EURÓPAI ADATVÉDELMI BIZTOS

Az Európai Adatvédelmi Biztos véleménye a hozzáférhetőség elve alapján történő információcseréről szóló tanácsi kerethatározati javaslatról (COM (2005) 490 végleges)

(2006/C 116/04)

AZ EURÓPAI ADATVÉDELMI BIZTOS,

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

tekintettel az Európai Unió alapjogi chartája, 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 rendelet 28. cikkének (2) bekezdése értelmében benyújtott vélemény iránti kérelemre,

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

I. ELŐZETES MEGJEGYZÉSEK

1. A hozzáférhetőség elve alapján történő információcseréről szóló tanácsi kerethatározati javaslatot a Bizottság 2005. október 12-i levelében megküldte az európai adatvédelmi biztosnak. Az európai adatvédelmi biztos ezt a levelet arra való felkérésnek értelmezi, hogy adjon tanácsot a közösségi intézményeknek és szerveknek a 45/2001/EK rendelet 28. cikkének (2) bekezdése szerint. Az európai adatvédelmi biztos szerint ez a vélemény megemlítendő a kerethatározat preambulumában.

2. A vélemény természetét a II. pont alatt leírtak összefüggésében kell értelmezni. A II. pont alatt jelezzük, hogy egyáltalán nem nyilvánvaló, hogy a jelenlegi javaslat – illetve a hozzáférhetőségnek a javaslat által képviselt megközelítése – végül valóban elvezet-e egy jogi eszköz elfogadásához. Számos tagállam más megközelítések mellett száll síkra.

3. Nyilvánvaló azonban, hogy a bűnüldözési információk belső határokon átnyúló hozzáférhetőségének témája – illetve tágabb értelemben ezen információk cseréje – a tagállamokat élénken foglalkoztatja, mind a Tanácson belül, mind a Tanácson kívül, valamint az Európai Parlamentben is.

4. Egyértelmű továbbá, hogy ez a téma a személyes adatok védelmét is nagymértékben érinti, amint arra a jelen vélemény is ki fog térni. Az európai adatvédelmi biztos emlékeztet arra, hogy a jelen javaslatot a Bizottság nyújtotta be szorosan kacsolódóan a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló tanácsi kerethatározatra irányuló javaslathoz, amelyet 2005. december 19-én nyújtottak be, és amely az európai adatvédelmi biztos véleményének tárgyát képezi.

5. Az európai adatvédelmi biztos megragadja ezt az alkalmat arra, hogy jelen véleményben kifejtse néhány általános és alapvető jellegű nézetét a bűnüldözési információk cseréjének témájával és az e téma szabályozásához tartozó megközelítésekkel kapcsolatban. E vélemény előterjesztésével az európai adatvédelmi biztos biztosítani kívánja, hogy az adatvédelem szempontját a téma megvitatásakor a jövőben megfelelő súllyal vegyék figyelembe.

6. Az európai adatvédelmi biztos rendelkezésre áll a későbbiek folyamán további konzultációkra, miután az itt tárgyalt, valamint más kapcsolódó javaslatokhoz tartozó jogalkotói folyamatban releváns fejlemények mutatkoznak.

II. A JAVASLAT ÖSSZEFÜGGÉSEIBEN SZEMLÉLVE

7. A hozzáférhetőség elvét – mint fontos új jogi alapelvet – a hágai program vezette be. Kimondja, hogy a bűnözés elleni küzdelemhez szükséges információk akadálymentesen kell, hogy átlépjék az EU belső határait. Jelen javaslat célja ezen alapelv átültetése jogilag kötelező erejű formába.

8. A rendőrségi információk különböző országok közötti cseréje a jogalkotók körében népszerű téma, az EU keretein belül és kívül egyaránt. Nemrégiben a következő kezdeményezések vonták magukra az európai adatvédelmi biztos figyelmét.

9. Először is 2004. június 4-én Svédország javasolt egy kerethatározat-tervezetet az információk és bűnüldözési operatív információk Európai Unió tagállamai bűnüldöző hatóságai közötti cseréjének egyszerűsítéséről. Ezen javaslattal kapcsolatban a Tanács 2005. december 1-jei ülésén megállapodásra jutott az általános megközelítésről.

10. Másodsorban 2005. május 27-én hét tagállam aláírta Prümben (Németország) a határokon átnyúló együttműködés, legfőképp a terrorizmus, a nemzetközi bűnözés és az illegális bevándorlás elleni küzdelem megerősítését célzó egyezményt. Ez többek között DNS- és ujjnyomat-információk cseréjének javítását célzó intézkedéseket is bevezet. Az egyezményhez csatlakozhat az Európai Unió bármely tagállama. A szerződő felek az egyezmény rendelkezéseit igyekeznek beépíteni az Európai Unió jogi keretrendszerébe.

11. Harmadsorban a bűnüldözési információknak az Európai Unió belső határait átlépő hozzáférhetőségét tovább fogják könnyíteni más jogi eszközök, úgymint a második generációs Schengeni Információs Rendszerre (SIS II) vonatkozó javaslat, a vízuminformációs rendszerhez (VIS) biztosított keresési célú hozzáférésre vonatkozó javaslat, és a bűnügyi nyilvántartásokból készített kivonatolt információk tagállamok közötti cseréjének szervezésére és tartalmára vonatkozó kerethatározatról szóló javaslat. E tekintetben fontos megemlíteni, hogy a Bizottság 2005. november 25-én közleményt adott ki az európai adatbázisok közötti hatékonyság fokozásáról, interoperabilitásuk javításáról és szinergiahatásaikról a bel- és igazságügyi együttműködés területén.

12. Tekintve, hogy mindezen kezdeményezések megvalósultak, a hozzáférhetőségről szóló jelen kerethatározati javaslatot nem önmagában kell vizsgálni, hanem figyelembe kell venni a bűnüldözési információk cseréjéről szóló egyéb megközelítéseket is. Ez azért is fontos, mert a Tanácsnál jelenleg megfigyelhető az a tendencia, hogy az információk cseréjére vonatkozóan más megközelítéseket, illetve a hozzáférhetőség koncepcióját részesítik előnyben, szemben a Bizottság által az ezen javaslatban szereplő általános megközelítéssel. A javaslat ezen szövege esetleg nem is képezi eszmecsere tárgyát a Tanácsban.

13. Továbbá, a javaslat szorosan kapcsolódik a személyes adatok védelméről szóló kerethatározati javaslathoz. Az ezen véleményt ez utóbbi kerethatározatról szóló mélyenszántóbb vélemény összefüggésében kell értelmezni.

14. A személyes adatok védelméről szóló kerethatározati javaslatról szóló véleményében az európai adatvédelmi biztos kiemeli a megfelelő adatvédelem jelentőségét, mint a hozzáférhetőségről szóló jogi eszközből származó szükségszerű következményt. Az európai adatvédelmi biztos szerint egy ilyen jogi eszközt nem szabadna alapvető adatvédelmi garanciák nélkül elfogadni.

15. Az európai adatvédelmi biztos ugyanezt az álláspontot képviseli egyéb olyan jogi eszközök elfogadásával kapcsolatban is, amelyek megkönnyítik a bűnüldözési információk áramlását az EU belső határain keresztül. Az európai adatvédelmi biztos üdvözli, hogy a Tanács, valamint az Európai Parlament prioritásként kezeli a fent említett, a személyes adatok védelméről szóló kerethatározati javaslatot.

