EURÓPAI ADATVÉDELMI BIZTOS

Az európai adatvédelmi biztos véleménye a vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről szóló európai parlamenti és tanácsi rendeletre vonatkozó javaslatról (COM(2004)835 végleges)

(2005/C 181/06)

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 Bizottságtól 2005. január 25-én kapott, a 45/2001/EK rendelet 28. cikkének (2) bekezdése szerinti véleménykérésre;

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

1. BEVEZETÉS

1.1. Előzetes megjegyzések

A vízuminformációs rendszer (VIS) létrehozása jelentős részét képezi az EU közös vízumpolitikájának, és több, összefonódó eszköz is szabályozza.

– 2003 áprilisában a Bizottság megbízása alapján megvalósíthatósági tanulmány ([1]) készült a VIS-ről.

– 2003 szeptemberében a Bizottság egy korábbi, a vízumok egységes formátumának meghatározásáról szóló rendelet módosítását ([2]) javasolta. Ennek fő célja biometrikus adatoknak (arcképnek és két ujjlenyomatnak) az új vízumformátumba való bevezetése volt. Ezeket a biometrikus adatokat mikrochipen kellene tárolni.

([1]) Vízuminformációs rendszer, végleges jelentés, végezte az EK megbízása alapján a Trasys, 2003. április.
([2]) COM(2003)558 végleges, a 2003/0217 (CNS) és a 2003/0218 (CNS) dokumentummal.

– 2004 júniusában egy tanácsi határozat ([1]) megkezdte a vízuminformációs rendszer kiépítésének folyamatát, biztosítva a rendszernek az EU költségvetésébe való belefoglalása jogalapját. Ez a határozat a vízumkérelemmel kapcsolatos információkat tartalmazó központi adatbázisra tett javaslatot, és a VIS műszaki fejlesztésének irányítására komitológiai folyamatot vett tervbe.

2004 decemberében a Bizottság a vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről javaslatot ([2]) (a továbbiakban: a javaslat) fogadott el, amely e vélemény tárgya. A kibővített hatásvizsgálatra vonatkozó tanulmányt ([3]) mellékelték a javaslathoz.

Az indokolásban kifejtettek szerint azonban e rendelet kiegészítéséhez további jogi eszközökre lesz szükség, különösen az alábbiak tekintetében:

– a Schengeni Egyezmény Szerződő Feleinek diplomáciai missziói és konzuli posztjai számára kiadott vízumokra vonatkozó közös konzuli utasítások (a továbbiakban: Közös Konzuli Utasítások) módosítása a biometrikus adatoknak az eljárásokba való bevonásával kapcsolatban;

– új mechanizmus kifejlesztése az Írországgal és az Egyesült Királysággal folytatott adatcseréhez;

– a hosszú távú tartózkodásra jogosító vízumokra vonatkozó adatcsere.

A Bel- És Igazságügyi Tanács 2003. június 5–6-i ülésén hozott döntésnek és a fent említett, 2004. júniusi tanácsi határozat 1. cikkének (2) bekezdésében leírtaknak megfelelően a VIS egy adatbázist tartalmazó centralizált architektúrán alapul, amely a vízumkérelmi fájlokat tároló adatbázisból: a Központi Vízuminformációs Rendszerből (CS-VIS) és a tagállamokban lévő Nemzeti Interfészből (NI-VIS) áll. A tagállamok kijelölnek ([4]) egy olyan központi nemzeti hatóságot, amely kapcsolódik a Nemzeti Interfészhez, és amelyen keresztül az illetékes hatóságaik hozzáférnek a CS-VIS-hez.

1.2. **A javaslat fő elemei az adatvédelem szempontjából**

A javaslat célja a közös vízumpolitika igazgatásának javítása a tagállamok közti adatcserét megkönnyítő központi adatbázis létrehozása révén. A rendelet tervbe veszi a biometrikus adatok (fénykép és ujjlenyomat) bevezetését a kérelmezési eljárásba, és ezek központi adatbázisban való tárolását.

A biometrikus adatok a vízumbélyegre is rákerülhetnek egy mikrochipen tárolt fénykép és ujjlenyomat bevonásával, amint azt a Bizottságnak az egységes vízumformátumról szóló rendelet módosítására vonatkozó javaslata jelezte (a folyamatban lévő elemzés eredményeire alapuló tanácsi határozat még nem készült el.)

A javaslat részletesen leírja az adatokon végzett különböző műveleteket (bevitel, módosítás, törlés, megtekintés) és a VIS-be a kérelem állásától függően bevezetendő különféle további adatokat (elfogadás, elutasítás stb.)

A javaslat valamennyi kérelemmel kapcsolatban ötéves adattárolási időszakot ír elő.

A javaslat korlátozásokkal felsorolja a vízumhatóságokon kívüli illetékes hatóságokat, amelyek hozzáféréssel fognak rendelkezni a VIS-hez, és meghatározza a nekik nyújtandó hozzáférési jogokat:

– a külső határokon és a tagállamok területén belüli vízumellenőrzéseket folytató illetékes hatóságok;

– az illetékes bevándorlási hatóságok;

([1]) 2004/512/EK, HL L 213., 2004.6.15., 5. o.
([2]) COM(2004) 835 végleges, a 2004/0287 (COD) dokumentummal.
([3]) Tanulmány a vízuminformációs rendszer kiterjesztett hatásvizsgálatáról, EPEC végleges jelentés, 2004. december.
([4]) A javaslat 24. cikkének (2) bekezdése

– az illetékes menekültügyi hatóságok.

A VIS működésének és a kapcsolódó felelősségi köröknek a leírása során a javaslat hangsúlyozza, hogy a Bizottság a tagállamok nevében dolgozza fel a VIS adatait. Leírja, hogy az adatbiztonság garantálása érdekében szükséges az adatfeldolgozási nyilvántartások használata, és részletezi az e biztonsági szintet garantáló felelősségi köröket.

A javaslat tartalmaz egy fejezetet az adatvédelemre vonatkozóan, amely a nemzeti adatvédelmi hatóságok, valamint az európai adatvédelmi biztos szerepét részletesen leírja.

A javaslat a VIS műszaki bevezetésével és a szükséges technológiák kiválasztásával a Schengeni Információs Rendszer második generációjának (SIS II) kifejlesztéséről szóló 2424/2001/EK rendelet 5. cikkének (1) bekezdésével létrehozott bizottságot bízza meg.

A VIS-ről a Bizottság megbízásából készített és az EPEC által elvégzett hatásvizsgálat e javaslat mellékletét képezi. E hatásvizsgálat arra a következtetésre jut, hogy a biometriával támogatott VIS a rendelkezésre álló lehetőségek közül a legjobb megoldás a közös vízumpolitika javítására.

2. **A VONATKOZÓ JOGI KERET**

A javaslat jelentős hatást fog gyakorolni az egyének személyiségi és egyéb alapvető jogaira; ezért az adatvédelmi elvek szempontjából ellenőrizni kell. Vizsgálatunk főbb hivatkozási pontjai a következők:

– A magánélet tiszteletben tartását az Európa Tanács által 1950-ben elfogadott, az emberi jogok és alapvető szabadságok védelméről szóló egyezmény elfogadása óta biztosítják Európában. Ezen egyezmény 8. cikke előírja a „magán- és a családi élet tiszteletben tartásához való jogot".

  A 8. cikk (2) bekezdése szerint e jog gyakorlásába hatóság csak a „törvényben meghatározott esetekben" avatkozhat be, amikor az „egy demokratikus társadalomban" fontos érdekek védelme érdekében „szükséges". Az Emberi Jogok Európai Bíróságának esetjogában e feltételek a beavatkozás jogalapjának minőségét, az intézkedések arányosságát és a visszaéléssel szembeni megfelelő biztosítékok szükségességét illetően további követelmények megjelenéséhez vezettek.

  Az egyénnek a személyes adatok feldolgozásával kapcsolatos védelmére vonatkozó alapelveket az Európai Tanács által elkészített és 1981-ben elfogadott adatvédelmi egyezmény alakította ki.

– A magánélet tiszteletben tartásához való jogot és a személyes adatok védelmét a közelmúltban az Európai Unió alapjogi chartájának 7. és 8. cikkében írták elő, amely az Unió új alkotmányának II. részét képezi.

  A charta 52. cikke szerint ezek a jogok korlátozhatók, amennyiben az emberi jogok és alapvető szabadságok védelméről szóló egyezmény 8. cikke szerinti feltételekhez hasonló feltételek teljesülnek. E feltételeket a lehetséges beavatkozásra vonatkozó javaslatok értékelése során figyelembe kell venni.

