I

(Állásfoglalások, ajánlások és vélemények)

VÉLEMÉNYEK

EURÓPAI ADATVÉDELMI BIZTOS

Az európai adatvédelmi biztos véleménye a 2008/…/IB kerethatározat 11. cikke alkalmazásában az Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS) létrehozásáról szóló tanácsi határozati javaslatról

(2009/C 42/01)

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,

tekintettel a 45/2001/EK rendelet 28. cikkének (2) bekezdése szerint az európai adatvédelmi biztoshoz 2008. május 27-én eljutatott véleménykérelemre,

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

I. BEVEZETŐ MEGJEGYZÉSEK

1. A Bizottság 2008. május 27-én elfogadta a 2008/…/IB kerethatározat 11. cikke alkalmazásában az Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS) létrehozásáról szóló tanácsi határozati javaslatot (a továbbiakban: a javaslat) ([1]). A 45/2001/EK rendelet 28. cikke (2) bekezdésével összhangban a Bizottság konzultáció céljából megküldte a javaslatot az európai adatvédelmi biztosnak.

2. A javaslat célja a bűnügyi nyilvántartásból származó információk tagállamok közötti cseréjének megszervezéséről és azok tartalmáról szóló tanácsi kerethatározat ([2]) (a továbbiakban: a tanácsi kerethatározat) 11. cikkének végrehajtása az információk tagállamok közötti cseréjére szolgáló számítógépes rendszer megalkotása és fejlesztése érdekében ([3]). A kerethatározat 1. cikke létrehozza az Európai Bűnügyi Nyilvántartási Információs Rendszert (ECRIS), meghatározza továbbá az információk elektronikus úton történő cseréje egységes formátumának elemeit, valamint az információcsere megszervezésével és megkönnyítésével kapcsolatos egyéb általános és technikai végrehajtási aspektusokat.

3. Az európai adatvédelmi biztos üdvözli azt a tényt, hogy bevonták a konzultációba, és ajánlja, hogy a javaslat preambulumában hivatkozzanak erre a konzultációra, ahhoz hasonlóan, ahogyan az több más olyan jogalkotási szövegben is történt, amelyek esetében az európai adatvédelmi biztossal – a 45/2001/EK rendeletnek megfelelően – konzultációra került sor.

II. HÁTTÉR ÉS ÖSSZEFÜGGÉSEK

4. Az európai adatvédelmi biztos emlékeztet arra, hogy 2006. május 29-én kiadta a tanácsi kerethatározatról szóló véleményét. E vélemény néhány említésre méltó részlete az alábbiakban következik:

   – az egységes formátum – mint a bűnügyi nyilvántartásból származó információtartalom kétértelműségének kizárását biztosító eszköz – fontosságának hangsúlyozása,

([1]) COM(2008) 332 végleges.

([2]) Még nem fogadták el; a javaslatnak a Tanács által átdolgozott legújabb változata a Tanács nyilvántartásában megtalálható (5968/08 dokumentum).

([3]) A javaslat (6) preambulumbekezdése.

– annak a döntésnek a támogatása, hogy a tanácsi kerethatározat nem ír elő központosított európai adatbázist, és nem teszi lehetővé az adatbázisokhoz való közvetlen hozzáférést, mert mindkettő nehezen ellenőrizhető lenne,

– a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló tanácsi kerethatározat alkalmazása a bűnügyi nyilvántartásból származó információkra a személyes adatok harmadik országok felé történő továbbításának vonatkozásában is,

– az információcsere hatékonysága, figyelemmel a bűnügyi nyilvántartásokról szóló nemzeti jogszabályok közötti nagymértékű eltérésekre, ami miatt további rendelkezésekre van szükség a működőképesség biztosításához,

– a tagállamok közti felelősségmegosztás és az ebből fakadó nehézségek a megfelelő felügyelet szempontjából. Az európai adatvédelmi biztos kedvezően ítélte meg a nemzeti szintű központi hatóság kijelölését,

– a tanácsi kerethatározat széles körű hatálya, mely a bűnügyi nyilvántartásba továbbítandó valamennyi büntetőítéletre vonatkozik.

