

Adatvédelem a biometrikus adatok tükrében – különös tekintettel a biometrikus útlevele

Szerző: Nagy Klára

Témavezető: **Dr. Halmi Gábor**, egyetemi tanár

„Nem sokra haladunk azszal, ha egyszerűn csak megpróbáljuk elnyomni mindazt, ami gonosz. Legnagyobb reményünk abban van, hogy kibontakoztassuk mindazt, ami jó.”

Ismeretlen szerző

1. Bevezető gondolatok

A személyes adatok védelméhez való jog mögött nem az adatok, hanem az ember személyiségének és jogainak védelme húzódik meg. A passzív minősége mellett meg kell különböztetni az aktív oldalát is, ez az információs önrendelkezés. A személyes adatok védelme pedig éppen azt a célt szolgálja, hogy meghatározzon olyan korlátokat, amelyen keresztül az állam már nem szólhat bele a magánszférába. Ezzel szemben az információs jogok másik csoportja, a közérdekű adatok nyilvánosságához való jog a közéleti kommunikáció szabadságát és a közélet átláthatóságát hivatott biztosítani. Az egyéni autonómia és a közérdek sokszor összeütközésbe kerül, a konfliktust a jog próbálja feloldani.

A biometrikus rendszerek kiépítésénél is ez történik: a testi integritáshoz való jog és a biztonsághoz való jog, mint közérdek ellentétbe kerül. A biometrikus adatok kezelése olyan súlyosan érinti a személyiséget, hogy fokozottan szükséges lett volna az ütköző érdekeket a mérleg két serpenyőjébe tenni, de még csak társadalmi vita sem előzte meg – dolgozatom megírásának is ez az egyik oka – pedig ez a szabályozás mintegy 450 millió polgár személyi szabadságát érinti!

Az ember amit tesz, azt a jövőért teszi, de legalábbis annak a jövőben lesz hatása, ezért kell, hogy minden tettet kellőképpen mérlegeljünk. A döntéseket jól átgondolva, megvitatva, a lehetőségeket mérlegelve kell meghozni, mert azután egy rossz döntést, főleg ha az emberek szabadságát ilyen mértékben érinti, nehéz vagy akár lehetetlen helyreállítani.

2. A biometrikus útlevel két elemének áttekintése

2.1. A személyes adat és a különleges adat elhatárolása, az adatkezelés követelményei

A személyes adatok nyilvántartásának, feldolgozásának szabályozása és alkotmányos védelemben való részesítése a modern államok feladata volt, aminek még nagyobb jelentősége lett az elektronikus adatfeldolgozás elterjedésével.¹ Igaz, magánéleti jogokat már a XIX. század elején elismertek angolszász területen, de a jogi koncepció csak a XX. század hetvenes éveiben született meg Európában. A szabályozást elsőként a központi adatgyűjtés biztonságossá tételének követelménye váltotta ki. Az adatvédelmi normák ezután a magánéleti adatok

¹ Sári, 103. oldal

védelmének biztosítása felé fordultak. A harmadik lépés pedig az volt, amelyet ² a 11/1990. (V. 11.) és a 15/1991. (IV. 13.) alkotmánybírósági határozatok is egységesen követnek: a személyes adatok védelméhez való jognak mind a passzív, mind az aktív oldalát (információs önrendelkezési jogot) is figyelembe kell venni. ³

A dolgozatom elején szükségesnek tartom a fogalmi alapvetést. **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, eszerint személyes adatnak minősül

„bármely meghatározott (azonosított vagy azonosítható) természetes személlyel kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés (Avtv. 2. § 1. pont 1. mondat).”

A definícióban talán magyarázatra szorul, hogy a személy mikor azonosítható. Akkor tudjuk az egyént azonosítani, ha a személy neve, azonosító jele, egy (pl. ujjlenyomat) vagy több fizikai, fiziológiai, kulturális, szociális... stb. azonosságára jellemző adata alapján következtetni tudunk személyére. Az embernek ez az adata mindaddig személyes adatnak minősül, amíg a kapcsolata az érintettel helyreállítható.

Ezt az adatfajtát elsősorban a különleges adattól kell elválasztani, amely

„a) a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra,

b) az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkozó adat, valamint a bűnügyi személyes adat (Avtv. 2. § 2. pont).” ⁴

Az ujjlenyomatot ezek alapján a személyes adatok kategóriájába sorolhatjuk, de ha a nemzeti, nemzetiségi és etnikai hovatartozására következtetni lehet, akkor különleges adatnak minősül. ⁵ Következésképpen az ilyen adatok kezelésére, tárolására alkalmazni kell az adatvédelmi törvény szabályait. ⁶

A személyes adatok feltárásánál és feldolgozásánál érvényesülnie kell:

- a célhoz kötöttség elvének, azaz csak pontosan meghatározott és jogszerű (törvényszerű) célra lehet adatot gyűjteni, felhasználni...stb. ⁷

Az Avtv. szerint az adatkezelésnek 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. ⁸ A szükségtelen adatkezelés tehát jogellenes, ezért törölni kell.

² Sándor, 4. oldal

³ Sári, 103-104. oldal

⁴ A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény 2. § 1. és 2. pontja

⁵ Dr. Nyiri, 118. oldal

⁶ Szabó, 85. oldal

⁷ Sári, 104. oldal

⁸ A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény 5. § (1) és (2) bekezdése

Jogszabály-értelmezéssel azt a konklúziót is levonhatjuk, hogy ha a cél elérése kisebb beavatkozással is elérhető, akkor azt a megoldást kell választani. Az adatok kezelése akkor jár az érintett jogainak legkisebb sérelmével, ha annak nem marad nyoma, vagy az adat az érintett birtokában marad. Ezt támasztja alá a 29. Munkacsoport [Working Party (WP) lásd. 25. oldal] álláspontja is, miszerint elkerülendő a biometrikus adatok adatbázisban történő rögzítése. A beavatkozás mértékét érinti az egyes biometriai adatok azon az alapon történő megkülönböztetése, hogy az mennyire érinti magát a személyiséget. 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.

Az adatfelvétel tisztességességének követelményéből fakad az Avtv. azon szabályozása, ⁹ hogy még az adat felvétele előtt közölni kell az érintettel, hogy az adatszolgáltatás önkéntes-e, ha pedig kötelező, meg kell jelölni azt a jogszabályt, amely ezt elrendeli. Emellett az érintettet egyértelműen és részletesen tájékoztatni kell az adatkezelés céljáról, időtartamáról, az adatkezelő személyéről, és hogy kik azok, akik ehhez hozzáférhetnek. Az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire a tájékoztatásnak feltétlenül ki kell terjednie. ¹⁰

▪ A célhoz kötöttség követelménye mellett fontos, hogy mindenki számára követhető és ellenőrizhető legyen az adatfeldolgozás egésze (mikor, hol, milyen célra használják fel az egyén személyes adatait). ¹¹

▪ Az érintett tudatos hozzájárulása is elengedhetetlen, amelynek kifejezettnek, határozottnak, önkéntesnek ¹² és félreérthetetlennek ¹³ kell lennie, (valamint különleges adat esetén írásban kell történnie). Vannak viszont olyan biometrikus adatok, amelyek az érintett tudta nélkül is gyűjthetők (pl. ujjlenyomat a pohárról), ezért is lényeges a törvényi feltételek fennálljanak minden egyes adatgyűjtésnél. ¹⁴ Fontos kikötés még, hogy az adatok mindig csak arra a célra használhatók fel, amelyhez az érintett hozzájárulását adta, ¹⁵ (az önkéntesség néha megkérdőjelezhető, pl. munkahelyre pályázókat az egzisztenciájuk szorítja rá arra, hogy a beléptető rendszerrel felszerelt munkahelyen dolgozzanak).

▪ Törvény azonban kivételesen elrendelheti a személyes adat kötelező kiszolgáltatását, és előírhatja felhasználásának módját, de mindez nem ütközhet a **Magyar Köztársaság Alkotmányának** 8. §-ába: ¹⁶

„8. § (1) A Magyar Köztársaság elismeri az ember sérthetetlen és elidegeníthetetlen alapvető jogait, ezek tiszteletben tartása és védelme az állam elsődrendű kötelessége.

(2) A Magyar Köztársaságban az alapvető jogokra és kötelességekre vonatkozó szabályokat törvény állapítja meg, alapvető jog lényeges tartalmát azonban nem korlátozhatja.”

⁹ Szabó, 85-88. oldal

¹⁰ A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény 6. § (1) és (2) bekezdése

¹¹ Sári, 104. oldal

¹² Kerekes – Zombor, 47. oldal

¹³ Szabó, 88. oldal

¹⁴ Munkaanyag a biometrikus azonosítókról (WP 80) (abiweb.obh.hu/abi/index.php)

¹⁵ Kerekes – Zombor, 34. oldal

¹⁶ Sári, 105. oldal

Rendkívüli állapot, szükségállapot vagy veszélyhelyzet idején bizonyos alapvető jogok gyakorlása felfüggeszthető vagy korlátozható, ilyen az Alkotmány 59. § (1) bekezdése által deklarált mindenkit megillető magántitok és személyes adatok védelméhez való jog is.¹⁷ Az Alkotmányon kívül más törvényeink is szankcionálják a személyes adatokkal kapcsolatos sértéseket. A Polgári Törvénykönyv így kimondja, hogy adatkezelés – és feldolgozás a személyhez fűződő jogokat nem sértheti. A Büntető Törvénykönyv a jogosulatlan adatkezelést és a különleges adatokkal való visszaélést bűncselekménnyé nyilvánítja a 177/A. §-ában, illetve a 177/B. §-ában.¹⁸

A fentebb említett rendelkezések és egyébként az adatvédelmi szabályozás egésze összhangban van az Európai Tanács jogalkotási gyakorlatával. Az **Európai Tanács Adatvédelmi Egyezményének** 2. cikkének a) pontja szerint személyes adat minden azonosított vagy azonosítható személyt érintő információ. Az Egyezmény 6. cikke azt is előírja, hogy nem szabad automatikusan kezelni azon személyes adatokat, amelyekből faji eredetre lehet következtetni, hacsak belső jog megfelelő biztosítékot nem nyújt. Azt a következtetést vonhatjuk le ebből, hogy eltérni ettől a rendelkezéstől akkor lehet, ha erről az érintett ország törvénye rendelkezik, és arra egy demokratikus társadalomban szükség van.

A Schengeni Egyezmény 3. cikke is tartalmazza, hogy személyes adatot külföldi adatkezelő részére csak akkor lehet továbbítani, ha az érintett ahhoz hozzájárult, vagy a törvény azt lehetővé teszi, feltéve, hogy az adatkezelés feltételei a külföldi adatkezelőnél minden egyes adatára nézve teljesülnek.¹⁹

Hazánkban a **Rendőrségről szóló 1994. évi XXXIV. törvény VIII. fejezete** tartalmazza a személyes és különleges adat kezelésére vonatkozó szabályokat, amelyben a rendőrség kap felhatalmazást ezen adatok kezelésére, de csakis a törvényben meghatározott bűnüldözési feladatainak ellátása érdekében és ideig kezelheti. A törvény azt is meghatározza, hogy mely esetekben milyen adatot lehet rögzíteni. A példa kedvéért kiemelnék egy ilyen lehetséges esetet: a szándékos bűncselekmény elkövetésének alapos gyanúja miatt kihallgatott személy adatait, ujjnyomatát, hang- és szagmintáját...stb. a bűncselekmény büntethetőségének elévülésétől vagy elítélés esetén a büntetett előlethez fűződő hátrányok alóli mentesítéstől számított 20 évig lehet kezelni.