A jelenlegi uniós jogszabályok szerinti alapvető adatvédelmi szabályokat az alábbi jogi aktusok határozzák meg:

– 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 irányelv (HL L 281., 31. o.). Erre az irányelvre a 95/46/EK irányelvként történik hivatkozás. Ez az irányelv meghatározza azokat a részletes elveket, amelyekkel a javaslatot – olyan mértékben, amennyire az a tagállamokra alkalmazandó – összevetik. Ez a relevánsabb, mivel a javaslatot az irányelvnek érvényt szerző nemzeti jogszabályokkal együtt kell alkalmazni. A javasolt rendelkezések és biztosítékok hatékonysága így minden egyes esetben e kombináció hatékonyságától függ.

– 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 (HL L 8., 1. o.) Erre a rendeletre 45/2001/EK rendeletként történik hivatkozás. A 95/46/EK irányelvben meghatározottakhoz hasonló elveket ír elő, és ebben az összefüggésben annyira releváns, amennyiben a javaslat a Bizottság tevékenységeire alkalmazandó, a rendelet rendelkezéseivel együtt. Ez a kombináció ezért szintén érdemel némi figyelmet.

A 95/46/EK irányelv és a 45/2001 rendelet más eszközökkel együtt értelmezendő. Más szóval, az irányelv és a rendelet, amennyiben a személyes adatoknak az alapvető szabadságok, különösen a magánélet tiszteletben tartásához való jog megsértésével fenyegető feldolgozásával foglalkozik, az alapvető jogokra figyelemmel értelmezendő. Ez az Európai Közösségek Bíróságának esetjogából is következik ([1]).

– Végezetül az európai adatvédelmi biztos elemzésébe belefoglalja a 29. cikkel létrehozott adatvédelmi munkacsoport ([2]) 2004. augusztus 11-i 7/2004. sz. véleményét „a biometrikus elemeknek a tartózkodási engedélyekbe és vízumokba való, az európai vízuminformációs rendszer (VIS) létrehozására figyelemmel történő bevezetéséről". Ebben a véleményben a munkacsoport a javaslat bizonyos elemeivel kapcsolatban aggodalmát fejezte ki. Az európai adatvédelmi biztos meg kívánja vizsgálni, hogy a javaslat figyelembe vette-e ezeket az aggályokat, és ha igen, hogyan.

3. **A JAVASLAT ELEMZÉSE**

3.1. **Általános szempontok**

Az európai adatvédelmi biztos elismeri, hogy a közös vízumpolitika továbbfejlesztéséhez szükség van a megfelelő adatok hatékony cseréjére. A zavartalan információáramlást biztosítani képes mechanizmusok egyike a VIS. Egy ilyen új eszköznek azonban az adatgyűjtésre és -cserére kell korlátozódnia, amennyiben ez a gyűjtés vagy csere szükséges a közös vízumpolitika fejlesztéséhez, és arányos ezzel a céllal.

Bár a VIS létrehozása pozitív következményekkel járhat más jogos közérdekek tekintetében, ez nem változtatja meg a VIS célját. A rendszer körülhatárolt célja jelentős szerepet játszik a rendszer jogszerű tartalma és használata meghatározásában, és így a tagállami hatóságok számára a VIS-hez (vagy adatai egy részéhez) való hozzáférési jog – jogos közérdekből való – biztosításában is,

Továbbá a javaslat bevezeti a biometria VIS-ben való használatát. Az európai adatvédelmi biztos elismeri a biometria használatának előnyeit, hangsúlyozza azonban az ilyen adatok használatának jelentős hatását, és a biometrikus adatok használatára vonatkozóan szigorú biztosítékok bevezetését javasolja.

Ezt a véleményt e főbb megfontolásokat tekintetbe véve kell értelmezni. Megjegyzendő, hogy ezt a véleményt a rendelet preambulumában meg kell említeni, a preambulumbekezdések előtt („tekintettel a … véleményére …")

([1]) Ezzel összefüggésben érdemes a Bíróság „Österreicher Rundfunk és mások" (a C-465/00., C-138/01. és C-139/01. egyesített ügyek, 2003. május 20-i ítélet, teljes kamara, (2003) ECR I-4989) ügyben hozott ítéletére hivatkozni. A Bíróság egy olyan osztrák törvényt vizsgált, amely előírta a közszférában dolgozók fizetésével kapcsolatos adatoknak az Osztrák Számvevőszék számára történő átadását, és ezen adatok ezt követően történő közzétételét. A Bíróság ítéletében számos, az Emberi Jogok Európai Egyezményének 8. cikkéből átvett kritériumot határoz meg, amelyeket a 95/46/EK irányelv alkalmazása során alkalmazni kell, amennyiben az irányelv a magánélethez való jog bizonyos korlátozását engedélyezi.

([2]) Ez egy független tanácsadó csoport, amely a tagállamok adatvédelmi hatóságainak, az európai adatvédelmi biztosnak és a Bizottságnak a képviselőiből áll, és a 95/46/EK irányelv hozta létre.

3.2. **Célkitűzés**

A VIS célja kulcsfontosságú, mind az emberi jogok európai egyezményének 8. cikke, mind az általános adatvédelmi jogi keret fényében. A 95/46/EK irányelv 6. cikke szerint a személyes adatok „gyűjtése csak meghatározott, egyértelmű és törvényes célból történhet, és további feldolgozása nem végezhető e célokkal összeférhetetlen módon." Csak a célok egyértelmű meghatározásával lehet a személyes adatok feldolgozásának arányosságát és adekvátságát helyesen értékelni, ami – tekintve az adatok (beleértve a biometrikus adatokat is) jellegét és a tervezett feldolgozási művelet nagyságrendjét – kulcsfontosságú.

A VIS célját a javaslat 1. cikkének (2) bekezdése egyértelműen meghatározza:

„A kérelmek és az arra vonatkozó határozatok adatai tagállamok közötti cseréjének megkönnyítésével a VIS elősegíti a közös vízumpolitika ügyvitelét, a konzuli együttműködést és a központi konzuli hatóságok közötti konzultációt."

Tehát e szakpolitikai célkitűzésnek a közös vízumpolitika érdekében történő elérése végett a VIS valamennyi elemének szükséges és arányos eszköznek kell lennie.

Az 1. cikk (2) bekezdése a vízumpolitika javításának további előnyeit is felsorolja, például:

a) a belső biztonságot fenyegető veszélyek megelőzése,

c) a csalás elleni küzdelem megkönnyítése,

d) a külső határellenőrző pontokon végzett ellenőrzések megkönnyítése.

Az európai adatvédelmi biztos szerint ezek az elemek a VIS felállításának és a közös vízumpolitika javításának pozitív következményei, azonban nem önálló célok.

Ez ebben a szakaszban két főbb következménnyel jár:

– Az európai adatvédelmi biztos tudatában van annak, hogy a bűnüldöző szervek érdeklődnek a VIS-hez való hozzáférés számukra történő biztosítása iránt; 2005. március 7-én ilyen értelmű tanácsi következtetések elfogadására került sor. Mivel a VIS célja a közös vízumpolitika javítása, meg kell jegyezni, hogy a bűnüldöző szervek általi rutinszerű hozzáférés nem lenne összhangban e céllal. Míg a 95/46/EK irányelv 13. cikke szerint ilyen hozzáférés eseti alapon, meghatározott körülmények között és megfelelő jogi biztosítékok mellett biztosítható, szisztematikus hozzáférés nem engedélyezhető.

  Általánosabban fogalmazva, az arányosság és szükségesség értékelése kulcsfontosságú, ha a jövőben arra vonatkozóan hoznak döntést, hogy bizonyos hatóságok hozzáférhessenek-e a VIS-hez. Azoknak a feladatoknak, amelyek elvégzéséhez a hozzáférést biztosították, összhangban kell lenniük a VIS céljaival.

– Az „egyes tagállamok belső biztonságát fenyegető veszélyek" megakadályozásának az a) pontban való kifejezett említése nem szerencsés. A VIS által jelentett legfőbb előny a csalás és a vízumkereskedelem megakadályozása (a biometrikus adatok rendszerbe való bevezetésének fő célja szintén a csalás elleni küzdelem) ([1]) A biztonság elleni fenyegetések megakadályozását ezért „másodlagos", noha nagyon is kívánatos előnynek kell tekinteni.