5. A 2006-os vélemény ezen elemei a jelenlegi javaslat elemzésének összefüggésében is érvényesek. Különösen meghatározó a bűnügyi nyilvántartásokról szóló nemzeti jogszabályok közötti eltérés. Ez az eltérés kiegészítő intézkedéseket tesz szükségessé a csererendszer működőképessé tétele érdekében. Az ECRIS-ről szóló javaslat ilyen kiegészítő intézkedés. Ugyanakkor az összefüggések is változnak.

6. Először is, a tanácsi kerethatározat és annak az ECRIS-ről szóló javaslatban foglalt végrehajtása azon új jogi eszközök közé tartozik, amelyek célja a tagállamok és az Európai Unió közötti, bűnüldözési információcsere megkönnyítése. Ezen eszközök mindegyike tartalommal tölti meg a 2004-es hágai program által bevezetett hozzáférhetőség elvét ([1]). Míg ezen eszközök többsége a rendőrségi együttműködésre összpontosít, e jogszabály az EUSz. 31. cikkének értelmében vett, büntetőügyekben folytatott igazságügyi együttműködés eszköze ([2]). A célja ugyanakkor azonos: a bűnüldözési célú információcsere megkönnyítése. Sok esetben az ilyen eszközök informatikai rendszereket foglalnak magukba, vagy informatikai rendszerek támogatásával és/vagy az információcserére vonatkozó gyakorlatok egységesítése révén működnek. Az ECRIS-re vonatkozó javaslat nem egyedülálló e tekintetben. E javaslat értékelése során az európai adatvédelmi biztos kihasználja a hasonló eszközök terén korábban szerzett tapasztalatokból fakadó előnyöket.

7. Másodszor, az adatvédelemre vonatkozó uniós jogi keret fejlődik. A büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló tanácsi kerethatározat (FDDP) elfogadása – amelyre a (14) preambulumbekezdés a bűnügyi nyilvántartásból származó információk számítógépesített cseréjével összefüggésben alkalmazandó általános keretként hivatkozik – 2008 végére várható. Ez a tanácsi kerethatározat rendelkezni fog a személyes adatok tagállamok közötti átadására vagy elérhetővé tételére vonatkozó minimális adatvédelmi garanciákról ([3]). Ez a személyes adatok felhasználási feltételeire vonatkozó nemzeti jogszabályok nagyobb összhangját fogja eredményezni (*a bűnügyi nyilvántartásból származó információk cseréjéről szóló* tanácsi kerethatározat 9. cikkében foglaltak értelmében).

8. Ezzel kapcsolatban hangsúlyozni kell, hogy az FDDP-ről folytatott tárgyalások olyan változásokat eredményeztek, melyek közül néhány konkrétan érinti azt a jogi keretet, amelyben a bűnügyi nyilvántartásban szereplő információk cseréje történik:

– az alkalmazási kör korlátozása, amely most csupán a más tagállamokkal kicserélt személyes adatokra alkalmazandó, és nem alkalmazandó a csupán egy tagállamon belül, belföldön feldolgozott adatokra,

– nincsenek előírva az adatvédelmi hatóságok közötti hatékony koordinációt biztosító mechanizmusok.

9. Fentiek ismeretében a bűnügyi nyilvántartásból származó információk cseréjéről szóló kerethatározat 9. cikke – mely meghatározza a személyes adatok felhasználásának feltételeit – az adatvédelemről szóló különös szabálynak tekintendő, amely további garanciákat ír elő a az általános szabályban, azaz az FDDP-ben meghatározottakon túl. Ez a cikk – és különösen annak (2) és (4) bekezdése – pontosítja a célhoz kötöttség elvét a bűnügyi nyilvántartásból származó információk cseréjének vonatkozásában. Ezen elv alól csak a fenti rendelkezésekben konkrétan megemlített körülmények esetén tesz kivételt.

10. Harmadszor, e javaslattal szoros összefüggésben a Bizottság előterjesztette az európai e-igazságügyi stratégiáról szóló közleményét ([4]). Ezzel a közleménnyel az Európai Bizottság az európai szintű e-igazságügyi eszközök megerősítéséhez és fejlesztéséhez kíván hozzájárulni. A közlemény több, a személyes adatok védelmére jelentős hatással lévő kezdeményezést tartalmaz, mint például az információk igazságügyi hatóságok közötti biztonságos cseréjére szolgáló hálózat megteremtése és a jogi szakfordítók és tolmácsok európai adatbázisának létrehozása. Az európai adatvédelmi biztos külön dokumentumban kíván reflektálni erre a közleményre.