A rendőrség – a törvény szerint - külföldi bűnüldözési és igazságügyi szervezeteknek, illetve nemzetközi bűnüldöző szervezeteknek személyes adatot kizárólag nemzetközi kötelezettségvállalás alapján, valamint bűnüldözési érdekből a személyes adatok védelmére vonatkozó előírások és e törvény keretei között továbbíthat.²⁰

*A belügyminiszter pedig abban a tekintetben kapott felhatalmazást, hogy rendeletben szabályozza az adatok levételét, kezelését, tárolását.*²¹

A személyes adatok hosszas tárgyalása után úgy tűnhet, hogy ilyen adata csak természetes személynek van.²² A **34/1994. (VI. 24.) AB határozat** viszont az Avtv. 2. § -ában meghatározott személyes adat fogalmát kiterjeszti a jogi személyekre is, amit azzal indokol,

¹⁷ 1949. évi XX. törvény A Magyar Köztársaság Alkotmányának 8. §-a és 59. § (1) bekezdése

¹⁸ Kerekes – Zombor, 37-38. oldal

¹⁹ Dr. Nyíri, 118-119. oldal

²⁰ A Rendőrségről szóló 1994. évi XXXIV. törvény 84. §-ának c) pontja és 87. §-a

²¹ Dr. Nyíri, 121. oldal

²² Kerekes – Zombor, 34. oldal

hogy „az alapjogok rendszerint a jogi személyekre is vonatkoznak, így az alapjogok alkotmányos védelmét általában a jogi személyek is érvényesíthetik.”²³

Szükségesnek tartom röviden megemlíteni a közérdekű adat fogalmát, amely esetünkben azért érdekes, mert a közérdekre (biztonságra) való hivatkozással vezették be a biometrikus útlevélt, de ettől még nem változik meg a biometrikus adat minősége. Az adatvédelmi törvény a közérdekű adatnak negatív fogalmát adja, amely így hangzik: „az állami vagy helyi önkormányzati feladatot valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó, a személyes adat fogalma alá nem eső adat, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől (Avtv. 2. § 4. pont.)”²⁴

2.2. Az útlevél fejlődéstörténete

A biometrikus útlevél egyik elemet, a biometrikus adatot mint személyes adatot az előző alfejezetben vizsgáltam, most pedig rátérnék a másik összetevőjére, az útlevélre.

Az útlevél kialakulását kutatva a középkorig kell visszamennünk, amikor különféle, az országba történő belépésre, áthaladásra, elhagyásra jogosító engedélyek léteztek. Az engedélyek mellett a tengerészeti és hajózási menleveleknek is nagy gyakorlata volt, amely a járványok elterjedésének megakadályozására is szolgált. Ebben az időben viszont még nem volt egységes igazgatás-rendészeti gyakorlat, csak a XVIII. századra alakult ki, amikor Európában már mindenütt útlevélre volt szükség, kivéve, ha Angliába mentek az emberek. A zarándoklaton lévőknek a lelkipásztorok adtak igazolást, amely szintén azt a funkciót töltötte be, mint az engedély.

A francia forradalom idején az önkény és despotizmus szimbóluma volt. Ennek eredményeképpen az 1791-es francia alkotmány a korlátozás nélküli utazás szabadságát természetes alapvető jogként deklarálta. 1792-ben az első útlevél törvényt is elfogadta a Nemzetgyűlés.

A porosz útlevélrendszer a francia szabályozással ellentétben szigorú volt. Útlevélkényszer volt, és idegenkönyveket kellett vezetni. Szállást is például csak azok kaphattak, akik rendelkeztek útlevéllel.

Az I. világháborúig aztán a jelentősége csökkent. Lassanként felszámolták az emberek röghöz kötöttségét, és a szabad költözködés joga polgári joggá vált országon belül. Az útlevél, mint okmány gyakorlatilag az I. világháborút követően minden különösebb nemzetközi kodifikáció és nemzetközi jogi kétoldalú szerződés nélkül alakult ki a mai napig is ismert formájában, funkciójában.²⁵

Az útlevél szavunk a passeport szó fordítása, amely a passer (áthaladás) és port (kapu) szavak összetételéből keletkezett.

Az úti okmány és az útlevél a rész-egész viszonyában áll egymással. „Úti okmány az útlevél, valamint nemzetközi szerződésben, továbbá a kormány rendeletében meghatározott, a külföldre utazásra, illetőleg az onnan való visszatérésre jogosító hatósági igazolvány, bizonyítvány vagy irat.” Vagyis az útlevél mellett az úti okmány a jelenlegi szabályozás alapján magában foglalja a határátlépési igazolványt, a hazatérési igazolványt, a menekültként elismert személyek kétnyelvű úti okmányát, bevándorolt, letelepedett és hontalan külföldi úti okmányát és a személyazonosító okmányt. Az útlevélnek alapvetően két fajtája van: magánútlevél és a hivatalos útlevél. A

²³ 34/1994. (VI. 24.) AB határozat

²⁴ A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény 2. §-a

²⁵ Dr. Hargitai, 712-713. oldal

magánútlevélben belül külön kell kezelni az ideiglenes magánútlevelet, a hivatalos útlevél speciális fajtái pedig a diplomata, a külügyi szolgálati, szolgálati és hajós szolgálati útlevél.²⁶

Az útlevél a külföldre utazást és a hazatéréshez való jogot biztosítja, illetve a külföldön tartózkodóknak is védelmet nyújt (konzuli védelem). A két előbbi funkciót először az 1948. december 10-én elfogadott Emberi Jogok Egyetemes Nyilatkozatának 13. cikke (2) bekezdésében mindenkit megillető jogként deklarálták, ezt követően az Egyesült Nemzetek XX. ülészakán 1966. december 16-án elfogadott „*Polgári és Politikai Jogok Egyezségokmánya*” 12. cikkében. A magyar Alkotmányba és az 1998. évi XII. törvénybe is belefoglalták.²⁷ Az említett funkciók mellett az állampolgárság igazolására is szolgál.

Napjainkban két tendencia figyelhető meg. Az egyik szerint a személyazonosító igazolványok használatával az útlevelek használata háttérbe szorult, hiszen a magyar állampolgároknak 2004. május 1-jétől az Európai Unión belül, illetve Liechtensteinbe, Norvégiába és Izlandba utazva nem kell útlevél.²⁸ Ugyanakkor egy időben felmerült a tagállami útlevél bevezetése, de erre nem került sor.²⁹ A másik tendencia pedig a biometrikus azonosítókat is tartalmazó útlevelek követelménye, amely e téren szigorítást jelent.³⁰

Az a tétel, miszerint az adott állam szuverén hatáskörében szabályozza a beutazást, és annak konkrét esetekben való engedélyezését, már nem biztos, hogy napjainkban teljes egészében megállja a helyét, hiszen a biometrikus útlevél bevezetésével egy bizonyos kört ki akarnak zárni, de ebben nem a szuverenitása körében határozott Magyarország (sem). Az útlevél tulajdonosa továbbra is a Magyar Állam, az állampolgár csak birtokolja.³¹

3. A biometrikus útlevél

3.1. 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, ma pedig már ellenőrzési, bizonyítási, igazolási, azonosítási célul is szolgálnak. Fennáll annak a veszélye, hogy teljesen mindennapivá válik. A 29. Munkacsoport felhívta erre a figyelmet, amelyet azzal a példával illusztrált, ha a gyermekek az iskolai könyvtárba is biometrikus adataik szolgáltatásával lépnek be, a későbbi életükben sokkal kevésbé lesznek elővigyázatosak a személyes adataikat illetően, mivel ez már számukra természetes lesz.

A biometrikus adatokra jellemző, hogy

- univerzálisak - abban az értelemben, hogy ilyen adatokkal mindenki rendelkezik,
- az univerzalitás mellett viszont egyedi is, azaz mindenkinek különbözőek ezek az adatai, az adott személyt egyértelműen megjelölik,
- és általában elmondhatjuk, hogy ezek nem változnak, tartósan és változatlanul megmaradnak minden személynél. Ez az állítás nem minden biometrikus adatra

²⁶ Gúr, Belügyi Szemle 57-58. oldal

²⁷ Gúr, Európai Jog 18. oldal

²⁸ Gúr, Belügyi Szemle 58-59. oldal

²⁹ Gúr, Európai Jog 20-21. oldal

³⁰ Gúr, Belügyi Szemle 58. oldal

³¹ Gúr, Európai Jog 18. oldal

igaz, de azonosítási célokra (elvileg) csak ilyenek használhatók fel, hiszen az ujjlenyomat is változik, de erre még később visszatérek.³²

A biometrikus útlevelelről szóló WP 80 állásfoglalás a biometrikus adatokat a következőképpen határozza meg: „*Biometrikus adatok a személyes adatok olyan különleges fajtái, melyek egy adott személy magatartási jellegzetességeire, élettani, fiziológiai ismertetőjegyeire vonatkoznak. A biometrikus adatokat leggyakrabban igazolásra, azonosításra használják fel (például beléptető rendszereknél ellenőrzéshez).*” Tehát a biometrikus technikák egyrészt a személy magatartását elemzik (például aláírás, járáselemzés), másrészt a fiziológiai jellemzőit (például ujjlenyomat igazolása, retinaelemzés, hangfelismerés, DNS minták elemzése).³³

A biometrikus azonosításra leggyakrabban a kéz, a szem, az arc, az aláírás, a hang vizsgálata és a DNS-azonosítás alapján kerül sor.