  Az európai adatvédelmi biztos azt javasolja, hogy az 1. cikk (2) bekezdésében a „cél" és az „előny" e megkülönböztetését határozottabbá kell tenni, például a következőképpen:

  „A VIS célja, hogy a kérelmek és az arra vonatkozó határozatok adatai tagállamok közötti cseréjének megkönnyítésével elősegítse a közös vízumpolitika ügyvitelét, a konzuli együttműködést és a központi konzuli hatóságok közötti konzultációt Ennek során ahhoz is hozzájárul, hogy …"

([1]) A kiterjesztett hatásvizsgálat (6. o., §2.7) mindezt egyértelműen leszögezi: *„a vízumkereskedelem és a csalás elleni küzdelem, valamint az ellenőrzések hatékonyságának elégtelensége a tagállamok belső biztonsága tekintetében is a hatékonyság elégtelenségéhez vezet."* Ebből az következik, hogy a biztonságot fenyegető veszélyekért részben a nem eléggé hatékony vízumpolitika okolható. E téren az első feladat a vízumpolitika javítása, főként a csalás elleni küzdelem és jobb ellenőrzések révén. A biztonság javulását a vízumpolitika javulása fogja eredményezni.

E tekintetben azt is érdemes megjegyezni, hogy „A vízumadatok cseréje közös rendszerének bevezetésére vonatkozó iránymutatás", amelyet az IB-Tanács 2002. június 13-án fogadott el [1], a belső biztonságot fenyegető veszélyek megakadályozását a felsorolás végére helyezte. Ennél a javaslatnál is lehetne így eljárni, és ez sokkal inkább összhangban lenne a VIS céljával.

3.3. **Adatminőség**

A 95/46/EK irányelv 6. cikke alapján a személyes adatok „gyűjtésük és/vagy további feldolgozásuk célja szempontjából megfelelőek, relevánsak és nem túlzott mértékűek". Ez magának a VIS-nek az arányosságára vonatkozik, de egyúttal a VIS-be felveendő és ott tárolandó adatokra, valamint ezek későbbi felhasználására is, továbbá az ezzel összefüggésben alkalmazandó további biztosítékokra. Ezek az elemek az emberi jogok európai egyezményének 8. cikkére figyelemmel alapvetően fontosak a javaslat értékelésében is.

A VIS létrehozása kétségtelenül jelentős beavatkozást jelent a magánélet tiszteletben tartásához való jog gyakorlásába, már csak nagyságrendje és a feldolgozott személyes adatok kategóriái miatt is. Ezért a 29. cikk által létrehozott munkacsoport 7/2004. sz. véleményében azt kívánta megtudni, milyen, az e jelenségek nagyságrendjére és súlyosságára irányuló vizsgálatok tártak fel a közbiztonsággal vagy közrenddel kapcsolatos kényszerítő, e megközelítést igazoló indokokat.

Az európai adatvédelmi biztos a kibővített hatásvizsgálatban megfogalmazott bizonyítékokat gondosan megvizsgálta. Noha ez a bizonyíték nem teljesen döntő, úgy tűnik, a VIS-nek a közös vízumpolitika javítása céljából történő létrehozása kellőképpen indokolt.

Ezzel összefüggésben úgy tűnik, a VIS-nek mint a tagállamok általi vízumkiadás feltételeit javító eszköznek a létrehozására vonatkozó döntés a jogalkotás mérlegelési jogkörébe tartozik. Egy ilyen rendszer önmagában jól illeszkedik az EK-Szerződésben tervbe vett, a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség fokozatos létrehozásába, és támogatja azt.

Mindazonáltal a VIS létrehozásának és használatának soha nem szabad azzal a hatással járnia, hogy a személyes adatok magas szintű védelmét e területen többé ne lehessen biztosítani. Az európai adatvédelmi biztos feladatai közé tartozik annak vizsgálata, milyen mértékben fogja a VIS befolyásolni az érintett személyek adatvédelmének jelenlegi szintjét.

Ezek alapján az európai adatvédelmi biztos véleményében az alábbi kérdésekre összpontosít:

– az adatok, valamint felhasználásuk arányossága és adekvátsága (például adatkategóriák, hozzáférés az adatokhoz minden egyes érintett hatóság számára, tárolási időszak);

– a rendszer működése (felelősségi körök, biztonság);

– az érintettek jogai (például tájékoztatás, a pontatlan vagy nem releváns adatok helyesbítése vagy törlése);

– a rendszer ellenőrzése és felügyelete.

Az alábbi bekezdésektől eltekintve a javaslathoz a VIS-be beviendő adatok kategóriái és használatuk tekintetében nem volt szükséges jelentősebb megjegyzést fűzni. A vonatkozó rendelkezéseket kellő gondossággal szövegezték meg, és teljes egészükben következetesnek és adekvátnak tűnnek.

[1] „A terrorizmus elleni közdelemről szóló, 2002. június 13-i 2002/475/IB tanácsi kerethatározat", HL L 164., 2002.6.22., 3. o.

3.4. **Biometria**

3.4.1. *A biometria használatának hatása*

A biometria információs rendszerekben való használatához folyamodás soha nem jelentéktelen lépés, különösen ha a szóban forgó rendszer ilyen nagyszámú személyt érint. A biometria nem csupán egy újabb információs technológia. A test és az identitás közötti kapcsolatot visszafordíthatatlanul megváltoztatja annyiban, hogy az emberi test jellemzõit „géppel olvashatóvá" és további felhasználás tárgyává teszi. Ha a biometrikus jellemzõket az emberi szem nem is tudja leolvasni, megfelelõ eszközökkel leolvashatók és felhasználhatók, örökre, bárhová megy is az illetõ.

Bármilyen hasznos is a biometria bizonyos célokra, elterjedt használata jelentõs hatással lesz a társadalomra, és széleskörû, nyílt vita tárgyát kell képeznie. Az európai adatvédelmi biztosnak meg kell állapítania, hogy ilyen vitára a javaslat kialakítását megelõzõen nemigen került sor. Ez még inkább kiemeli annak jelentõségét, hogy a biometrikus adatok használatára vonatkozóan szigorú biztosítékokra van szükség, a jogalkotási folyamat során pedig alapos mérlegelésre és vitára kell sort keríteni.

3.4.2. *A biometrikus jellemzõk specifikus jellege*

Amint azt a 29. cikk által létrehozott munkacsoport néhány véleményében ([1]) már hangsúlyozta, a biometrikus adatok személyazonossági dokumentumok esetében való bevezetése és feldolgozása különösen következetes és szigorú biztosítékokat követel. A biometrikus adatok ugyanis bizonyos különleges jellemzőiknek köszönhetően rendkívül érzékenyek.

Kétségtelen, hogy – ellentétben a jelszavakkal és a kulcsokkal – a biometrikus adatok elvesztése az érintett személy számára szinte lehetetlen. A biometrikus adatok *kvázi abszolút megkülönböztető jelleggel* bírnak, azaz minden ember egyedi biometrikus adatokkal rendelkezik. Az ember élete során szinte soha nem változnak, ami *állandó jelleget* kölcsönöz ezeknek az adatoknak. Továbbá mindenki ugyanazokkal a fizikai „elemekkel" rendelkezik, ennek köszönhetően a biometrikus adatok *univerzális* természetűek.

Azonban a biometrikus adatok visszavonása szinte lehetetlen: az ujjat vagy az arcot nehéz megváltoztatni. Ez a sok szempontból előnyös tulajdonság jelentős hátránnyá válik a sz*emélyazonosság-lopás* esetében: ha egy adatbázisban az ujjlenyomatokhoz és a fényképhez lopott személyazonosság kapcsolódik, ez a személyazonosság valódi birtokosa számára súlyos és állandó problémákat okozhat. Mi több, a biometrikus adatok természetüknél fogva *nem titkosak*, és olyan *nyomokat* is *hagyhatnak* (ujjlenyomatok, DNS), amelyek lehetővé teszik ezen *adatok tulajdonosuk tudta nélküli* összegyűjtését.

Ezen, a biometria természetéből adódó kockázatok miatt komoly biztosítékok alkalmazása szükséges (különösen a cél körülhatárolása elvének tiszteletben tartása, a hozzáférés korlátozása és a biztonsági intézkedések tekintetében.)

3.4.3. *Az ujjlenyomatok technikai tökéletlensége*

A biometria fentebb jellemzett legfőbb előnyei (az adatok univerzális és megkülönböztető volta, állandóság, használhatóság stb.) soha nem abszolútak. Ennek közvetlen hatása van a rendeletben tervezett biometrikus nyilvántartásba vételi és igazolási folyamatok hatékonyságára.