III. A HOZZÁFÉRHETŐSÉG ELVE, MINT OLYAN

16. A hozzáférhetőség elve önmagában egyszerű elv. Az egyik tagállamban a hatóságok rendelkezésére álló információkat meg kell adni a más tagállamok egyenértékű hatáskörrel rendelkező hatóságainak. Az információkat a lehető leggyorsabban és legzökkenőmentesebben kell továbbítani a tagállamok hatóságai között, lehetőleg közvetlen online hozzáférés biztosításával.

17. A nehézségek oka az a környezet, amelyben a hozzáférhetőséget hatékonnyá kell tenni:

– A tagállamokban a rendőrség és igazságszolgáltatás heterogén módon van megszervezve, máshol vannak a fékek és ellensúlyok.

– Különböző típusú (érzékeny) információk szerepelnek (úgymint DNS vagy ujjnyomatok).

– Még a tagállamokon belül is az illetékes hatóságok különböző módokon juthatnak hozzá a releváns információkhoz.

– Nehéz biztosítani, hogy egy másik tagállamból származó információt megfelelően értelmezzenek, a nyelvekből, a technológiai rendszerekből (átjárhatóság) és a jogi rendszerekből adódó eltérések miatt.

– Ezt bele kell foglalni azon jogi rendelkezések meglévő és terjedelmes szövevényébe, amelyek a bűnüldözési információk országok közötti cseréjével foglalkoznak.

18. Ettől a bonyolult környezettől eltekintve, egyetértés uralkodik azon a téren, hogy az elv önmagától nem működik. Kiegészítő intézkedések szükségesek annak biztosításához, hogy az információkat hatékonyan meg lehessen találni, és hozzájuk lehessen férni. Mindenesetre ezek az intézkedések meg kell, hogy könnyítsék a bűnüldöző hatóságok számára annak kiderítését, hogy más tagállamok bűnüldöző hatóságai rendelkeznek-e releváns információval, és hogy hol lelhető fel ez az információ. Az ilyen kiegészítő intézkedések olyan interfészekből állhatnának, amelyek közvetlen hozzáférést biztosítanak valamennyi vagy bizonyos, más tagállam birtokában lévő adathoz. A hozzáférhetőségről szóló kerethatározati javaslat ebből a célból vezeti be a „jegyzékadatok”, amely azon egyedi adatokat jelöli, amelyek a határokon túlról is közvetlenül hozzáférhetőek.

19. Általános értelemben a hozzáférhetőségi elv meg kellene, hogy gyorsítsa az információáramlást a tagállamok között. A belső határokat el fogják törölni, és a tagállamoknak lehetővé kell tenniük, hogy a rendőri hatóságaik számára rendelkezésre álló információk növekvő mértékben hozzáférhetőek legyenek más hatóságok számára is. A tagállamok elveszítik az információáramlás ellenőrzésére vonatkozó hatáskörüket, amely azt is eredményezi, hogy többé már nem hagyatkozhatnak nemzeti jogszabályaikra, mint az információk védelmének megfelelően elégséges eszközére.

20. Ezért kell a javaslatra a személyes adatok védelemének szemszögéből különös figyelmet fordítani. Először is a normál esetben bizalmas és jól biztosított információkat kell megadni más tagállamok hatóságainak. Másodsorban ahhoz, hogy a rendszer jól működjön, létre kell hozni a rendszer működtetéséhez szükséges jegyzékadatokat, és azokat más tagállamok hatóságai számára rendelkezésre kell bocsátani. Ennek az elvnek a megvalósítása következésképp több adatot fog generálni, mint amennyi rendelkezésre áll jelenleg.

IV. **A FŐ ELEMEK**

A hozzáférhetőség elvének hatálya

21. Legelsősorban nélkülözhetetlen annak meghatározása, hogy a hozzáférhetőség elve milyen fajta információkra vonatkozik. Ezen elv alkalmazási területe általános értelemben a javaslat 2. cikkében kerül meghatározásra, az 1. cikk (1) bekezdésével és a 3. cikk (a) pontjával összefüggésben. Az elv az olyan információkra vonatkozik, amelyek:

– meglévő információk;

– szerepelnek a II. mellékletben lévő felsorolásban, amely hat információtípust határoz meg;

– az illetékes hatóságok rendelkezésére állnak.

Ez a három leglényegesebb eleme a Bizottság javaslatában szereplő elv hatályának. A hatály további újrameghatározásra kerül a 2. cikkben. A 2. cikk (1) bekezdése a hozzáférhetőségi elv alkalmazását a büntetőeljárás megkezdése előtti szakaszra korlátozza, míg a 2. cikk (2), (3) és (4) bekezdése ennél konkrétabb korlátozásokról rendelkezik.

22. A javaslat következményeinek megértéséhez szükséges a fent említett három leglényegesebb elem mélyrehatóbb elemzése. A hatály első két eleme önmagában is elég egyértelmű. A „meglévő információ” meghatározását a 2. cikk (2) bekezdése fejti ki, leszögezvén, hogy a kerethatározati javaslat nem foglal magában semmilyen olyan kötelezettséget, hogy információt kellene gyűjteni és tárolni kizárólag abból a célból, hogy azt hozzáférhetővé tegyék, míg a II. mellékletben lévő lista nem értelmezhető másképp. A harmadik leglényegesebb elem az, amelyik mind önmagában, mind pedig az első két elemmel fennálló kombinációban további tisztázásra szorul.

23. A javaslat nem konkretizálja, hogy a „rendelkezésre álló” információ csupán már az illetékes hatóság ellenőrzése alatt álló információt jelöli, vagy szintén beletartozik az az információ, ami ezen hatóságok által potenciálisan megszerezhető. Azonban az európai adatvédelmi biztos szerint a javaslatot lehet úgy értelmezni, hogy mindkettőt tartalmazza.

24. Valójában míg a 2. cikk (2) bekezdése szűkebb hatályt látszik sugallni, leszögezve azt, hogy a kerethatározat „nem foglal magában semmilyen olyan kötelezettséget, hogy információt kellene gyűjteni és tárolni kizárólag abból a célból, hogy azt hozzáférhetővé tegyék”, a 3. cikk (a) pontja megengedi a tágabb értelmezést, mikor azt mondja, hogy az „információ” „a II. mellékletben felsorolt létező információt” jelenti.

25. A II. melléklet legalább két olyan adatkategóriát említ, amely általában nem a rendőrség ellenőrzése alá esik. Az első kategória a jármű-nyilvántartási információ. Sok tagállamban az ilyen információt tartalmazó adatbázisokat nem a bűnüldöző hatóságok tartják ellenőrzésük alatt, noha az ezekhez való hozzáférést ezek a hatóságok rendszeresen igénybe veszik. Tartozzon ez a fajta információ a „rendelkezésre álló információ” hatálya alá, amelyet az 1. cikk szerint meg kell adni más tagállamok egyenértékű hatáskörrel rendelkező illetékes hatóságainak? A II. mellékletben felsorolt második megemlítendő adatkategória a telefonszámok és egyéb kommunikációs adatok: tekintsük-e ezeket az adatokat „rendelkezésre állónak” még akkor is, ha ezek az adatok nem az illetékes hatóságok, hanem magánkézben lévő cégek ellenőrzése alatt állnak?

