NAGY KLÁRA

A biometrikus[1] azonosítás új iránya

Napjainkban a személyes adatok védelméhez fűződő jognak egyre nagyobb szerepe lesz, és egyre több kihívás éri, hiszen a technika és a tudomány fejlődésével az emberekről egyre több adatot egyre könnyebben lehet megszerezni és kezelni. Az egyén szokásai, kapcsolatai is jelentős részben adatok formájában jelenik meg. A személyes adatok védelméhez való jog mögött tehát nem csak az adatok, hanem az ember egész személyiségének és jogainak védelme húzódik meg.

A BIOMETRIKUS AZONOSÍTÁS

1. A biometrikus adat fogalma

A biometrikus adat olyan adat, amely az emberek mérhető testi adatait képezik le. Nem tévedünk, ha azt mondjuk, hogy biometrikus adat alapján azonosítjuk azt, aki szembe jön velünk az utcán, vagy akivel telefonon beszélünk stb. Ehhez képest a mostani tendencia abban különbözik, hogy egyrészt nemcsak az ember tud összehasonlítani, hanem erre a célra létrehozott számítástechnikai eszközök is. Másrészt pedig a felhasználási terület kiszélesedik, hiszen az ujjlenyomat eddig lényegében csak a büntetőeljárásban volt ismert, de egyre több területen lesz felhasználható, napjainkban például már ellenőrzési, bizonyítási, igazolási, azonosítási célul is szolgál. Fennáll annak a veszélye, hogy teljesen mindennapivá válik.[2]

Biometrikus azonosításra leggyakrabban a kéz, a szem, az arc, az aláírás, a hang vizsgálata és a DNS-azonosítás szolgál.

1. A kéz vizsgálata több mint 100 éves múltra tekint vissza, amely kétféle módon is szolgálja az azonosítást. Az azonosítás történhet egyrészt ujjlenyomat vagy tenyérlenyomat alapján, másrészt a kézgeometria is szolgálhat azonosítás alapjául. Ujjlenyomat, illetve tenyérlenyomat alapján történő azonosítás esetében az ujjbegy, illetve a tenyér mintázatát jegyzik fel, amely ujjlenyomat esetén körülbelül 40–60 pontot jelent, de már 8–12 pont esetén is azonosítható az érintett (sic!). A pontokból ugyanakkor nem állítható helyre az eredeti ujjlenyomat, ezért nem tartják a támogatói ezt a módszert személyiségi jogokat sértőnek. Ugyanakkor az ujjlenyomatnál a kesztyű viselése megakadályozza a pontos felismerést, a tenyérlenyomatnál pedig a rendszert megzavarhatja gyűrű viselése, illetve a nyomás nagysága, a kéznedvesség változása is.

[1] A biometria szó görög eredetű, a bios (élet) és a metrein (megmér, összemér) szavakból származik.
[2] Szabó, 2004, 82–83.

2. A retina is szolgálhat biometrikus adatként, amelyet egy alacsony intenzitású fényforrással tapogatnak le, amely idő alatt a fejet nem lehet megmozdítani, és egy adott pontra kell összpontosítani. Ettől az azonosítástól az írisz letapogatása annyiban különbözik, hogy ebben az esetben nincs fizikai kapcsolat a szem és a letapogató eszköz között.
3. Míg az előző esetben pontos képet kapunk, az arc vizuális felismerése egypetéjű ikrek esetében nem lehetséges. Arc-thermogrammal viszont olyan felvételt lehet készíteni, amely az arc hőtérképét rögzíti. Ez nem változik meg akkor sem, ha a testhőmérséklet esetleg nőne, vagy csökkenne. Ez a legpontosabb módszer az azonosításban, de nagyon költséges.
4. Hasonlóan pontos módszer az aláírás ellenőrzése is, amely alapján annak tulajdonosa szinte teljes bizonyossággal megállapítható akkor is, ha a két aláírás teljesen azonosnak tűnik, hiszen az írás dinamikáját, idejét, alak- és mozgáseltéréseit nem lehet utánozni.
5. A hanganalízis is egy sokrétű művelet, amelynek során az akusztikai jellemzők vizsgálata során sok millió ellenőrzés történik, mégis rövid ideig tart, de a háttérzaj, a rekedtség, esetleg a hangfelvétel minősége módosíthatja az ember hangját.
6. Utolsóként a DNS-azonosítást említeném. A DNS-vizsgálatok a büntetőeljárásban terjedtek el, hiszen ez a módszer segíti a bűncselekmény elkövetőjének kézre kerítését, míg másokat egyértelműen kizár az elkövetői körből.
   A DNS-minta elkészítése viszont nagy szakértelmet és komoly laborfelszerelést igényel. Időigényessége miatt naponta csak kb. 100 minta készíthető el, amelynek ára 100 000 $ mintánként, egy DNS-chip elkészítése ennek ötszöröse, és ebből kifolyólag, illetve természetesen adatvédelmi okból nem alkalmazható útlevélben.[3]

A biometrikus technikák, azonosító rendszerek egy része tehát a személy magatartását elemzik (például az aláírásmintát vizsgálják, a járást elemzik, a test illatát vagy a hangot felismerik), míg más részük a fiziológiai jellemzőket elemzi (például ujjlenyomat igazolása, retinaelemzés, hangfelismerés, DNS minták elemzése esetén).[4]

2. A biometrikus adatok rögzítése

Az egyes biometrikus adatok rögzítése, ellenőrzése természetesen eltérő technikákat igényel, viszont valamennyi adatfelvétel esetén elkülöníthetünk több fázist. Az első fázisban készül el a biometrikus minta. Ebből a nyers adatokat tartalmazó mintából valamilyen algoritmus segítségével kiemelnek bizonyos számú jel-

[3] Török Csaba projektje (Letöltés forrása, ideje: http://www.szgti.bmf.hu/~mtoth/download/Hallgatoi%20projektek/T%F6r%F6k%20Csaba%20-%20Biometria.pdf 2009. 12. 20.) 24–31.
[4] Lásd. I. számú melléklet
Munkaanyag a biometrikus azonosítókról (WP 80) (Letöltés forrása, ideje: http://abiweb.obh.hu/abi/index.php?menu=209 2009. 11. 10.)

lemzőt, így jön létre a biometrikus sablon. A biometrikus rendszerek többnyire csak ezt a sablont tárolják — és nem magát a képet, hangmintát stb. — valamilyen digitalizált formában, bár vannak olyan rendszerek is, amelyek ezeket a nyers adatokat tárolják sablon képzése nélkül. A folyamat végén csak egy vektortérkép marad az ujjlenyomat meghatározó pontjaival. Ezt a számítógépek számára értelmezhető számsorokká, algoritmusokká alakítják át, és a chipen rögzítik.[5]

A tárolás, azaz a sablon formája eltérő lehet attól függően, hogy mi a felhasználás célja, mekkora a sablon mérete. Ezek alapján három kategóriába sorolhatjuk a tárolási módszereket. Központi adatbázisban történő tárolás esetén van csak a személyazonosság megállapítására lehetőség.[6] A tárolás történhet továbbá magukon az azonosítást végző eszközökön, illetve valamilyen adathordozón (pl. mágnescsíkos vagy mikrochipes kártyán). Valamennyi esetében felmerülnek azonban technikai és alkotmányossági aggályok, amelyekre a későbbiekben még kitérek.

3. A biometrikus azonosító rendszerek

A biometrikus adatok áttekintését követően rátérek az azonosító rendszerek tárgyalására. A biometrikus azonosító rendszereken olyan eszközöket és eljárásokat kell érteni, amelyek a személyek mérhető testi tulajdonságait használják fel azonosításra vagy személyazonosság megállapítására valamilyen technika segítségével. A definíció pontos megértéséhez szükséges elhatárolni az azonosítást a személyazonosságtól. Míg az azonosítás az „az vagyok, akinek mutatom magam?" típusú kérdésre ad választ, addig a személyazonosság megállapításánál a „ki vagyok én?" típusú kérdést kell megválaszolni. Előbbi estben a tárolt adatoknak a személy testével való összehasonlítása után az igen vagy nem választ kapjuk, utóbbi esetben viszont a rendszer felismeri a személyt oly módon, hogy megkülönbözteti másoktól, akiknek a biometrikus adatai már tárolásra kerültek. Itt egy adatot hasonlít össze az összes többivel, az azonosítás során viszont két adatot mér össze.[7]

Az azonosító rendszerek közül csak egyik a biometrikus, emellett létezik még az eszköz és a jelszó alapján történő azonosítás. Ez utóbbi két esetben a rendszer nem a személyt (a jelszó, illetve az eszköz tulajdonosát), hanem magát a kódot, illetve az eszközt azonosítja. A kód szerinti felismerés a logikai világ (What You know?) része, amelynek a veszélye az, hogy az ember elfelejtheti, másokkal közölheti a jelszót, így visszaélésekre adhat okot.

[5] Szabó, 2004, 84–89.
[6] Lásd A biometrikus azonosító rendszerek c. alfejezetet
[7] Szabó, 2004, 83–84.
[8] Török Csaba projektje (Letöltés forrása, ideje: http://www.szgti.bmf.hu/~mtoth/download/Hallgatoi%20projektek/T%F6r%F6k%20Csaba%20-%20Biometria.pdf 2009. 12. 20.) 20–21.