Becslések szerint ([2]) az emberek maximum 5 %-át nem lehet nyilvántartásba venni (mivel ujjlenyomatuk nem leolvasható, vagy egyáltalán nem létezik.) A javaslathoz csatolt kibővített hatásvizsgálat előrejelzései szerint 2007-ben a vízumkérelmezők száma körülbelül 20 millió lesz, azaz akár 1 millió is lehet azok száma, akik a „normális" nyilvántartásba vételi folyamatban nem tudnak részt venni, ami a vízumkérelem és a határon történő ellenőrzés tekintetében nyilvánvalóan következményekkel jár majd.

([1]) A biometrikus elemeknek a tartózkodási engedélyekbe és vízumokba való, az európai vízuminformációs rendszer (VIS) létrehozására figyelemmel történő bevezetéséről szóló 7/2004. sz. vélemény (Markt/11487/04/EN - WP 96), valamint a biometriáról szóló munkadokumentum (MARKT/10595/03/EN - WP 80).

([2]) A. Sasse, *Cybertrust and Crime Prevention: Usability and Trust in Information Systems*, in:„Foresight cybertrust and crime prevention project". 04/1151, 2004. június 10., 7. o., valamint Technology Assessment, „Using Biometrics for Border Security", United States General Accounting Office, GAO-03-174, 2002. november.

A biometrikus azonosítás lényegénél fogva statisztikai folyamat. 0,5–1 %-os hibaarány tekinthető normálisnak ([1]), ami azt jelenti, hogy a külső határokon való ellenőrzési rendszer 0,5–1 %-os téves elutasítási aránnyal (FRR) működik. Ezt az arányt az illetékes hatóság kockázatvállalási politikáján alapuló küszöbérték révén állítják be (a tévesen elutasított és a tévesen elfogadott személyek közötti egyensúlynak felel meg.) Túlzás tehát úgy vélekedni, hogy ezek a technológiák biztosítják az adatalany „pontos azonosítását", ahogyan azt a rendeletjavaslat 9. preambulumbekezdése megállapítja.

Egy nemrégiben megjelent, az Európai Parlament Polgári Szabadságjogi, Bel- és Igazságügyi Bizottsága megbízásából készített előretekintő tanulmány ([2]) szerint a biometrikus nyilvántartás bevezetésének alapvető biztosítékaként rendelkezésre kell állniuk *tartalékeljárásoknak*, mivel a biometrikus nyilvántartásba vétel nem mindenki számára hozzáférhető, és nem teljesen pontos. Ezeket az eljárásokat azért kell végrehajtani és használni, hogy azon személyek méltóságát, akiknek az esetében a nyilvántartásba vételi folyamat sikertelen volt, tiszteletben tartsák, valamint annak elkerülése érdekében, hogy a rendszer tökéletlenségének terhét ők viseljék ([3])

Az európai adatvédelmi biztos ezért tartalékeljárások kidolgozását és a javaslatba való beillesztését javasolja. Ezek az eljárások nem csökkenthetik a vízumpolitika biztonsági szintjét, és nem bélyegezhetik meg azokat a személyeket, akiknek az ujjlenyomata nem olvasható le.

3.5. **Különleges adatkategóriák**

Bizonyos adatkategóriák esetében (a biometrikus adatokon túlmenően) különleges mérlegelésre van szükség: a vízumelutasítási indokokra vonatkozó adatok (3.5.1) és a csoport más tagjaira vonatkozó adatok (3.5.2).

3.5.1. *A vízum elutasításának indokai*

A javaslat 10. cikkének (2) bekezdése előírja az elutasítás indokaira vonatkozó adatok feldolgozását, amennyiben a vízum elutasítására vonatkozó döntés született. Ezek az elutasítási indokok teljes mértékben szabványosítottak.

– Az a) és b) albekezdésben szereplő első két indok inkább adminisztratív természetű: érvényes úti okmány vagy a kívánt tartózkodás célját és feltételeit igazoló érvényes dokumentumok benyújtásának elmulasztása.

– A c) albekezdés említi a „figyelmeztető jelzést a kérelmezőről annak belépése megtagadása céljából", ami feltételezi a SIS-adatbázisba való betekintést.

– Végül a d) albekezdés a vízum elutasításnak okaként említi azt, ha a kérelmező „fenyegeti a tagállamok valamelyikének közrendjét, belső biztonságát, közegészségügyét vagy nemzetközi kapcsolatait".

([1])

Biometrikus adatok	Arc	Ujj	Szivárványhártya
FTE % Meghiúsult nyilvántartásba vétel	n/a	4	7
FNMR % elutasítási arányok	4	2.5	6
FMR 1 % megerősítési egyezés hibaaránya	10	< 0.01	< 0.001
FMR2 % azonosítási hibaarányok, ha az adatbázis mérete > 1 m	40	0.1	N/A
FMR3 % szűrési egyezés hibaaránya, ha az adatbázis mérete = 500	12	< 1	N/A

A. K. Jain et al., *Biometrics: A grand Challenge*, Proceedings of International Conference on Pattern Recognition, Cambridge, UK., 2004. augusztus

([2]) *Biometrics at the frontiers: assessing the impact on Society*, 2005. február, Előretekintő Technológiai Tanulmányok Központja, Közös Kutatási Központ Főigazgatóság, EK.

([3]) *Időközi jelentés az Egyezmény 108. cikke elveinek a biometrikus adatok gyűjtésére és feldolgozására való alkalmazásáról*, Európa Tanács, 2005., 11. o.

Valamennyi elutasítási indokot nagy körültekintéssel kell alkalmazni azon következmények miatt, amelyekkel az egyén számára járnak. Továbbá néhányuk, a c) és d) albekezdésben említettek, a 95/46/EK irányelv 8. cikke szerinti „szenzitív adatok" feldolgozásához vezet.

Az európai adatvédelmi biztos kifejezetten felhívja a figyelmet a közegészségüggyel kapcsolatos feltételre, amelynek homályos a megfogalmazása, és nagyon szenzitív adatok feldolgozásával jár. A javaslathoz mellékelt, a cikkekkel kapcsolatos kommentárok szerint a közegészség veszélyeztetésére való hivatkozás a személyek határátlépésére irányadó szabályok Közösségi Kódexének létrehozásáról szóló tanácsi rendeletre vonatkozó javaslaton (COM (2004)391 végleges) alapul.

Az európai adatvédelmi biztos tudomással bír arról, hogy a közegészségügyi kritérium a személyek szabad mozgására vonatkozó közösségi jogszabályokban széles körben használatos és azt szigorúan alkalmazzák, amint azt az Unió polgárainak és családtagjaiknak a tagállamok területén történő szabad mozgáshoz és tartózkodáshoz való jogáról szóló, 2004. április 29-i 2004/38/EK európai parlamenti és tanácsi irányelv is mutatja. Az irányelv 29. cikke meghatározza a közegészségre jelentett veszély figyelembe vételének feltételeit: „A mozgás szabadságát korlátozó intézkedéseket egyedül olyan, esetlegesen járványt okozó betegségek indokolják, amelyeket az Egészségügyi Világszervezet megfelelő jogi eszközei határoznak meg, valamint más fertőző betegségek vagy ragályos parazitás megbetegedések, ha a fogadó tagállam állampolgáraira vonatkozó védelmi rendelkezések hatálya alá tartoznak."

– Meg kell jegyezni azonban, hogy a korábban említett javaslat jelenleg még csak javaslat, és a közegészség nem veszélyeztetése feltételének beillesztése a VIS-rendeletbe a Közösségi Kódex elfogadásától függ.

– Továbbá ha elfogadják, a beutazás elutasításának ezt az indokát korlátozóan kell értelmezni. Valójában a Közösségi Kódexre vonatkozó javaslat pedig az előbb említett 2004/38/EK irányelven alapul.

Az európai adatvédelmi biztos ezért azt ajánlja, hogy a javaslat szövegében meg kell említeni a 2004/38/EK irányelv 29. cikkét, hogy a „közegészség veszélyeztetését" e rendelkezés alapján értelmezzék. Az adatok bármely esetben, figyelembe véve szenzitivitásukat, csak akkor dolgozhatók fel, ha a közegészségre jelentett veszély valós, fennálló és kellően súlyos.