- I. A kéz vizsgálata több mint 100 éves múltra tekint vissza, ami történhet egyrészt ujjlenyomat, tenyérlenymat alapján, ilyenkor az ujjbegy, illetve tenyér mintázatát jegyzik fel, ami ujjlenyomat esetén körülbelül 40-60 pontot jelent, de már 8-12 pont esetén azonosítható az érintett. A pontokból ugyanakkor nem állítható helyre az eredeti ujjlenyomat, ezért nem tartják a támogatói ezt a módszert személyiségi jogokat sértőnek. Másrészt a kézgeometria is pontos azonosítást tesz lehetővé. Ugyanakkor az ujjlenyomathoz a kesztyű viselése megakadályozza a pontos felismerést, a tenyérlenymathoz pedig a rendszert megzavarhatja gyűrű viselése, illetve a nyomás nagysága, a kéznedvesség változása is.
- II. A retina is szolgálhat biometrikus adatként, amit egy alacsony intenzitású fényforrással tapogatnak le, amely idő alatt a fejet nem lehet megmozdítani, és egy adott pontra kell összpontosítani. Az íriszletapogatásnál nincs fizikai kapcsolat a szem és a letapogató eszköz között. Mindkét esetben pontos képet kapunk.
- III. Az arc vizuális felismerése egytetű ikrek esetében nem lehetséges, viszont az arc-thermogrammal olyan felvételt lehet készíteni, ami az arc hőterképét rögzíti. Ez nem változik meg akkor sem, ha a testhőmérséklet esetleg nőne, vagy csökkenne. Ez a legpontosabb módszer az azonosításban, de nagyon költséges.
- IV. Az aláírás ellenőrzése alapján annak tulajdonosa szinte teljes bizonyossággal megállapítható - a hibaarány 1% alatt van - akkor is, ha a két aláírás teljesen azonosnak tűnik, hiszen az írás dinamikáját, idejét, alak- és mozgáseltéréseit nem lehet utánozni. Ehhez viszont nagyon bonyolult és megfizethetetlen berendezésre van szükség.
- V. Hanganalízis során az akusztikai jellemzők vizsgálata sok millió műveletet jelent, mégis rövid ideig tart, de a háttérzaj, rekedtség, esetleg hangfelvétel módosíthatja az ember hangját.
- VI. DNS-minta elkészítése 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.³⁴ A DNS-vizsgálatok a büntetőeljárásban terjedtek el, hiszen ez a módszer segíti a bűncselekmény elkövetőjének kézre kerítését, míg másokat egyértelműen kizár az elkövetői körből. Az elkövetést is visszaszoríthatja, hiszen a bűncselekmények elkövetésében annak lehet visszatartó hatása, ha elkövetőket elfogják, és nem annak, hogy milyen szigorú a büntetés. A bizonyítékok megbízhatósága a bíróság előtt sokkal nagyobb, így a lakosság bizalma a bírósággal szemben nőhet.³⁵

³² Szabó, 82- 83. oldal

³³ Munkaanyag a biometrikus azonosítókról (WP 80) (abiweb.obh.hu/abi/index.php?menu=209)

³⁴ www.szgti.bmf.hu/~mtoth/download/Hallgatoi_projektek/Török_Csaba-Biometria.pdf Török Csaba projektje

³⁵ Woller, 46. oldal

A biometrikus adatok előnyeit és hátrányait mérlegelve határoznak egyik vagy másik mellett az azonosításnak ezt a formáját választók (I. számú melléklet).³⁶

A biometrikus adatok kezelését tehát nem minden esetben kell szükséges rossznak tekinteni, hiszen adatvédelmi célokat is szolgálhatnak. Erre lehet példa, amikor több személyes adat együttes kezelésének helyettesítésre irányul.

A biometrikus adatok felvételét több fázisra különíthetjük el. Az első fázisban készül el a biometrikus minta. Ebből a nyers adatokat tartalmazó mintából valamilyen algoritmus segítségével kiemelnek bizonyos számú jellemzőt, 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.³⁷ A folyamat végén csak egy vektortérkép marad az ujjlenyomat meghatározó pontjaival, ezt a számítógépek számára értelmezhető számsorokká, algoritmusokká alakítják át, és a chipen rögzítik.³⁸ 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 (a személyazonosság megállapítása csak ilyen módon érhető el),
- magukon az azonosítást végző eszközön, illetve
- valamilyen adathordozón (pl. mágnescsíkos vagy mikrochipes kártyán) történő tárolás. Ez utóbbi esetben az érintettek maguknál tarthatják a sablonjukat.³⁹

A központi tárolás esetén probléma lehet, hogy nincs meg mindenhol a műveletek elvégzéséhez szükséges gyorsaságú számítógépes hálózat, illetve kezelni kell valahogyan a hálózatkiesését is. Az olvasóeszköz ezzel szemben viszonylag gyors, ugyanakkor fennakadások, újbóli regisztrációk, esetleg adatvédelmi aggályok merülhetnek fel, ha az eszköz nem vagy rosszul működik. Adathordozón történő tárolásnak is meg van a maga hátránya, hiszen elveszthető, ellophatják, ugyanakkor adatvédelmi szempontból ez a legelfogadhatóbb.

Az ellenőrzés vagy azonosítás végrehajtásához valamely adatunkat kéri az azonosító berendezés, azt összeveti a rendszerben tárolt másik adattal, vagy összeméri a két adatot. A tranzakciót végül regisztrálja, és tárolja vagy maga a leolvasó berendezés vagy valamilyen más számítógépes hálózat.⁴⁰

Az adatkezelő köteles az adatok felvétele, tárolása, kezelése alatt az adatok biztonságáról gondoskodni mind technikai, mind szervezeti-eljárési értelemben. Így garanciálisan szabályozni kell a jogosulatlan hozzáférés, megváltoztatás, továbbítás, törlés, megsemmisítés, megsemmisülés ...stb. eseteit. Ha például egy ujjlenyomatot a rendszer nem a hozzá tartozó személyhez köt, akkor a továbbiakban ez a személy fog hozzáférni ahhoz, amihez az ujjlenyomat tulajdonosának kellene, ez pedig elvezethet a személyiséglopáshoz, hiszen a meglöpött személy ujjlenyomata megbízhatatlan azonosítónak válik. Hiba esetén pedig az adatalanyunk nagyon nehéz bizonyítani, hogy az azonosítás hibás.⁴¹ „Az ilyen automatizált egyedi döntések esetében lehetőséget kell biztosítani az érintettnek álláspontja kifejtésére (Avtv. 9/A. § (1) bekezdés). Ha pedig az esetből bírósági eljárás lesz, az adatkezelés jogszerűségét (így az adatok pontosságát is) az adatkezelőnek kell majd bizonyítani (Avtv. 17. § (2) bekezdés).”⁴²

³⁶ www.szgti.bmf.hu/~mtoth/download/Hallgatoi projektek/Török Csaba-Biometria.pdf Török Csaba projektje

³⁷ Szabó, 84-89. oldal

³⁸ Poór, 68. oldal

³⁹ Szabó, 84. oldal

⁴⁰ www.szgti.bmf.hu/~mtoth/download/Hallgatoi projektek/Török Csaba-Biometria.pdf Török Csaba projektje

⁴¹ Szabó, 89-90. oldal

⁴² A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény 9/A. § (1) bekezdése és 17. § (2) bekezdése

3.2. A biometrikus azonosító rendszerek

A biometrikus azonosító rendszereket olyan eszközök és eljárások összességéként foghatjuk fel, amelyek a személyek mérhető testi tulajdonságait használják fel valamilyen technika segítségével személyek azonosítására vagy személyazonosságának megállapítására. 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 esetben 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.

A biometrikus azonosító rendszerek magukban foglalják a személy fiziológiai tulajdonságait alapul vevő technológiák mellett a viselkedési tulajdonságokat vizsgáló módszereket is, ilyen például a test illatának felismerése, a hangfelismerés, az aláírásminta vizsgálata...stb.⁴³

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 eszközt azonosítja. A kód szerinti felismerés a logikai világ (What You know?) része, amelynek a veszélye az, hogy az ember elfelejtheti, másokkal közölheti azt, így visszaélésekre adhat okot. Az eszköz segítségével történő azonosításnál egy fizikai vizsgálatra (What You have?) kerül sor. Ebben az esetben előfordulhat, hogy magát a dolgot elvesztjük, elfelejtjük magunkkal vinni, ellopják, lemásolják. Többben ezen okokból kifolyólag érvelnek a biometriai azonosítás alkalmazása mellett, de mint lentebb látni fogjuk, a biometrikus rendszernek is van olyan formája, amely valamilyen eszközön tárolja a biometrikus adatot, így az is elveszthető...stb., de a többi fajtájának is meg van a hátránya. A biometriai azonosítót úgy lehet a többitől elhatárolni, hogy az nem ruházható át, mert egyedi biológiai jellemzőket vizsgál (Who You are?).⁴⁴

A biometrikus azonosító rendszereknek három fajtáját különíthetjük el:

- Van olyan, amelyik kombinálja az egyes biometrikus adatfajták felhasználását, pl. ujjlenyomat és hang együttes alkalmazása.
- Lehetséges az is, hogy a biometrikus azonosítást más azonosítási módszerrel egészítik ki, pl. jelszóval, PIN-kóddal.
- A harmadik fajtáját pedig az a csoport képezi, amely a személy birtokában lévő tárgyakat vizsgálja, pl. kulcs, kártya.

Egy másik csoportosítás is elképzelhető azon az alapon, hogy az érintett tudtával vagy tudta nélkül (pl. billentyűleütés vizsgálata) gyűjtik az adatokat.⁴⁵

A biometrikus rendszerek **előzményeként** fogják fel, hogy az évezredes múltra visszatekintő Nílus mentén élők rutinszerűen alkalmazták az azonosításnak ezt a módját a mindennapi üzlet során, mint pl. gabonavételnél a vásárlókat sebhely, arcvonás alapján azonosították.

⁴³ Szabó, 83. oldal

⁴⁴ [www.szgti.bmf.hu/~mtoth/download/Hallgatoi projektek/Török Csaba-Biometria.pdf](http://www.szgti.bmf.hu/~mtoth/download/Hallgatoi%20projektek/Török%20Csaba-Biometria.pdf) Török Csaba projektje

⁴⁵ Szabó, 84. oldal

Ezt követően a kriminológiában jelent meg a kriminálantropológiai irányzat, amely egyes emberi jellemzők alapján az egyént stigmatizálta. Napjainkban a büntetőeljárásban létezik az ujjlenyomat alapján történő azonosítás.

A technika fejlődésével a kézgeometria olvasót alkalmazták először, az 1990-es évektől terjedtek el a biometrikus azonosító rendszerek, amelyek előnyeit a támogatói a következőkben látják, de ezeket én meg is cáfolnám:

- Egyszerűbbnek tartják, mint más azonosítási módszert. Szerintem viszont, ha egy ellenőrzési folyamatba egy újabb fázist ültetnek be- aminek nem az a célja hogy a folyamatot lerövidítse – nem egyszerűsödhet az ellenőrzés.
- Pontosságát is kiemelik, arra hivatkozva, hogy nem lehet könnyen becsapni. Ezt azzal támasztják alá, hogy nagyon kicsi, szinte lehetetlen, hogy két DNS-készlet azonos legyen. Egy későbbi fejezetben majd megmutatok néhány olyan lehetőséget, amivel a rendszert ki lehet játszani.
- A költséghatékonyságot is említik, amit részben el tudok fogadni, abban az esetben, ha egy vállalat beléptető rendszert alkalmaz olyan célból, hogy a munkából kimaradókat kiszűrje, és így az általuk okozott kár esetleg nem következik be. Ezt a formáját viszont azért tartom elfogadhatatlannak, mert véleményem szerint előállhat az a helyzet, hogy más módszert is alkalmaznak ebből a célból, akkor pedig a szükségesség-arányosság elve sérül.