Az eszköz segítségével történő azonosításnál viszont egy fizikai vizsgálatra (What You have?) kerül sor. Ebben az esetben előfordulhat, hogy magát a dolgot elveszítjük, elfelejtjük magunkkal vinni, ellopják, vagy lemásolják.

A biometrikus azonosítás a jelszó és az eszköz alapján történő azonosítástól akként lehet elhatárolni, hogy a biometrikus azonosító nem ruházható át, mert egyedi biológiai jellemzőket vizsgál (Who You are?). A biometikus azonosítás az élet számos területén jelen van, ennek egyik új iránya a biometrikus adatoknak útlevélben történő alkalmazása.[8]

A BIOMETRIKUS ÚTLEVÉL MEGJELENÉSE ÉS SZABÁLYOZÁSA AZ EURÓPAI UNIÓ TERÜLETÉN

1. Előzmények és az Európai Tanács 2252/2004/EK rendelete

Az Európai Bizottság dolgozta ki a jogharmonizáció jegyében azt a javaslatot, amely a biztonságpolitika területén a minimum követelményeket tartalmazza, köztük a biometrikus azonosítót tartalmazó útlevél kívánalmait. Brüsszelben már két évvel azelőtt, hogy az Amerikai Egyesült Államok a vízummentesség feltételéül szabta volna a biometrikus azonosítóval ellátott útlevelet, megállapodtak abban, hogy az útlevél két biometrikus azonosítót fog tartalmazni.[9] A Bizottság az ujjlenyomatot csak opcióként vetette fel, amely a tagállamok mérlegelésétől függött. Ezzel együtt egy központi adatbázis létrehozására is javaslatot tett, amely az európai polgárok összességének — tehát nem kevesebb, mint 450 millió uniós polgár ujjlenyomatát tartalmazta volna. Ezt az intézményt egyelőre azonban nem hozzák létre.[10]

Az útlevél mellett a vízum és a tartózkodási engedély biometrikus azonosítóval történő ellátása is napirenden volt az Unióban. Az eredeti elképzelések szerint a vízum is tartalmazott volna biometrikus azonosítót, de ezt technikailag kivitelezhetetlennek ítélték, mivel a chipet tartalmazó útlevél és vízum kölcsönösen működésképtelenséget idézett volna elő.[11]

2004. december 13-án született meg az új útlevél biometrikus és biztonsági tulajdonságait tartalmazó közösségi rendelet (2252/2004/EK rendelet), majd 2006. február 28-án ezeket az előírásokat konkretizáló európai bizottsági határozat.
A tagállamoknak a digitális fényképet tartalmazó útlevéllel kapcsolatos előírásokat 2006. augusztus 28-ig kellett kivitelezniük, amely előírásokat februárban közzétettek. Az ujjlenyomat szabályozására vonatkozó rendelkezéseket 2006. június 28-án hozták nyilvánosságra. Ezen részletszabályok megvalósítására 2009. június 28-ig kaptak az uniós országok haladékot.

[9] Az Egyesült Államok csak egy azonosítót kívánt meg, az EU pedig kettőt vezetett be.
[10] EU Commission proposal for biometrics in passports (Letöltés forrása, ideje: http://www.edri.org/edrigram/number2.4/biometrics 2008. 10. 17.)
[11] A hét elejétől itt a biometrikus útlevél (Letöltés forrása, ideje: http://www.tasz.hu/index.php?op=contentlist2&catalog_id=3097 2007. 10. 20.)
[12] Az Európai Tanács 2252/2004/EK rendelete (2004. december 13.) 1. cikk, 6. cikk

Az érintett országok kötelezettséget vállaltak arra nézve, hogy az általuk „kiállított útlevelek és úti okmányok megfelelnek a (...) meghatározott minimum biztonsági előírásoknak. Az útleveleknek és úti okmányoknak magukban kell foglalniuk egy arcképet tartalmazó tároló elemet, (...) ujjlenyomatokat is. Az adatokat védeni kell, (...), és garantálnia kell az adatok sértetlenségét, valódiságát és bizalmasságát."

A tagországoknak az általuk kiállított úti okmányra és útlevélre kell az Európai Tanács rendeletét alkalmazni a személyazonosító igazolvány és a tizenkét hónap vagy annál rövidebb érvényességi időre szóló, ideiglenes útlevél, illetve úti okmány kivételével.[12] A magyar szabályozás ezzel a rendelkezéssel nincs teljesen összhangban, mivel a hazai jogszabály a 12 hónapra vagy annál rövidebb érvényességi időre szóló ideiglenes magánútlevelet veszi ki a biometrikus útlevélre vonatkozó rendelkezések hatálya alól.[13]

A rendelet meghatározza, hogy a biometrikus jellemzők kizárólag az okmány valódiságának ellenőrzésére, valamint az okmány birtokosának személyazonosságának megállapítására használhatók fel a „közvetlenül hozzáférhető, összehasonlítható jellemzők segítségével, amennyiben az útlevelek és egyéb úti okmányok felmutatásáról törvény rendelkezik." Amennyiben a rendelet ezen célt határozza meg, mennyiben lesz törvényesen (alkotmányosan) használható az útlevél bűnmegelőzési és bűnüldözési célra? Hiszen a célhoz kötöttség garanciális korlátot jelent, amely az úti okmányok esetében azt jelenti, hogy csak azon igazolási célul szolgálhat, amely alapján az okmányon lévő adatot és az okmányt átadó tulajdonos adataival hasonlítja össze.[14]

A 29. cikk szerinti Munkacsoport a rendelet végrehajtásával kapcsolatban széles körű társadalmi vitát tartott volna szükségesnek, hiszen a biometrikus adatokat tartalmazó úti okmány jogi problémákon túl komoly etikai és technikai kérdéseket is felvet, a pénzügyi vonatkozásokat nem is említve.[15]

Az ujjlenyomatvétel a lakosság körében aggályokat vet fel, hiszen erről az embereknek a bűnügyi nyilvántartás jut eszükbe. Azt azonban meg kell itt jegyezni, hogy ha biometrikus útlevélről van szó, akkor digitális ujjlenyomatról beszélhetünk, míg előbbi esetében pedig tintás rögzítésről van szó. Azaz a DNS-ujjlenyomat olyan kriminalisztikai azonosító, amely a keresett személy vagy tárgy olyan ismérveit tükrözi, amelyekből vissza lehet következtetni azok sajátosságaira, majd megtalálása és vizsgálatra küldése után segítségükkel az azonosítás is elvégezhető.[16]

Technikai problémaként merül fel, hogy néhány szakértő szerint a chipek élettartama nem is éri el az érvényességi idejüket.[17]

[13] A külföldre utazásról szóló 1998. évi XII. törvény 7. § (2) bekezdés
[14] Az Európai Tanács 2252/2004/EK rendelete (2004. december 13.) 4. cikk (3) bekezdés
[15] Vélemény a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló, 2004. december 13-i 2252/2004/EK tanácsi rendelet végrehajtásáról (WP 112) Letöltés forrása, ideje: http://abiweb.obh.hu/abi/pdf/nemz/2005/tagallamoktlevelek.pdf 2008. 10. 27., 13.
[16] Nyiri, 1998, 118.
[17] V. ö. A magyar szabályozás c. alfejezet
Kockázatos a biometrikus útlevél (Letöltés forrása: http://www.hetek.hu/?q=node/11028 2008. 10. 17.)

A rendelet módosítása több okból is szükségessé vált. 2007-ben érkezett javaslat a Bizottságtól arra nézve, hogy a norma nem határozott meg kivételt az ujjlenyomatok levételével kapcsolatban, jóllehet vannak olyan élethelyzetek, életkorok, amikor ennek minősége nem tesz lehetővé egyértelmű azonosítást. Az Európai Bizottság nem tartotta célszerűnek sem nemzetbiztonsági, sem jogi szempontból, hogy ezt a tagállamok szabályozzák, ezért két mentesülési lehetőséget állapított meg az ujjlenyomat-adási kötelezettség alól. A kivételek személyben rejlő okból fakadnak: a hat év alatti gyermekeknek nem kell ujjlenyomatot adni, hiszen az ujjlenyomatok kiskorban még változhatnak, illetve azon személyeknek, akik fizikailag nem képesek ujjlenyomatot adni.[18]

A probléma egy része azonban továbbra sem megoldott, mert a magas hibaszázalék nemcsak a kisgyermekeknél, hanem az időseknél is fennáll. Hollandia felmérést végzett az ujjlenyomat azonosíthatóságával kapcsolatban, és arra a következtetésre jutott, hogy a 6 évesnél fiatalabbak és a 60 évesnél idősebbek esetében nem elég megbízható az azonosításnak ez a módja. Ez az eredmény a holland kormányt elbizonytalanította, hiszen ez a módszer funkcióját kérdőjelezi meg.[19] Az Európai Unióban is arról folyt a vita, hogy hány éves kortól vegyék le az ujjlenyomatot, amely a fentebb ismertetett adatok miatt a szakértői testületnek is nagy fejtörést okozott.[20] További problémát okozhat az azonosításnál, hogy az emberi ujjlenyomat például kemény fizikai munka vagy bőrbetegségek következtében is változhat.