26. Továbbá a javaslat egyéb rendelkezései, különösen a javaslat 3. cikkének d) pontja és a 4. cikk (1) bekezdésének c) pontja, alátámasztják azt a nézetet, hogy a „kijelölt hatóságok”, sőt még a „kijelölt felek” is tarthatják ellenőrzésük alatt azt az információt, amely az „illetékes hatóságok rendelkezésére” áll. Szintén a javaslat szövegéből következik, hogy „egy tagállam illetékes hatósága” olyan hatóság, amelyre az EU szerződés 29. cikkének első francia bekezdése vonatkozik, míg a nemzeti hatóság „kijelölt hatóságnak” minősülhet.

27. Az európai adatvédelmi biztos szerint a kijelölt hatóságok és kijelölt felek ellenőrzése alatt álló információhoz való hozzáférhetőség elvének alkalmazása a következő kérdéseket veti fel:

– A 30. cikk (1) bekezdésének b) pontja megfelelő jogalapot teremt-e, mivel az információt a kijelölt hatóságoknak és kijelölt feleknek rendelkezésre kell bocsátaniuk, és olyan adatbázisokból, amelyek nem tartoznak a harmadik pillér keretébe?

– A személyes adatok védelméről szóló keretrendelet úgy alkalmazandó-e, amint azt pl. a javaslat 8. cikke feltételezi?

– Ha nem, akkor a feldolgozás összhangban van-e a 95/46/EK irányelv szerinti kötelezettségekkel?

28. Egy ilyen tágan értelmezett elv megvalósítása, mint a „hozzáférhetőség elve", a rendelkezésre állónak tekintett adat világos és pontos meghatározását igényli. Az európai adatvédelmi biztos ezért a következőket javasolja:

– A hatály tisztázása.

– Első választási lehetőségként a hozzáférhetőség elvének hatályát az illetékes hatóságok ellenőrzése alatt álló információkra korlátozva.

– Második választási lehetőségként, tágabb hatály esetén, megfelelő biztosítékokkal biztosítani a személyes adatok védelmét. A fenti 27. pontban felvetett kérdéseket figyelembe kell venni.

A hatályhoz kapcsolódó egyéb kérdések

29. A javaslat 2. cikkének (1) bekezdése szerint a kerethatározat alkalmazandó a büntetőeljárás megkezdése előtt történő információfeldolgozásra. Hatálya korlátozottabb, mint a személyes adatok védelméről szóló kerethatározati javaslat, amely teljes mértékben alkalmazandó a büntetőügyekben folytatott igazságügyi együttműködésre.

30. Az európai adatvédelmi biztos szerint azonban ez a korlátozás önmagában nem korlátozza a rendőrségi együttműködési javaslat hatályát. Tartalmazhatná a büntetőügyekben folytatott igazságügyi együttműködést is, mivel számos tagállamban az igazságügyi hatóságok a bűnügyi nyomozások terén is rendelkeznek jogkörrel, még a büntetőeljárás megkezdése előtt is. Azonban az a tény, hogy a javaslat kizárólag az EUSz 30. cikke (1) bekezdésének b) pontján alapul, azt jelzi, hogy az csak rendőrségi együttműködésre vonatkozik. Ezen vonatkozás tisztázását szívesen vennénk.

31. A jelen javaslat az Europolnak történő információszolgáltatásra vonatkozik, míg a személyes adatok védelméről szóló kerethatározati javaslat kizárja a személyes adatoknak az Europol által történő feldolgozását. Az európai adatvédelmi biztos azt tanácsolja, hogy az Europollal történő információcserét korlátozzák az Europol saját céljaira, amint azt az Europol egyezmény 2. cikke és melléklete is említi. Továbbá figyelembe kellene venni az Europollal történő adatcserére vonatkozó részletes szabályokat, amelyeket már több tanácsi aktusban is meghatároztak.

Ne legyenek olyan új adatbázisok, amelyek személyes adatokat tartalmaznak

32. A javaslat kiindulópontja, hogy az nem fog személyes adatokat tartalmazó új adatbázisok létrehozásához vezetni. Ebből a szempontból a 2. cikk (2) bekezdése világosan fogalmaz: nem foglal magában semmilyen olyan kötelezettséget, hogy információt kellene gyűjteni és tárolni kizárólag abból a célból, hogy azt hozzáférhetővé tegyék. Az adatvédelem szempontjából ez a javaslat fontos és pozitív eleme. Az európai adatvédelmi biztos emlékeztet a nyilvános elektronikus kommunikációs közszolgáltatások nyújtása keretében feldolgozott adatok megőrzéséről szóló irányelvjavaslatra vonatkozó véleményére [1], amelyben hangsúlyozta, hogy az olyan jogi kötelezettségek, amelyek tetemes adatbázisokhoz vezetnek, különösen nagy kockázatot hordoznak magukban az érintettek számára, többek között a jogosulatlan felhasználás kockázata miatt.

33. Azonban:

– Fontos biztosítani, hogy a javaslat nem mozdítja elő az adatbázisok feltétel nélküli összekapcsolását, és ily módon az adatbázisok olyan hálózatát, amelyet nehéz felügyelni.

– A fent említett kiindulóponthoz képest van egy kivétel: A javaslat 10. cikke, amely biztosítja, hogy a jegyzékadatok online elérhetőek. A jegyzékadatok tartalmazhatnak személyes adatokat, illetve mindenesetre felfedhetik létezésüket.

Az információhoz való közvetlen és közvetett hozzáférés

34. A javaslat szól az információhoz való közvetlen és közvetett hozzáférésről is. A javaslat 9. cikke közvetlen online hozzáférést határoz meg az azon adatbázisokban lévő információkhoz, amelyekhez a nemzeti hatóságoknak közvetlen online hozzáférésük van. A 10. cikk közvetett hozzáférésről szól. Az online nem hozzáférhető információ jegyzékadatait az Europol és más tagállamok egyenértékű hatáskörrel rendelkező illetékes hatóságai online keresésre bocsátják rendelkezésre. Amennyiben a jegyzékadatok között megtalálják a keresett adatot, akkor ez a hatóság benyújthatja információigényét a kijelölt hatósághoz a jegyzékadatok által azonosított információ megszerzése érdekében.

35. A közvetlen hozzáférés nem vezet új adatbázisokhoz, hanem a tagállamok egyenértékű hatáskörrel rendelkező illetékes rendszereinek adatbázisai közötti átjárhatóságot igényli. Továbbá szükségszerűen a meglévő adatbázisok új használatát vezeti be azáltal, hogy olyan lehetőséget ad a tagállamok illetékes hatóságainak, amely eddig csak az illetékes nemzeti hatóságok előtt volt nyitva. A közvetlen hozzáférés automatikusan azt jelenti, hogy számos személynek lesz hozzáférése egy adatbázishoz, és éppen ezért megnövekszik a visszaélés kockázata.

[1] Az elektronikus kommunikációs közszolgáltatások nyújtásával összefüggésben feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról szóló európai parlamenti és tanácsi irányelvjavaslatról (COM (2005) 438 végleges) szóló 2005. szeptember 26-i vélemény.