A felhasználói pszichológia szerint a tapasztalatok azt mutatják, hogy az emberek még idegenkednek ezen új azonosítási módszernek a bevezetésétől. Azt állítja, hogy ha az ember nem örül valaminek, akkor azt nem a rendeltetésének megfelelően fogja használni, ez pedig a biometrikus azonosító berendezéseknél nagyobb hibaarányal járhat. Azt tanácsolják ennek megelőzésére, hogy oktatásban kell részesíteni a rendszer használóit, és további tájékozódásra is meg kell adni a lehetőséget.⁴⁶ Ehhez csak egy rövid megjegyzést tennék hozzá: nem hallottam még olyan továbbképzésről, ahol a hétköznapi embereket a biometrikus azonosító rendszerek alkalmazásáról vagy éppen a biometrikus útlevélről oktatták volna.

3.3. A biometrikus útlevél fogalma, jellemzői

A biometrikus útlevél az emberi test biometrikus adatait tartalmazza (, ilyen például az ujjlenyomat, az arc, az emberi test formája, a testrészek egymáshoz viszonyított aránya), amelyeket elektronikusan, egy chipen az útlevél belsejében helyeznek el.⁴⁷ A mostani szabályozás alapján az útlevélbe bekerül a digitális arckép mellett az ujjlenyomat is.

Az ujjlenyomatvétel a lakosság körében aggályokat vet fel, hiszen az embereknek a bűnügyi nyilvántartás jut erről eszükbe, de azt meg kell 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.⁴⁸

Ennél viszont nagyobb gond, hogy kisgyermeknél és időseknél nagy a hibaszázalék, amelyet akkor lehetett volna kiküszöbölni, ha második azonosítóként a szívrághártyát határozzák meg⁴⁹, amely esetében 131 ezerre jut egy hiba,⁵⁰ de erre adatvédelmi okokból nem

⁴⁶ www.szgti.bmf.hu/~mtoth/download/Hallgatoi projektek/Török Csaba-Biometria.pdf Török Csaba projektje

⁴⁷ Lencsés, 10. oldal

⁴⁸ Dr. Nyíri, 118. oldal

⁴⁹ Lencsés, 10. oldal

⁵⁰ Poór, 68. oldal

került sor.⁵¹ Retinaazonosításkor pedig a tévedés aránya egy a 10 millióhoz. Igaz, az orvosoknak egy csoportja azt állítja, hogy a retina képe változhat, míg az íriszé nem.⁵² Más tanulmányok azt az elméletet képviselik, hogy az ujjlenyomat alapján lehet az embert leginkább azonosítani.⁵³ Mégsem ezen orvosi kérdések alapján döntöttek az ujjlenyomat mellett, hanem az adatfelvétel egyszerűsége miatt. Hiszen a szem jellegzetességeit csak kellemetlen, illetve a cukorbetegség estében az egészséget veszélyeztető módon lehetett volna megállapítani.⁵⁴ 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.⁵⁵

A bírálói hangsúlyozzák azt is, hogy nem megbízható. Erre példaként hozzák fel, hogy megesett már, hogy az eljárásban nőt férfiként azonosított. Az arcfelismerő rendszert ki lehet úgy játszani, hogy a kamera elé fényképet tartunk, illetve az ujjlenyomat-leolvasót egy emberi ujj műanyag másolatával.

A biometrikus útlevelel a terrorizmus elleni hatékonyságát is sokan megkérdőjelezi azon az alapon, hogy csak a már nyilvántartásba vett bűnözőket, illetve hamis úti okmánnyal érkezőket szűrnie ki, míg a 2001. szeptember 11-i támadás elkövetői legalisan érkeztek az Egyesült Államokba.

A biometrikus eljárással szemben ellenérvként hozzák fel azt, hogy a számítógépes adatazonosítás nem mindenhol működik a gyakorlatban. Tel-Avivban a Ben Gurion repülőtéren évente mindössze 1 millió utas van, míg az USA egyik repülőtérén több mint 200 millió.⁵⁶

Tartani kell attól, hogy az ember egyediségére vonatkozó adatok kiszolgáltatása általánossá válik. Ezt támasztja alá az is, hogy az Európai Unió kívül más szervezetek (pl. Gazdasági Együttműködési és Fejlesztési Szervezet (OECD)) is tárgyalnak a biometrikus adatok felhasználásáról, itt a cél viszont már nem a terror megfékezése.⁵⁷ 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 700 000-et. Angliában pedig néhány önkormányzat bevezette az ún. „polgárkártyát”, amivel a helyi üzletekben a kártyatulajdonos kedvezményekben részesül, vagy bizonyos szolgáltatásokat igénybe vehet... Egyre több gépjárművezetői engedélybe is bekerül a chip a másolás megnehezítése céljából. Ide sorolhatjuk az indításgátlóval felszerelt gépkocsikat is. A jogtalan igénylők kiszorítása érdekében a támogatási rendszerben is terjed. A pénzkidő automatáknál is alkalmazzák már az azonosításnak ezt a módját, de erre még nem került sor, ezt azzal magyarázzák, hogy az emberek idegenkednek tőle.⁵⁸

Azt is külön kell szabályozni, hogy a sérült kezű személyekkel kapcsolatosan az általános szabályok hogyan érvényesülnek.⁵⁹

A rendszer kiépítése rengeteg költséggel jár. Németországban ez 700 millió eurót jelent, Magyarországon 2-20 milliárd forintba teszik. Kiadást jelent az adatfelvétel, -feldolgozás, -tároláshoz kapcsolódó berendezések, szoftverek beszerzése, karbantartása... stb.⁶⁰

⁵¹ Lencsés, 10. oldal

⁵² Poór, 68. oldal

⁵³ Útlevelel digitális ujjlenyomattal, Világ gazdaság 2005. szeptember 23. 4. oldal

⁵⁴ Poór, 68. oldal

⁵⁵ www.tasz.hu/index.php?op=contentlist18&catalog_id=3097 A hét elejétől itt a biometrikus útlevelel

⁵⁶ Poór, 69. oldal

⁵⁷ Szabó, 82. oldal

⁵⁸ www.szgti.bmf.hu/~mtoth/download/Hallgatoi_projektek/Török_Csaba-Biometria.pdf Török Csaba projektje

⁵⁹ Ujjlenyomat az útlevelelben, Magyar Hírlap 2004. december 3. 15. oldal

⁶⁰ Poór, 69. oldal

A sok ráfordítással járó technika biztonságos voltát egy augusztus elején tartott konferencián Lukas Grunwald, a számítástechnikai rendszerek szakértője megkérdőjelezte azzal a kijelentésével, hogy sikerült feltörnie az új német biometrikus útlevélet, 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.⁶¹

Ennek tükrében feltenném az általam költőinek tartott kérdést: alkalmas a biometrikus adatot tartalmazó útlevél a cél elérésre?

Mindezek ellenére az okmányt minden eddiginél biztonságosabbnak tartják.⁶²

Az Európai Unió szabályozással kapcsolatos vélemények is 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.⁶³

4. A biometrikus útlevél megjelenése és szabályozása az Európai Unió területén

Az EU-t az Amerikai Egyesült Államok készítette a biometrikus útlevél bevezetésére, hiszen vízummentesen csak ezen okmány birtokában lehet a nagyhatalom területére lépni.⁶⁴ A vízummentesség fenntartásához feltételként szabták a Nemzetközi Polgári Légiközlekedési Szervezet (ICAO) előírásainak teljesítését. Az USA elvárásai között szerepelt legalább egy biometrikus adat útlevélben történő rögzítése, amelynek eredetileg 2004 októberétől kellett volna eleget tenniük az európai országoknak. Az Európai Bizottság viszont ennek a határidőnek a megváltoztatásáról kezdeményezett tárgyalást az Egyesült Államokkal. Az USA e kötelezettség 2004. októberi számonkérését így egy évvel elhalasztotta. Ez a határidő leginkább azokat az országokat érintette, amelyek részei az amerikai vízummentes programnak (VWP): a tizenöt régi EU-s tagország, kivéve Görögországot, de beleértve Szlovéniát.

A másik ok, hogy a chipes útlevél bevezetésre került az, hogy az EU biztonság- és bevándorlás-politikai megfontolásait is szolgálja.⁶⁵ 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 kiválmait. Brüsszelben már két évvel ezelőtt megállapodtak abban, hogy az útlevél két biometrikus azonosítót fog tartalmazni. A Bizottság az ujjlenyomatot csak lehetőségként vetette fel, amely a tagállamok mérlegelésétől függött. Ezzel együtt egy központi adatbázis létrehozására is tett javaslatot, amely az európai polgárok összességének - tehát nem kevesebb, mint 450 millió uniós polgár ujjlenyomatát tartalmazta volna. Az intézményt egyelőre nem hozzák létre.

Az útlevél mellett a vízum és a tartózkodási engedély biometrikus azonosítóval történő ellátása is napirenden volt az Unióban.⁶⁶ 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

⁶¹ www.tasz.hu/index.php?op=contentlist18&catalog_id=3097 A hét elejétől itt a biometrikus útlevél

⁶² Lencsés, 10. oldal

⁶³ 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 (ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp110_hu.pdf)

⁶⁴ Útlevél digitális ujjlenyomattal, Világgazdaság 2005. szeptember 23. 4. oldal

⁶⁵ Lencsés, 10. oldal

⁶⁶ www.edri.org/edriagram/munber2.4/biometrics EU Commission proposal for biometrics in passports

elő. A technikai megoldások megtervezésével, kivitelezésével az Európai Bizottság által felállított, tagállami szakértőkből álló testület foglalkozott.⁶⁷

Több szervezet, köztük a **Privacy International, a Statewatch, az European Digital Rights** az Európai Parlamentnek címzett **nyílt levélben** a szabályozás alapját kérdőjelezi 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 rendelkeznek. Felhívja arra is a figyelmet, hogy 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.

A központi adatbázis létrehozása esetén a Közösség visszaéléseknek adna táptalajt, és így még egyszerűbb lenne az emberek adatait beleegyezésük nélkül gyűjteni. Az arcfelismerés estén pedig következtetni lehet a faji és etnikai eredetre, ami pedig az Európai Unió jogában az egyik legérzékenyebb természetű adat. Problematikusnak tartották azt is, hogy útlevélújításnál postán küldik meg az érvényeset. Utaltak arra is, hogy az ujjlenyomat megbízhatatlansága egy megrázó eset kapcsán be is bizonyosodott: a 2004. március 11-i madridi vonatrobbanás 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.

A levelükben ráirányították arra is a figyelmet, hogy egy 2003-ban tartott nemzetközi konferencián deklarálták, hogy a terrorizmus és szervezett bűnözés elleni harcban az országoknak az alapvető adatvédelmi elveket tiszteletben kell tartaniuk.⁶⁸

Felhívásához csatlakozott számos nyugat-európai ország közt Magyarország jelenlegi adatvédelmi biztosa, Péterfalvi Attila és elődje, Majtényi László is.⁶⁹

Az emberi jogok a demokráciamozgalomban húsz évvel ezelőtt – Az emberi jogok
c. 2005 novemberében megtartott kétnapos **konferencián** is napirendre került a biometrikus azonosítót tartalmazó útlevelel 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 megnyírbálja a szabadságjogokat, mint a 2001. szeptember 11-i terrortámadás után elfogadott „hazafias” törvény, Patriot Act. Haraszti leginkább az háborítja fel, hogy az európaiak nem is elleneztek ezeket az intézkedéseket. Ezt valószínű az is befolyásolja, hogy jó eszköznek látják a terrorizmus és menekültek problémájának megoldásához, míg az amerikaiak már megtanultak ezekkel a problémákkal együtt élni.⁷⁰ Prof. Steven Peers szerint az Európai Közösség túllépi hatáskört azzal, hogy ilyen intézkedéseket vezet be, valamint sérti a közösségi jog általános elveit, amelybe beletartozik a magánélethez fűződő jog védelme.