Magyar jogszabály ilyen kivételeket nem szabályoz, jóllehet számos jogvédő szervezet felhívta a biometrikus adatok kezelésével kapcsolatos veszélyekre a figyelmet. Az európai adatvédelmi biztos a kivételekre vonatkozó uniós szabályozást sem tartja azonban tudományos szempontból kellően megalapozottnak. Véleménye szerint „az ujjlenyomat-adásra vonatkozó korhatárt egy olyan szisztematikus és részletes tanulmányban kell meghatározni, amelynek megfelelő módon azonosítania kell a valós körülmények között működő rendszerek pontosságát, és tükröznie a feldolgozott adatok sokrétűségét. A kísérleti projektek önmagukban nem nyújtanak elegendő információt ahhoz, hogy a közösségi törvényhozó alapvető választásai azokra épülhessenek." A tudományos kutatás az időskorúak vonatkozásában is nélkülözhetetlen. Ennek tükrében pedig az életkor felülvizsgálatát tartja szükségesnek.[21] A 29. Munkacsoport nemcsak az életkorra nézve tartja kívánatosnak a korlátokat, hanem azt is előírná, hogy ezeken milyen ellenőrzéseket kell elvégezni a tárolás ideje alatt.

[18] Javaslat a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló 2252/2004/EK tanácsi rendelet módosításáról (Letöltés forrása, ideje: http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=hu&ihmlang=hu&lng1=hu,mt&lng2=bg,cs,da,de,el,en,es,et,fi,fr,ga,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=461472:cs&page 2008. 10. 27.)

[19] Mégsem jó a biometrikus útlevél? (Letöltés forrása, ideje: http://www.nol.hu/cikk/377129 2007. 10. 20.)

[20] A hét elejétől itt a biometrikus útlevél (Letöltés forrása, ideje: http://www.tasz.hu/index.php?op=contentlist2&catalog_id=3097 2007. 10. 20.)

[21] Az európai adatvédelmi biztos véleménye a tagállamok által kiállított útlevelek és úti okmányok

Az európai uniós szabályozással kapcsolatos vélemények mindezeken túl az arányosság fontosságát hangsúlyozzák. A szükségtelen jogkorlátozás elkerülésére és ezen intézkedések bevezetésének veszélyeire is felhívják a figyelmet: az azonosító adatok és az ujjlenyomat rossz összepárosítása komoly problémákhoz vezet.[22]

Az uniós polgárok útlevelének biztonsági sajátosságaira és biometrikus adataira vonatkozó szabványokról szóló tanácsi rendeletre irányuló módosító javaslatok szerint sem világos, hogy a biometrikus azonosítók bevezetése valóban hozzájárul-e a biztonság növekedéséhez, vagy inkább veszélyt jelent a biztonságra a visszaélések, műszaki hibák kockázata, illetve az átláthatóság és a megfelelő adatvédelem hiánya miatt. Nem kellően megindokolt az arányosság, a megfelelőség és a hozzáadott érték sem a biztonság területén. Nem ad választ arra az Unió, hogy miért nem elég csak egy biometrikus elemet (pl. az arcképet) a chipen rögzíteni. Az arányosság elvének tiszteletben tartása továbbá megkövetelné annak bizonyítását, hogy nem áll rendelkezésre más eszköz a dokumentumok biztonságának növelésére, illetve a terroristák kiszűrésére vonatkozó célkitűzés eléréséhez.[23] Az EU Adatvédelmi Bizottságának Munkacsoportja is úgy foglalt állást, hogy komoly kételyek merülnek fel az elektronikus útlevelek megfelelő alkalmazása kapcsán. Emellett pedig a bevezetés szükségessége sincsen kellőképpen igazolva.[24]

2. Emberi jogi szervezetek álláspontja

Több szervezet, köztük a Privacy International, a Statewatch, a European Digital Rights az Európai Parlamentnek címzett nyílt levélben[25] a szabályozás alapját kérdőjelezik meg, miszerint ennek a gyakorlatnak a bevezetése szükségtelen, és az emberek magánszféráját indokolatlanul nagy kontroll alá vonja. Levelükben magyarázatot kértek arra, hogy miért vezetik be az ujjlenyomattal is ellátott útlevelet, amikor az Egyesült Államok ezt nem kérte, és a saját polgáraitól sem követeli ezt meg, valamint arra is, hogy miért nem csak egy biometrikus azonosítóról

biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló 2252/2004/EK tanácsi rendelet módosításáról szóló európai parlamenti és tanácsi rendeletjavaslatról (2008/C 200/01) (Letöltés forrása, ideje: http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-03-26_Biometrics_passports_HU.pdf 2008. 10. 27.) 3.

[22] A 29. Munkacsoport 3/2007. sz. véleménye a diplomáciai és konzuli képviseletek számára kibocsátott, a vízumokra vonatkozó Közös Konzuli Utasításnak a biometrikus adatok bevezetésével, valamint a vízumkérelmek fogadása és feldolgozása megszervezésének rendelkezéseivel kapcsolatos módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról (WP 134) (Letöltés forrása, ideje: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp134_hu.pdf 2008. 10. 27.) 5.

[23] Az uniós polgárok útlevelének biztonsági sajátosságaira és biometrikus adataira vonatkozó szabványokról szóló tanácsi rendeletre irányuló javaslat (Letöltés forrása, ideje: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/am/544/544525/544525hu.pdf 2008. 10. 20.) 2.

[24] EU's data-protection commissioners concerned about biometrics on smartcards (Letöltés helye, ideje: http://www.bjhcim.co.uk/news/1/2004/n41006.htm 2008. 10. 27.)

[25] A felhívásához csatlakozott számos nyugat-európai ország mellett Magyarország korábbi adatvédelmi biztosa, Péterfalvi Attila és elődje, Majtényi László is.

rendelkeznek. Felhívja arra is a figyelmet, ha az útlevélnek ez a típusa bevezetésre kerül, a szükségesség-arányosság elvét átlépik, ami pedig a Közösség tevékenységének jogszerűségét kérdőjelezi meg, és beleütközik a közösségi jog által deklarált magánszférához való jogba. Levelükben ráirányították arra is a figyelmet, hogy egy 2003-ban tartott nemzetközi konferencián deklarálták, a terrorizmus és szervezett bűnözés elleni harcban az országoknak az alapvető adatvédelmi elveket tiszteletben kell tartaniuk. Utaltak arra is, hogy az ujjlenyomat megbízhatatlansága egy megrázó eset kapcsán be is bizonyosodott: a 2004. március 11-i madridi vonatrobbantás után a spanyol rendőrség és a három legnagyobb gyakorlattal rendelkező FBI ujjlenyomat-szakértő bevonásával egy fel nem robbant bombán azonosított egy ujjlenyomatot, amit Brandon Mayfieldnek tulajdonítottak — tévesen.[26] Továbbá megesett már, hogy az eljárásban nőt férfiként azonosított. Az arcfelismerő rendszert ki lehet úgy játszani, hogy a kamera elé fényképet tartanak, illetve az ujjlenyomat-leolvasót egy emberi ujj műanyag másolatával is. Emellett a biometrikus útlevél terrorizmus elleni hatékonyságát is sokan megkérdőjelezik azon az alapon, hogy csak a már nyilvántartásba vett bűnözőket, illetve hamis úti okmánnyal érkezőket szűri ki, míg a 2001. szeptember 11-i támadás elkövetői legálisan érkeztek az Egyesült Államokba. A biometrikus útlevél sem képes tehát másra, mint a személyazonosság megállapítására, nem tükrözi az adott személy utazási célját, szándékát.[27]

Az emberi jogok a demokrácia mozgalomban húsz évvel ezelőtt — Az emberi jogok című 2005 novemberében megtartott kétnapos konferencián is napirendre került a biometrikus azonosítót tartalmazó útlevél problémája. Legnagyobb nyilvánosságot az Európai Biztonsági és Együttműködési Szervezet (EBESZ) sajtószabadság-biztosa, Haraszti Miklós felszólalása kapta, amelyben azt állította, hogy Európa túlzottan támadja az amerikai politikát, ugyanakkor az EU jobban megnyirbálja a szabadságjogokat, mint a 2001. szeptember 11-i terrortámadás után elfogadott „hazafias" törvény, a Patriot Act, hiszen az Egyesült Államok nem kért két biometrikus azonosítót. Harasztit leginkább az háborítja fel, hogy az európaiak nem is ellenezték ezeket az intézkedéseket. Ezt valószínűleg az is befolyásolja, hogy jó eszköznek látják a terrorizmus és menekültek problémájának megoldásához, míg az amerikaiak már megtanultak ezekkel a problémákkal együtt élni.[28]

Az adatvédelmi aggályokon túl további problémák is megkérdőjelezik ezen szabályozás létjogosultságát. Prof. Steven Peers (University of Essex) elemzése szerint az Európai Közösség túllépi hatásköri jogosultságát, mert a külső határaira nézve nem fogadhat el határellenőrzéssel kapcsolatos intézkedést. Az EK

[26] An Open Letter To The European Parliament On Biometric Registration Of All EU Citizens And Residents (Letöltés forrása, ideje: http://www.edri.org/campaigns/biometrics 2008. 10. 17.)
[27] Poór, 2005, 69.
[28] Haraszti: a szabadság korlátozásában Európa túltesz Amerikán (Letöltés forrása, ideje: http://hvg.hu/itthon/20051122harasztieuropa.aspx?s=hk 2008. 10. 17.)