([1]) HL C 53., 2005.3.3., 1. o.

([2]) Másik példa az Eurojuston keresztül történő információcsere. Ezen információcsere jogi kerete módosulni fog az Eurojust megerősítéséről és a 2002/187/IB határozat módosításáról szóló tanácsi határozat (lásd az alábbi kezdeményezést: HL C 54., 2008.2.27., 4. o.) elfogadása után.

([3]) Lásd az ezen tanácsi kerethatározatra vonatkozó javaslat 1. cikkét (a legújabb változat megtalálható a Tanács nyilvántartásában, 2008. június 24., 9260/08).

([4]) A Bizottság közleménye a Tanács, az Európai Parlament és az Európai Gazdasági és Szociális Bizottság számára – Úton az európai e-igazságügyi stratégia felé (COM(2008) 329 végleges).

III. A TANÁCSI KERETHATÁROZATBAN ELŐÍRT INFORMÁCIÓCSERE

11. A tanácsi kerethatározat 11. cikke – pontosabban annak (1) bekezdése – megadja, hogy mely információkat kell vagy lehet továbbítani; a (3) bekezdés pedig tartalmazza e javaslat jogi alapját. A tanácsi kerethatározat II. mellékletében található az információcseréhez használandó adatigénylő lap. Ez tartalmazza a megkereső államra vonatkozó adatokat és a kérelemre válaszként adandó információkat. A Bizottság jelenlegi javaslata szerint az adatlapot tanácsi határozattal lehet megváltoztatni.

12. A 11. cikk (1) bekezdése kötelező információkat, nem kötelező információkat, kiegészítő információkat és egyéb információkat különböztet meg. A II. mellékletben foglalt adatlap nem tükrözi ezeket a különbségtételeket. Az elítélt személy szüleinek neve például nem kötelező információként szerepel a 11. cikkben, melyet csak a bűnügyi nyilvántartásban való rögzítés esetén kell továbbítani. A II. melléklet nem tükrözi ezen információ továbbításának nem kötelező jellegét.

13. Az európai adatvédelmi biztos szerint ez jó alkalom arra, hogy az adatlapot teljes mértékben hozzáigazítsák a 11. cikkhez. Így a személyes adatok továbbítása az információcsere szempontjából valóban szükséges adatokra fog korlátozódni. A fenti példában láthatólag nem szükséges az elítélt személy szülei nevének automatikus továbbítása. Ez az eljárás feleslegesen ártana az érintett személyeknek, azaz a szülőknek.

IV. AZ ECRIS-RENDSZER

Általános megjegyzések

14. A 3. cikk alkotja a javaslat lényegét. Létrehozza az ECRIS-t, amely osztott információtechnológiai rendszer, és három elemből épül fel: tagállamok bűnügyi nyilvántartási adatbázisai, a közös kommunikációs infrastruktúra és az összeköttetést biztosító szoftver.

15. Az európai adatvédelmi biztos támogatja az ECRIS létrehozására irányuló jelenlegi javaslatot, amennyiben az e véleményben tett észrevételeket figyelembe veszik.

16. Ezzel összefüggésben hangsúlyozza, hogy egyrészt a jogszabály nem hoz létre központi európai adatbázist, és nem írja elő a más tagállamok bűnügyi nyilvántartási adatbázisaihoz való közvetlen hozzáférést, másrészt azonban nemzeti szinten centralizálja a felelősségi köröket a tagállamoknak a tanácsi kerethatározat 3. cikkének értelmében kijelölt központi hatóságai révén. Ez a mechanizmus a minimálisra csökkenti a személyes adatok tárolását és cseréjét, ugyanakkor pontosan meghatározza a központi hatóságok felelősségét. E mechanizmus értelmében a tagállamok felelősek a nemzeti bűnügyi nyilvántartási adatbázisok működéséért, és az információcsere hatékonyságáért. Hasonlóképp ők felelősek az összeköttetést biztosító szoftverért (a javaslat 3. cikkének (2) bekezdése).