36. Más tagállam illetékes hatósága általi közvetlen hozzáférés esetében a származás szerinti tagállam kijelölt hatóságainak nincs ellenőrzése az adatokhoz való hozzáférés és az adatok további felhasználása fölött. A közvetlen hozzáférésnek a javaslat által meghatározott eme következményét megfelelően kell kezelni, mivel:

– Úgy tűnik ezzel érvényét veszti a kijelölt hatóságok azon hatásköre, hogy megtagadják az információ megadását (a 14. cikk értelmében).

– Az adatokhoz való hozzáférést követően azok pontosságához és aktualizálásához kapcsolódó felelősség kérdése is felvetődik. A származás szerinti tagállam kijelölt hatósága hogyan tudja biztosítani, hogy az adatok mindig aktuálisak legyenek?

– Nem csak a kijelölt hatóság, amely többé nem tud eleget tenni az adatvédelmi törvény által ráháruló kötelezettségeinek, hanem a származás szerinti tagállam nemzeti adatvédelmi hatósága sem tudja többé felügyelni a kötelezettségek alkalmazását, mivel nincs semmilyen hatásköre más tagországok bűnüldözési hatóságaival szemben.

– Ezek a problémák még súlyosabbak, olyan esetekben, amikor olyan kijelölt hatóságok és kijelölt felek adatbázisaihoz való hozzáférésről van szó, amelyek nem bűnüldözési hatóságok (lásd ezen vélemény 25-28 pontját).

A közvetlen hozzáférés eme következménye fontos oka annak, hogy az ezen javaslat elfogadása miért függjön a személyes adatok védelméről szóló kerethatározat elfogadásától. Marad viszont egy probléma: Nehéz belátni, hogy a kijelölt hatóságok miként tudják a 14. cikk szerint megtagadni az információhoz való hozzáférést.

37. Ami a jegyzékadatokon keresztül történő közvetett hozzáférést illeti, az információt szolgáltat arról, hogy van-e vagy nincs-e a rendszerben találat: Ez nem új jelenség. Ez az alapja az olyan európai nagyszabású információs rendszerek működésének, mint például a Schengeni Információs Rendszer. A jegyzékadatok rendszere létrehozásának megvan az az előnye, hogy lehetővé teszi a származás szerinti tagállamok számára a rendőrségi adatállományukból lehívott információk ellenőrzését. Ha a jegyzékadatok megtekintése alapján van találat, akkor a megkereső hatóság tájékoztatási igénylést nyújt be az érintettre vonatkozóan. Ezt az igényt aztán megfelelően értékelheti a megkeresett hatóság.

38. Mindazonáltal megfelelő elemzés szükséges, mivel a jegyzékadatok rendszerének létrehozása – azokon a területeken, ahol ezek a rendszerek eddig nem léteztek, eltekintve az európai nagyszabású információs rendszerektől – új kockázatokkal járhat az érintett számára. Az európai adatvédelmi biztos hangsúlyozza, hogy noha a jegyzékadatok nem tartalmaznak adatokat az érintettről, a jegyzékadatokba történő betekintés igen érzékeny eredményhez vezethet. Felfedheti, hogy bűncselekményekkel kapcsolatban szerepel-e egy személy rendőrségi adatállományban.

39. Tehát rendkívül fontos, hogy az európai jogalkotó megfelelő szabályokat alkosson, legalább a jegyzékadatok létrehozásáról, a jegyzékadatok nyilvántartási rendszerének kezeléséről és a jegyzékadatokhoz történő hozzáférés megfelelő megszervezéséről. Az európai adatvédelmi biztos szerint a javaslat ezen szempontok szerint nem kielégítő. Ebben a szakaszban az európai adatvédelmi biztos három észrevételt tesz:

– A jegyzékadatok meghatározása nem egyértelmű. Nem egyértelmű, hogy a jegyzékadatokat meta-adatoknak, elsődleges kulcsnak, vagy netán mindkettőnek tekintik-e. A jegyzékadat fogalmát tisztázni kell, mivel közvetlen hatással van az adatvédelem szintjére és a szükséges biztosítékokra.

– A javaslatnak tisztáznia kell a nemzeti kapcsolattartók szerepét a jegyzékadatok tekintetében. A nemzeti kapcsolattartók bevonása szükséges lehet, különösen olyan esetekben, amikor a jegyzékadatok értelmezése speciális ismereteket igényel, például az ujjnyomatok esetleges összevetésekor.

– A javaslat a jegyzékadatok létrehozásához szükséges szabályok elfogadását a végrehajtási jogszabályra hagyja, a 19. cikkben meghatározott komitológiai eljárással összhangban. Jóllehet végrehajtási szabályokra szükség van, a jegyzékadatok létrehozását meghatározó alapvető szabályokat magában a kerethatározatban kellene lefektetni.

Előzetes engedélyezés az igazságügyi hatóság által

40. Az információcsere nem akadályozza meg a tagállamokat abban, hogy az igazságügyi hatóság által megadott előzetes engedélyhez kössék a megkereső hatóság számára történő adattovábbítást, amennyiben ez az információ a megkeresett országban igazságügyi ellenőrzés alatt áll. Ez azért fontos, mert a személyes adatok cseréje ügyében fennálló rendőrségi hatáskörről szóló felmérés szerint [1] nem minden tagállam rendőrsége tud önállóan hozzáférni ezekhez az adatokhoz. Az európai adatvédelmi biztos szerint a hozzáférhetőségi elv nem szabad, hogy aláaknázza a nemzeti jog szerinti azon előírást, hogy az információhoz való hozzáféréshez előzetes engedély szükséges, vagy legalábbis állapítson meg konkrét szabályokat azon adatkategóriákhoz, amelyekhez előzetes engedélyezés szükséges, és amelyek minden tagállamban alkalmazandóak.

[1] Az Európai Unió tagállamainak bűnüldözési hatóságai közötti, különösen a súlyos bűncselekményekre, köztük a terroristacselekményekre vonatkozó információk és bűnüldözési operatív információk cseréjének leegyszerűsítéséről (5815/1/05 tanácsi dok.) szóló kerethatározattal kapcsolatos kérdőívre adott válaszok.

41. E kötelezettséget a személyes adatok védelméről szóló kerethatározati javaslat 11. cikkének (2) bekezdésével kapcsolatban kell értelmezni, amely szintén kilátásba helyezi, hogy az adattovábbító tagállamnak legyen beleszólása az adatok azon tagállam által történő további felhasználásába, amelynek az adatot továbbították. Az európai adatvédelmi biztos kiemeli ezen elv jelentőségét, amely annak biztosításához szükséges, hogy a hozzáférhetőség ne vezessen a személyes adatok további felhasználására vonatkozó korlátozó jellegű nemzeti jogszabályok megkerüléséhez.

Zárómegjegyzés

42. Ezen elemek magas színvonalú adatvédelmet igényelnek. Különös figyelmet kellene fordítani a célhozkötöttség és a további feldolgozás elvének biztosítására, valamint a hozzáférés tárgyát képező információk pontosságára és megbízhatóságára (lásd az európai adatvédelmi biztos véleményét a személyes adatok védelméről szóló kerethatározatról, IV.2 és IV.6).