Alapszerződésének 18. cikk (2) és (3) bekezdése[29] egyértelműen kizárja a Közösségnek — a szabad mozgás területén történő rendelkezéseknél — az úti okmányra vonatkozó szabályok megalkotását. Ez tehát éppen a szabad mozgás jogának érvényesülése érdekében tesz kivételt a jogalkotási felhatalmazás keretében.[30] Az Egyesült Királyság viszont úgy érvel, hogy a Schengeni jegyzőkönyv figyelembevételével lehetővé válik ezen tárgykör szabályozásának „opt in"-je.[31]

3. A magyar szabályozás

Magyarországon az Országgyűlés a 2003 tavaszi ülésszak utolsó napján az üvegzseb-program keretében elfogadta az adatvédelmi törvény módosításait. A biometrikus útlevélre vonatkozó szabályok 2006. augusztus 29-étől hatályosak. A módosítás érintette továbbá a külföldre utazásról szóló törvényt is. A chipes útlevelek kibocsátása 2006 szeptemberében kezdődött, de a korábbi útleveleket az Európai Unióban a lejáratukig elfogadják. Ha a normál típusú útlevél birtokosának mégis az új útlevélre lenne szüksége, például amiatt, mert az USA-ba utazik, az úti okmány cseréjét illetékmentesen végrehajtják.[32]

Törvényi előírás, hogy a személyes adatok tároló elemben történő tárolását az elérhető legmagasabb szintű technikai módszerek alkalmazásával kell megvalósítani.

Utaltam már korábban arra a problémára, hogy szabályozást igényel az is, ha az útlevél érvényességi idején belül a tároló elem adattartalmi ellenőrzésre alkalmatlanná válik. Ez az eset nem eredményezheti az útlevél érvénytelenségét, hiszen a leolvasásra alkalmatlan tároló elem esetén a hagyományos útlevél ellenőrzési módszerei alkalmazásával továbbra is megbízhatóan megállapítható a kapcsolat az útlevél és birtokosa között.[33] Mivel az útlevél működésképtelensége esetén is érvényesnek tekintendő, az adatvédelmi aggályok elkerülése érdekében egy biztonsági szakember azt tanácsolta a megfigyeléstől vagy személyiséglopástól tartó résztvevőknek, hogy egy jól irányzott kalapácsütéssel zúzzák össze az adatokat tartalmazó chipet.[34]

[29] Az Európai Tanács 2252/2004/EK rendelete (2004. december 13.) 18. cikk
(1) (...) minden uniós polgárnak joga van a tagállamok területén való szabad mozgáshoz és tartózkodáshoz.
(2) Ha a Közösség fellépése bizonyul szükségesnek ahhoz, hogy e célkitűzés megvalósuljon, (...), az (1) bekezdésben említett jogok gyakorlásának megkönnyítése érdekében a Tanács rendelkezéseket fogadhat el.
(3) A (2) bekezdés az úti okmányokra, személyazonosító igazolványokra, a tartózkodási engedélyekre vagy bármely egyéb ilyen okmányra vonatkozó rendelkezésekre (...) nem alkalmazható.
[30] Statewatch Analysis: The Legality of the Regulation on EU Citizens' Passports (Letöltés forrása, ideje: http://www.statewatch.org/news/2004/nov/11biometric-legal-analysis-htm.htm 2007. 10. 10.)
[31] Biometrics and secure travel documents (Letöltés forrása, ideje: http://www.euractiv.com/en/security/biometrics-secure-travel-documents/article-132063 2008.10. 27.)
[32] A hét elejétől itt a biometrikus útlevél (Letöltés forrása, ideje: http://www.tasz.hu/index.php?op=contentlist2&catalog_id=3097 2007. 10. 20.)
[33] A külföldre utazásról szóló 1998. évi XII. törvény 20. §, 32/A. § (2) bek.
[34] Feltörték a mikrochipes útlevelet (Letöltés forrása, ideje: http://ww.ok.hu/techbazis/hightech/20080807-feltortek-a-mikrochipes-utlevelet.html 2008. 10. 27.)

Az útlevél érvényessége lényegében az útlevél „feltörhetetlenségi idejét" jelenti. A sok ráfordítással járó technika biztonságos voltát azonban már a 2006. augusztus elején megrendezett konferencián Lukas Grunwald számítástechnikai szakértő megkérdőjelezte azzal a kijelentésével, hogy sikerült feltörnie az új német biometrikus útlevelet, amely technikai standardja alapján a magyar is készül. Előadásában azt is kifejtette, hogy ezt a világon létező összes biometrikus útlevéllel meg lehet tenni, mert mindegyik a Nemzetközi Polgári Légiközlekedési Szervezet szabványa alapján készül.[35] Az útlevelek klónozása csak az első lépés lehet a technika megkerülésében. Ettől már csak egy lépés, hogy az útlevél ellenőrző programját átkódolják, amely akár a rendszer összeomlásához is vezethet. A klónozás kiküszöbölésére azt az érvet hozzák fel, hogy könnyen felismerhető, mert a chipen tárolt kulcsot csak össze kell vetni a kibocsátó által gondozott adatbázissal. Sajnos ez csak az elméletben van így, mert a közös adatbázisba a biometrikus útlevelet alkalmazó országok közül mintegy tíz szállt be, ezek közül is csak öt ellenőrzi az egyezőséget.[36]

A polgároknak viszont biztosítani kell azt a lehetőséget, hogy saját maguk is ellenőrizhessék a chipen lévő adatokat, ezért a Rendőrség határforgalom-ellenőrzést végző szerve mellett az okmányirodákat is ellátták olvasó-berendezéssel. Ahol viszont nem rendelkeznek az adatok leolvasásához szükséges berendezéssel, ott az útlevél nyomtatott adatai ellenőrizhetők. Az úti okmány ellenőrzésére jogosult más hatóságok viszont ezen adatokhoz nem juthatnak hozzá.[37] Az útlevélhatóság is a tároló elemben rögzített személyes adatokat csak az úti okmány kiadásáig jogosult kezelni, azután törölni kell, míg a Rendőrség határforgalom-ellenőrzést végző szerve ezt csak leolvashatja.[38] Tehát nem lesz — legalábbis egy ideig — központi nyilvántartás. Egyelőre azt csak azonosításra lehet használni.

A központi adatbázis komoly veszélyt rejt magában. A 29. cikk szerinti Munkacsoport is kiemelte, hogy különösen a biometrikus adatok vonatkozásában meg kell fontolni, hogy milyen információkat vesznek fel a központosított adatbázisba (C-VIS), mert komoly hatása lehet az emberi méltóságra és alapvető jogokra. A biometrikus adat mint keresőkulcs alapján aztán könnyebbé válik más adatbázisban is a keresés, amely azonban már azt idézi elő, hogy a felvett adatokat az adatkezelés eredeti céljától eltérően is használják. Az EU-ban létezik több biometrikus adatokat tartalmazó adatbázis is, így például az EURODAC, amely a menedékkérelmek elbírálását segítő ujjlenyomat-azonosító rendszer. Az adatbázisok összekapcsolásával az is lehetővé válhat, hogy kialakítják az egyén személyiségprofilját, amely szigorúan tilos.[39]

[35] A hét elejétől itt a biometrikus útlevél (Letöltés forrása, ideje: http://www.tasz.hu/index.php?op=contentlist2&catalog_id=3097 2007. 10. 20.)
[36] Feltörték a mikrochipes útlevelet (Letöltés forrása, ideje: http://ww.ok.hu/techbazis/hightech/20080807-feltortek-a-mikrochipes-utlevelet.html 2008. 10. 27.)
[37] Lencsés, 2005, 10.
[38] A külföldre utazásról szóló 1998. évi XII. törvény 32/A. §
[39] A 29. Munkacsoport 3/2007. sz. véleménye a diplomáciai és konzuli képviseletek számára kibocsátott, a vízumokra vonatkozó Közös Konzuli Utasításnak a biometrikus adatok bevezetésével, valamint a vízumkérelmek fogadása és feldolgozása megszervezésének rendelkezéseivel kapcsolatos

Az adatok továbbítására vonatkozóan továbbá az általános szabályozástól eltérő rendelkezések vonatkoznak a biometrikus útlevélre. Eszerint „az útlevélhatóság, illetőleg a központi adatkezelő szerv — törvényben meghatározott feladataik ellátása céljából — a büntetőügyekben eljáró hatóságoknak, a rendőrségnek, a nemzetbiztonsági szolgálatoknak, a vám- és pénzügyőrségnek, a nyugdíjbiztosítási igazgatási szervnek, az állampolgársági ügyekben eljáró szervnek, valamint a menekültügyi hatóságnak adhat át adatot." „Az útlevélhatóság, valamint a központi adatkezelő szerv az általa nyilvántartott adatot statisztikai célra felhasználhatja, abból ilyen célra, személyazonosító adat nélkül adatot szolgáltathat."[40]

Hazánkban több szervezet is kifejezte tiltakozását az új útlevél bevezetése ellen. Így az Eötvös Károly Központi Intézet, a Magyar Helsinki Bizottság, a No Camera Csoport, a Társaság a Szabadságjogokért és a Technika az Emberért Alapítvány nyílt levélben fordult a kormányhoz, amelyben megfogalmazták ellenvetéseiket. Támadták a kormányt azért, mert a nélkül döntött ebben a kérdésben, hogy azt valamilyen nyilvános vitafórumon megtárgyalták volna.