17. Közös infrastruktúrát fognak kialakítani. Kezdetben ez az S-TESTA hálózat ([1]) lesz, amelyet felválthat a Bizottság által működtetett más biztonságos hálózat (a javaslat 3. cikkének (4) bekezdése). Az európai adatvédelmi biztos tudja, hogy a Bizottság felel a közös infrastruktúráért, noha ezt a 3. cikk nem pontosítja. Az európai adatvédelmi biztos javasolja, hogy a jogbiztonság érdekében ezt a felelősséget rögzítsék a szövegben.

Az első elem: a tagállamok bűnügyi nyilvántartási adatbázisai

18. Az európai adatvédelmi biztos 2006. május 29-i véleményében támogatását fejezte ki a decentralizált rendszer iránt. Ezzel elkerülhető többek között a személyes adatoknak a központi adatbázisban való tárolással történő megduplázása. Az ilyen decentralizált rendszer automatikusan azt vonja maga után, hogy a tagállamok felelősek a bűnügyi nyilvántartási adatbázisokért és a személyes adatoknak az ezen adatbázisokban történő feldolgozásáért. Konkrétabban, ezen adatbázisok adatkezelői a tagállamok központi hatóságai. Adatkezelőként ők felelnek az adatbázis, valamint a kicserélt információk tartalmáért. A tanácsi kerethatározat előírja az ítélethozatal szerinti tagállam és az adott személy állampolgársága szerinti tagállam kötelezettségeit.

19. Ennek keretében az ECRIS egyenrangú résztvevők együttműködésén alapuló hálózat, melynek rendeltetése a nemzeti adatbázisok közötti információcsere. Az egyenrangú résztvevők együttműködésén alapuló, az ECRIS-hez hasonló hálózatoknak vannak bizonyos kockázatai, melyeket kezelni kell:

   – a gyakorlatban a tagállamok központi hatóságai közötti felelősségmegosztás nem működik magától. További intézkedésekre van szükség például annak biztosításához, hogy a küldő és a fogadó tagállam (az ítélethozatal szerinti tagállam és az adott személy állampolgársága szerinti tagállam) által rögzített adatok naprakészek és azonosak legyenek,

   – ez a rendszer azt eredményezi, hogy az egyes tagállamok meglehetősen eltérően alkalmazzák, ami még szembetűnőbb a nemzeti jogszabályok közötti jelentős különbségek vonatkozásában (hasonlóan a bűnügyi nyilvántartások esetéhez).

20. Ezért rendkívül fontos magának a hálózat használatának, valamint a használatával kapcsolatos eljárásoknak a harmonizációja. Az európai adatvédelmi biztos kiemeli annak fontosságát, hogy a hálózat használata összehangolt legyen és magas szintű adatvédelmi előírások figyelembevételével történjen. A javaslat 6. cikke alapján elfogadandó végrehajtási intézkedések ezért rendkívül fontosak. Az európai adatvédelmi biztos azt javasolja, hogy a 6. cikkben történjen utalás a magas szintű adatvédelemre mint a későbbiekben elfogadandó valamennyi végrehajtási intézkedés előfeltételére.

([1]) A közigazgatási rendszerek közötti transzeurópai telematikai szolgáltatások.

21. A nemzeti adatvédelmi hatóságoknak szerepe lehet ebben, amennyiben összehangolt módon működnek. Az európai adatvédelmi biztos azt javasolja, hogy illesszenek be egy olyan preambulumbekezdést, amely hangsúlyozza az adatvédelmi hatóságok szerepét, hasonlóan ahhoz, ahogyan a (11) preambulumbekezdés és a 3. cikk (5) bekezdése utal arra, hogy a Bizottság segítséget nyújt a tagállamoknak. Az új preambulumbekezdésnek együttműködésre kellene buzdítania az adatvédelmi hatóságokat.

22. Végezetül az európai adatvédelmi biztos üdvözli a 3. cikk (3) bekezdésének azon rendelkezését, amely a más tagállamoknak továbbított bűnügyi nyilvántartási adatok titkosságának és integritásának biztosítása érdekében az elérhető legjobb technikák alkalmazását írja elő. Kívánatos lenne ugyanakkor, hogy – a tagállamokkal (vagy azok központi hatóságaival) és a Bizottsággal együtt – az illetékes adatvédelmi hatóságok is szerephez jussanak ezen technikák meghatározásában.