V. EGYÉB MEGKÖZELÍTÉSEK

A svéd javaslat

43. A svéd javaslat nem korlátozódik információk meghatározott típusára, hanem minden információra *és bűnüldözési operatív információra* kiterjed, még az olyan információra is, amely nem az illetékes bűnüldöző hatóság birtokában van. A javaslat előmozdítja az együttműködést azáltal, hogy időkorlátokat határoz meg a tájékoztatási megkeresésekre történő válaszadáshoz, és eltörli a tagállamon belüli, illetve a határokon átnyúló információcsere közötti különbségtételt. Nem rendelkezik olyan kiegészítő intézkedésekről, amelyek biztosítanák, hogy az információhoz hatékonyan hozzá lehessen férni. Ez okból tehát érthető, hogy a Bizottság a svéd javaslattal, mint a hozzáférhetőség megfelelő eszközével, nem volt elégedett. ([1])

44. Az adatvédelem szempontjából a svéd megközelítés jelentősége általában véve a következőkben foglalható össze:

– Üdvözlendő, hogy a javaslat szigorúan a meglévő adatok feldolgozására vonatkozik, és nem vezet új adatbázisokhoz, még „jegyzékadatokhoz” sem.

– Azonban a „jegyzékadatok” hiánya önmagában még nem feltétlenül pozitív elem. Megfelelő biztosítékok mellett a jegyzékadatok megkönnyíthetik az érzékeny adatok körében történő célzott, és épp ezért kevésbé befurakodó jellegű kutatást. Lehetővé teszi a megkeresések jobb szűrését és jobb felügyeletét is.

– Mindazonáltal a javaslat a személyes adatok határokon átnyúló cseréjének növekedéséhez vezet, ami kockázatot jelent a személyes adatok védelme szempontjából, többek között azért, mert érinti a tagállamoknak az adatok továbbítója felett meglévő ellenőrzési hatáskörét. Nem kellene a személyes adatok védelméről szóló kerethatározat elfogadásától függetlenül elfogadni.

A prümi egyzmény

45. A prümi egyezmény a hozzáférhetőség elvének megvalósítása szempontjából más megközelítést képvisel. Míg a kerethatározatra irányuló jelen javaslatnak van általános megközelítése – az egyes információtípusok cseréjéhez nem rendel különös szabályokat, hanem minden információtípusra egyaránt alkalmazandó, már amennyiben azok szerepelnek a II. melléklet felsorolásában (lásd az ezen vélemény 21-28. pontját) –, a prümi egyezmény megközelítése fokozatos.

46. Ezt a megközelítést olykor „adatmezőnkénti megközelítésnek” is nevezik. Egyes információtípusokra vonatkozik (DNS, ujjnyomatok adatai és jármű-nyilvántartási adatok), és megállapítja azt a kötelezettséget, hogy figyelembe kell venni az adat egyedi jellegét. Az egyezmény megállapítja azt a kötelezettséget, hogy DNS elemzési állományokat kell nyitni és megőrizni a bűncselekmények nyomozásához. Hasonló kötelezettség vonatkozik az ujjnyomatok adataira is. Ami a jármű-nyilvántartási adatokat illeti, azokhoz más tagállamok nemzeti kapcsolattartói számára közvetlen hozzáférést kell biztosítani.

47. A prümi egyezmény megközelítéséhez három észrevétel kívánkozik.

48. Először is természetesnek vesszük, hogy az európai adatvédelmi biztos nem helyesli az ezen egyezményhez vezető folyamatot, amely az Európai Unió intézményi keretrendszerén kívül esik, és következésképp a Bizottság érdemi bevonása nélkül zajlott. Továbbá ez azt jelenti, hogy sem az Európai Parlament által gyakorolt demokratikus ellenőrzés, sem pedig a Bíróság által gyakorolt igazságügyi ellenőrzés nem érvényesül, amelynek eredményeképp kevesebb garancia van arra, hogy valamennyi (köz)érdek egyenlő hangsúlyt kap. Ebbe beletartozik a személyes adatok védelmének szempontja is. Más szóval, az Európai Unió intézményeinek nincs alkalmuk arra, hogy értékeljék – a rendszer létrehozása előtt –, hogy a választott koncepciónak milyen hatása van a személyes adatok védelmére.

49. Másodsorban nyilvánvaló, hogy a prümi egyezmény némely eleme az érintett számára egyértelműen tolakodóbb jellegű, mint a hozzáférhetőségről szóló kerethatározati javaslat. Az egyezmény szükségszerűen új adatbázisok létrehozásához vezet, ami önmagában véve kockázatot jelent a személyes adatok védelmére nézve. Ezen új adatbázisok szükségességét és arányosságát demonstrálni kellene. A személyes adatok védelmét megfelelő garanciákkal kell biztosítani.

([1]) Lásd a Bizottság szolgálatai által benyújtott munkadokumentum mellékletét a hozzáférhetőség elve értelmében történő információcseréről szóló tanácsi kerethatározatra irányuló javaslathoz (SEC 2005 (1270), 2005.10.12).

Az „adatmezőnkénti megközelítés”

50. Harmadsorban, mint már korábban említettük, az egyezmény az „adatmezőnkénti megközelítést” alkalmazza. A fentiekben az európai adatvédelmi biztos megemlítette az ahhoz a környezethez kapcsolódó nehézségeket és bizonytalanságokat, amelyben a hozzáférhetőség elvét hatékonyabbá kell tenni. E körülmények között az európai adatvédelmi biztos szerint célravezetőbb tartózkodni egy adatkör számára történő rendszer létrehozásától, és inkább egy óvatosabb megközelítéssel kellene kezdeni, amely egy fajta adattípust tartalmazna, és figyelni kellene, hogy a hozzáférhetőség elve milyen mértékben tudja hatékonyan támogatni a bűnüldözést, valamint, hogy a személyes adatok védelmét milyen konkrét kockázatok érintik. Ezen tapasztalatok fényében a rendszert esetleg majd ki lehet bővíteni más adattípusokra is, illetve módosítani lehetne a hatékonyság fokozása érdekében.

51. Ez az „adatmezőnkénti megközelítés” jobban megfelelne az arányosság elve által támasztott követelményeknek is. Az európai adatvédelmi biztos szerint a bűnüldözési céllal történő, határokon átnyúló jobb adatcsere szükségletei EU-szintű jogi eszköz elfogadását indokolják, de az eszköznek az arányosság szem előtt tartása mellett kellene megfelelően elérni célját, amelyet jobban meg lehet állapítani a gyakorlati tapasztalatok gyűjtésére szánt időszak elteltével. Továbbá, az eszköz ne sértse aránytalanul az érintettet. A cserének nem többet, csak a szigorúan szükséges adattípusokat kellene érintenie, a név nélküli adatcsere lehetőségével, és az adatvédelem szigorú feltételeinek betartásával kellene zajlania.

52. Továbbá az európai adatvédelmi biztos által képviselt óvatosabb megközelítés – esetleg az „adatmezőnkénti megközelítésen” túlmenően – magában foglalhatná a hozzáférhetőségi elv csupán közvetett hozzáféréssel, tehát a jegyzékadatok útján történő megvalósítását. Az európai adatvédelmi biztos ezt a további jogalkotási folyamat során megfontolásra érdemesnek javasolja.