A jelenlegi szabályok két biometrikus azonosítót tartalmazó útlevél használatát írják elő, amelyet még a terrorizmus elleni harc mellett elkötelezett Egyesült Államok sem követel meg. Korábban az Európai Bizottság volt az, amelyik egy ehhez hasonló tervet elvetett, arra való hivatkozással, hogy az alapvető jogokat csorbít. Felhívták a figyelmet arra is, hogy a megfelelő adatvédelmi garanciák hiányának súlyos következményei lehetnek. A biometrikus azonosítók ilyen széles körű alkalmazása általános elvárássá emelné az ujjnyomat-azonosítást, amelyre eddig csak büntetőeljárás keretében került sor. Ennek nyomán az EU valamennyi polgárának mozgása megfigyelhetővé válhat, és ez visszaéléseknek lehet táptalaja.[41] Hiszen a folyamat arra felé mutat, hogy az ember egyediségére vonatkozó adatok kiszolgáltatása általánossá válik. Ezt támasztja alá az is, hogy az Európai Unión kívül más szervezetek (pl. a Gazdasági Együttműködési és Fejlesztési Szervezet / OECD/) is tárgyalnak a biometrikus adatok felhasználásáról, itt a cél viszont már nem a terror megfékezése.[42] A biometrikus adatokat ma is több helyen alkalmazzák. A büntetés-végrehajtási intézetben a látogatóknak is valamely adatát rögzítik. Bruneiben a 300 000 helyi lakos, a tartózkodási engedéllyel rendelkező vendégmunkások és a gyakori beutazók személyigazolványa is tartalmaz chipet. Ennek száma megközelíti a hétszázezret. Angliában pedig néhány önkormányzat bevezette az ún. „polgár-kártyát", amivel a helyi üzletekben a kártyatulajdonos kedvezményekben részesül, vagy bizonyos szolgáltatásokat igénybe vehet. A jogtalan igénylők kiszorítása érdekében a támogatási rendszerben is terjed.[43] Felmerült a

módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról (WP 134) (Letöltés forrása, ideje: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp134_hu.pdf 2008. 10. 27.) 5–7.

[40] A külföldre utazásról szóló 1998. évi XII. törvény 27. § (1) bek., 28. § (3) bek.

[41] Nyílt levél az ujjnyomatos útlevelek ügyében (Letöltés forrása, ideje: http://www.tasz.hu/index.php?op=contentlist2&catalog_id=1216 2007. 10. 20.)

[42] Szabó, 2004, 82.

[43] Török Csaba projektje (Letöltés forrása, ideje: http://www.szgti.bmf.hu/~mtoth/download/Hallgatoi%20projektek/T%F6r%F6k%20Csaba%20-%20Biometria.pdf 2009. 12. 20.) 28–31.

vízumokban, illetve a tartózkodási engedélyben való alkalmazásuk lehetősége is, de ez technikai nehézségek miatt nem valósult meg.[44]

A Helsinki Bizottság elnöke, Kőszeg Ferenc is azt a véleményt képviseli, miszerint ezek az adatok súlyosan sértik az egyének emberi jogait, hiszen az ujjlenyomat alapján következtetni lehet az etnikai jellemzőkre is.[45]

A MAGYAR JOGVÉDŐ SZERVEZETEK (LEHETSÉGES) ÁLLÁSPONTJA

1. Az adatvédelmi biztos gyakorlata a biometrikus adatok vonatkozásában

A biometrikus adatok megítélése alapjául az adatvédelmi biztos gyakorlatában egyrészt az ujjlenyomat-nyilvántartásokra, másrészt a beléptető rendszerekre vonatkozó állásfoglalásai szolgálnak.[46]

Majtényi László, korábbi adatvédelmi biztos a 832/K/2000 állásfoglalásában kifejtette, hogy elvi korlátját nem látja a biometrikus azonosító rendszerek bevezethetőségének, ugyanakkor az adatok biztonságos kezelésének szigorú feltételeit meg kell teremteni. Adatvédelmi szempontból ezek az azonosító rendszerek annyiban újak, hogy a hagyományos (azonosító + jelszó) módszerek helyett a felhasználók testi tulajdonságai alapján azonosítják az érintettet. Ezeket az adatokat az Avtv. alapján személyes adat (sic!) védelmében kell részesíteni.[47]

Az adatvédelmi biztos az Avtv. 2. § 1. pontja alapján azt mondja, hogy „a személy különösen akkor tekinthető azonosíthatónak, ha őt — közvetlenül vagy közvetve — név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet." Az Alkotmány 59. § (1) bekezdésében deklarált személyes adatok védelméhez való jogból kifolyólag, főszabály szerint, személyes adatot felvenni és felhasználni az érintett hozzájárulása nélkül csak kivételes esetben, törvény felhatalmazása alapján lehet. Ez a korlátozás csak akkor tekinthető alkotmányosnak, ha megfelel az Alkotmány 8. §-ban meghatározott feltételeknek.

Ujjlenyomat-leolvasó rendszer is csak akkor működtethető, ha az elérni kívánt cél más módon nem valósítható meg, és az ezzel okozott alapjogi korlátozás, illetve egyéb jogszabályban meghatározott jogok korlátozása arányban áll az elérni kívánt céllal. Az azonosítás „akkor tekinthető elfogadhatónak, ha annak során csak a megjelölt cél megvalósulásához elengedhetetlenül szükséges adatokat kezelik, és az ellenőrzéshez nem tartanak fenn két eltérő technológiát, illetve ebből következően két különálló adatkezelést." Egyazon célra több azonosító használata nem felel meg az adatvédelmi törvényben foglaltaknak. Ha ezek az azonosí-

[44] Interinstitutional File about integration of aspects of biometric identifiers in the uniform visa format and in the uniform residence permit for third country-nationals (Letöltés forrása, ideje: http://www.statewatch.org/news/2005/jan/bio-visas-16257.pdf 2008. 11. 02.)
[45] Nyílt levél az ujjnyomatos útlevelek ügyében (Letöltés forrása, ideje: http://www.tasz.hu/index.php?op=contentlist2&catalog_id=1216 2007. 10. 20.)
[46] Az adatvédelmi biztos beszámolója 2005, 129.
[47] V. ö. Az Alkotmánybíróság gyakorlata c. alfejezet, 832/K/2000 adatvédelmi biztosi állásfoglalás

tók nem egymás megerősítésére szolgálnak, hanem párhuzamosan, de egymástól függetlenül szolgálják ugyanazt a célt, nem ütközik adatvédelmi szabályokba.[48]

Péterfalvi Attila azt is leszögezi, hogy Magyarország az Unió előírásait nem lépheti túl, és az útlevélen lévő adatokat nem lehet más célra felhasználni. A legnagyobb veszélynek az automatizáltság lehetőségét tartja, hiszen ma már léteznek automatikus arcfelismerő rendszerrel kombinált kamerák, amelyek képesek automatikusan nyomon követni a megfigyelt polgár útvonalát ott, ahol ezek a rendszerek kiépítésre kerültek. Egy másik fenyegető veszély, hogy a technológiai kutatások a passzív azonosítás felé haladnak, ami azt jelenti, hogy az azonosításhoz nem szükséges az érintett közreműködése — így például az íriszletapogató készülékhez nem kell közel állni, mert a rendszer automatikusan, akár az érintett tudta nélkül is elvégzi az azonosítást.

Adatvédelmi szempontból komoly aggályokat vet fel, hogy a biometrikus azonosító rendszerek egymással való kombinálása hova vezethet, hiszen ezzel lehetővé válik, hogy egy gombnyomással mindent megtudjunk valakiről: mikor, hol járt (arcfelismerő kamera segítségével), mikor ért be a munkahelyére, mikor használta ujjlenyomat-azonosítóval kombinált bankkártyáját stb. Mindez egyik oldalról tűnhet egyszerű, biztonságos (?) világnak, de ott van mögötte a totális ellenőrzés közeli lehetősége. A nagyszerűségéről lehet ódákat zengeni — mint ahogy teszik ezt nagyon sokan, de túlértékelik a biometrikus azonosítás lehetőségeit.[49] A biztos a visszaélések megakadályozásához szükségesnek tartja, hogy az adatokat ne adatbázisban, hanem kártyán tárolják. Ebben az esetben az érintett a leolvasó rendszerhez teszi az ujját a kártyájával együtt, és a rendszer az adatokat összeveti.