A második elem: a közös kommunikációs infrastruktúra

23. A Bizottságnak a közös kommunikációs infrastruktúráért való felelőssége azt eredményezi, hogy a Bizottságot kell hálózati szolgáltatónak tekinteni. Az adatvédelem céljából a Bizottságot a személyes adatok védelméről szól tanácsi kerethatározat 2. cikkének i) pontja értelmében vett – jóllehet korlátozott feladatkörrel rendelkező – adatkezelőnek lehet minősíteni, aki a hálózatot működteti és garantálja biztonságát. Amennyiben a hálózat üzemeltetésével kapcsolatban személyes adatok feldolgozására kerül sor, vagy ha adatvédelmi kérdések merülnek fel a hálózat biztonságával kapcsolatban, akkor ezekért adatkezelőként a Bizottság felel. A Bizottság ezen szerepe a SIS, VIS és Eurodac rendszerekben betöltött szerepéhez hasonló, amikor is az operatív irányításért (és nem pedig a személyes adatok tartalmáért) felel. Ezt az európai adatvédelmi biztos „sajátos adatkezelői szerepnek” ([1]) minősítette.

24. A közös kommunikációs infrastruktúra – legalábbis rövid távon – az S-TESTA hálózaton fog alapulni. Az S-TESTA célja az uniós szerveknek a nemzeti hatóságokkal, például a közigazgatási szervekkel és az Európa különböző pontjain elhelyezkedő ügynökségekkel való összekapcsolása. Ez egy külön telekommunikációs hálózat. A szolgáltatás operatív központja Pozsonyban található. Ez alkotja továbbá olyan más információs rendszerek gerincét a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben, mint a Schengeni Információs Rendszer. Az európai adatvédelmi biztos támogatja, hogy az S-TESTA hálózatára esett a választás, mely igazoltan megbízható információcsere-rendszer.

25. A Bizottság sajátos adatkezelői felelősségi köre hatással van az alkalmazható adatvédelmi jogszabályokra és a felügyeletre is. A 45/2001/EK rendelet 3. cikke alapján „e rendeletet kell alkalmazni a személyes adatok bármely közösségi intézmény és szerv által történő feldolgozására, ha a feldolgozás részben vagy teljes egészében a közösségi jog hatálya alá tartozó tevékenységek gyakorlása során történik”.

26. Amennyiben a Bizottság által végzett adatfeldolgozó tevékenységek részben vagy egészben a közösségi jog hatálya alá esnek, akkor a 45/2001/EK rendelet alkalmazhatósága nem kétséges. Különösen e rendelet 1. cikke rendelkezik úgy, hogy a közösségi intézmények és szervek gondoskodnak a természetes személyek alapvető jogainak és szabadságainak – különösen a magánélet tiszteletben tartásához való joguknak – a személyes adatok feldolgozásával összefüggő védelméről. E rendelet 22. cikke alapján a Bizottság „megfelelő műszaki és szervezeti intézkedéseket hajt végre annak érdekében, hogy biztosítsa az adatok feldolgozásával járó kockázatnak és a védelmet igénylő személyes adatok jellegének megfelelő szintű biztonságot”. E tevékenységek végrehajtására az európai adatvédelmi biztos felügyelete mellett kerül sor.

27. Ugyanakkor, ezen esetben megjegyzendő, hogy a Schengeni Információs Rendszertől ([2]) eltérően az adatfeldolgozási tevékenységek jogalapja az EU-Szerződés VI. címében (a harmadik pillérben) található. Ez azt jelenti, hogy a 45/2001/EK rendelet nem alkalmazandó automatikusan, továbbá az adatvédelemre és felügyeletre vonatkozó semmilyen más jogi keret sem alkalmazandó a Bizottság adatfeldolgozási tevékenységére. Ez nyilvánvalóan azért nem szerencsés, mert nincs biztosítva az érintett védelme, főleg mivel a büntetőítéletekkel kapcsolatos személyes adatok feldolgozása kényes terület, amint azt a 45/2001/EK rendelet 10. cikkének (5) bekezdése is mutatja, melynek okán a büntetőítéletekre vonatkozó adatok feldolgozása bizonyos kockázatokkal jár. Annál is kevésbé szerencsés, mivel az európai adatvédelmi biztos – más jogi eszközök alapján – részt vesz az S-TESTA felügyeletében. Emiatt az európai adatvédelmi biztos azt javasolja, hogy adjanak hozzá egy olyan rendelkezést a határozathoz ([3]), amely kimondja, hogy a 45/2001/EK rendelet alkalmazandó a személyes adatoknak a Bizottság felelőssége alatt történő feldolgozására.