VI. **MELY ADATOK?**

53. A II. melléklet számba veszi azokat az információtípusokat, amelyeket a javasolt kerethatározat értelmében meg lehet szerezni. Mind a hat ott felsorolt információtípus a legtöbb körülmény között személyes adat, mert mindegyiknél fennáll egy azonosított vagy azonosítható személyhez való viszonyulás.

54. A javaslat 3. cikkének g) pontja szerint a jegyzékadatok „azon adatok, amelyek célja megkülönböztetően azonosítani az információkat, és amelyek között keresőrutin segítségével ellenőrizhető, van-e rendelkezésre álló információ”. A „hozzáférhetőség elvének végrehajtására vonatkozó megközelítés” ([1]) című anyagban a következő adatok szerepelnek jegyzékadatokként:

– az érintett személyek személyazonosító adatai;

– az érintett tárgyak (járművek, dokumentumok) azonosítószáma;

– ujjnyomatok, digitális fényképek.

A DNS-profil lehetne egy másik olyan adattípus, amely jegyzékadatnak minősülhetne. A jegyzékadatok ezen felsorolásából kiderül, hogy a jegyzékadatok tartalmazhatnak személyes adatokat, és ily módon azok megfelelő védelme szükséges.

55. Az európai adatvédelmi biztos külön foglalkozik a DNS profilok kérdésével. A DNS elemzés értékesnek bizonyult a bűnügyi nyomozások során, és a DNS adatok cseréje alapvető fontosságú lehet a bűnözés elleni küzdelemhez. Azonban az is alapvető fontosságú, hogy a DNS adatok fogalmát egyértelműen meghatározzák, és hogy ezen adatok sajátos jellemzőit megfelelően figyelembe vegyék. Valójában adatvédelmi szempontból nagy különbség van a DNS minták és DNS profilok között.

56. A DNS mintákat (amelyeket gyakran gyűjtenek illetve tárolnak a bűnüldöző hatóságok) különösen érzékenynek kellene tekinteni, mert valószínűbb, hogy a teljes DNS „képet” tartalmazzák. A genetikai jellemzőkről és az illető személy egészségi állapotáról adhatnak felvilágosítást, ami teljesen különböző célokból lehet szükséges, úgymint például személyeknek, vagy fiatal pároknak történő orvosi tanácsadás.

57. A DNS profilok – épp ellenkezőleg – csak a DNS mintából kivonatolt részleges DNS információkat tartalmaznak: Személyek azonosításához lehet ezeket felhasználni, de elvileg nem derülnek ki belőle egy személy genetikai jellemzői. Mindazonáltal a tudomány előrehaladtával a DNS profilokból kideríthető információk száma növekedhet majd: amit „ártatlan” DNS profilnak tekintenek egy adott pillanatban, egy későbbi időszakban sokkal több információt árulhat el, mint várható vagy szükséges lenne, különösen egy személy genetikai jellemzőire vonatkozó információkat. A DNS profilokból leszűrhető információkat épp ezért dinamikusnak kellene tekinteni.

58. Ebből a szempontból az európai adatvédelmi biztos megjegyzi, hogy mind a prümi egyezmény, mind pedig a bizottsági javaslat támogatja a DNS adatok bűnüldözési szervek közötti cseréjét, de lényeges különbséggel teszik ezt.

([1]) Az elnökség által a Tanácsnak megküldött anyag, 2005. április 5. (7641/05).

59. Az európai adatvédelmi biztos üdvözli, hogy a Bizottság javaslata nem támaszt DNS adatgyűjtési kötelezettséget, és egyértelműen korlátozza a DNS adatok és DNS profilok cseréjét. A II. mellékletben a kriminalisztikai DNS elemzésekben használt DNS-markerek előzetes közös listája révén meghatározzák a DNS profilokat. Ez a lista – amely hét, a DNS-analízis eredményeinek cseréjéről szóló 2001. június 25-i tanácsi állásfoglalás ([1]) I. mellékletében meghatározott európai szabványban foglalt DNS markeren alapul – garantálja, hogy a kivonatolt DNS profilok nem tartalmaznak semmilyen információt az egyes öröklődő tulajdonságokról.

60. Az európai adatvédelmi biztos kiemeli, hogy ez a tanácsi állásfoglalás nagyon fontos garanciákat határoz meg, amelyek konkrétan a DNS profilok dinamikus jellegével kapcsolatosak. Az állásfoglalás III. szakasza, miután a DNS elemzések eredményeinek cseréjét azon „kromoszóma zónákra korlátozza, melyekről […] nem ismeretes az, hogy konkrét örökletes tulajdonságokról információt nyújtanának", azt ajánlja a tagállamoknak, hogy ne használják többé azokat a DNS markereket, amelyek a tudomány fejlődése következtében konkrét örökletes tulajdonságokról nyújthatnak információt.

61. A prümi egyezmény más megközelítést alkalmaz, mivel a szerződő feleket arra kötelezi, hogy a bűncselekmények nyomozásához DNS elemzési állományokat nyissanak és őrizzenek meg. Tehát ez feltételezi az új DNS adatbázisok létrehozását, és a DNS adatok fokozott gyűjtését. Továbbá nem világos, hogy mely adatok szerepelnek a „DNS elemzési állományokban", és az egyezmény nem veszi figyelembe a DNS profilok dinamikus fejlődését sem.

62. Az európai adatvédelmi biztos rámutat arra, hogy a DNS adatok cseréjével foglalkozó bármely jogi eszköznek:

– egyértelműen korlátozni kell és meg kell határoznia a megadható DNS információkat (tekintettel a DNS minták és a DNS profilok között fennálló alapvető különbségre is);

– meg kell állapítania közös technikai szabványokat annak érdekében, hogy nehogy eltérő legyen a tagállamok kriminalisztikai DNS adatbázisaival kapcsolatos gyakorlat, amely nehézségekhez és pontatlan eredményekhez vezethet, amikor adatcserére kerül sor,

– megfelelő, jogilag kötelező érvényű garanciákat kellene nyújtania annak megelőzése céljából, hogy a tudomány fejlődése ne eredményezze azt, hogy a DNS profilokból olyan személyes adatokhoz lehessen hozzájutni, amelyek nemcsak érzékenyek, hanem szükségtelenek is ahhoz a célhoz képest, amiért gyűjtötték őket.

([1]) HL C 187., 1. o.

63. Ebből a szempontból az európai adatvédelmi biztos ezennel megerősíti és integrálja a személyes adatok védelméről szóló kerethatározatról szóló véleményében elmondottakat (80. pont). Abban a véleményben az európai adatvédelmi biztos rámutatott, hogy a DNS adatok tekintetében konkrét biztosítékokat kell nyújtani a következők garantálása céljából: A rendelkezésre álló információt csak személyek azonosítására lehet felhasználni bűncselekmények megelőzéséhez, felderítéséhez és nyomozásához; a DNS profilok pontossági szintjét körültekintően figyelembe kell venni, annak helyességét az érintett könnyen hozzáférhető módon megkérdőjelezheti; az emberi méltóság tiszteletét teljes mértékben biztosítani kell. ([2])

64. Ezek a megfontolások hovatovább arra a következtetésre engednek jutni, hogy a DNS-állományok létrehozásáról és az ezen állományokból történő adatcseréről szóló jogszabályokat csak egy olyan hatásvizsgálat után kellene elfogadni, amelyben az előnyöket és a kockázatokat megfelelő mértékben értékelhették. Az európai adatvédelmi biztos azt ajánlja, hogy ez a jogszabály a hatályba lépése után tegye kötelezővé a rendszeres értékelést.