3.5.2. *Valamely csoport többi tagjára vonatkozó adatok*

A 2. cikk (7) bekezdésének meghatározása szerint a „csoporttagok" „azokat a kérelmezőket jelenti, akikkel a kérelmező együtt utazik, beleértve a kérelmezőt elkísérő házastársát és gyermekeit". A cikkekkel kapcsolatos kommentárok megemlítik, hogy a javaslat 2. cikkében szereplő meghatározások a Szerződés vagy a schengeni vívmányok vízumpolitikára vonatkozó rendelkezéseire vonatkoznak, néhány kifejezés – például a „csoporttagok" – kivételével, amelyeket kifejezetten e rendelet céljára határoztak meg. Feltételezhető ezért, hogy e meghatározás nem vonatkozik a „csoportos vízumnak" a Közös Konzuli Utasítások 2.1.4. cikkében szereplő meghatározására. A cikkekkel kapcsolatos kommentárok említik azon „kérelmezőket, akik más kérelmezőkkel egy csoportban utaznak", például jóváhagyott célország státusára vonatkozó (ADS) megállapodás keretén belül, vagy családtagokkal együtt.

Az európai adatvédelmi biztos hangsúlyozza, hogy a rendeletben pontos és kimerítő meghatározást kell adni a „csoporttagok" kifejezésre vonatkozóan. A jelenlegi javaslatra vonatkozóan a Szerződésre vagy a schengeni vívmányokra való pontos hivatkozás hiánya miatt az európai adatvédelmi biztosnak meg kell állapítania, hogy a meghatározás túl homályos. E megfogalmazás szerint a „csoporttagok" kifejezés magában foglalhatja a munkatársakat, ugyanazon utazási iroda más, szervezett társasutazásban részt vevő ügyfeleit, stb. A következmények pedig nagyon jelentősek:

a rendelettervezet 5. cikke szerint a kérelmező kérelemfájlját a többi csoporttag kérelemfájljaihoz csatolják.

3.6. **Az adatok tárolása**

A rendelettervezet 20. cikke előírja, hogy minden kérelemfájlt öt évig kell tárolni. A közösségi szabályozásban szakpolitikai döntésen múlik az ésszerű időtartam meghatározása.

Nincs bizonyíték annak feltételezésére – különösen a cikkekkel kapcsolatos kommentárokban említett indokok fényében –, hogy a javaslatban hozott szakpolitikai döntés nem ésszerű, vagy annak elfogadhatatlan következményei lennének, feltéve, hogy valamennyi megfelelő helyesbítési mechanizmust beindítják. Ez azt jelenti, hogy biztosítani kell az adatok helyesbítését vagy törlését, amennyiben azok már nem pontosak, és különösen akkor, ha egy személy megszerezte valamely tagállam állampolgárságát, vagy olyan státust szerzett, amely nem követeli meg bevitelét a rendszerbe.

Továbbá, ha az adatok továbbra is szerepelnek a rendszerben, semmilyen módon nem érinthetik egy új döntés meghozatalát. Az elutasítás bizonyos okai (különösen a beléptetési tilalmat elrendelő figyelmeztető jelzés hatálya alatt álló személy, a közegészségre nézve fennálló veszély) időben korlátozott érvényességűek. Az a tény, hogy ezek az okok egy adott pillanatban érvényes indokai voltak a belépés elutasításának, nem befolyásolhatja egy új döntés meghozatalát. Valamennyi új vízumkérelem esetén teljes egészében újra kell értékelni a helyzetet, és ezt a rendeletben a megfelelő helyeken egyértelművé kell tenni.

3.7. **Az adatokhoz való hozzáférés és adathasználat**

3.7.1. *Elõzetes észrevételek*

Előzetes megjegyzésként az európai adatvédelmi biztos elismeri, milyen körültekintően jártak el a VIS-adatokhoz való hozzáférést és az ilyen adatok felhasználását szabályozó rendszer kialakításakor. Valamennyi hatóság különböző adatokhoz különböző okokból rendelkezik hozzáféréssel. Ez egy olyan megfelelő megközelítés, amelyet az európai adatvédelmi biztos csak támogatni tud. A következő észrevételek e megközelítés lehető legszélesebb körű alkalmazását célozzák.

3.7.2. *A külsõ határellenõrzõ pontokon és a tagállamok területén belüli vízumellenõrzések*

A vízumok külső határokon történő ellenőrzése esetére a javasolt rendelet 16. cikke világosan meghatározza a két pontos célt:

– „a személy személyazonosságának ellenőrzése”, ami a megadott meghatározás szerint egyénenkénti összehasonlítást jelent;

– „a vízum eredetiségének ellenőrzése”. Az ICAO-szabványokban javasoltak szerint a vízum mikrochipje nyilvános/titkos kulcsú rendszert (PKI) használhatna az eredetiségvizsgálati folyamat során.

A vízumok ellenőrzéséhez ez a két cél megfelelőképpen elérhető az illetékes hatóságoknak kizárólag a védett mikrochipekhez való hozzáférésével. A VIS központi adatbázishoz való hozzáférés ezért e konkrét esetben nem lenne arányos. Ez utóbbi lehetőség azt vonná maga után, hogy több hatóság kapcsolódna a VIS-hez, ami növelheti a visszaélések kockázatát. Ez egyúttal drágább megoldás is lenne, tekintve, hogy a VIS-hez való biztonságos és ellenőrzött hozzáférések száma, illetve a hozzáféréssel kapcsolatos külön képzések szükségessége szintén jelentősen megnövekedne.

Kétségek állnak fenn továbbá az adatokhoz való hozzáférés adekvátságát illetően, ami a 16. cikk második pontját illeti. A (2) bekezdés a) pontja ugyanis kimondja, hogy amennyiben egy első keresést követően úgy találják, hogy a kérelmező adatai szerepelnek a VIS-ben (elvileg ez lenne mindig az eset), az illetékes hatóság – továbbra is a személyazonosság ellenőrzéséhez – további adatokat is megtekinthet. Ezek az adatok valamennyi, a kérelemmel kapcsolatos információt tartalmazzák, fényképeket, ujjlenyomatokat, illetve bármely korábban kiadott, törölt, visszavont vagy meghosszabbított vízumot.

Amennyiben a személyazonosság ellenőrzése sikeres volt, egyáltalán nem világos, miért szükségesek ezek a további adatok. Ezekhez valójában kizárólag akkor lehetne korlátozott feltételek mellett hozzáférni, ha az ellenőrzési eljárás sikertelen volt. Ebben az esetben a 16. cikk (2) bekezdésében említett adatok megfelelő segítséget nyújtanának az adott személy személyazonosságának megállapítását elősegítő tartalékeljáráshoz. Ebben az esetben ezekhez az adatokhoz nem kellene hozzáférést biztosítani a határállomás valamennyi alkalmazottjának, kizárólag korlátozottan azoknak a tisztviselőknek, akik a nehéz eseteket vizsgálják.

Végezetül, a hozzáféréssel rendelkező hatóságok meghatározásának pontosabbnak kellene lennie. Különösen az nem világos, hogy mit jelent „a tagállamok területén belüli ellenőrzéseket" folyatató illetékes hatóságok. Az adatvédelmi biztos feltételezi, hogy ez a tagállamok területén belüli *vízum*ellenőrzéseket jelenti, így a 16. cikket ennek megfelelően kellene módosítani.

3.7.3. *Adathasználat az illegális bevándorlók azonosításához és kitoloncolásához, illetve a menekültügyi eljáráshoz*

A 17., 18. és 19. cikkben meghatározott esetekben (illegális bevándorlók kitoloncolása, menekültügyi eljárás) a VIS-t a személyazonosításhoz használják. A személyazonosításhoz használt adatok közé tartoznak a fényképek. Ugyanakkor az ilyen összetett IT-rendszerekhez használt, az automatikus arcfelismeréssel kapcsolatos technológia jelenlegi állása szerint a fényképek nem használhatók személyazonosításra (egy és több összehasonlítása); ugyanis nem szolgálnak megbízható eredménnyel. Ezért ezek nem tekinthetők a személyazonosítás céljából megfelelő adatoknak.

Következésképpen az adatvédelmi biztos nyomatékosan javasolja, hogy „a fényképeket" töröljék e cikkek első feléből, és azokat a cikkek második felében említsék csak meg (a fényképeket lehet a személyazonosság ellenőrzési eszközeként használni, de nem használhatók az összetett adatbázisokban való azonosításra).

Egy másik lehetőség a 36. cikk módosítása lenne abban az értelemben, hogy csak abban az esetben lehetne bevezetni a személyazonosításhoz használt fénykép-feldolgozási funkciókat, ha e technológiát megbízhatónak minősítik (lehetőség szerint a technikai bizottság véleményét követően).

3.7.4. *A hozzáféréssel rendelkezõ hatóságok közzététele*

A rendelettervezet 4. cikke rendelkezik azoknak az illetékes hatóságoknak az Európai Unió Hivatalos Lapjában való közzétételéről, amelyeket az egyes tagállamokban a VIS-hez való hozzáférésre kijelöltek. Erre a közzétételre rendszeresen (évente) sort kellene keríteni, a nemzeti helyzetben beállt változásokról való tájékoztatás miatt. Az európai adatvédelmi biztos hangsúlyozza e közzététel fontosságát, mivel az nélkülözhetetlen ellenőrzési eszköz európai, nemzeti és helyi szinten is.