Péterfalvi Attila a biometrikus azonosítóval ellátott útlevél bevezetésével kapcsolatos kormány-előterjesztés véleményezésekor hívta fel a figyelmet, hogy a „biometrikus adatokat tartalmazó állami adatbázis üzemeltetése nem kerülhet magánkézbe. A biztos óvott attól, hogy a biometrikus azonosítást bárki is a terrorizmus elleni harc csodafegyverének tekintse, és a polgárok automatizált megfigyelésére alkalmas rendszert próbáljon létrehozni. A biometrikus azonosítót tartalmazó útlevelekre irányuló bármely szabályozás csak olyan formában elfogadható, ha az megmarad az uniós tagságunkból eredő kötelezettségek szabta, az állampolgárok alkotmányos jogait a lehető legkevésbé korlátozó keretek között”.[50]

A biometria mögött álló ipar rendkívüli tőkét képvisel. A részvények árfolyama szárnyalt, amikor a biztonságért felelős szervek kijelentették, hogy a biometrikus azonosítók által nyújtott lehetőséget kívánják felhasználni a terrorizmus ellen. Arról nagyon kevés helyen lehet olvasni, hogy a szakáll növesztése még nem, de egy szemüveg vagy egy sapka már megtévesztheti a rendszert. És arról sem lehet hallani, hogy ma Európában egy helyen alkalmaznak arcfelismerő rendszereket

[48] 290/A/2005 adatvédelmi biztosi állásfoglalás
[49] Az adatvédelmi biztos beszámolója 2005, 130.
[50] 1485/J/2005 adatvédelmi biztosi állásfoglalás

széles körben közterületi ellenőrzésre: Londonban, Európa leginkább bekamerázott városában, amely védtelenül állt a terrortámadás előtt.[51] Azt tapasztaljuk, hogy a terrorizmus és a bűnözői szervezetek elleni harc jegyében soha nem lesz határ, amely gátat szabna a személyes adatok védelméhez fűződő szabadságjog sérelmének, mert a nemzetbiztonság mindig egy jó hivatkozási alap lesz.[52]

2. Az Alkotmánybíróság gyakorlata

A biometrikus jellemzők kérdésköre alapvetően a személyes adatok védelméhez való jog aktív és passzív oldalához kapcsolódik. Azonban nemcsak a magyar, hanem a német szövetségi alkotmánybíróság gyakorlatában is megjelent, hogy az információs önrendelkezési jog az általános személyiségi jog része, amely az emberi méltósághoz kapcsolódik. A magánélet is vitathatatlanul érintett, amikor egy közhatalom adatot gyűjt, tárol vagy továbbít.[53]

A fogalmi tisztázást szükségessé teszi, hogy a biometrikus adatok valamely adatfajtába történő besorolása a szakirodalomban sem egységes. A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (továbbiakban: Avtv.) az egyes adatfajták definíciójának meghatározása alapján segíti azok elhatárolását.

Az *ujjlenyomatot* ezek alapján a személyes adatok kategóriájába sorolhatjuk, de ha ebből a nemzeti, nemzetiségi és etnikai hovatartozására következtetni lehet vagy éppen bűnügyi nyilvántartásban jelenik meg, akkor különleges adatnak minősül.[54] A 29. Munkacsoport az útlevelekben, egyéb úti okmányokban, illetve személyazonosító igazolványokban szereplő biometrikus jellemzőket azonban különösen szenzitív adatnak minősítette. A Nemzetközi Polgári Légiközlekedési Szervezet (ICAO) a digitális arcképet nem tekinti szenzitív adatnak, de az ujjlenyomatok és egyéb további biometrikus jellemzők felvételét az útlevélbe különösen szenzitív jellegűnek minősítette.[55] Véleményem szerint ezért a biometrikus útlevélben szereplő ujjlenyomat nem kezelhető úgy, mint csupán egy személyes adat, mert annak szenzitív jellege nagyobb védelmet igényel. Az ujjlenyomat az ember személyiségének része, ami nemcsak a személyes adatok védelméhez fűződő jog alkotmányos garanciáját követeli meg, hanem az emberi méltóság biztosítását is.

[51] Az adatvédelmi biztos beszámolója 2005, 131.
[52] Rech, 2007, 5.
[53]Golembiewski–Probst: Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen (Letöltés forrása, ideje: https://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf 2008. 10. 27.), 34.
[54] Nyiri, 1998, 118.
[55] Vélemény a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló, 2004. december 13-i 2252/2004/EK tanácsi rendelet végrehajtásáról (WP 112) Letöltés forrása, ideje: http://abiweb.obh.hu/abi/pdf/nemz/2005/tagallamoktlevelek.pdf 2008. 10. 27.

Ebből kifolyólag a biometrikus adatok problémáját nemcsak a személyes adatok védelméhez való jog, hanem az emberei méltósághoz fűződő joghoz való viszonyában is vizsgálni kell.

A biometrikus adatok adatvédelmi szempontú elemzése

Az Alkotmány kimondja, hogy alapvető jogra és kötelességre vonatkozó szabályokat törvény állapítja meg, de alapvető jog lényeges tartalmát nem korlátozhatja.[56] Az Alkotmánybíróság megállapította az egyes alapjogok korlátozásának alkotmányos követelményét. A korlátozásnak a szükségesség-arányosság tesztjének kell megfelelnie. Egy alapjog csak akkor korlátozható, ha *„másik alapvető jog és szabadság védelme vagy érvényesülése, illetve egyéb alkotmányos érték védelme más módon nem érhető el."*[57]

Az elv egyik eleme tehát a szükségesség. A szükségességet úgy kell értelmezni, hogy a cél ne csak „kívánatos" legyen az adatkezelő számára, hanem amely nélkül a szándékolt cél nem is lenne kivitelezhető. Vajon a terrorizmus elleni harcban a cél elérhető-e ezzel a módszerrel? Egyáltalán törvényes cél-e a bűnmegelőzés?

A szükségesség magában foglalja azt is, hogy az adatok kezelése akkor jár az érintett jogainak legkisebb sérelmével, ha annak nem marad nyoma, vagy az adat az érintett birtokában marad. Ezzel függ össze az adatbázis létrehozásának a problematikája, hiszen ebben az esetben az adat kikerül az érintett birtokából, míg például a biometrikus útlevéllel történő jelenlegi azonosítás esetében az adatokat az egyénnel hasonlítja össze, és nem mások adataitól különbözteti meg.

A beavatkozás mértékét érinti az is, hogy az egyes biometriai adatok mennyire vonatkoznak magára a személyiségre. Például az emberi hang többet elárul az érintett személyiségéről, mintha a fül geometriáját vizsgálnánk. Erre tekintettel, a francia adatvédelmi hatóság egy iskolai étkező bejáratánál működtetett beléptető rendszer esetében elfogadhatatlannak tartotta az ujjlenyomat használatát, de a kéz geometriáját alkalmasnak találta erre a célra. Ebből következik, hogy ha a cél elérése kisebb beavatkozással is elérhető, akkor azt a megoldást kell választani.[58] Valamely alapjog alkotmányosan megengedhető korlátozásánál az Alkotmánybíróság állandó kritériuma, hogy „a korlátozásnak kényszerítő okból és arányosan kell történnie. Az arányosság követelménye pedig magába foglalja a legkevésbé korlátozó és az alkalmas eszköz használatát." Az ezzel ellentétes szabályozás alkotmányellenes.[59]

Nem elegendő, ha az lapjog korlátozása valamilyen megengedett, alkotmányos cél érdekében történik, hanem az arányosság követelményének is meg kell felelnie. Alkotmányos követelmény, hogy „az elérni kívánt cél fontossága és az ennek érdekében okozott alapjogsérelem súlya megfelelő arányban legyen egymással."[60]

[56] Alkotmány 8. § (2) bek.
[57] 30/1992. (V. 26.) AB határozat
[58] Szabó, 2004, 85–88.
[59] 20/1990. (X. 4.) AB határozat
[60] 30/1992. (V. 26.) AB határozat

Hogyan egyeztethető ez össze azzal az állásponttal, miszerint ha az adatkezelő számára több, az adatkezelési cél megvalósítására alkalmas eljárás is adott, ezen elv nem követeli meg azt, hogy a kevesebb adat kezelésével járó módszert kellene választania a költségekre való tekintet nélkül?[61]

A célhoz kötöttség az adatvédelem garanciája. Csak pontosan meghatározott és jogszerű (törvényszerű) célra lehet adatot gyűjteni, felhasználni stb.[62] Az Avtv. szerint az adatkezelés minden szakaszában meg kell felelnie e célnak. Csakis olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, annak elérésére alkalmas. Fontos eleme a célhoz kötöttség elvének, hogy csak a cél megvalósulásához szükséges mértékben és ideig lehet kezelni ezeket az adatokat.[63] A szükségtelen adatkezelés tehát jogellenes. A taláros testület megállapította, hogy ha a felvett adatok „...megfelelően alkalmasak bizonyítani, azaz a cél elérésére önmagukban elegendő adatok", akkor „a személyi szám közlésének és felhasználásának előírása az adatkezelés céljának megvalósításához már nem szükséges", ezért sérti a személyes adatok védelméhez való jogot, és az Alkotmány 8. § (2) bekezdését.[64] Ezt a gyakorlatot kell az útlevél céljával, annak alkotmányossági problémájával párhuzamba állítani. Az útlevél funkciója kizárólag az egyén azonosítása lehet, amely viszont a korábbi útlevél esetében is maradéktalanul megvalósult.