Az **EK Alapszerződésének** 18. cikk (3) bekezdése is egyértelműen kizárja a Közösségnek - a szabad mozgás területén történő rendelkezéseknél - az úti okmányra vonatkozó szabályok megalkotását:

⁶⁷ www.tasz.hu/index.php?op=contentlist18&catalog_id=3097 A hét elejétől itt a biometrikus útlevelel

⁶⁸ www.edri.org/campaigns/biometrics An Open Letter to the European Parliament on Biometric Registration of all EU Citizens and Residents

⁶⁹ Ujjlenyomat az útlevelelben, Magyar Hírlap 2004. december 3. 15. oldal

⁷⁰ hvg.hu/itthon/20051122haraszti.europa.aspx?s=hk Biometrikus útlevelel, Haraszti: a szabadság korlátozásában Európát túlszár Amerikán

„18. cikk

- (1)(...) minden uniós polgárnak joga van a tagállamok területén való szabad mozgáshoz és tartózkodáshoz.
- (2) Ha a Közösség fellelése 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.”⁷¹

2004. december 13-án született meg az új útlevél biometrikus és biztonsági tulajdonságait tartalmazó közösségi rendelet (2252/2004 EK rendelet), majd február 28-án ezeket az előírásokat konkretizáló európai bizottsági határozat.⁷²

Már egy 2000. október 17-i állásfoglalás előírja, hogy a tagállamoknak a lehető legkorábban, de legkésőbb 2006. január 1-jétől meg kell felelniük a Tanács meghatározott biztonsági előírásainak. Annak érdekében, hogy az útlevél hamisításával szemben védve legyenek, az Európai Tanács 2003. június 19-20-i thesszaloniki ülésén megerősítette, hogy egységes megközelítésre van szükség a harmadik országbeli okmányokhoz, az uniós polgárok útlevéljeihez, és az információs rendszerekhez (VIS, SIS II) szükséges biometrikus adatok és azonosítók vonatkozásában.⁷³

Luxembourgban az EU tagországok bel-és igazságügy miniszterei képviseltették magukat. Magyarországról Lampert Mónika belügyminiszter és Petrétei József igazságügy miniszter volt jelen.⁷⁴ A szabályozás Európai Parlamentben történt elfogadása során tulajdonképpen a liberálisok és a zöldek maradtak alul. A magyar Európai Parlamenti képviselők közül egyedül Szent-Iványi István szavazott nemmel, ő a biometrikus útlevél bevezetésének veszélyét abban látja, hogy az adatok biztonságos tárolásának nincsenek meg a feltételei.

Az Európai Unió tagállamai eddig azt az elvet képviselték, hogy szabadságukból csak annyit áldoznak fel, amennyi feltétlenül szükséges, ugyanakkor, ahogy ezt a magyar képviselők szavazatai is mutatják, a helyzet teljesen megváltozott. Az említett elvnek az is ellentmond, hogy az Egyesült Államok csak egy azonosítót kívánt meg, az EU pedig kettőt vezet be.⁷⁵

A tagállamoknak a digitális fényképet tartalmazó útlevéllel kapcsolatos előírásokat 2006. augusztus 28-ig kell kivitelezniük, amely előírásokat februárban közzétettek. Az ujjlenyomat szabályozására vonatkozó rendelkezéseket 2006. június 28-án hozták nyilvánosságra. Ezeket a részletszabályok megvalósításra 2009. június 28-ig kaptak az uniós országok haladékot.⁷⁶

4.1. A 95/46/ EK irányelv

A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelvet 1995. október 24-én alkotta meg az

⁷¹ <http://www.statewatch.org/news/2004/nov/11biometric-legal-analysis.htm> Statewatch Analysis: The Legality of the Regulation on EU Citizens' Passports

⁷² Poór, 68. oldal

⁷³ ARTICLE 29 Data Protection Working Party WP 96 (209.85.129.104/search?q=cache:Dty6zaJiXiQJ:cc.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp96_en.pdf+Working+Party+96&chl=hu&gl=hu&ct=clnk&cd=2)

⁷⁴ Ujjnyomatot vesznek az útlevélhez, Népszabadság 2004. október 26. 3. oldal

⁷⁵ Gúr, Európai Jog 21. oldal

⁷⁶ www.tasz.hu/index.php?op=contentlist18&catalog_id=3097 A hét elejétől itt a biometrikus útlevél

Európai Parlament és a Tanács, amelyben meghatározták azt az általános keretet, amelynek a tagországok szabályozásának meg kell felelnie.

Ebben fontos elvként rögzítették, hogy a személyes adatok gyűjtésének törvényesnek és tisztességesnek kell lennie. Meghatározott, egyértelmű és törvényes célból, a cél szempontjából releváns és szükséges mértékű gyűjtés lehet csak megengedett. Az adatfeldolgozási műveletek nyilvánosak. Minden ésszerű intézkedést meg kell tenni annak érdekében – mondja az irányelv, hogy a hibás vagy hiányos adatok javításra, illetve törlésre kerüljenek. Az adatkezelő tájékoztatási kötelezettsége kiterjed saját személyére, az adatfeldolgozás céljára, az adatok címzettjeire, kötelező vagy önkéntes válaszadásra és a helyesbítéshez való jogra.

A tagállamok minden személynek kötelesek biztosítani azt a jogot, hogy automatizált döntés ne terjedhessen ki, ami rájuk nézve jogi hatással járna.

Különleges adat feldolgozását a tagállamok megtilthatják, kivéve, ha az érintett kifejezett hozzájárulását adta, de a tagállam a hozzájárulás lehetőségét ki is zárhatja. A bűncselekményekre, büntetőítéletekre vagy biztonsági intézkedésekre vonatkozó adatok feldolgozása viszont kizárólag hatóság ellenőrzése mellett történhet.

Az irányelv előírja, hogy adatkezelőnek meg kell tenni a megfelelő technikai és szervezési intézkedéseket a személyes adatok véletlen megsemmisülésére, elvesztésére, megváltoztatására, a hozzáférés elleni védelemre és a jogosulatlan nyilvánosságra hozatalra. Az irányelvnek ez egy olyan szabálya, amelynek véleményem szerint szinte bármivel meg lehet felelni, mert a „megfelelő intézkedésbe” sok minden belefér. Igaz, hogy az irányelv csak egy irányvonalat ad, de bizonyos esetekben konkrétabb megfogalmazásra van szükség, főleg, hogy itt az adatok biztonságáról van szó.

Tartalmazza, hogy harmadik országba történő adattovábbításra csak annyiban van lehetőség, ha az ország megfelelő védelmet biztosít.

Minden tagállamnak rendelkeznie kell egy olyan felügyelő hatóságról, amely a nemzeti szabályozás betartását ellenőrzi. A felügyelő hatóság határozatai ellen a bírói út biztosított.

Ez az irányelv hozta létre a személyes adat feldolgozása vonatkozásában az egyének védelmével foglalkozó munkacsoportot. A munkacsoportot az egyes tagállamok által kijelölt felügyelő hatóság vagy annak képviselője, a közösségi intézmények és szervek által létrehozott hatóság vagy hatóság képviselője, illetve a Bizottság egy képviselője alkotja. Határozatait egyszerű többséggel hozza. A munkacsoport hatáskörébe tartozik a nemzeti szabályozás megvizsgálása, arról véleménynyilvánítás, ajánlástétel. Javaslatot tehet a Bizottságnak az irányelv módosítására.

Az irányelv célkitűzéseit 1998-tól kell a tagállamoknak teljesíteni.⁷⁷

4.2. Az Európai Tanács 2252/2004/EK rendelete

Az Európa Tanács a harmonizáció jegyében és az irányelv adta keretek között alkotta meg a 2252/2004/EK rendeletet, amelynek célja a biztonságos biometrikus útlevelek és információs rendszer alapjainak letétele, hiszen a Tanács előírásait azzal összhangban a tagállamok konkretizálják.

A rendelet kimondja, hogy a nemzeti jogszabályok határozzák meg, mely hatóság, illetve szerv az, amely a tároló elemekben rögzített adatokhoz hozzáférhet, de mindezt a közösségi jogra, az Európai Unió jogára, valamint nemzetközi megállapodások vonatkozó rendelkezéseire tekintettel. A tagországoknak egyetlen olyan szervet kell jogszabályban kijelölni, amely az útlevelek előállításáért felel, és fel kell hatalmazni azzal a joggal, hogy szükség esetén más szervre átruházhatja ezt a kizárólagos jogkört.

⁷⁷ A 95/46 EK irányelv

Az érintett országok kötelezettséget vállaltak arra nézve, hogy

„1.cikk

- (1) *A tagállamok által kiállított útlevelek és úti okmányok megfelelnek a (...) meghatározott minimum biztonsági előírásoknak.*
- (2) *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, valóságát és bizalmasságát.”*

A rendelet kötelezi a tagállamokat a biztonsági követelmények és műszaki előírások meghatározására. Az útlevelelben rögzítésre kerülő két biometrikus adat, az arckép és az ujjlenyomat minőségére vonatkozó szabályozást is a tagállamokra bízta. Meg kell jelölni azt a szervet, amely az úti okmányok nyomtatásáért felelős, ezt közölni kell a Bizottsággal és a többi tagállammal. Később lehetőség van a szerv megváltoztatására, de ebben az esetben is úgy kell eljárni, mint a bejelentéskor.

Az úti okmány birtokosának biztosítania kell azt a jogot, hogy az abban tárolt adatokat ellenőrizhesse, szükség esetén pedig helyesbítthesse, illetve töröltethesse.

A tagországoknak az általuk kiállított úti okmányra és útlevelekre kell az Európai Tanács rendeletét alkalmazni a személyazonosító igazolvány és a tizenkét hónap vagy annál rövidebb érvényességi időre szóló, ideiglenes útlevelel, illetve úti okmány kivételével. A rendelet meghatározza, hogy biometrikus jellemzők kizárólag az okmány valóságának ellenőrzésére használhatók fel, valamint az okmány birtokosának személyazonosságának megállapítására „közvetlenül hozzáférhető, összehasonlítható jellemzők segítségével, amennyiben az útlevelek és egyéb úti okmányok felmutatásáról törvény rendelkezik.”