3.8. **Felelősségek**

Emlékeztetőül: a VIS centralizált architektúrán alapul, egy olyan központi adatbázissal, ahol a vízumokkal kapcsolatos valamennyi információt tárolják, valamint a tagállamokban található nemzeti interfészekkel, amelyek lehetővé teszik a tagállamok illetékes hatóságai számára a központi rendszerhez való hozzáférést. A (14) és (15) preambulumbekezdésnek megfelelően a rendelet alkalmazásakor a 95/46/EK irányelvet kell alkalmazni a személyes adatok tagállamok általi feldolgozására, és a 45/2001/EK rendeletet kell alkalmazni a Bizottságnak a személyes adatok védelmével kapcsolatos intézkedéseire. Ahogy azt a preambulumbekezdések ezzel kapcsolatban említik, a javaslat tisztázni kíván egyes pontokat, többek között ami az adatfelhasználással kapcsolatos felelősséget és az adatvédelem ellenőrzését illeti.

Úgy tűnik, hogy ezek a pontok néhány kulcsfontosságú részletre vonatkoznak, amelyek nélkül a 95/46/EK irányelv és a 45/2001 rendelet biztosítéki rendszere nem lenne alkalmazható, vagy nem lenne teljes mértékben koherens a javaslattal. Az irányelv értelmében a nemzeti jog alkalmazhatósága alapjában feltételezi, hogy létezik az adott tagállamban egy adatkezelő (4. cikk), míg a rendelet alkalmazhatósága a személyes adatoknak valamely közösségi intézmény vagy szerv által történő feldolgozásától függ az olyan tevékenységek gyakorlása során, amelyek részben vagy teljes egészében a közösségi jog hatálya alá tartoznak (3. cikk).

A rendelettervezet 23. cikke (2) bekezdésének megfelelően az adatokat „a tagállamok nevében a VIS-ben kell feldolgozni". A 23. cikk (3) bekezdése szerint a tagállamok kijelölik azt a hatóságot, amely a 95/46/EK irányelv 2. cikkének d) pontjával összhangban az adatrögzítésért felelős. Úgy tűnik, ez azt feltételezi, hogy az irányelv rendszere szerint a Bizottság adatfeldolgozónak tekintendő. A cikkek magyarázataiban ezt megerősítik. ([1])

Ez a megfogalmazás kevesebbnek tünteti fel a Bizottságnak a rendszer fejlesztési fázisában és normál működése során játszott nagyon fontos, sőt, kulcsfontosságú szerepét. Nehéz a Bizottság szerepét az adatkezelő vagy adatfeldolgozó koncepciójához kötni; vagy szokatlan hatáskörrel rendelkező (többek között a rendszer kijelöléséért felelős) feldolgozó, vagy korlátok között működő adatkezelő (mivel az adatokat a tagállamok viszik be és használják). A Bizottságnak valóban *sui generis*-ként elismerendő szerepe ([2]) van a VIS-ben.

Ezt a jelentős szerepet a Bizottság feladatainak részletes leírása révén kellene elismerni az olyan megfogalmazás helyett, amely nem egészen felel meg a valóságnak, mivel túlságosan korlátozó, nem változtat a VIS működésén, és csak félreértésekhez vezet. Ez a VIS következetes és hatékony ellenőrzésének céljából is fontos (lásd a 3.11. bekezdést). Ezért az adatvédelmi biztos a 23. cikk (2) bekezdésének elhagyását javasolja.

Az európai adatvédelmi biztos hangsúlyozni kívánja, hogy a Bizottság VIS-t érintő feladatainak teljes körű leírása annál inkább fontos, ha a Bizottság az irányítási feladatokat egy másik szervre kívánja bízni. A javaslathoz csatolt „Fiche Financière" megemlíti annak lehetőségét, hogy ezeket a feladatokat a külső határokért felelős ügynökségre ruháznák. Ezzel kapcsolatban rendkívül fontos, hogy a Bizottság ne hagyjon kétségeket hatáskörei terjedelmére vonatkozóan annak érdekében, hogy az utódja tisztában legyen azokkal a határokkal, amelyek között tevékenységét folytathatja.

3.9. **Biztonság**

A VIS-t érintő optimális biztonsági szint kezelése és tiszteletben tartása előfeltétel az adatbázisban tárolt személyes adatok megkövetelt védelmének biztosításához. A védelem kielégítő szintjének eléréséhez megfelelő biztosítékokat kell bevezetni a rendszer infrastruktúrájával és a bevont személyekkel kapcsolatos lehetséges kockázatok kezelésére. Erre a javaslat több része kitér, és e kérdésben még némi javítás szükséges.

A javaslat 25. és 26. cikke különböző intézkedéseket tartalmaz az adatbiztonságra vonatkozóan, és meghatározza azokat a fajta visszaéléseket, amelyeket meg kell előzni. Ugyanakkor ezeket a rendelkezéseket hasznos lenne olyan intézkedésekkel kiegészíteni, amelyek a már említett biztonsági intézkedések szisztematikus ellenőrzésére és a hatékonyságáról szóló jelentésre vonatkoznak. Az adatvédelmi biztos konkrétan azt javasolja, hogy a biztonsági intézkedések szisztematikus (ön)ellenőrzésére vonatkozó rendelkezésekkel egészítsék ki ezeket a cikkeket.

Ez a javaslat 40. cikkével áll kapcsolatban, amely az ellenőrzésről és az értékelésről rendelkezik. Ezeknek nemcsak a kibocsátásra, a költséghatékonyságra és a szolgáltatás minőségére kellene kiterjedniük, hanem a jogi követelményeknek való megfelelésre is, különösen az adatvédelem területén. Ezért az európai adatvédelmi biztos azt javasolja, hogy a 40. cikk alkalmazási körét terjesszék ki az adatfeldolgozás jogszerűségének ellenőrzésére és az ezzel kapcsolatos jelentésre is.

Továbbá, az adatokhoz való hozzáféréssel meghatalmazott személyekkel kapcsolatos 24. cikk (4) bekezdése c) pontjának és 26. cikk (2) bekezdése e) pontjának kiegészítéseként a javaslatba be kellene illeszteni, hogy a tagállamoknak biztosítani kell a pontos felhasználói profilok rendelkezésre állását (amelyeket ellenőrzés céljából a nemzetközi felügyeleti hatóságok rendelkezésére kell bocsátani). A felhasználói profilokon kívül a tagállamoknak létre kell hozniuk a felhasználók személyazonosságát tartalmazó teljes listát, és ezeket folyamatosan frissíteniük kell. Ugyanez vonatkozik a Bizottságra is: ezért a 25. cikk (2) bekezdésének b) pontját ugyanilyen módon ki kell egészíteni.

([1]) Lásd a javaslat 37. oldalát.

([2]) Igaz, hogy a 95/46/EK irányelvben és a 45/2001 rendeletben az „adatkezelő" meghatározása szintén a különböző felelősségi körökkel rendelkező több adatkezelő lehetőségéről rendelkezik.

Ezeket a biztonsági intézkedéseket ellenőrzési és szervezési biztosítékok egészítik ki. A javaslat 28. cikke felsorolja mindazokat a feltételeket és célokat, amelyek alapján valamennyi adatfeldolgozási műveletről nyilvántartást kell vezetni. Ezeket a nyilvántartásokat nemcsak az adatvédelem ellenőrzésére és az adatbiztonság biztosítására tárolják, hanem a VIS rendszeres önellenőrzésének lebonyolításához is. Ezek az önellenőrzési jelentések elősegítik a felügyeleti hatóságok feladatainak hatékony végrehajtását, amelyek ily módon be tudják azonosítani a leggyengébb pontokat, és saját önellenőrzésük során ezekre tudnak összpontosítani.

3.10. **Az érintett személyek jogai**

3.10.1. *Az érintett személyek tájékoztatása*

Rendkívül fontos az érintett személyek tájékoztatása a tisztességes adatfeldolgozás biztosításához. Ez az egyén jogainak nélkülözhetetlen biztosítéka. A javaslat 30. cikke alapjában véve a 95/46/EK irányelvet követi e tekintetben.