A „készletre" történő adatfeldolgozás önmagában alkotmányellenes.[65] Az AB gyakorlata szerint két személyazonosító jelrendszer kötelező alkalmazása ugyanarra a célra általában alkotmányellenes, mert sérti az információs önrendelkezési jog lényeges tartalmát. Ez a fajta azonosítás lehetővé teszi az adatfeldolgozó rendszerek összekapcsolását, illetve megnehezítik a jogalany azon jogosultságának gyakorlását, hogy az adatfeldolgozás egész útját figyelemmel kísérhesse, valamint ellenőrizhesse. Ezzel a célhoz kötöttség elve is sérül.[66] Az Avtv. ezzel összhangban mondja ki, hogy „korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása tilos." (Avtv. 7. § (2) bekezdés) Az univerzális személyazonosító természeténél fogva veszélyt jelent a(z alapvető) személyiségi jogokra, még pedig úgy, hogy az adatbázisok összekapcsolása révén lehetővé válik a személyiségprofil kialakítása, amely az emberi méltóságot sérti. Az adatkezelő képes lesz arra, hogy adott személyre vonatkozó adatokat összességükben és összefüggésükben elemezze. Az adatalanyok ezzel teljesen kiszolgáltatottá válnak: a magánéletük lényegében egy nyitott könyv lesz annak minden intim mozzanatával együtt. Egy egyenlőtlen kommunikációs „hatalom" jön létre.

[61] Jóri, 2005, 218.
[62] Sári–Somody, 2008, 134.
[63] A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény 5. § (1) és (2) bekezdés
[64] 29/1994. (V. 20.) AB határozat
[65] Lásd. Előzmények és az Európai Tanács 2252/2004/EK rendelete c. alfejezetet
15/1991. (IV. 13.) AB határozat
[66] 29/1994. (V. 20.) AB határozat

A személyiségi jogok védelme az állam Alkotmányba foglalt elsőrendű kötelessége. Ennek érdekében két feltételnek kell teljesülnie:
1) Egyrészt a biometrikus adatok nem kerülhetnek egy központi nyilvántartásba.
2) Másrészt az államnak kötelessége jogi szabályozás útján intézkedéseket tenni annak érdekében, hogy a visszaalakíthatatlan sablonok előállítása más eljárással történjen az egyik adatkezelőnél, mint a másiknál, azért, hogy a sablonok ne legyenek összehasonlíthatók egymással.[67]

A biometrikus adatok univerzális jellegével kapcsolatosan szeretném megemlíteni, hogy a testület megállapította az általános és egységes, azaz minden állampolgárnak és lakosnak ugyanazon elv szerint kiosztott személyi szám alkotmányellenességét. Hiszen a személyi szám „... mint többcélú személyazonosító technikailag megkönnyítette az egészségi állapotra vonatkozó szenzitív adatok összekapcsolását is az érintett más személyes adataival." Ha ezt párhuzamba állítjuk azzal, hogy az élet számos területén ugyanazt a biometriai adatot használjuk, nem állunk messze a valóságtól, ha azt mondjuk, hogy esetleg a biometriai adatok sorsa a jövőben oszthatja a személyi szám sorsát.[68] Hiszen az ujjlenyomat alapján történő azonosítást is egyre nagyobb teret nyer, így nemcsak az útlevélben, hanem a személyigazolványban, a vízumban, a tartózkodási engedélyben, a beléptető rendszereknél stb. is előfordulhat.

Az ujjlenyomat egyéb szempontú alkotmányossági vizsgálata

Az emberi méltósághoz való jog minden ember veleszületett joga, amelyet a taláros testület az ún. általános személyiségi jog egyik megfogalmazásának tekint. Az általános személyiségi jog aspektusának tekinti még például a személyiség szabad kibontakoztatásához való jogot, az önrendelkezés szabadságához való jogot, az általános cselekvési szabadságot, avagy a magánszférához való jogot.[69] A „magánszférához való jogot" tehát az alaptörvényünk konkrét, szubjektív alapjogként nem deklarálja, de az kétségkívül az egyén autonómiájának védelmére szolgáló olyan alapjog, amely az ember veleszületett méltóságából eredeztethető, amelynek tehát az általános személyiségi jog szubszidiárius alapjoga.[70] Az általános személyiségi jog anyajognak tekintendő, azaz egy olyan szubszidiárius alapjognak, amelyet „mind az Alkotmánybíróság, mind a bíróságok minden esetben felhívhatnak az egyén autonómiájának védelmére, ha az adott tényállásra a konkrét, nevesített alapjogok egyike sem alkalmazható."[71]

Az Alkotmánybíróság a 15/1991. (IV. 13.) határozata óta az információs önrendelkezést közvetlenül az Alkotmány 59. § (1) bekezdésében szabályozott személyes adatok védelméhez fűződő jogból származtatja, míg közvetve az 54. § (1) bekezdésben deklarált, élethez és emberi méltósághoz való jogból vezeti le. Az in-

[67] Szabó, 2004, 91.
[68] 29/1994. (V. 20.) AB határozat
[69] 8/1990. (IV. 23.) AB határozat
[70] 56/1994. (XI. 10.) AB határozat
[71] 8/1990. (IV. 23.) AB határozat

formációs önrendelkezési jog az alkotmányos védelemben részesülő személyiségi jogok közé tartozik, és szoros kapcsolatban áll a magánszférához fűződő joggal.[72]

Az Avtv. személyes adatnak a természetes személlyel kapcsolatba hozható adatot minősíti. Ennél szélesebben definiálja a személyes adatot az egyének védelméről a személyes adatok gépi feldolgozása során Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről szóló 1998. évi VI. törvény 2. cikke, amely bármely olyan információt a fogalom alá esőnek tekint, amely egy azonosított egyénre vonatkozik. Ebből a rendelkezésből sem következik az, hogy például az ujjlenyomatra azonos szabályt kellene alkalmazni, mint az adatokra (pl. név, lakcím stb.).

Az AB már korai határozatai egyikében kifejtette, hogy az emberi méltósághoz való jog az „általános személyiségi jog" egyik megfogalmazása, és „ez a jog szolgáltatja a személyiség védelmének alkotmányjogi alapját minden olyan esetben, amelyben az Alkotmány nem határoz meg külön nevesített jogot" (8/1990. (IV. 23.) AB határozat). Az AB a személyazonosító igazolványról szóló szabályokat vizsgáló határozatában úgy foglalt állást, hogy az azonosító adatok (név, lakcím) elválnak az azonosításnál egyébként szintén szerepet játszó fényképtől és aláírástól (1202/B/1996. AB határozat).

Az 1993. évi XXXI. törvénnyel kihirdetett, az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt Egyezmény nem tartalmazza a személyiségi jogok általános védelmét, és ezt nem is vezette le a 8. cikkben deklarált magán- és családi élet, a lakás és levelezés tiszteletben tartásához való jogból, amelyet azonban a privátszféra védelméről szóló rendelkezésnek tekintett.

„Az Egyezmény 8. cikke megsértésének tekintették azt, hogy a rendőrség valakinek a magánéletéről adatokat őrzött, hogy kihallgatás során ujjlenyomatokat vett és fényképet készített, de a Bizottság nem állapította meg a 8. cikk megsértését akkor, amikor a fénykép tüntetésen résztvevő személyről készült (Friedl v. Austria, No. 15225/89, Commission's Report 19 May 1994, 45–51. pont). Bár a Bíróság gyakorlata az Egyezmény szövegéhez igazodik és ezért eltér az Alkotmány alapján vizsgálandó szabályoktól, annyi megállapítható, hogy a Bíróság a fénykép és a hangfelvétel készítését, nyilvántartásba vételét más esetektől eltérő, sajátos kérdésként kezeli (ezt megerősíti a P.G. and J. H v. The United Kingdom eset, No. 44787/98, amelyben 2001. szeptember 25-én született ítélet, 56–59. pont)."[73]

Az Alkotmánybíróság eddigi gyakorlata alapján az előbb vázoltakat tartom egy lehetséges álláspontnak. Nem látom még annak a veszélyét, hogy a biometrikus adatbázisok összekapcsolásával egy lehetséges személyiségprofilt kialakítsanak, legalábbis az útlevél jelenleg nem rejti magában ezt a kockázatot, hiszen adatainkat nem tárolják még adatbázisban.

[72] 35/2002. (VII. 19.) AB határozat, Dr. Kiss László és Dr. Kukorelli István alkotmánybírók különvéleménye

[73] 35/2002. (VII. 19.) AB határozat, Dr. Erdei Árpád és Dr. Harmathy Attila alkotmánybírók párhuzamos indokolása

További garanciális szempont, hogy a visszaalakítatlan sablonokat eltérő módon képezzék az egyes adatkezelőknél, ezzel elkerülhetővé válik, hogy a biometrikus azonosítás azonos adat folytán se vezessen el a teljes ellenőrzés, totalitás rémképéhez, az emberi méltóság megcsúfolásához.