A rendelet teljes egészében kötelező és közvetlenül alkalmazandó a tagállamokban. A rendelet a tagállamok általi elfogadást követő 18 hónapon belül lép hatályba az arckép tekintetében, míg az ujjlenyomat tekintetében legfeljebb 36 hónappal. ⁷⁸

4.3. Az Európai Unió tagországainak szabályozása

A biometrikus útlevelek kibocsátást Németország az elsők között 2005 novemberétől kezdte el, amelyekért az állampolgároknak 59 eurót kell fizetniük, míg ez az USA-ban 79 euró vagy a briteknél 103 euró. A németeknél az útlevelel jelezni fogják, hogy melyik elektronikus. A chip tartalmazni fogja az utazó személy fényképét – amelynél arra is ügyelni kell, hogy szemből készítsék, komoly arcot kell vágni, és kerülni kell a szemüvegen megjelenő fényt -, digitális arcképet, személyes adatait és két ujjlenyomatát, amelyet a legtöbb országban csak később rögzítenek. ⁷⁹

A svájciakkal ellentétben, akik ezt az okmányt öt évre bocsátják ki, az osztrákok tíz évben gondolkodnak. ⁸⁰

Olaszország is részt vesz másik 26 országgal együtt a „vízum nélküli utazás programjában”. Olaszországban a vízum nélküli utazást biztosító biometrikus útlevelekről szóló rendelkezések 2005. október 26-ától lépnek hatályba. A csip tartalmazni fogja a személyes adatokat, egy digitális fényképet és más biometrikus azonosítókat. Külön kiemelném, hogy a cikk „több azonosítót” említ, ugyanakkor nem részletezi, hogy melyek ezek. Ezzel az úti okmánnyal legfeljebb 90 napot lehet eltölteni az amerikai kontinensen akár

⁷⁸ Az Európai Tanács 2252/2004/EK rendelete (2004. december 13.)

⁷⁹ Lencsés, 10. oldal

⁸⁰ Útlevelel digitális ujjlenyomattal, Világgazdaság 2005. szeptember 23. 4. oldal

üzleti okból, akár turizmus céljából látogatott el oda a külföldi.⁸¹ A 2005. október 25-ig kibocsátott útlevelek a lejáratukig érvényesek maradnak, de aki ezután az Egyesült Államokba akar utazni, azt csak ilyen digitális fényképpel ellátott útlevéllel teheti meg.⁸² 2006. október 26-ától pedig már más biometrikus azonosítót is tartalmazó útlevéllel lehet a tengeren túlra utazni.⁸³ Az úti okmány ára változatlan marad.⁸⁴

Hollandia felmérést végzett az ujjlenyomat azonosíthatóságával kapcsolatban. És arra a következtetésre jutottak, hogy a 6 évesnél fiatalabbak és 60 évesnél idősebbek esetében nem elég megbízható. Ez a holland kormányt elbizonytalanította, hiszen ez a módszer funkcióját kérdőjelezi meg. Felmerül a kérdés, arányban áll-e a jogkorlátozás az elérni kívánt céllal.⁸⁵

4.4. A magyar szabályozás

Az Országgyűlés 2003 tavaszi ülészak utolsó napján az üvegzséb-program keretében elfogadta az adatvédelmi törvényt módosításait, amely az európai uniós jogharmonizáció része.⁸⁶ Az uniós joganyagot a magyar jogalkotó az augusztus 29-étől hatályos törvénymódosítással ültette át a magyar jogba.⁸⁷

A módosítás érinti a külföldre utazásról szóló törvényt is. A törvény 7. §-a megjelöli azokat az adatokat, amelyeket egy útlevélnek tartalmaznia kell. A 12 hónapra vagy annál rövidebb időtartamra kiállított magánútlevelek kivételével az útleveleket biometrikus azonosítót tartalmazó tároló elemmel látják el. Szabályozni kellett azt a problémát is, hogy ha az útlevél érvényességi idején belül a tároló elem adattartalmi ellenőrzésre alkalmatlanná válik, nem eredményezheti az útlevél érvénytelenségét, hiszen a leolvasásra alkalmatlan tároló elem esetén a hagyományos útlevél ellenőrzési módszere alkalmazásával továbbra is megbízhatóan megállapítható a kapcsolat az útlevél és birtokosa között. A személyes adatok védelmét szolgálja a törvénynek az az előírása, hogy az útlevélhatóság a tároló elembe rögzített személyes adatokat csak az úti okmány kiadásáig jogosult kezelni, azután törölni kell, míg a Határőrség ezt csak leolvassa.

Az általános szabályozástól eltérő rendelkezések vonatkoznak a biometrikus útlevélre az adatok továbbítására vonatkozóan, eszerint az útlevélhatóság, illetőleg a központi adatkezelő szerv a büntetőügyekben eljáró hatóságoknak, a rendőrségnek, a nemzetbiztonsági szolgálatoknak, a határőrségnek, a vám- és pénzügyőrségnek, a nyugdíjbiztosítási szervnek, a Belügyminisztérium állampolgársági ügyekkel foglalkozó szervének, valamint a menekültügyi hatóságnak nem adhat át adatot. Az útlevélhatóság, valamint a központi adatkezelő szerv az általa nyilvántartott adatot statisztikai célra felhasználhatja, abból ilyen célra, személyazonosító adat nélkül adatot nem szolgáltathat.

Törvényi előírás, hogy a személyes adatok tároló elembe történő tárolását az elérhető legmagasabb szintű technikai módszerek alkalmazásával kell megvalósítani. De ha ez mégsem így történne, nem von maga után szankciót, és egyébként is „az elérhető legmagasabb szint” egy relatív kategória, amibe szinte minden belefér.⁸⁸

⁸¹ milan.usconsulate.gov/pressreleases/PR_ITA_062006_VWP_Oct_26_2006.htm Passaporto biometrico: le norme in vigore per il programma „viaggio senza visto”

⁸² guide.supereva.com/usa/interventi/2006/01/241316.shtml Il passaporto per entrare negli Stati Uniti

⁸³ milan.usconsulate.gov/pressreleases/PR_ITA_062006_VWP_Oct_26_2006.htm Passaporto biometrico: le norme in vigore per il programma „viaggio senza visto”

⁸⁴ guide.supereva.com/usa/interventi/2006/01/241316.shtml Il passaporto per entrare negli Stati Uniti

⁸⁵ www.nol.hu/cikk/377129 Mégsem jó a biometrikus útlevél?

⁸⁶ origo.hu/uzletinegyed/hirek/hazaihirek/20030522tiltakozas.html Személyes adatok uniós jogvédelme

⁸⁷ www.tasz.hu/index.php?op=contentlist18&catalog_id=3097 A hét elejétől itt a biometrikus útlevél

⁸⁸ A külföldre utazásról szóló 1998. évi XII. törvény 7. §-a, 20. §-a, 32/A. §-a

A vázolt módosítások mellett bevezetésre került a közérdekből nyilvános adat fogalma. A módosítás keretében az adatvédelmi biztos hatósági jogkört kapott. A törvény hatályát kiterjesztették minden a Magyar Köztársaság területén folytatott adatkezelésre.⁸⁹ Az adatkezelést a törvény akként határozza meg, hogy „*az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is (Avtv. 2. § 9. pont).*”⁹⁰

A chipes útlevélek kibocsátása 2006 szeptemberében kezdődött, de a korábbi útleveleket az Európai Unióban a lejáratokig elfogadják.⁹¹ Ha a normál típusú útlevelel birtokosának mégis az új útlevelelre lenne szüksége, pl. a miatt, mert az USA-ba utazik, az úti okmány cseréjét illetékmentesen végrehajjták.⁹² Urbán György, a Nemzeti Vízum – és Okmánybizottság elnökének tájékoztatása szerint a magyar biometrikus útlevelel színe az Európai Unió elóírásoknak megfelelően burgundi vörös, és felirat utal rá, hogy európai unió ország bocsátotta ki. A jelenlegihez hasonló, fűzött könyvecskében a lézergravírozással kitöltött adatoldal az utolsóól az első oldalra került, a 64 kilobájtos csipet és az antennát pedig a borítólap tartalmazza⁹³, amely nem is kitapintható.⁹⁴

A polgároknak biztosítani kell azt a lehetőséget, hogy saját maguk is ellenőrizhessék a chipen lévő adatokat, ezért a határórség mellett az okmányirodákat is ellátták olvasóberendezéssel.⁹⁵ Ahol viszont nem rendelkeznek az adatok leolvasásához szükséges berendezéssel, ott az útlevelel nyomtatott adatai ellenőrizhetők.⁹⁶ Az úti okmány ellenőrzésére jogosult más hatóságok viszont ezen adatokhoz nem juthatnak hozzá.⁹⁷ Ahogy már írtam az útlevelelhatóság is kizárólag a kiadásig jogosult ezeket az adatokat kezelni, azután törölni kell a nyilvántartásból. Tehát nem lesz –legalábbis egy ideig – központi nyilvántartás.⁹⁸

Az okmányt változatlanul a BM Központi Hivatala készíti el.⁹⁹

Hazánkban több szervezet is kifejezte tiltakozását az új útlevelel 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 döntöttek ebben a kérdésben, hogy azt valamilyen nyilvános vitafórumon megtárgyalták volna.

A jelenlegi szabályok két biometrikus azonosítót tartalmazó útlevelel használatát írják elő, amelyet még a terrorizmus elleni harc mellet elkötelezett Egyesült Államok sem követel meg. Korábban az Európai Bizottság volt az, aki ehhez hasonló tervet elvetett, arra való hivatkozással, hogy alapvető jogot csorbít.

⁸⁹ origo.hu/uzletinegyed/hirek/hazaihirek/20030522tiltakozas.html Személyes adatok uniói jogvédelme

⁹⁰ A személyes adatok védelméről és a közérdekből nyilvános adatok nyilvánosságáról szóló 1992. évi LXIII. törvény 2.§ 9.pontja

⁹¹ Lencsés, 10. oldal

⁹² www.tasz.hu/index.php?op=contentlist18&catalog_id=3097 A hét elejétől itt a biometrikus útlevelel

⁹³ Lencsés, 10. oldal

⁹⁴ Ujjlenyomat az útlevelelben, Magyar Hírlap 2004. december 3. 15. oldal

⁹⁵ Lencsés, 10. oldal

⁹⁶ Ujjlenyomat az útlevelelben, Magyar Hírlap 2004. december 3. 15. oldal

⁹⁷ Lencsés, 10. oldal

⁹⁸ www.tasz.hu/index.php?op=contentlist18&catalog_id=3097 A hét elejétől itt a biometrikus útlevelel

⁹⁹ Lencsés, 10. oldal

Felhívták a figyelmet arra, 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 válik, és ez visszaéléseknek lehet táptalaja.¹⁰⁰

A Helsinki Bizottság elnöke, Kőszeg Ferenc is azt a véleményt képviseli, miszerint ezek az adatok súlyosan sértik az egyének emberi jogait. Ezt támasztja alá, hogy az ujjnyomat alapján következtetni lehet az etnikai jellemzőkre.

Az Igazságügyi Minisztérium is jelezte aggályait az Európai Bizottság felé. Kifejtette, hogy garanciális szabályozásra van szükség. Az adatokhoz csak a felhatalmazott hatóságok férhessenek hozzá a jogorvoslati út biztosítása mellett, és kizárólag törvényben meghatározott céllal lehessen felvenni ezeket az azonosítókat.¹⁰¹

Az említett szervezetek és személy által felvetett kérdésekre nem találtam érdemi választ, szerintem ez is azt támasztja alá, hogy ez csak üzlet.