Ezen a rendelkezésen ugyanakkor végre lehetne hajtani néhány módosítást annak érdekében, hogy jobban illeszkedjen a VIS keretébe. Az irányelv valóban rendelkezik egyes információk megadásáról, de adott esetben több információ adását is lehetővé teszi ([1]). Következésképpen a 30. cikket módosítani kell annak érdekében, hogy tartalmazza a következő pontokat:

– Az érintetteket az adataik tárolási idejéről is tájékoztatni kell.

– A 30. cikk (1) bekezdésének e) pontja az adatokhoz való hozzáférés és az adatok helyesbítési jogával kapcsolatos. Helyesebb lenne, ha az adatokhoz való hozzáférés, illetve az adatok helyesbítésére vagy *törlésére* irányuló *kérelem* jogáról lenne szó. Ezzel kapcsolatban tájékoztatni kellene az érintetteket a megfelelő felügyeleti hatóságoktól való tanács- vagy segítségkérés lehetőségéről.

– Végül a 30. cikk (1) bekezdése az adatkezelőnek, vagy ha van ilyen, akkor képviselőjének személyazonosságával kapcsolatos tájékoztatást említi. Mivel az adatkezelő minden esetben az Európai Unió területén letelepedett személy, ezért szükségtelen az utóbbi lehetőség jelzése.

3.10.2. *Betekintési, javítási és törlési jog*

A 31. cikk (1) bekezdésének utolsó mondata szerint „az ilyen, adatba való betekintést csak egy tagállam engedélyezheti." Ez feltételezhetően azt jelenti, hogy a központi egység nem engedélyezheti az adatokba való betekintést (vagy azok közlését), ugyanakkor bármely tagállam ezt megteheti. Az európai adatvédelmi biztos javaslata szerint egyértelművé kell tenni, hogy az ilyen jellegű tájékoztatás bármely tagállamban kérhető.

Továbbá e rendelkezés megfogalmazása szerint úgy tűnik, hogy a betekintés nem utasítható vissza, és a felelős tagállam engedélye nélkül lehetséges. Ez megmagyarázná, hogy miért kell a nemzeti illetékes hatóságoknak együttműködni a 31. cikk (2), (3) és (4) bekezdésében meghatározott jogok betartásában, a 31. cikk (1) bekezdésében említettekkel kapcsolatban viszont nem ([2]).

3.10.3. *A felügyeleti hatóságok által nyújtott segítség*

A 33. cikk (2) bekezdése meghatározza, hogy a nemzeti felügyeleti hatóságoknak az érintett személynek nyújtandó segítségnyújtásra és tanácsadásra vonatkozó kötelezettsége fennmarad a bírósági eljárás során is. Nem világos, mit jelent ez a bekezdés. A nemzeti felügyeleti hatóságok különbözőképpen viszonyulnak a bírósági eljárás során betöltendő szerepük kérdéséhez. Úgy tűnik, mintha a panaszos védőjének szerepét töltenék be a bíróságon, ami több államban nem lehetséges.

([1]) Amint említi: „további információk(…), amennyiben e további információk, tekintettel az adatgyűjtés sajátos körülményeire, az érintett vonatkozásában a tisztességes adatfeldolgozás biztosításához szükségesek."

([2]) Következésképpen a nemzeti hatóságok közötti, a javítási vagy törlési jog gyakorlásában való együttműködéssel kapcsolatos 31. cikk (3) bekezdését az egyértelműség kedvéért a következőképpen lehetne módosítani: „ha … *a 31. cikk (2) bekezdésében említett* kérelem". A 31. cikk (1) bekezdésében említett (betekintési) kérelmekre nem vonatkozik a hatóságok közötti együttműködés.

3.11. **Felügyelet**

A javaslat megosztja a felügyeleti feladatot a nemzeti felügyeleti hatóságok és az európai adatvédelmi biztos között. Ez összhangban áll a javaslatnak a VIS működésére és használatára vonatkozó jogot és felelősségeket érintő megközelítésével, valamint a hatékony felügyelet szükségességével. Ezért az európai adatvédelmi biztos üdvözli a 34. és a 35. cikkben foglalt megközelítést.

A nemzeti felügyeleti hatóságok ellenőrzik a személyes adatok tagállamok által történő feldolgozásának jogszerűségét, *beleértve azok VIS-be és VIS-ből történő továbbítását*. Az adatvédelmi biztos ellenőrzi a Bizottság tevékenységeit, *(…) beleértve azt is, hogy a nemzeti interfészek és a központi vízuminformációs rendszer közötti adatátvitel jogszerű*-e. Ez átfedéseket eredményezhet, mivel mind a nemzeti felügyeleti hatóság, mind pedig az adatvédelmi biztos felelős annak ellenőrzéséért, hogy a nemzeti interfészek és a központi vízuminformációs rendszer közötti adatátvitel jogszerű-e.

Ezért az adatvédelmi biztos a 34. cikk módosítását javasolja annak egyértelművé tétele érdekében, hogy a nemzeti felügyeleti hatóságok ellenőrzik a személyes adatok tagállamok által történő feldolgozásának jogszerűségét, beleértve azoknak a VIS nemzeti interfészébe és a VIS nemzeti interfészéből történő továbbítását.

A VIS felügyeletét illetően fontos hangsúlyozni azt is, hogy a nemzeti felügyeleti hatóságok és az európai adatvédelmi biztos tevékenységeit bizonyos mértékig össze kellene hangolni a kellő mértékű koherencia és az általános hatékonyság biztosításához. Valóban szükséges a rendelet harmonizált végrehajtása, illetve a közös problémákkal kapcsolatos közös megközelítés kidolgozása. Ezenkívül ami a biztonságot illeti, megemlíthető, hogy a VIS biztonsági szintjét végül a leggyengébb láncszemének biztonsági szintje határozza meg. E tekintetben is ki kell építeni és meg kell erősíteni az adatvédelmi biztos és a nemzeti hatóságok közötti együttműködést. A 35. cikknek tehát ezért olyan rendelkezést kellene tartalmaznia, hogy az európai adatvédelmi biztos legalább évente egyszer megbeszélést hív össze a nemzeti felügyeleti hatóságokkal.

3.12. **Végrehajtás**

A javaslat 36. cikkének (2) bekezdése előírja: „Az *(1) bekezdésben említett működtetések műszaki bevezetéséhez szükséges intézkedéseket a 39. cikk (2) bekezdésében említett eljárással összhangban kell elfogadni*". A 39. cikk olyan, a Bizottságot segítő bizottságot említ, amelyet 2001 decemberében hoztak létre ([1]), és amelyet több jogi eszközben alkalmaztak.

A VIS működtetések műszaki bevezetésének (az illetékes hatóságokkal való interakciók, egységes vízumformátum) több, az adatvédelem szempontjából esetleg kritikus hatása lehet. Például az a választás, hogy a vízumban lesz-e mikrochip vagy nem – ami a központi adatbázis használatának módjára lesz hatással –, illetve a biometrikus adatok cseréjéhez használt szabványformátum fogja kialakítani vagy vezérelni a kapcsolódó adatvédelmi politikát ([2]).

A technológiák ilyen fajta megválasztása meghatározó hatással lesz majd a cél és arányosság elveinek megfelelő végrehajtására, és ezért ezt felügyelni kell. Ezért az olyan műszaki választásokat, amelyek jelentős hatást gyakorolnak az adatvédelemre, lehetőleg rendeleti úton, az együttdöntési eljárás elvével összhangban kell meghozni. Csak ebben az esetben biztosítható a szükséges politikai ellenőrzés. Valamennyi további, az adatvédelemre hatással bíró esetben lehetőséget kell biztosítani az európai adatvédelmi biztos számára, hogy tanácsot adjon a bizottság általi választásokhoz.

3.13. **Interoperabilitás**

Az interoperabilitás kritikus és rendkívül fontos előfeltétele az olyan összetett IT-rendszerek hatékony működésének, mint a VIS. Az interoperabilitás lehetővé teszi az összköltségek következetes csökkentését, illetve a heterogén elemek természetes redundanciájának elkerülését. Hozzájárulhat a közös vízumpolitika céljához is azáltal, hogy e politika valamennyi alkotóelemére ugyanazt az eljárási szabványt vezeti be. Rendkívül fontos ugyanakkor megkülönböztetni az interoperabilitás két szintjét:

– Az uniós tagállamok közötti interoperabilitás mindenképpen kívánatos; a valamely tagállam hatóságai által küldött vízumkérelmeknek ugyanis interoperábilisnak kell lenniük a bármely más tagállam által küldött kérelmekkel.

([1]) A Tanács 2001. december 6-i 2424/2001 rendelete a Schengeni Információs Rendszer második generációjának (SIS II) kifejlesztéséről.