A harmadik elem: az összeköttetést biztosító szoftver

28. A javaslat különbséget tesz az adatbázisok összekapcsolásához szükséges rendes műszaki infrastruktúra és az összeköttetést biztosító szoftver között. Mint elmondtuk, a tagállamok felelnek az összeköttetést biztosító szoftverért. A (11) preambulumbekezdés szerint a Bizottság a tagállamok rendelkezésére bocsáthatja ezt a szoftvert, de látszólag a tagállamok döntik el, hogy alkalmazzák-e ezt a szoftvert a saját, összeköttetést biztosító szoftverjük helyett vagy sem.

([1]) Lásd a Schengeni Információs Rendszer második generációjával (SIS II) kapcsolatos három javaslatról szóló 2005. október 19-i véleményt (HL C 91., 2006.4.19., 38. o., 5.1. pont).

([2]) Továbbá eltérően a VIS és Eurodac rendszerektől, amelyek teljes mértékben a közösségi jog hatálya alá esnek.

([3]) Lásd ugyanebben az értelemben a harmadik pilléren belül az Európai Rendőrségi Hivatal (Europol) létrehozásáról szóló tanácsi határozat 39. cikkének (6) bekezdését, amely biztosítja, hogy az Europol személyzete személyes adatainak kezelésével kapcsolatban az Europol a 45/2001/EK rendelet elveit alkalmazza (2008. június 24-i szöveg, tanácsi dok. sz. 8706/08).

29. Felmerül a kérdés, hogy miért kell különbséget tenni a műszaki infrastruktúráért és az összeköttetést biztosító szoftverért való felelősség között, és miért nem a Bizottság felel mindkettőért. Ezenkívül mindkét esetben a tagállamok központi hatóságai (a hálózathoz való nemzeti hozzáférési pontok) közötti hálózatról, és nem a tagállamokon belüli információcseréről van szó.

30. Ezen újabb felelősségi körnek a Bizottságra való ruházása nem befolyásolná az információtechnológiai rendszer decentralizált jellegét, ugyanakkor biztosítaná az információcsere optimális hatékonyságát. A hatékonyság fokozása adatvédelmi szempontból az adatminőség miatt fontos: csak valóban lényeges adatokat kell kicserélni, és a rendszer tökéletlenségei miatt nincs szükség további információkra. A rendszer jobban felügyelhető, ha a közös kommunikációs infrastruktúráért és az összeköttetést biztosító szoftverért egyetlen szerv felel.

31. Ez annál inkább fontos, mivel a szoftver az információcsere eszközeként működik. Az összeköttetést biztosító szoftver fontos tulajdonságai, hogy képes legyen a küldő fél személyazonosságának, valamint a kérelmek megfelelőségének és hiánytalanságának az ellenőrzésére, és végül lehetővé tegye a kérelmek érvényesítését. Ennek előfeltétele a tagállamok által használt szoftverek kölcsönös átjárhatósága. Nem minden tagállamnak kell feltétlenül ugyanazt a szoftvert használnia (noha ez lenne a legpraktikusabb), ám a szoftvernek teljes mértékben átjárhatónak kell lennie.

32. A javaslat elismeri az összeköttetést biztosító szoftverrel kapcsolatos kérdések harmonizációjának szükségességét. A 6. cikkben felsorolt – komitológiával elfogadandó – végrehajtási intézkedések között megtalálhatók például „a szoftveralkalmazásoknak műszaki előírásoknak való megfelelését ellenőrző eljárások". A 6. cikk megemlíti továbbá a közös protokollokat. Az összeköttetést biztosító szoftver tekintetében azonban nem ír elő ilyen közös protokollokat. A 6. cikk nem írja elő továbbá a szoftverrendszerek azonosítását sem.