IRODALOM

Könyvek, tanulmányok, cikkek

- Az adatvédelmi biztos beszámolója 2005, Adatvédelmi Biztos Irodája, Budapest, 2006
- Jóri András (2005): *Adatvédelmi kézikönyv,* Osiris Kiadó, Budapest,
- Lencsés Károly (2005): *Jön a biometrikus útlevél,* In: Népszabadság október 21., 10.
- Nyiri István (1998): A „DNS-ujjlenyomat" — adatvédelem, In: *Belügyi Szemle 3.* szám, 118–121.
- Poór Csaba (2005): Biometrikus útlevelek, In: *HVG.* március 26., 68–69.
- Rech, Elisabeth (2007): Freiheit versus Sicherheit, *Juristl,* november, 5.
- Sári János–Somody Bernadette (2008): *Alapjogok,* Alkotmánytan II., Osiris Kiadó, Budapest
- Szabó Máté Dániel (2004): Biometrikus azonosítás és adatvédelem, *Acta Humana* XV. évf., 1. szám, 81–92.
- Woller János (1997): Kriminalisztikai célú DNS-vizsgálatok és DNS adatbázisok, *Belügyi Szemle.* december, 45–49.

Internetes források

- *A 29. Munkacsoport 3/2007. sz. véleménye a diplomáciai és konzuli képviseletek számára kibocsátott, a vízumokra vonatkozó Közös Konzuli Utasításnak a biometrikus adatok bevezetésével, valamint a vízumkérelmek fogadása és feldolgozása megszervezésének rendelkezéseivel kapcsolatos módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról (WP 134)* (Letöltés forrása, ideje: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp134_hu.pdf 2008. 10. 27.)
- *A hét elejétől itt a biometrikus útlevél* (Letöltés forrása, ideje: http://www.tasz.hu/index.php?op=contentlist2&catalog_id=3097 2007. 10. 20.)
- *An Open Letter To The European Parliament On Biometric Registration Of All EU Citizens And Residents* (Letöltés forrása, ideje: http://www.edri.org/campaigns/biometrics 2008. 10. 17.)
- *Az európai adatvédelmi biztos véleménye a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló 2252/2004/EK tanácsi rendelet módosításáról szóló európai parlamenti és tanácsi rendeletjavaslatról (2008/C 200/01)* (Letöltés forrása, ideje: http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-03-26_Biometrics_passports_HU.pdf 2008. 10. 27.)
- *Az uniós polgárok útlevelének biztonsági sajátosságaira és biometrikus adataira vonatkozó szabványokról szóló tanácsi rendeletre irányuló javaslat* (Letöltés forrása, ideje: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/am/544/544525/544525hu.pdf 2008. 10. 20.)
- *Biometrics and secure travel documents* (Letöltés forrása, ideje: http://www.euractiv.com/en/security/biometrics-secure-travel-documents/article-132063 2008.10. 27.)

• *EU Commission proposal for biometrics in passports* (Letöltés forrása, ideje: http://www.edri.org/edrigram/number2.4/biometrics 2008. 10. 17.)
• *EU's data-protection commissioners concerned about biometrics on smartcards* (Letöltés helye, ideje: http://www.bjhcim.co.uk/news/1/2004/n41006.htm 2008. 10. 27.)
Feltörték a mikrochipes útlevelet (Letöltés forrása, ideje: http://ww.ok.hu/techbazis/hightech/20080807-feltortek-a-mikrochipes-utlevelet.html 2008. 10. 27.)
• *Golembiewski, Claudia–Probst, Thomas: Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen* (Letöltés forrása, ideje: https://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf 2008. 10. 27.)
• *Haraszti: a szabadság korlátozásában Európa túltesz Amerikán* (Letöltés forrása, ideje: http://hvg.hu/itthon/20051122harasztieuropa.aspx?s=hk 2008. 10. 17.)
• *Interinstitutional File about integration of aspects of biometric identifiers in the uniform visa format and in the uniform residence permit for third country-nationals* (Letöltés forrása, ideje: http://www.statewatch.org/news/2005/jan/bio-visas-16257.pdf 2008. 11. 02.)
• *Javaslat a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló 2252/2004/EK tanácsi rendelet módosításáról* (Letöltés forrása, ideje: http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=hu&ihmlang=hu&lng1=hu,mt&lng2=bg,cs,da,de,el,en,es,et,fi,fr,ga,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=461472:cs&page 2008. 10. 27.)
• *Kockázatos a biometrikus útlevél* (Letöltés forrása: http://www.hetek.hu/?q=node/11028 2008. 10. 17.)
• *Mégsem jó a biometrikus útlevél?* (Letöltés forrása, ideje: http://www.nol.hu/cikk/377129 2007. 10. 20.)
• *Munkaanyag a biometrikus azonosítókról* (WP 80) (Letöltés forrása, ideje: http://abiweb.obh.hu/abi/index.php?menu=209 2009. 11. 10.)
• *Nyílt levél az ujjnyomatos útlevelek ügyében* (Letöltés forrása, ideje: http://www.tasz.hu/index.php?op=contentlist2&catalog_id=1216 2007. 10. 20.)
• *Statewatch Analysis: The Legality of the Regulation on EU Citizens' Passports* (Letöltés forrása, ideje: http://www.statewatch.org/news/2004/nov/11biometric-legal-analysis-htm.htm 2007. 10. 10.)
• *Török Csaba projektje* (Letöltés forrása, ideje: http://www.szgti.bmf.hu/~mtoth/download/Hallgatoi%20projektek/T%F6r%F6k%20Csaba%20-%20Biometria.pdf 2009. 12. 20.)
• *Vélemény a 2/2005 vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről szóló európai parlamenti és tanácsi rendeletre vonatkozó javaslatról* (Letöltés forrása, ideje: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp110_hu.pdf 2007. 10. 10.)
• *Vélemény a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló, 2004. december 13-i 2252/2004/EK tanácsi rendelet végrehajtásáról (WP 112)* (Letöltés forrása, ideje: http://abiweb.obh.hu/abi/pdf/nemz/2005/tagallamoktlevelek.pdf 2008. 10. 27.)

Felhasznált jogforrások

- A Magyar Köztársaság Alkotmánya
- A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény
- A külföldre utazásról szóló1998. évi XII. törvény
- Az Európai Tanács 2252/2004/EK rendelete (2004. december 13.)
- 8/1990. (IV. 23.) AB határozat
- 20/1990. (X.4.) AB határozat
- 15/1991. (IV. 13.) AB határozat
- 30/1992. (V. 26.) AB határozat
- 29/1994. (V. 20.) AB határozat
- 56/1994. (XI. 10.) AB határozat
- 35/2002. (VII. 19.) AB határozat
- 832/K/2000 adatvédelmi biztos állásfoglalása
- 290/A/2005 adatvédelmi biztos állásfoglalása
- 1485/J/2005 adatvédelmi biztos állásfoglalása

Módszer	Egyediség	Változatlanság	Hamisíthatóság, Másolhatóság	Megtévesztés	Kényszerítés	Ikrek	Megvalósításuk
DNS	*tökéletes*	*jó*	akár egy hajszálból	másolás	kivédhetetlen	*?*	*bonyolult*
Ujjlenyomat	*szinte tökéletes*	műtét, baleset	*jó*	*jó*	*másik zaj*	*92%*	*működik*
Tenyér	*jó*	műtét, baleset	*jó*	*jó*	észrevehetetlen	*?*	*működik*
Írisz	*tökéletes*	*jó*	*jó*	*jó*	csak a szemet látja	*?*	*működik*
Retina	*tökéletes*	*jó*	*jó*	*jó*	csak a szemet látja	*?*	kényelmetlen
Kézírás	*jó*	változik	*dinamika lehetetlen*	*kizárt*	talán	*megkülönböztethető*	*alakul*
Hang	*jó*	nátha	*jó*	*magnó*	csak a szemet látja	*hallható különbség*	*működik*
Vizuális	*jó*	*jó*	*jó*	*jó*	*látható, hányan vannak*	*elég hasonló*	*túl komplex*

Egyediség azt jelenti, hogy van-e másnak ugyanolyan, mint nekem.
Változatlanság azt mutatja meg, hogy az azonosítandó tulajdonság változik-e.
A hamisíthatóságot abból a szempontból vizsgáljuk, hogy mi kell ahhoz, hogy mások számára a tulajdonság elérhető legyen.
A megtévesztésnél azt elemezzük, hogyan valósítható meg a rendszer kijátszása.
A következő oszlop azt jelzi, hogy kényszer alkalmazásával beengedi-e a rendszer a kényszerítőt.
Az egypetéjű ikrek közti különbségtételre mennyiben van lehetőség.
Az utolsó oszlopban a kivitelezés lehetőségeit, korlátait tüntetem fel.

A dőlt betűvel kiemelt szöveg a pozitív, az eredeti szöveg a negatív jellemzőket jelenti. A szaggatott vonallal jelölt jellemzők hatása az azonosításra nem ismert.

(I. számú melléklet)[74]

[74] Török Csaba projektje (Letöltés forrása, ideje: http://www.szgti.bmf.hu/~mtoth/download/Hallgatoi%20projektek/T%F6r%F6k%20Csaba%20-%20Biometria.pdf 2009. 12. 20.), 32. o.