

# Személyazonosítási technikák

*Kósa Zsuzsanna*

*A szolgáltatási szektor kiterjedése és a személyek mobilitásának növekedése szükségessé teszi, hogy gépekkel biztonságosan kezelhető személyazonosítási technikák terjedjenek el; amelyekben a biometria azonosítás hangsúlyos szerepet kap, és a kombinált műszaki megoldásokon túlmenően, társadalmi kérdések is felmerülnek.*

## 1. Témakör

A felhasználó különböző üzleti szolgáltatási (például banki, informatikai, munkahelyi) és közszolgálati (például igazgatási, egészségügyi, munkaügyi) rendszerekkel kerül kapcsolatba, ahol személyre szabott kiszolgálást vár el, ugyanakkor személyes és üzleti adatainak védelmét is igényli. A különböző szolgáltatási kapcsolatokhoz ma különböző azonosítós számok, kártyák, kódok és eljárások tartoznak. Ezek a személyazonosítási technikák teszik lehetővé, hogy a felhasználók úgy vegyék igénybe a szolgáltatásokat, hogy ne kelljen minden szolgáltatási szerződésüket magukkal hordozniuk, szükségük van azonban az azonosító kártyákra, és meg kell jegyezniük a különböző PIN kódjaikat, ha valóban használni akarják a szolgáltatásokat.

A különböző szituációk más-más azonosítási eljárást és biztonsági szintet igényelnek. Az azonosítások alapja a születéskor felvett anyakönyv, amely egy életen át bizonyítja az állampolgárságot. Az állampolgárság bizonyítására, öt-tíz éves időtartamra adják ki a személyi igazolványt, amely már fényképet és aláírást is tartalmaz. Időleges azonosításra szolgál a munkahelyi beléptető kártya vagy a diákigazolvány. Egy egyszerű online vásárlásnál elég lehet egy bankkártya néhány adata is. Az elemzés a ma működő személyi azonosítási technológiákat veszi célba, ezek fejlődését és jövőképét vizsgálja. Részletesebben meg kívánjuk vizsgálni a személyi azonosítási technikák integrálására vonatkozó lehetőségeket, és ezek adatvédelmi, valamint biztonsági vonatkozásait.

## 2. Jelenlegi helyzet

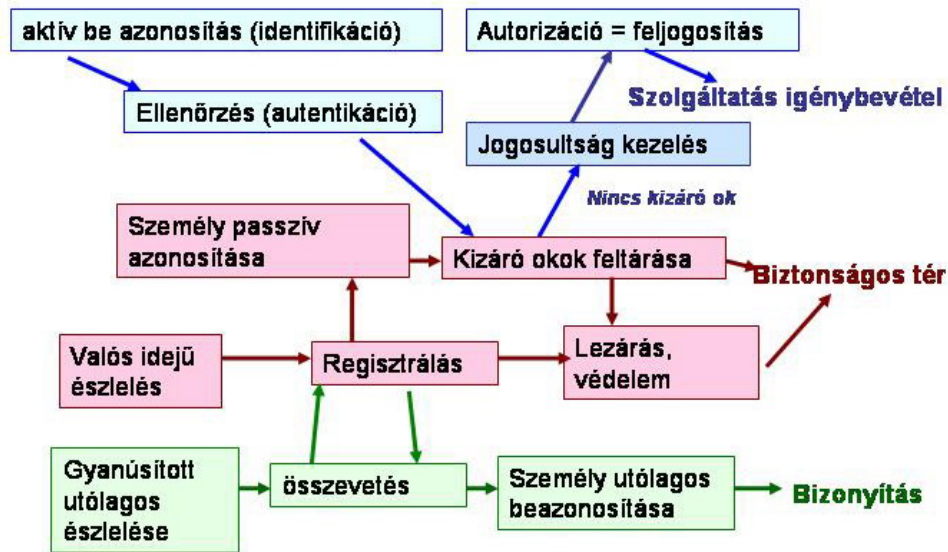
### 2.1. Személyi azonosítási szituációk

*Az azonosítások szólhatnak egész életre, egy időszakra vagy egy tranzakcióra.*

Igényelhetik a személy aktív közreműködését, vagy passzívan is azonosíthatják a személyt. Gyengének mondjuk, ha csak egyetlen eljárást alkalmaz, erősnek, ha több eljárást egyidejűleg.

