltérő a DNS-adatbázisok megléte és szerkezete. Az egyes országokban különböző darabszámú és különböző összetételű lókuszokat alkalmaznak. A melléklet előírja, hogy az egyezéshez legalább 6 lókusz szükséges, azonban a rendszerben várhatóan előforduló hibaarányról nem nyújt információt. Ezzel kapcsolatban az Európai Adatvédelmi Biztos megjegyzi, hogy számos országban nagyobb számú lókuszszal dolgoznak a párosítás pontosságának fokozása és a téves párosítások előfordulásának csökkentése érdekében ([1]). Ezért, a tervezett rendszer pontosságának helyes megítélése érdekében, lényeges volna valamennyi összehasonlított lókuszszámra vonatkozóan megadni a várható hibaarányt.

37. Mindez azt is jelenti, hogy a lókuszok minimális száma lényeges tényező, és ezért azt magában a kezdeményezésben, és nem a mellékletében (amelyet a Tanács a kezdeményezés 18. cikke értelmében minősített többséggel, a Parlamenttel folytatott konzultáció nélkül is módosíthat) kellene szabályozni annak elkerülése céljából, hogy a lókuszok számának csökkenése befolyásolja a pontosságot. A hibák és téves párosítások lehetőségét megfelelően figyelembe kell venni, és ezért rendelkezni kell arról, hogy közeli egyezések jelentésekor ezt a tényt kifejezetten fel kell tüntetni (ezáltal a fogadó hatóságok számára egyértelmű lesz, hogy ez az egyezés nem olyan megbízható, mint egy pontos egyezés).

38. Továbbá, a kezdeményezés maga is elismeri annak lehetőségét, hogy a keresések és összehasonlítások többszörös egyezést mutassanak, ezt a DNS-profilokkal kapcsolatban a kezdeményezés 8. cikke, a gépjárművekkel kapcsolatban pedig a melléklet 3. fejezete (1.2. pont) kifejezetten megemlíti. Minden ilyen esetben, mielőtt az egyezésre alapozva a személyes adatok további cseréjére kerülne sor, újabb ellenőrzéseket kell végezni a többszörös egyezés okainak kiderítésére és a pontos egyezés megtalálására.

39. Ehhez kapcsolódóan az Európai Adatvédelmi Biztos azt javasolja, hogy – különösen a DNS-összehasonlításokkal és keresésekkel foglalkozó bűnüldöző szervek körében – jobban kell tudatosítani azt a tényt, hogy a DNS-profilok nem kizárólagos azonosítók: még bizonyos számú lókusz pontos egyezése sem zárja ki a téves párosítás lehetőségét, azaz a DNS-profilnak valamely személyhez történő téves hozzárendelését. A DNS-profilok összehasonlítása és keresése több ponton eredményezhet hibát: a mintavétel időpontjában a DNS-minta gyenge minősége, a DNS-vizsgálat során előforduló esetleges technikai hibák, beviteli hibák, vagy egyszerűen mert az összehasonlítás során az adott lókuszok véletlenül megegyeznek. Az utolsó ponttal kapcsolatban, a hibaarány várhatóan magasabb, amikor a lókuszok száma csökken vagy az adatbázis mérete növekszik.

40. Hasonló gondolatmenet alkalmazható az ujjlenyomatok egyezésének pontosságára. A kezdeményezés 12. cikke előírja, hogy a daktiloszkópiai adatok digitalizálását és továbbítását az e határozat mellékletének 2. fejezetében meghatározott egységes adatformátumnak megfelelően kell végezni. Továbbá, a tagállamok biztosítják, hogy a daktiloszkópiai adatok minősége az automatizált ujjlenyomat-azonosító rendszerrel (AFIS: Automated Fingerprint Identification System) végzett összehasonlításhoz megfelelő legyen. A melléklet 2. fejezete az alkalmazandó formátum néhány jellemzőjéről rendelkezik. Az Európai Adatvédelmi Biztos ezzel kapcsolatban megjegyzi, hogy az összepárosítási eljárás pontosságának biztosítására a kezdeményezésnek és mellékletének a lehetőségekhez mérten össze kell hangolnia a tagállamokban alkalmazott különböző AFIS-rendszereket és alkalmazásuk módját, különös tekintettel a téves elutasítási arányra. Az Európai Adatvédelmi Biztos véleménye szerint ezt az információt a kezdeményezés 18. cikkének 2. pontja szerint összeállított kézikönyvnek tartalmaznia kell.