5. A magyar jogvédő szervezetek (lehetséges) álláspontja

5.1. Az adatvédelmi biztos gyakorlata a biometrikus adatok vonatkozásában

A biometria kérdéskörével a korábbi adatvédelmi biztos, Majtényi László is foglalkozott. 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 védelmében kell részesíteni. A személyes adatok kezelése pedig az érintett előzetes önkéntes hozzájárulása alapján lehetséges, amely hozzájárulás megadásakor az érintettnek tudnia kell, hogy milyen célra, és kik fogják kezelni a személyes adatait.

Fontosnak tartom megemlíteni, hogy az érintettek a hozzájárulásuk megadását követően is maguk rendelkeznek, tehát hozzájárulásukat visszavonhatják, a további adatkezelést megtilthatják, illetve kérhetik az adatok törlését. Az érintett kifejezett kérése nélkül is törölni kell azokat az adatokat, amelyek kezelésének célja megszűnt.¹⁰²

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*”.

¹⁰³

Az adatvédelmi biztos **2005. évi beszámolójában** is foglalkozott ezzel a problémával, és leszögezi, hogy a biometria egy adatkezelési módszer, az azonosítók mögött áll a technológia, azok az eszközök, melyek képesek az azonosítót az azt hordozó emberről leolvasni, tárolni.

¹⁰⁰ www.tasz.hu/index.php?op=contentlist2&catalog_id=1216 Nyílt levél az ujjnyomatos útlevelek ügyében

¹⁰¹ Ujjnyomat az útlevélben, Magyar Hírlap 2004. december 3. 15. oldal

¹⁰² 830/K/2000 állásfoglalás: biometrikus azonosító garanciákkal, az érintett tudatos beleegyezésével alkalmazható

¹⁰³ 1485/J/2005 adatvédelmi biztos állásfoglalása

Az adatvédelmi biztos gyakorlatában a beléptető rendszerek esetében alkalmazott ujjlenyomattal kapcsolatban merülnek fel alkotmányos aggályok a legnagyobb számban. Ennek egyik példája az alábbi eset:¹⁰⁴

Az adatvédelmi biztos állampolgári beadványok nyomán vizsgálta a repülőtéri ujjlenyomat-olvasó működését, mert azt személyiségi jogok oldaláról sérelmesnek vélték. Az adatvédelmi biztos az **Avtv. 2. § 1. pontja** alapján mondja azt, 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 azonosítókra jellemző tényező alapján azonosítani lehet.*” A Magyar Légiközlekedési Rt.-nél működtetett ujjlenyomat-olvasó rendszer adatkezelési műveletet végez, amely az **Avtv. 2. § 9. pontja** alapján egyértelműen besorolható ebbe a kategóriába. Ennek a rendszernek a kialakítását viszont törvény nem rendeli el, és az érintettek előzetes hozzájárulásukat nem adták, ami így ellentétes az **Avtv. 3. § (1) bekezdésével**,¹⁰⁵ ami azt mondja, hogy az érintett hozzájárulása és törvény felhatalmazása nélkül személyes adat nem kezelhető.¹⁰⁶

Az adatkezelés folyamatáról is szükséges az érintetteket tájékoztatni akár szóban akár írásban. Az elektronikus adatkezelés veszélyeire is felhívja a figyelmet Péterfalvi Attila, amely az adatállományok összekapcsolása folytán realizálódhat leginkább.

A célhoz kötöttség elve magában foglalja azt, hogy a belépéshez szükséges adatokat csak addig lehet tárolni, kezelni...stb., amíg a munkaviszonyból eredő jogok, kötelezettségek ezt szükségessé teszik. Vizsgálni kell, hogy a jogkorlátozás arányban áll- az elérni kívánt céllal, ami ebben az esetben az, hogy ellenőrizték az alkalmazottak munkahelyen tartózkodásának idejét. De emellett munkaidő-nyilvántartó rendszert is működtetnek.

Mindezek alapján az adatvédelmi biztos megállapította, hogy „*adatvédelmi szempontból az igazgatóságon működtetett, a munkavállalók beléptetését végző rendszer 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.*”¹⁰⁷

Hasonló volt a helyzet egy egyetem kollégiuma esetében. Ebben az esetben is többes azonosításról volt szó, amelynek kapcsán az adatvédelmi biztos megállapította, hogy egyazon célra több azonosító használata nem felel meg az adatvédelmi törvényben foglaltaknak. Ha ezek az azonosítók nem egymás megerősítésére szolgálnak, hanem párhuzamosan, de egymástól függetlenül szolgálják ugyanazt a célt, nem ütközik az adatvédelmi szabályokba.

Visszatérve a beszámolóhoz, a biztos megoldást ajánlott a visszaélések megakadályozására: az adatokat nem adatbázisban, hanem egy kártyán kéne tárolni, és az érintett a leolvasó rendszerhez tenné az ujját a kártyájával együtt, és a rendszer az adatokat összevetné, de adatkezelésre nem kerülne sor.

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. A kutatások pedig a passzív azonosítás felé haladnak, ami azt jelenti, hogy az azonosításhoz nem szükséges az érintett közreműködése, a rendszer automatikusan, akár az érintett tudta nélkül is elvégzi az azonosítást.

¹⁰⁴ Az adatvédelmi biztos 2005. évi beszámolója (www.mkogy.hu/irom37/19341/19341.pdf)

¹⁰⁵ 418/A/2005 adatvédelmi biztos állásfoglalása

¹⁰⁶ 1992. évi LXIII. törvény 3.§-a

¹⁰⁷ 418/A/2005 adatvédelmi biztos állásfoglalása

A biometrikus azonosító rendszerek egymással való kombinálása lehetővé teszi, 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 világnak, de ott van mögötte a totális ellenőrzés közeli lehetőségének. A nagyszerűségéről lehet ódákat zengení - mint ahogy teszik ezt nagyon sokan, de túlértékelik a biometrikus azonosítás lehetőségeit.

A mögötte álló ipar rendkívüli tőkét képvisel, és a részvények árfolyama szárnyal, mióta a biztonságért felelős szervek 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 kijátssza a rendszert. És arról sem lehet hallani, hogy ma Európában egy helyen alkalmaznak arcfelismerő rendszereket széles körben közterületi ellenőrzésre: Londonban, Európa leginkább bekamerázott városában, amely védtelenül állt a terrortámadás előtt.¹⁰⁸

Az adatvédelmi biztos beszámolója alapján egy idézet jutott eszembe, amivel talán meg lehet magyarázni, de semmiképp sem megérteni, hogy mégis miért kezdték meg az új útlevelek kibocsátást:

„Az az elképzelés, miszerint a „közérdek” felette áll az egyéni érdekeknek és jogoknak, csak egyetlen dolgot jelenthet, nevezetesen, hogy egyes egyének érdekei és jogai felette állnak más egyének érdekeinek és jogainak.” (Ayn Rand, amerikai író)

Jogállami garancia a bíróság előtti jogérvényesítés. A jogaiban megsértett személy az adatkezelő ellen fordulhat. Ebben az esetben az adatkezelőnek van bizonyítási kötelezettsége. A bíróság döntésében kötelezheti az adatkezelőt a tájékoztatás megadására, az adat helyesbítésére, törlésére, kiadására (csak bizonyos esetekben), egyedi döntés megsemmisítésére és az érintett tiltakozási jogának figyelembe vételére.¹⁰⁹ Az adatvédelmi biztosnak joga van az adatvédelmi aggályok felmerülése esetén az Európai Bírósághoz fordulni.¹¹⁰

Az Európai Parlament és a Tanács 2000. december 18-án elfogadott 45/2001/ EK rendeletében egy független ellenőrző hatóság létrehozását írja elő, ez pedig az európai adatvédelmi biztos megválasztásával meg is valósult. 2003. december 22-én az EU első adatvédelmi biztosává megválasztották Peter Johan Hustinxot, aki korábban Hollandiában volt adatvédelmi biztos. Az európai adatvédelmi biztos hivatalból és panasz alapján folytat vizsgálatot, emellett felügyeli a közösségi szerveket, azok aktusait, és tanácsokkal látja el őket.

111

5.2. Az Alkotmánybíróság gyakorlata

A biometrikus adatok univerzális jellegével kapcsolatosan szeretném megemlíteni az Alkotmánybíróság 11/1990. (V. 1.) és 15/1991. (IV. 13.) határozatát, amelyben az Alkotmánybíróság megállapította az általános és egységes, azaz minden állampolgárnak és lakosnak ugyanazon elv szerint kiosztott személyi szám alkotmányellenességét. 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.¹¹² A 35/2002. (VII. 19.) AB határozat is a fent említett két AB határozat tartalmával azonosan ítéli meg a személyi szám kérdést.

¹⁰⁸ Az adatvédelmi biztos 2005. évi beszámolója (www.mkogy.hu/irom37/19341/19341.pdf)

¹⁰⁹ Kerekes – Zombor, 57. oldal

¹¹⁰ Ujjlenyomat az útlevelemben, Magyar Hírlap 2004. december 3. 15. oldal

¹¹¹ www.abiweb.obh.hu/abi/index.php?menu=30002&docid=10451&key=biometrikus Az európai adatvédelmi biztos

¹¹² Szabó, 91. oldal

A személyi szám feltüntetést több helyen megkívták, így a népi kezdeményezést és a népszavazást kezdeményező íveken is fel kellett tüntetni. Ezt a rendelkezést úgy változtatták meg, hogy választási jogot biztosít a tekintetben, hogy milyen személyazonosítóval kíván az érintett az íveken szerepelni.

A társadalombiztosítás egészségügyi szolgáltatásának igénybevételére jogosító igazolványról szóló 54/1992. (III. 21.) Korm. rendelet 3. számú mellékletének 3. pontja szerint az igazolvány érvényesítésére, illetőleg kiállítására jogosult szervezetnek az alábbi adatokat kellett nyilvántartásba venni: az igazolvány számát, az igazolvány tulajdonosának nevét, személyi számát, lakcímét és aláírását. Az Alkotmánybíróság álláspontja szerint „*az igazolványok egyedi, vonalkóddal is feltüntetett igazolványszáma - a tulajdonos nevével, lakcímével és aláírásával együtt - a társadalombiztosítás egészségügyi szolgáltatásának igénybevételére vonatkozó jogosultság fennállását megfelelően alkalmasak bizonyítani, azaz a cél elérésére önmagukban elegendő adatok, így a személyi szám közlésének és felhasználásának előírása az adatkezelés céljának megvalósításához már nem szükséges. A betegbiztosítási igazolványon a személyi szám feltüntetése, mint többcélú személyazonosító technikailag megkönnyítette az egészségi állapotra vonatkozó szenzitív adatok összekapcsolását is az érintett más személyes adataival. A személyi számnak az állami szervek körén kívüli használata egyben lehetővé teszi ezeknek a privátszférát érintő adatoknak a közigazgatás engedélyezett nyilvántartásaival való összekapcsolását és ez az állami ellenőrzés fokozódásával, egyúttal a szabadságjogok fokozott veszélyeztetésével járhat.*”¹¹³

A **11/1990. (V. 1.) AB határozatban** leszögezik, hogy a személyi szám az állampolgár személyazonosítására szolgáló adat, és önmagában is adatokat tartalmaz az állampolgár személyére. Minderre tekintettel a személyi számot is olyan személyes adatnak kell tekinteni, amelynek védelméhez való jog mindenkit megillet, azaz a személyi szám nyilvános használatának kötelező elrendelése a személyes adat védelméhez fűződő alapvető jog gyakorlásának korlátozása, tehát ilyen tartalmú rendelkezést csak törvény írhat elő. A személyi szám univerzális lényegénél fogva ellentétes az információs önrendelkezési joggal.¹¹⁴

A **15/1991. (IV. 13.) AB határozatban** az Alkotmánybíróság értelmezése szerint az Alkotmány 59. §-ában biztosított személyes adatok védelméhez való jog esetén mind annak aktív mind passzív oldalára tekintettel kell lenni.