A személyazonosítás három alapesete a szolgáltatás-igénybevétel, a biztonságos tér kialakítása (legyen fizikai vagy virtuális) és az utólagos bizonyítás valamely bizonyítandó cselekedet után (amikor a felelősséget kívánják megállapítani).

A tipikus személyazonosítási szituációkat az 1. ábra mutatja be.



1. ábra: Személyazonosítási szituációk

- a.) A szolgáltatás igénybevétele esetén a személy valamilyen módon, aktívan beazonosítja önmagát, azaz állít magáról egy személyazonosságot, ezt valamely független forrásból ellenőrizni kell. Ezután, a beazonosított személyre vonatkozó, a korábbi szolgáltatás-igénybevételek során kialakult vagy egyéb okból direkt beállított, kizáró okok feltárandók. Ha nincs kizáró ok, a szolgáltatási szerződés alapján kell beállítani a jogosultságait, majd feljogosítani a szolgáltatás igénybevételére, azaz vissza kell jelezni neki és kiszolgálni.
- b.) A biztonságos terek kialakításához érzékelni kell, ha valaki ott megjelenik, regisztrálni a jelenlétét és passzív módon (aktív együttműködése nélkül is) azonosítani a személyét. A beazonosított személyre vonatkozó kizáró okokat fel kell tární, és ha nincs ilyen, akkor be kell engedni a biztonságos térbe. Ha a korábbi magatartásból adódóan vagy egyéb direkt beállított paraméter (például rendőrségi körözés) alapján van ilyen, akkor a biztonságos teret le kell zárni, és védeni kell a szóban forgó személytől.
- c.) Az utólagos bizonyítás esetén korábban regisztrált jelenlétet és cselekedeteket kell egy adott személyhez kapcsolni úgy, hogy minden kétséget kizáró legyen. Ehhez, az utólag azonosítandó személy észlelt jellemzőit össze kell vetni a korábban regisztrált jelenlevők észlelt jellemzőivel, és le kell szűrni a kellő pontossággal egyező adathalmazokat.

A három, egymástól eltérő személyazonosítási szituáció néhány ponton összekapcsolódhat, legalábbis elvben, mert a kizáró okot vizsgálni kell mind a szolgáltatás-igénybevétel, mind a biztonságos tér kialakítása érdekében, de más-más lehet a kritérium.

## 2.2. Személyi okmányok

A személyi okmányok elvi alapja az „identitás” – ami egyszerre jelent egy csoporthoz

való tartozást<sup>1</sup>, és a csoporton belüli egyedi megjelölést. Az identitás alapállapotának- és változásainak rögzítésére szolgálnak az anyakönyvek. Az alapregiszter a születési anyakönyv, amely a nevet, születési helyet és időt, valamint a szülők nevét tartalmazza. Hasonló anyakönyv készül a házasságkötésről és az elhalálozásról is. Ezen kívül, bevándorlási anyakönyv is létezik, amely éppen az állampolgárság-váltás különböző állapotait rögzíti: pl.: hontalan, menedékes, menekült, letelepedett, új állampolgár. *A személyi okmányok olyan tárgy alapú azonosítók, amelyek hosszú távú és hiteles személyi azonosítást tesznek lehetővé.* Kapcsolódnak valamely ország identitást elismerő alapregiszteréhez<sup>2</sup>. Eddig általában papír alapú fényképes igazolványok voltak (ezek egy része ma is érvényes). Később áttértek a kártya jellegű igazolványokra. A kártya alapú személyigazolvány már megmásíthatatlanul tartalmazza a személy fényképét és aláírását is. Újabb tendenciaként, géppel leolvasható adathordozókat is elhelyeznek a kártyán: mágneses csíkot vagy chipet is. Ezekbe az adathordozókba bele lehet tárolni a biztonságot növelő és ellenőrző adatokat, kódokat is. Ha az okmány használatakor van mód a biometria adatok azonosítására, akkor célszerű azt használni ellenőrző adatnak. Új tendencia, hogy a chipbe egy vagy több biometria azonosítót is bekódolnak. Személyek esetében a biometria azonosítók, mint például a DNS vagy egyéb biológiai jellemzők egyediek és egész életen át megmaradnak.