41. A DNS-adatbázisokkal (és ujjlenyomat-adatbázisokkal) kapcsolatban lényeges dolog még, hogy azokat pontosan körül kell határolni, ugyanis a tagállamoktól függően különböző kategóriájú adatalanyokhoz (bűnözők, gyanúsítottak, bűncselekményekkel összefüggésbe hozható egyéb személyek stb.) tartozó DNS-profilokat és ujjlenyomatokat tartalmazhatnak. E különbségek ellenére a kezdeményezés nem határolja be az egyes tagállamok által használandó adatbázistípusokat, és a melléklet ilyen értelmű nyilatkozatokat sem tartalmaz még. Ezért előfordulhatnak az adatalanyok nem egynemű és gyakran nem érintett kategóriáihoz kapcsolódó DNS- és ujjlenyomatadatok közötti egyezések.

42. Az Európai Adatvédelmi Biztos véleménye szerint a kezdeményezésben meg kell határozni, hogy az adatcsere mely adatalany-kategóriákra terjed ki, és az összehasonlítás vagy keresés szempontjából hogyan tájékoztatják a többi tagállamot ezek eltérő helyzetéről. Például, a kezdeményezés előírhatná azt a kötelezettséget, hogy az egyezésről szóló jelentésben – amennyiben ez az információ a megkeresett hatóságok rendelkezésére áll – fel kell tüntetni, hogy a DNS-adatokat vagy ujjlenyomatokat milyen kategóriájú adatalanyokkal vetették össze.

([1]) Az Egyesült Királyságban például az országos DNS-adatbázisban a DNS-profilokhoz használt lókuszok számát hatról tízre emelték, szintén a rendszer megbízhatóságának fokozására.

Az adatcsere értékelése

43. Az Európai Adatvédelmi Biztos üdvözli, hogy a kezdeményezés 21. cikke és a melléklet 4. fejezete előírja az adatcsere-értékelést. Ezek a rendelkezések azonban kizárólag az automatizált adatcsere adminisztratív, technikai és pénzügyi végrehajtásával foglalkoznak, és az adatvédelmi szabályok végrehajtásának értékeléséről említést sem tesznek.

44. Az Európai Adatvédelmi Biztos ezért azt javasolja, hogy kezeljék kiemelten az adatcsere adatvédelmi vetületeinek értékelését, különös tekintettel az adatcsere céljaira, az adatalanyok tájékoztatásának módjaira, a kicserélt adatok pontosságára és a téves párosításokra, a személyes adatokba való betekintés iránti kérelmekre, az adattárolás időtartamára és a biztonsági intézkedések hatékonyságára. Ebbe a tevékenységbe be kell vonni az illetékes adatvédelmi hatóságokat és szakértőket, például annak elrendelésével, hogy adatvédelmi szakértők vegyenek részt a melléklet 4. fejezetében előírt értékelő látogatásokon, és az érintett adatvédelmi hatóságok kapják meg a kezdeményezés 20. cikkében és a melléklet 4. fejezetében említett értékelő jelentést.