33. Fentiek miatt az európai adatvédelmi biztos az információcserék hatékonyságának és biztonságának növelése érdekében az alábbiakat ajánlja:

– minimális feltétel, hogy a végrehajtási intézkedéseket a szoftver kölcsönös átjárhatóságának biztosítása mellett fogadják el,

– a szövegnek lehetőség szerint kötelezni kell a Bizottságot és a tagállamokat arra, hogy – valószínűleg komitológiával – fejlesszenek ki és határozzanak meg egy olyan szoftverrendszert, amely a fenti követelmények mindegyikének megfelel,

– a szövegnek elő kell írnia, hogy a Bizottság felel az összeköttetést biztosító szoftverért.

V. EGYÉB KÉRDÉSEK

A kézikönyv

34. A 6. cikk b) pontja alapján az információcsere eljárását egy komitológiával elfogadandó kézikönyv határozza meg, amely „különösen az elkövetők azonosításának szabályaival" foglalkozik. Az európai adatvédelmi biztos nem tudja, hogy pontosan mit fog tartalmazni ez a kézikönyv, és hogy rendelkezni fog-e például a biometrikus eszközökkel történő azonosításról.

35. Az európai adatvédelmi biztos hangsúlyozza, hogy az elkövetők azonosítása nem járhat olyan személyes adatoknak a cseréjével, melyeket a kerethatározat nem tartalmaz kifejezetten. Ezenkívül a kézikönyvnek megfelelő garanciákat kell tartalmaznia a különleges kategóriába tartozó, pl. biometrikus adatok feldolgozására és továbbítására vonatkozóan.

Statisztikai adatok gyűjtése

36. A 6. cikk c) pontja és a 8. cikk szól a statisztikai adatok gyűjtéséről, ami kulcsfontosságú tényező nem csupán az adatcserélési rendszer hatékonyságának felmérése, hanem az adatvédelmi garanciák betartásának felügyelete szempontjából is. Ennek figyelembevételével az európai adatvédelmi biztos azt ajánlja, hogy – a személyes adatok cseréjéről szóló más jogi eszközökkel összhangban ([1]) – pontosabban meg kell határozni a gyűjtendő statisztikai adatokat és kellően figyelembe kell venni az adatvédelmi felügyelet biztosításának szükségességét. A statisztikai adatok például kifejezetten tartalmazhatnak olyan elemeket, mint a hozzáférési kérelmeknek vagy a személyes adatok helyesbítésének száma, a naprakésszé tételi folyamat hossza és teljessége, az ezen adatokhoz hozzáférő személyek tisztsége, valamint a biztonság sérülésének esetei. Ezenkívül a statisztikai adatoknak és az ezeken alapuló jelentéseknek teljes mértékben elérhetőknek kell lenniük az illetékes adatvédelmi hatóságok számára.

Az adatfeldolgozás felügyeletének összehangolása

37. Az európai adatvédelmi biztos a bűnügyi nyilvántartásból származó információk cseréjéről szóló kerethatározatról kiadott 2006. május 29-i véleményében már rámutatott arra, hogy a javaslatnak nem csak a központi hatóságok közötti együttműködésre kell kiterjednie, hanem a különböző illetékes adatvédelmi hatóságok együttműködésére is. Ez még fontosabb most, hogy az FDDP-ről folytatott tárgyalások eredményeképp törölték azt a rendelkezést, amely létrehozta az uniós adatvédelmi hatóságokat tömörítő és azok tevékenységét a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében történő adatfeldolgozás tekintetében koordináló munkacsoportot.

([1]) Lásd például a dublini egyezmény hatékony alkalmazása érdekében az ujjlenyomatok összehasonlítására irányuló Eurodac létrehozásáról szóló, 2000. december 11-i 2725/2000/EK tanácsi rendelet 3. cikkének (3) és (4) bekezdését.

38. Ezért a hatékony felügyelet, valamint a bűnügyi nyilvántartásból származó adatok határokon átnyúló forgalma jó minőségének biztosítása érdekében megfelelő koordinációs mechanizmusokat kellene kialakítani az illetékes adatvédelmi hatóságok között. Ezeknek a mechanizmusoknak figyelembe kell vennie az európai adatvédelmi biztosnak az S-TESTA infrastruktúrával kapcsolatos felügyeleti illetékességét. E mechanizmusok külön rendelkezésben szerepelhetnének, vagy a javaslat 6. cikke alapján elfogadandó végrehajtási intézkedések közé lehetne beilleszteni őket.