Az okmányok között a lakcím azonosítás csak egy kapcsolódó adat regisztrálása, elvben nem része a személyazonosításnak; ugyanakkor, a lakcímgazoló kártyán van egy személyazonosító kód is, amely kapcsolatot teremt az alapregiszterrel. (Biztonsági szempontból nem tekinthető kiemelkedőnek, mert nincs benne fénykép vagy aláírás-kép, csak egy szám és egy vonalkód). Középtávú azonosítást szolgál az adókártya és a TB-kártya is, de valójában „csak” egy azonosító kódot jelenítenek meg, amelyen regisztrálva vagyunk az adóhivatalnál vagy a társadalombiztosítási rendszerben.

Kombinált (arcképet és aláírást is tartalmazó), papír alapú azonosító igazolvány az útlevelel, amely már több nyelven igazolja a személyazonosságot. A személyi okmányok sorát a jogosítvány egészíti ki, amely valamilyen vizsgálathoz kötött tevékenységre jogosít fel minket. Az új típusú, kártya alapú jogosítványoknak van személyazonosító okmány jellege is, aminek a lejárat ideje általában sokkal hosszabb, mint a vezetésre való feljogosításé.

A személyi okmányok közé csak azokat soroljuk, amelyek általánosan, többféle kapcsolatban is használhatók a személyazonosság igazolására. Az általános igazolványok mellett, azokhoz hasonlóan megjelennek a rövidebb időszakra szóló, ideiglenes igazolványok – diákigazolványok, munkahelyi belépők – is. Ezek általában szintén tartalmazzák fényképet és aláírást, de ezek nem elsősorban személyazonosítók, hanem inkább jogosultság-igazolók: tulajdonosuk jogosult valahova belépni, szolgáltatást igénybe venni. A felsorolás nem teljes, ezek a kártyák azt igazolják, hogy valamilyen regisztrált kapcsolatban állunk már egy szolgáltatóval vagy intézménnyel.

---

<sup>1</sup> Ez a csoporthoz való tartozás elismerését jelenti, amely legtöbb esetben állampolgárságot jelent. Egyes államok ma is megjelölik a nemzetiséghez való tartozást, régebben megjelölték a vallási hovatartozást is az anyakönyvekben.

<sup>2</sup> Legtöbb esetben a személy abban az országban él, ahol született, de ez nem mindig van így. Lehet kettős állampolgár is, vagy bevándorló, stb. Ezek miatt, a személyi okmányok több ország alapregiszteréhez is kapcsolódhatnak. Mindig van egy okmány-kiállító ország, amely elismeri az identitást, azaz a csoporthoz való tartozást és azon belül a személy egyedi megjelölését.

### 2.3. Személyazonosításhoz használt technikák

A személyazonosítási technikák, a fentebb leírt azonosítási folyamatokban az észleléshez, illetve az aktív vagy passzív beazonosításhoz használatosak. Egyes személyazonosítási technikával készülő adatcsoportok (például fényképek, aláírás) az alapregiszterben és személyi okmányok egy részében rögzítésre kerülnek.

**A személyi azonosítási technikákat tudásalapú, tárgyi alapú, biológiai és viselkedési csoportokba sorolhatjuk.** A tudáson alapuló: a név, jelszó, azonosító kód. A legelterjedtebb csoport a tárgyi alapú: kulcsok, pecsétek, jelvények, kítűzők, igazolvány, mágnescsíkos kártya, a chipes (smart) kártya, rádiófrekvenciás chip. A biológiai jellemzőkre épülő csoport: ujjlenyomat, kéznyomat, kézgeometria, arc (arckép, fénykép), termogram, szem (írisz, retina), illat, DNS. A viselkedési minta alapúak közül legismertebb a kézírás; ide tartozik a beszédhang, a gépelési ritmus, a járási mód, a szóhasználat, a testbeszéd és az arcmimika is. *A biológiai és viselkedési csoportot együttesen biometrikus azonosítóknak is nevezik.*

A különböző, időleges hatályú tárgyi alapú azonosítókat a személyeknek magukkal kell hordozniuk. Természetes az igény, hogy a többféle azonosítóját *(egyes kivételes és szabályozott esetektől eltekintve)* csakis az érintett személy „integrálhassa”. A személyes adatok integrálása azt jelenti, hogy a különböző relációkban használt azonosító kódokat és jeleket egyesítik, vagy egy közös tárba tárolják. Ez lehetővé teszi a különböző állományok összekapcsolását. Az igazgatás, csak az adatvédelmi szabályok betartásával, kapcsolhatja össze a személyes adatokat.