Kommunikációs hálózat és a rendszer technikai vetületei

45. A kezdeményezés 4. cikke előírja, hogy minden elektronikus adatcserét a TESTA II kommunikációs hálózaton keresztül kell lebonyolítani. Ezzel kapcsolatban a melléklet 76. oldalán az 54. pont megállapítja, hogy „A rendszer összhangban van a 45/2001/EK rendelet 21., 22. és 23. cikkében, valamint a 95/46/EK irányelvben tárgyalt adatvédelmi kérdésekkel". Az Európai Adatvédelmi Biztos e kijelentés tisztázását javasolja, mégpedig a közösségi intézmények által a rendszerben játszott szerep tekintetében is. A fentiekkel kapcsolatban a 45/2001/EK rendelet által az Európai Adatvédelmi Biztosra ruházott felügyeleti és tanácsadói szerepkört teljes mértékben figyelembe kell venni.

46. Továbbá, miután a melléklet véglegesítése megtörtént, és az a rendszer jellemzőit világossá tevő valamennyi részletet és nyilatkozatot tartalmazza, az Európai Adatvédelmi Biztos mérlegelni fogja, hogy szükség van-e a rendszer inkább technikai vetületeire vonatkozó további tanácsadásra.

VI. ÖSSZEGZÉS

– Az Európai Adatvédelmi Biztos a kezdeményezésnek és mellékletének nyílt megvitatását ajánlja, mégpedig valamennyi intézményi szereplő valóságos hozzájárulásával, és az Európai Parlament teljes körű társjogalkotói szerepének érvényesítésével, amely szerepet a december 13-án, Lisszabonban aláírt reformszerződés hatályba lépését követően e területen biztosítani fog számára.

– Az Európai Adatvédelmi Biztos felszólítja a jogalkotót, hogy az EU-Szerződés 30. cikke (1) bekezdésének b) pontjával összhangban biztosítsa, hogy a kérdéses kezdeményezés hatálybalépését megelőzően – az általános rendelkezéseket és a konkrét biztosítékokat tartalmazó különböző jogi eszközöket ötvöző – világos, hatékony és átfogó adatvédelmi jogi keret jöjjön létre.

– Ennek fényében az Európai Adatvédelmi Biztos egyrészt ismételten kijelenti, hogy a Prümről szóló tanácsi határozatoknak nem szabad hatályba lépniük addig, amíg a tagállamok nem hajtották végre a harmadik pillérbeli adatvédelemről szóló általános kerethatározatot, amely a „lex generalis" szerepét töltené be, és a prümi kezdeményezésében megállapított további konkrét garanciákat és szigorúbb egyedi előírásokat ezen felül kell alkalmazni.

– Másrészt a jogalkotónak egyértelművé kellene tennie azt is, hogy a prümi kezdeményezésének 6. fejezetében megállapított, a DNS-re, ujjlenyomatokra és gépkocsi-nyilvántartásra vonatkozó konkrét adatvédelmi szabályok nemcsak ezen adatok cseréjére, hanem összegyűjtésükre, tárolásukra és országon belüli feldolgozásukra, valamint a tanácsi határozat hatálya alá tartozó egyéb személyes adatok szolgáltatására is érvényesek.

– Az Európai Adatvédelmi Biztos az intézkedések átláthatóságának javítását ajánlja, mégpedig a melléklet végleges változatának mielőbbi elkészítése és olyan mechanizmusok kialakítása révén, amelyekkel az állampolgárok a rendszer jellemzőiről, saját jogaikról és ezek gyakorlásáról tájékoztathatók.

– Az Európai Adatvédelmi Biztos felkéri a jogalkotót, hogy a szóban forgó kezdeményezés további megvitatásakor megfelelően vegye figyelembe a rendszer méretét, és gondoskodjon arról, hogy a résztvevő tagállamok számának növekedése ne vonja maga után a hatékonyság csökkenését. Különösen, a végrehajtási szabályokban a nyelvi különbségeket is figyelembe vevő, egyedi adatközlési formátumokat kell megállapítani, és az adatcsere pontosságát folyamatosan felügyelni kell.