65. A II. melléklet végezetül más megadható információtípusokat is tartalmaz. Többek között olyan információkat, amelyek nem valamely hatóságtól származnak, tekintve, hogy a telefonszámok és más kommunikációs adatok, akárcsak a forgalmi adatok, normál esetben a távbeszélő üzemeltetőjétől származnak. Az indokolás megerősíti, hogy a tagállamoknak kötelező biztosítani, hogy a bűnüldözés szempontjából releváns, ebből a célból kijelölt hatósági vagy privát ellenőrzés alatt álló információkat megosszák más tagállamok egyenértékű hatáskörrel rendelkező hatóságaival és az Europollal. Míg a javaslat vonatkozik a nem valamely hatóságtól származó személyes adatokra, az alkalmazandó jogi keretnek – az európai adatvédelmi biztos véleménye szerint – tartalmaznia kellene pótlólagos garanciákat az érintett védelmére az adatok pontosságának biztosítása érdekében.

VII. AZ ADATVÉDELEM ELVEI

66. A személyes adatok védelmére vonatkozó szabályok nincsenek konkrétan lefektetve a javasolt tanácsi kerethatározatban, míg más eszközökben, mint például a prümi egyezményben vagy a svéd javaslatban a személyes adatok védelméről konkrét módon rendelkeznek. A személyes adatok védelmével kapcsolatos szabályok hiánya a hozzáférhetőségi javaslatban annyiban fogadható el, amennyiben a harmadik pillérben történő adatvédelemről szóló kerethatározati javaslatban fellelhető általános szabályok teljes mértékben alkalmazandók és elegendő védelmet nyújtanak. Továbbá az egyes eszközök – mint a svéd javaslat és a prümi egyezmény – által lefektetett, a személyes adatok védelmével kapcsolatos szabályoknak nem kellene csökkenteniük az általános keret által biztosított védelmi szintet. Az európai adatvédelmi biztos ajánlja, hogy kerüljön be egy külön klauzula a különböző adatvédelmi szabályok közötti esetleges ütközésekről.

([2]) Ugyanebben a vonatkozásban lásd még az Európa Tanácsnak az Egyezmény 108. cikke elveinek a biometrikus adatok gyűjtésére és feldolgozására való alkalmazásáról szóló, az elért eredményekről szóló jelentését, 2005. február.

67. Itt az európai adatvédelmi biztos ismételten kiemelné annak fontosságát, emlékeztetve a személyes adatok védelméről szóló kerethatározat kapcsán kinyilvánított véleményére, hogy olyan következetes és átfogó adatvédelmi szabályok vonatkozzanak a bűnüldözési együttműködésre, amelyek minden feldolgozásra alkalmazandóak. Az európai adatvédelmi biztos továbbá újfent megerősíti az előbb említett véleményben szereplő meglátásait. Ebben a bekezdésben a következő adatvédelmi kérdéseket hangsúlyozzuk:

– A személyes adatok jogszerű feldolgozása. Az európai adatvédelmi biztos támogatja azt a megközelítést, hogy az információt csak akkor lehet rendelkezésre bocsátani, ha azt jogszerűen gyűjtötték (amint azt a 2.2 cikk említi a kényszerítő intézkedések útján gyűjtött információk tekintetében). A személyes adatok jogszerű feldolgozása azt is biztosítaná, hogy a rendelkezésre bocsátott és megadott információkat megfelelően fel lehessen használni bírósági eljárás során is. Valójában, noha a büntetőeljárás kezdete után feldolgozott információ a javasolt eszköz hatályán kívül esik, mégis valószínű, hogy a bűnüldözési hatóságok között előzőleg kicserélt információ végül a bírósági eljárás során is felbukkan.

– A személyes adatok minősége különös jelentőséggel bír, mivel a hozzáférhetőségi elv amellett szól, hogy az információt olyan bűnüldöző hatóságok használják fel, amelyek azon összefüggésrendszeren kívül tényekednek, amelyben az adatokat begyűjtötték. Ezek a hatóságok még közvetlen hozzáféréssel is rendelkeznek más tagállamok adatbázisaihoz. A személyes adatok minőségét csak akkor lehet biztosítani, ha azok pontosságát rendszeresen és megfelelően ellenőrzik, ha az információkat az érintettek különböző kategóriái szerint megkülönböztetik (áldozat, gyanúsított, tanú, stb.), és ha szükség esetén a pontosság mértékét is feltüntetik (lásd az európai adatvédelmi biztos véleményét a személyes adatok védelméről, IV. 6.)

Ezek a szempontok újfent világossá teszik, hogy az adatvédelmi szabályokat, és különösen a pontosságról szóló szabályokat, miért kell minden fajta feldolgozásra alkalmazni, még a belföldiekre is. Máskülönben a közvetlenül hozzáférhető személyes adatok helytelenek, elavultak lehetnek, és ily módon sérthetik mind az érintett jogait, mind pedig a nyomozások hatékonyságát.

– A célok meghatározása. A hozzáférhetőség elve szerint a személyes adatokhoz más tagállamok egyenértékű hatáskörrel rendelkező hatóságai férhetnek hozzá. Mindazonáltal a bűnüldözési hatóságok hatásköre lényegesen eltérhet egymástól országonként. Épp ezért fontos biztosítani, hogy a célhozkötöttség elvét tiszteletben tartsák az adatok cseréjében részt vevő különböző illetékes hatóságok eltérő terjedelmű hatásköre ellenére. Egy bizonyos hatóság által sajátos céllal gyűjtött és feldolgozott információkat ezek után nem lehet – csupán arra hivatkozva, hogy az adatot megkapó hatóság eltérő, esetleg szélesebb körű, hatáskörrel rendelkezik – más célra felhasználni.

Következésképp az európai adatvédelmi biztos üdvözli a javasolt kerethatározat 7. cikkét, amely a személyes adatok védelméről szóló kerethatározati javaslatban foglalt általános szabályok részletesebb kibontásaként értelmezendő. Továbbá az európai adatvédelmi biztos megjegyzi, hogy a különböző hatóságok közötti ekvivalencia értékelését (amelyet a jelenlegi javaslat egy komitológiai eljárás keretébe utal) körültekintően és a célhozkötöttség elvének megfelelő tiszteletben tartásával kellene végezni.

– A megadott információk tárolásához megszabott határokat a célhozkötöttség elvének tükrében is kell szemlélni: egy bizonyos céllal hozzáfért vagy megadott információt azonnal ki kell törölni, mihelyst az adott célhoz már nem szükséges. Így az adatbázisok szükségtelen sokszorozódása is elkerülhető, ugyanakkor az illetékes hatóságok számára ismételten hozzáférhető az (aktualizált) rendelkezésre álló információ, amennyiben az másik jogszerű cél elérése érdekében szükséges.