Fordítások

39. A (6) és (8) preambulumekezdés, valamint a Bizottság indokolása szól a gépi fordítás széles körű használatáról. Az európai adatvédelmi biztos üdvözöl minden olyan kezdeményezést, amelynek célja a továbbított információ kölcsönös megértése, ugyanakkor rámutat, hogy pontosan meg kell határozni és le kell írni a gépi fordítás használatának eseteit. Miután elkészült a határozat mellékletében felsorolt bűncselekmény-kategóriák előfordítása, a közös kódok használata lehetővé teszi a nemzeti hatóságoknak, hogy nemzeti nyelvűkön olvassák e kategóriák gépi fordítását. A gépi fordítás ilyen használata hasznos eszköz, mely valószínűsíthetően elősegíti a szóban forgó bűncselekmények kölcsönös megértését.

40. Azonban a nem pontosan előfordított információk, mint például az egyes esetekhez fűzött kiegészítő megjegyzések vagy pontosítások esetében a gépi fordítás használata valószínűleg rontja a továbbított információ – és ezáltal az ez alapján hozott döntések – minőségét, és ezért elvben ki kell zárni. Az európai adatvédelmi biztos azt ajánlja, hogy ezt a kérdést a tanácsi határozat preambulumában pontosítsák.

VI. **KÖVETKEZTETÉSEK**

41. Az európai adatvédelmi biztos azt ajánlja hogy a javaslat preambulumában hivatkozzanak erre a konzultációra.

42. Javasolja, hogy használják ki ezt a lehetőséget arra, hogy az adatlapot teljes mértékben hozzáigazítsák a bűnügyi nyilvántartásból származó információk cseréjéről szóló tanácsi kerethatározat 11. cikkéhez, amely kötelező információkat, nem kötelező információkat, kiegészítő információkat és egyéb információkat különböztet meg.

43. Az európai adatvédelmi biztos támogatja az ECRIS létrehozására irányuló jelenlegi javaslatot, amennyiben az e véleményben tett és az alábbiakban összefoglalt észrevételeket figyelembe veszik:

– a jogbiztonság érdekében pontosítani kell a szövegben a Bizottságnak a közös kommunikációs infrastruktúráért való felelősségét,

– be kell illeszteni egy olyan rendelkezést a határozatba, amely kimondja, hogy a 45/2001/EK rendelet alkalmazandó a személyes adatoknak a Bizottság felelőssége alatt történő feldolgozására,

– a 6. cikkben utalni kell a magas szintű adatvédelemre mint a későbbiekben elfogadandó valamennyi végrehajtási intézkedés előfeltételére,

– külön preambulumbekezdésben kell hangsúlyozni az adatvédelmi hatóságoknak a végrehajtási intézkedésekkel kapcsolatos szerepét, és együttműködésre kell buzdítani az adatvédelmi hatóságokat,

– a végrehajtási intézkedéseket a szoftver kölcsönös átjárhatóságának biztosítása mellett kell elfogadni,

– a Bizottságot és a tagállamokat kötelezni kell arra, hogy – valószínűleg komitológiával – fejlesszenek ki és határozzanak meg egy olyan szoftverrendszert, amely a fenti követelmények mindegyikének megfelel,

– a szövegnek elő kell írnia, hogy a Bizottság felel az összeköttetést biztosító szoftverért.

44. Pontosabban meg kell határozni a gyűjtendő statisztikai adatokat és kellően figyelembe kell venni az adatvédelmi felügyelet biztosításának szükségességét.

45. Megfelelő koordinációs mechanizmusokat kell kialakítani az illetékes adatvédelmi hatóságok között, figyelemmel az európai adatvédelmi biztosnak az S-TESTA infrastruktúrával kapcsolatos felügyeleti illetékességére.

46. A tanácsi határozat preambulumában pontosítani kell, hogy a gépi fordítás használata nem terjedhet ki az előzőleg pontosan elő nem fordított információk továbbítására.

Kelt Brüsszelben, 2008. szeptember 16-án.

Peter HUSTINX

európai adatvédelmi biztos