– Az Európai Adatvédelmi Biztos azt ajánlja, hogy a végrehajtási szabályok és a mellékletek módosításáról (18. cikke), az adatvédelmi szabályok tagállami végrehajtásáról (20. cikk) és az adatcsere értékeléséről (21. cikk) szóló cikk kifejezetten ismerje el az adatvédelmi hatóságok alapvető tanácsadói szerepét. Továbbá, a kezdeményezésnek biztosítania kell, hogy a tagállamok (pótlólagos) forrásokat nyújtsanak az adatvédelmi hatóságoknak, amelyek a tervezett rendszer végrehajtásából eredő felügyeleti feladataik ellátásához szükségesek, és az illetékes adatvédelmi hatóságok rendszeres uniós szintű találkozót tartsanak tevékenységük összehangolása és az említett eszközök harmonizált alkalmazása céljából.

– Az Európai Adatvédelmi Biztos ezért ismételten felszólítja a jogalkotót, hogy szerepeltesse a személyes adatok világos és mindent magában foglaló meghatározását. Ennek fényében a végrehajtási rendelkezésekben egyértelművé kell tenni az adatvédelmi szabályoknak az azonosítatlan – vagyis még azonosított személyhez hozzá nem rendelt – DNS-profilokra való alkalmazhatóságát. Az Európai Adatvédelmi Biztos ismételten emlékeztet arra is, hogy a „DNS nem kódoló szakaszára" vonatkozó meghatározást rugalmasan kell megfogalmazni, és annak tartalmaznia kell azt a kitételt, amelynek értelmében tilos azon DNS-markereket felhasználni, amelyek a tudomány fejlődése következtében konkrét örökletes tulajdonságokról nyújthatnak információt.

– Az Európai Adatvédelmi Biztos azt ajánlja, hogy az automatizált keresések és összehasonlítások esetében az összepárosítási eljárás pontosságát kellően vegyék figyelembe.

  – Ez azt jelenti, hogy a DNS-összevetések és keresések tekintetében valamennyi összehasonlított lókuszszámra vonatkozóan meg kell adni a várható hibaarányt, a közeli egyezések esetében ezt a tényt kifejezetten fel kell tüntetni a jelentésekben, többszörös egyezések előfordulásakor további ellenőrzéseket kell végezni, és jobban kell tudatosítani azt a tényt, hogy a DNS-profilok nem kizárólagos azonosítók. Az ujjlenyomatok esetében a kezdeményezésnek a lehetőségekhez mérten össze kell hangolnia a tagállamokban alkalmazott különböző AFIS-rendszereket és alkalmazásuk módját, különös tekintettel a téves elutasítási arányra.

  – Továbbá, a DNS- és ujjlenyomat-adatbázisokat pontosan körül kell határolni, ugyanis a tagállamoktól függően különböző kategóriájú adatalanyokhoz tartozó DNS-profilokat és ujjlenyomatokat tartalmazhatnak. A kezdeményezésben meg kell határozni, hogy az adatcsere mely adatalany-kategóriákra terjed ki, és az összehasonlítás vagy keresés szempontjából hogyan tájékoztatják a többi tagállamot ezek eltérő helyzetéről.

– Az Európai Adatvédelmi Biztos azt javasolja, hogy kezeljék kiemelten az adatcsere adatvédelmi vetületeinek értékelését, különös tekintettel az adatcsere céljaira, az adatalanyok tájékoztatásának módjaira, a kicserélt adatok pontosságára és a téves párosításokra, a személyes adatokba való betekintés iránti kérelmekre, az adattárolás időtartamára és a biztonsági intézkedések hatékonyságára. E tevékenységbe megfelelő módon be kell vonni az illetékes adatvédelmi hatóságokat és szakértőket is.

– Az Európai Adatvédelmi Biztos azt javasolja, hogy tegyék egyértelművé a TESTA II kommunikációs hálózat alkalmazását és annak a 45/2001/EK rendeletnek való megfelelését, mégpedig a közösségi intézmények által a rendszerben játszott szerep tekintetében is.

Kelt Brüsszelben, 2007. december 19-én.

Peter HUSTINX

Európai Adatvédelmi Biztos