– A hozzáférhetőség elve szerint megadott információk naplózása. A naplózásra mindkét oldalon sort kellene keríteni: megkeresett és a megkereső tagállamban egyaránt. Hozzáférési naplókat – nem csak cserenaplókat – kell vezetni (a európai adatvédelmi biztos véleménye a személyes adatok védelméről, 133. pont), annak biztosítása érdekében is, hogy a nemzeti illetékes hatóságok bízzanak egymásban, és ne veszítsék el teljesen ellenőrzésüket a rendelkezésre álló információ fölött. Az információk nyomonkövethetőségének igénye azt a lehetőséget is magában foglalja, hogy aktualizálják illetve helyesbítsék az információkat.

– Az érintettek jogai. Az EU bűnüldöző hatóságai közötti információcserét szolgáló rendszerek megnövelik az olyan helyzetek számát, amelyekben személyes adatokat ugyanabban az időben különböző tagállamok illetékes hatóságai dolgoznak fel (ideiglenesen). Ez azt jelenti egyrészről, hogy az érintettek jogaira vonatkozó közös EU-követelményeket kellene létrehozni, másrészről pedig, hogy az érintettek gyakorolhassák jogaikat, olyan mértékben, amilyet a harmadik pillérhez tartozó adatvédelmi szabályok megengednek, mind azon hatóságokkal szemben, amelyek rendelkezésre bocsátják az adatokat, mind pedig azon hatóságokkal szemben, amelyek hozzáférnek azokhoz az adatokhoz és azokat feldolgozzák.

– Felügyelet. Az európai adatvédelmi biztos rámutat arra, hogy az esettől függően több, mint egyetlen nemzeti felügyeleti hatóságnak lehet hatásköre a személyes adatoknak a jelenlegi javaslatok alapján végrehajtott feldolgozását ellenőrizni. Ebben a tekintetben a bűnüldözési információkhoz történő közvetlen online hozzáférés az érintett nemzeti adatvédelmi hatóságok fokozott felügyeleti tevékenységét és összehangolását igényli.

VIII. **KÖVETKEZTETÉSEK**

A hozzáférhetőség elvével kapcsolatos általános következtetések

68. Az európai adatvédelmi biztos megragadja az alkalmat arra, hogy ebben a véleményben kifejtsen néhány általános és alapvető jellegű nézetet a bűnüldözési információk cseréjének témájával és az e téma szabályozásához tartozó megközelítésekkel kapcsolatban. Az európai adatvédelmi biztos a későbbiek folyamán további konzultációkra áll rendelkezésre, miután ezen, vagy más kapcsolódó javaslatokhoz tartozó jogalkotói folyamatban releváns fejlemények történnek.

69. Az európai adatvédelmi biztos szerint a hozzáférhetőség elvét jogilag kötelező erejű eszközként kellene megvalósítani, olyan óvatosabb és fokozatosabb megközelítés alkalmazásával, amely egyfajta adattípusról szól, és figyelni kellene, hogy a hozzáférhetőség elve milyen mértékben tudja hatékonyan támogatni a bűnüldözést, valamint a személyes adatok védelmével kapcsolatban milyen sajátos kockázatok merülnek fel. Ez az óvatosabb megközelítés magában foglalhatná azt, hogy a hozzáférhetőség elvének megvalósítása csupán közvetett hozzáféréssel, jegyzékadatok igénybevételével kezdődne. Ezen tapasztalatok fényében a rendszert esetleg majd ki lehet bővíteni más adattípusokra is, illetve módosítani lehetne a hatékonyság fokozása érdekében.

70. Nem szabadna bármilyen olyan jogi eszközt elfogadni, amely a hozzáférhetőség elvét valósítja meg, anélkül, hogy előtte el ne fogadnák az alapvető adatvédelmi garanciákat, amint az a személyes adatok védelméről szóló kerethatározati javaslatban szerepel.

Ajánlások a jelen javaslat módosítására

71. Az európai adatvédelmi biztos ajánlja a hozzáférhetőségi elv hatályának a következők szerinti tisztázását:

   – A rendelkezésre állónak tekintett adatok egyértelmű és pontos meghatározása.

   – Első választási lehetőségként korlátozva az illetékes hatóságok ellenőrzése alatt álló információkhoz való hozzáférhetőség elvének hatályát.

   – Második választási lehetőségként, tágabban értelmezett hatály esetén, megfelelő biztosítékokkal biztosítani a személyes adatok védelmét. Az ezen vélemény 27. pontjában felvetett kérdéseket figyelembe kell venni.

72. Az európai adatvédelmi biztos a következő észrevételeket teszi egy más tagállam illetékes hatósága által az adatbázisokhoz történő közvetlen hozzáféréssel kapcsolatban;

   – A kérdést megfelelően kell kezelni, mivel a közvetlen hozzáférés esetében a származás szerinti ország kijelölt hatóságainak nincs ellenőrzésük az adatokhoz történő hozzáférés és azok további felhasználása fölött.

   – A javaslat nem mozdíthatja elő az adatbázisok feltétel nélküli összekapcsolását, és ily módon adatbázisok olyan hálózatát, amelyet nehéz lesz felügyelni.

73. A kerethatározatnak pontosabban kellene fogalmazni a jegyzékadatok rendszerének létrehozásával kapcsolatban. Azaz különösen:

   – A javaslat alkosson megfelelő szabályokat, legalább a jegyzékadatok létrehozásáról, a jegyzékadatok nyilvántartási rendszerének kezeléséről és a jegyzékadatokhoz történő hozzáférés megfelelő megszervezéséről.

   – A jegyzékadatok meghatározását egyértelműsíteni kell.

   – A javaslatnak tisztáznia kellene a nemzeti kapcsolattartók szerepét a jegyzékadatok tekintetében.

   – A jegyzékadatok létrehozásának alapszabályait magába a kerethatározatba kellene foglalni, nem pedig a végrehajtási jogszabályra kellene bízni a komitológiai eljárás szerint.

74. Az európai adatvédelmi biztos rámutat, hogy a javaslat – amennyiben a DNS adatok cseréjéről rendelkezik – tegye meg a következőket:

   – Egyértelműen korlátozza és határozza meg a megadható DNS információkat (tekintettel a DNS minták és a DNS profilok között fennálló alapvető különbségre is).

   – Állapítson meg közös technikai szabványokat annak elkerülése céljából, hogy a tagállamok kriminalisztikai DNS adatbázisaival kapcsolatos gyakorlat eltérő legyen, mely nehézségekhez és pontatlan eredményekhez vezethet, amikor adatcserére kerül sor.

   – Nyújtson megfelelő, jogilag kötelező érvényű garanciákat annak megelőzése céljából, hogy a tudomány fejlődése ne eredményezze azt, hogy a DNS profilokból olyan személyes adatokhoz lehessen hozzájutni, amelyek nem csak hogy érzékenyek, hanem szükségtelenek is ahhoz a célhoz képest, amiért gyűjtötték őket.

   – Csak hatásvizsgálat után fogadják el.

75. Az európai adatvédelmi biztos azt tanácsolja, hogy az Europollal történő információcserét korlátozzák az Europol saját céljaira, amint azt az Europol egyezmény 2. cikke és melléklete is említi.

Kelt Brüsszelben, 2006. február 28-án.

Peter HUSTINX

Európai Adatvédelmi Biztos