Személyes adatot felvenni és felhasználni az érintett beleegyezésével, illetve törvény erejénél fogva lehet, és a feldolgozás útjának minden esetben követhetőnek kell lenni. Az adattovábbítást és az adatok nyilvánosságra hozatalát korlátozni kell. Adattovábbításra magánszemélyek jogos érdekük, illetve joguk igazolása után, szervezetek (államigazgatási és igazságszolgáltatási szervek) pedig feladataik ellátásához kérhetnek adatot a nyilvántartásból. Az adatfeldolgozás célját az érintettel úgy kell közölni, hogy megalapozottan dönthessen adatai kiadásáról, és hogy ezzel egyidejűleg milyen jogai keletkeznek.

Az Alkotmánybíróság azt is kimondta, hogy alapvető jogra és kötelességre vonatkozó szabályokat törvény állapítja meg, de alapvető jog lényeges tartalmát nem korlátozhatja.

A célhoz kötöttség az információs önrendelkezési jog garanciája. Tehát a „készletre” történő adatfeldolgozás önmagában alkotmányellenes.¹¹⁵

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. 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.

¹¹³ 29/1994. (V. 20.) AB határozat

¹¹⁴ 11/1990. (V. 1.) AB határozat

¹¹⁵ 15/1991. (IV. 13.) AB határozat

2) Másrészt az államnak kötelessége jogi szabályozás útján intézkedéseket tenni annak érdekében, hogy a visszaalakíthatatlan sablonok előállítását más eljárással történjen az az egyik adatkezelőnél, mint a másikinál, azért, hogy a sablonok ne legyenek összehasonlíthatóak egymással.¹¹⁶

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 személyiségprofil kialakítsanak, legalábbis az útlevél jelenleg nem rejt magában ezt a kockázatot, hiszen adatainkat nem tárolják még adatbázisban.

Érdekes kérdés lehet viszont az, hogy ha a későbbiekben a taláros testület valamely ok miatt alkotmányellenesnek mondja ki a biometrikus útlevél használatával kapcsolatos lényeges szabályt, mi marad: Alkotmány módosítás nélkül vagy uniós kötelezettség?

6. Záró gondolatok

Ha az emberek életén eluralkodó félelem és fenyegetettség érzését az alkotmányokban és nemzetközi dokumentumokban deklarált alapvető emberi jogok korlátozásával próbálják megoldani, a véres harcok és forradalmak által kivívott szabadságok veszélybe kerülhetnek.

Az emberek biztonsága és magánszférájának védelme között meg kell találni azt a határt, amikor az ember még elviseli, hogy bizonyos jogairól le kell mondania, és hogy a személyiségéből egy szeletet fel kell áldoznia azért, mert közösségben él. De itt nem a szabadság és a biztonság között kell választani, hiszen láhattuk, hogy a biometria sem teremti meg a biztonságot, de az ember totális ellenőrzéséhez vezethet. Ezt senki nem kívánhatja!

A szabadságot és a kivívott alapvető emberi jogokat azonban akkor fogjuk csak megbecsülni, ha újból megtapasztaljuk, milyen a nélkül élni. És ne felejtjük, „aki lemond szabadságáról, az ember voltáról, emberi jogairól, mi több: kötelességeiről mond le.” (Rousseau)

Mi lesz mégis a jövő? - kérdezem én egy kicsit félve. A tendenciát láhattuk. Az üzleti törekvések elnyomják a jogvédők hangját. De hiszem, és remélem, hogy az egyének is - ki előbb, ki utóbb - megérzik a veszélyt, és visszakövetelik a jogaikat.

Dolgozatomat John Pagetnek az 1835-ben az útlevélről alkotott véleményével zárnám, mert talán még mindig jobban tükrözi a valóságot, mint a biometriáról alkotott képzelte világ: „ha egy országban jól működik a rendőrség, amúgy sincs rá szükség, ha pedig rosszul, az útlevél nyújtotta képzelte biztonság csak tovább rontja a helyzetet.”¹¹⁷

¹¹⁶ Szabó, 91. oldal

¹¹⁷ Gúr, Belügyi Szemle 58. oldal

7. Felhasznált irodalom

7.1. Könyvek, folyóiratok, tanulmányok

- Gúr Roland: *Határát lépés útlevéllel vagy személyazonosító igazolvánnyal*, In: Belügyi Szemle 53. évfolyam 2005. 11. szám 57-66. oldal
- Gúr Roland: *Útlevél a nemzetközi jogban és fejlődésének új irányai az Európai Unióban*, In: Európai Jog 5. évfolyam 5. szám (2005. szeptember) 17-23. oldal
- Dr. Hargitai József: *Az útlevél és a külföldre utazáshoz való jog nemzetközi jogi alapjai*, In: Magyar Jog 42. évfolyam 12. szám (1995. december) 710-718. oldal
- Kerekes Zsuzsa - Zombor Ferenc: *Az információs jogok és a sajtó*, A média lehetőségei és korlátai, AduPrint Kiadó és Nyomda Kft., Budapest 1999, INDOK 31-59. oldal
- Lencsés Károly: *Jön a biometrikus útlevél*, Népszabadság 2005. október 21. 10. oldal
- Dr. Nyíri István: *A „DNS-újnyomtat” – adatvédelem*, In: Belügyi Szemle 1998. 3. szám 118-121. oldal
- Poór Csaba: *Biometrikus útlevelek*, HVG 2005. március 26. 68-69. oldal
- Sári János: *Alapjogok, Alkotmánytan II.*, Osiris Kiadó, Budapest, 2000 103-108. oldal
- Sándor Judit: *A genetikai adatok védelme*, In Acta Humana 14. évfolyam 2003. 3. szám 3-21. oldal
- Szabó Máté Dániel: *Biometrikus azonosítás és adatvédelem*, In: Acta Humana 15. évfolyam 2004. 1. szám 81-92. oldal
- *Újnyomtat az útlevélben*, Magyar Hírlap 2004. december 3. 15. oldal
- *Újnyomtatot vesznek az útlevélhez*, Népszabadság 2004. október 26. 3. oldal
- *Útlevél digitális újnyomattal*, Világgazdaság 2005. szeptember 23. (4. oldal)
- Woller János: *Kriminálisztikai célú DNS-vizsgálatok és DNS adatbázisok*, In: Belügyi Szemle 1997. december 45-49. oldal
- abiweb.obh.hu/abi/index.php?menu=118 Az európai adatvédelmi biztos
- www.edri.org/campaigns/biometrics An Open Letter To The European Parliament On Biometric Registration Of All EU Citizens And Residents
- www.edri.org/edrigram/number2.4/biometrics EU Commission proposal for biometrics in passports
- guide.supereva.com/usa/interventi/2006/01/241316.shtml Il passaporto per entrare negli Stati Uniti
- hvg.hu/itthon/20051122harasztieuropa.aspx?s=hk Biometrikus útlevél, Haraszti: a szabadság korlátozásában Európa túltesz Amerikán
- milan.usconsulate.gov/pressreleases/PR_ITA_062006_VWP_Oct_26_2006.htm Passaporto biometrico: le norme in vigore per il programma „viaggio senza visto”
- www.nol.hu/cikk/377129 Mégsem jó a biometrikus útlevél?
- origo.hu/uzletinegyed/hirek/hazaihirek/20030522tiltakozas.html Személyes adatok uniós jogvédelme
- www.statewatch.org/news/2004/nov/11biometric-legal-analysis-hm.htm Statewatch Analysis: The Legality of the Regulation on EU Citizens' Passports
- www.szgti.bmf.hu/~mtoth/download/Hallgatoi_projektek/Török_Csaba-Biometria.pdf Török Csaba projektje
- www.tasz.hu/index.php?op=contentlist2&catalog_id=1216 Nyílt levél az újnyomatos útlevelek ügyében

- www.tasz.hu/index.php?op=contentlist2&catalog_id=3097 A hét elejétől itt a biometrikus útleveél

7.2. Jogforrások

- A Magyar Köztársaság Alkotmánya 1949. évi XX. Törvény
- A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény
- A Rendőrségről szóló 1994. évi XXXIV. törvény
- A külföldre utazásról szóló 1998. évi XII. törvény
- 11/1990. (V. 1.) AB határozat
- 15/1991. (IV. 13.) AB határozat
- 29/1994. (V. 20.) AB határozat
- 34/1994. (VI. 24.) AB határozat
- Az adatvédelmi biztos 2005. évi beszámolója
- (www.mkogy.hu/irom37/19341/19341.pdf)
- 832/K/2000 állásfoglalás: biometrikus azonosító garanciákkal, az érintett tudatos beleegyezésével alkalmazható
- 418/A/2005 adatvédelmi biztos állásfoglalása
- 1485/J/2005 adatvédelmi biztos állásfoglalása
- Az Európai Tanács 2252/2004/EK rendelete (2004. december 13.)
- A 95/46 EK irányelv
- Munkaanyag a biometrikus azonosítókról (WP 80) (abiweb.obh.hu/abi/index.php?menu=209)
- ARTICLE 29 Data Protection Working Party WP 96 (209.85.129.104/search?q=cache:Dty6zaJiXiQJ:ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp96_en.pdf+Working+Party+96&hl=hu&gl=hu&ct=clnk&cd=2)
- 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 (ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp110_hu.pdf)

Módszer	Egyediség	Változatlanág	Hamisíthatóság, Másolhatóság	Megtévesztés	Kényszerítés	Ikek	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 hangot hallja	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.

Változatlanág 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 egyetétjű ikrek közti különbségtételre mennyiben van lehetőség.

Az utolsó oszlopban a kivitelezés lehetőségeit, korlátait tüntetem fel.

A piros színnel kiemelt szöveg a pozitív, a fekete szöveg a negatív jellemzőket jelenti. A szaggatott vonallal jelölt jellemzők hatása az azonosításra nem ismert.

Melléklet

(I. számú melléklet)*

* [www.szgti.bmf.hu/~mtoth/download/Hallgatoi projektek/Török Csaba-Biometria.pdf](http://www.szgti.bmf.hu/~mtoth/download/Hallgatoi%20projektek/Török%20Csaba-Biometria.pdf) Török Csaba projektje