([2]) Az 1683/95/EK tanácsi rendelet (egységes vízumformátum) módosítására irányuló 2003. szeptemberi javaslat szintén egy hasonló cikket tartalmaz.

– Ennél sokkal inkább megkérdőjelezhető a különböző célokból vagy harmadik országok rendszereivel kiépített rendszerek közötti interoperabilitás.

A rendszer céljainak körülhatárolására és a „funkcióbeli csúszások" megelőzésére használt, rendelkezésre álló biztosítékok között a különböző technológiai szabványok használata hozzájárulhat ehhez az elhatároláshoz. Továbbá a két különböző rendszer közötti interakció bármely formáját szigorúan dokumentálni kellene. Az interoperabilitás nem teremthet olyan helyzetet, amelyben egy hatóság, amely nem jogosult bizonyos adatokhoz való hozzáférésre vagy az adatok használatára, egy másik információs rendszeren keresztül hozzáférést szerezhet.

Ezzel kapcsolatban az európai adatvédelmi biztos utalni szeretne a 2004. március 25-i, a terrorizmus elleni küzdelemről szóló tanácsi nyilatkozatra, amelyben felkérik a Bizottságot, hogy terjesszen elő javaslatokat az információs rendszerek (SIS, VIS és Eurodac) közötti interoperabilitás és szinergiák megerősítésére.

Az európai adatvédelmi biztos szeretné továbbá megemlíteni az azzal kapcsolatban folyamatban lévő tárgyalásokat, hogy mely szervet lehetne megbízni a jövőben a különböző összetett rendszerek irányításával (lásd még e vélemény 3.8. pontját).

Az európai adatvédelmi biztos ismét hangsúlyozni kívánja, hogy a rendszerek interoperabilitása nem hajtható végre a célok körülhatárolása elvének megsértésével, és bármely, erre vonatkozó javaslatot be kell nyújtani az adatvédelmi biztoshoz.

4. KÖVETKEZTETÉSEK

4.1. Általános szempontok

1. Az európai adatvédelmi biztos elismeri, hogy a közös vízumpolitika továbbfejlesztéséhez szükség van a megfelelő adatok hatékony cseréjére. A zavartalan információáramlást biztosítani képes mechanizmusok egyike a VIS. Az európai adatvédelmi biztos a kiterjesztett hatástanulmányban megfogalmazott bizonyítékokat gondosan megvizsgálta. Noha ez a bizonyíték nem teljesen döntő, úgy tűnik, a VIS-nek a közös vízumpolitika javítása céljából történő létrehozása kellőképpen indokolt.

   Ennek az új eszköznek azonban az adatgyűjtésre és -cserére kell korlátozódnia, amennyiben ez a gyűjtés vagy csere szükséges a közös vízumpolitika fejlesztéséhez, és arányos ezzel a céllal.

2. Bár a VIS létrehozása pozitív következményekkel járhat más jogos közérdekek tekintetében, ez nem változtatja meg a VIS célját. Tehát a fent említett szakpolitikai célkitűzés elérése végett a VIS valamennyi elemének szükséges és arányos eszköznek kell lennie. Továbbá:

   – A bűnüldözési hatóságok rutinszerű hozzáférése nem áll összhangban e céllal.

   – Az európai adatvédelmi biztos azt javasolja, hogy az 1. cikk (2) bekezdésében a „cél" és az „előny" e megkülönböztetését határozottabbá kell tenni.

   – A más rendszerekkel való interoperabilitás nem hajtható végre a célok körülhatárolása elvének megsértésével.

3. Az európai adatvédelmi biztos elismeri a biometria használatának előnyeit, hangsúlyozza azonban az ilyen adatok használatának jelentős hatását, és a biometrikus adatok használatára vonatkozóan szigorú biztosítékok bevezetését javasolja. Ezen túlmenően az ujjlenyomatok technikai tökéletlensége tartalékeljárások kidolgozását és a javaslatba való beillesztését követeli meg.

4. Ezt a véleményt a rendelet preambulumában meg kell említeni, a preambulumbekezdések előtt („tekintettel a … véleményére …").

4.2. **Egyéb szempontok**

5. A vízum elutasításának indokaival kapcsolatban: a javaslat szövegében meg kell említeni a 2004/58/EK irányelv 29. cikkét, hogy a „közegészség veszélyeztetését" e rendelkezés alapján értelmezzék.

6. A valamely csoport tagjaival kapcsolatos adatok különleges jelentéssel bírnak a javaslatban: ezért pontos és kimerítő meghatározást kell adni a „csoporttagok" kifejezésre vonatkozóan.

7. Nincs bizonyíték arra, hogy a javaslatban az adatok tárolásával kapcsolatos időtartamra vonatkozóan hozott szakpolitikai döntés nem ésszerű vagy annak elfogadhatatlan következményei lennének, feltéve, hogy valamennyi megfelelő helyesbítési mechanizmust beindítják.

   Továbbá egyértelművé kell tenni a javaslatban, hogy valamennyi új vízumkérelem esetén teljes egészében újra kell értékelni a személyes adatokat.

8. A külső határokon végzett vízumellenőrzésekkel kapcsolatban: módosítani kell a javaslat 16. cikkét, mivel a VIS központi adatbázishoz való hozzáférés ezekben az esetekben nem lenne arányos. Az illetékes hatóságoknak kizárólag a védett microchipekhez való hozzáférése elégséges a vízumok ellenőrzéséhez.

   Továbbá, amennyiben a személyazonosság ellenőrzése sikeres volt, egyáltalán nem világos, miért szükségesek ezek a további adatok.

9. Az illegális bevándorlók azonosításához és kitoloncolásához, illetve a menekültügyi eljáráshoz való adathasználattal kapcsolatban: „a fényképeket" törölni kell e cikkek első feléből, és azokat a cikkek második felében kell csak megemlíteni.

10. A Bizottság és a tagállamok hatáskörét illetően: A 23. cikk (2) bekezdését el kell hagyni.

11. A biztonsági intézkedések szisztematikus (ön)ellenőrzésére vonatkozó rendelkezésekkel kellene kiegészíteni a javaslatot. A 40. cikk alkalmazási körét ki kell terjeszteni az adatfeldolgozás jogszerűségének ellenőrzésére és az ezzel kapcsolatos jelentésre is. Továbbá:

   – a tagállamoknak létre kell hozniuk a felhasználók személyazonosságát tartalmazó teljes listát, és ezeket folyamatosan frissíteniük kell. Ugyanez vonatkozik a Bizottságra is: ezért a 25. cikk (2) bekezdésének b) pontját ugyanilyen módon ki kell egészíteni.

   – A javaslat 28. cikke felsorolja mindazokat a feltételeket és célokat, amelyek alapján valamennyi adatfeldolgozási műveletről nyilvántartást kell vezetni. Ezeket a nyilvántartásokat nemcsak az adatvédelem ellenőrzésére és az adatbiztonság biztosítására kell tárolni, hanem a VIS rendszeres önellenőrzésének lebonyolításához is.

12. Az érintettek jogait illetően:

   – A 30. cikket módosítani kell annak biztosítása érdekében, hogy tájékoztassák az érintetteket adataik tárolási idejéről.

   – A 30. cikk (1) bekezdésének e) pontjának meg kellene említenie az adatok helyesbítésére vagy törlésére irányuló kérelem jogát.

   – A 31. cikk (1) bekezdésében egyértelművé kell tenni, hogy egyes tájékoztatások bármely tagállamban kérhetők.

13. A felügyeletre vonatkozóan:
   – A 34. cikket módosítani kell annak egyértelművé tétele érdekében, hogy a nemzeti felügyeleti hatóságok ellenőrzik a személyes adatok tagállamok által történő feldolgozásának jogszerűségét, beleértve azoknak VIS nemzeti interfészébe és a VIS nemzeti interfészéből történő továbbítását.
   – A 35. cikknek tehát ezért olyan rendelkezést kellene tartalmaznia, hogy az Európai Adatvédelmi Biztos legalább évente egyszer megbeszélést hív össze valamennyi nemzeti felügyeleti hatósággal.
14. A végrehajtásra vonatkozóan:
   – az olyan műszaki választásokat, amelyek jelentős hatást gyakorolnak az adatvédelemre, lehetőleg rendeleti úton, az együttdöntési eljárás elvével összhangban kell meghozni.
   – Más esetekben lehetőséget kell biztosítani az európai adatvédelmi biztos számára, hogy tanácsot adjon a bizottság általi, a rendeletben előirányzott döntésekhez.

Kelt Brüsszelben, 2005. március 23-án.

az Európai Adatvédelmi Biztos

Peter HUSTINX