Kezdetben kizárólag tárgyi technikákat (például személyes pecsétet, pecsétgyűrűket) használtak. Az írni tudás általánossá válásával felváltotta a személyes aláírás, amelyet a tudás alapú azonosítók közé sorolhatnánk. A közelmúltban és néhol a jelenben használatos személyazonosítási technikák kombinálják a tárgyi alapú és a tudásalapú technikákat. A tudáson alapuló technikákat (kódokat, jelszavakat) meg kell jegyezni és nem célszerű feljegyezve hordozni.

A gépi rendszerek fejlődésével, terjednek a biometriai azonosító eljárások, amelyeket korábban csak ritkán és kivételes esetekben (például nyomozáskor) alkalmaztak; ezek a biometriai azonosítók használhatók szinte egész életen át. A biometriai azonosítók közé bármely testrész bármely egyedi jellemzője felvehető, amely nem változik, vagy nem változik jelentősen az élet során. Már elterjedt technológiák vannak az ujjlenyomat, arc, a szemben az írisz és a retina rajzolata, a hanghordozás felismerésében. Újabb eljárások készülnek a szag, a bőr kémiai összetételének felismerésére és egyes viselkedési minták, mint például az aláírás dinamikájának, a billentyű-nyomások jellegzetességeinek stb. azonosítására. ***A korábbi tárgy + tudás alapú technikákról mostanában térnek át a biometriai azonosítókat is tartalmazó tárgyi azonosítókra.***

A biometriai adatokat is tartalmazó azonosító tárgyak nem átruházhatók, mert csak az eredeti személy testi jellemzőivel lehet összevetni a letárolt adatokat. Így a kombinált azonosítók a biológiai személyt azonosítják. A biometriai adatot nem tartalmazó azonosító tárgyak átruházhatók személyek közt, így egyszerűen megvalósítható a megbízott helyettesítés egyes ügyekben. Ebből is látható, hogy inkább a szolgáltatási viszonyok és egyes szerepek igazolására valók.

#### 2.3.1. Tárgy- és tudásalapú technikák

Kártya PIN-kóddal

A különböző szolgáltatási kapcsolatok meglétét igazolják a bankkártya típusú tárgyi személyazonosítók, amiket általában PIN-kóddal és jelszókkal is kiegészítenek. Több formája használatos: a chipes kártya, a mágnescsíkos kártya, egyszerűsített formája a vonalkódos azonosító papír alapon. Ebbe a sorba tud majd beilleszkedni a rádiófrekvenciás címkével<sup>3</sup> ellátott kártya is, amely már bizonyos távolságból is leolvasható.

#### Elektronikus aláírás

Az elektronikus aláírás egy, előzetes regisztrációhoz kötött kódolási eljárás, és az aláírt elektronikus dokumentumokra idő- és tartalom-pecsétet is rak. Ehhez az elsődleges azonosításkor a személy megadja a szükséges paramétereit, és kap egy géppel leolvasható aláírás-kártyát, amivel a gépi kódolást elvégezheti. Az elektronikus dokumentumokat ezzel be lehet kódolni úgy, hogy az elektronikus aláírás és az időpecsét is visszafejthető.

#### Tárgyi azonosítások integrálása

A személy többféle önazonosító tárgyi eszközt és eljárást is használ, minden kapcsolatához egyet-egyét, de a formát és a biztonsági szintet nem maga választja meg. Felelőssége a tárgyi azonosítókat őrizni, és a tudásalapú azonosítási eljárásokkal kiegészíteni. Munkával túlterhelt, idős, alulképzett, fogyatékkal élő, a technológiákat egyébként is nehezen kezelő személyek ezt a tárgyi- és tudásalapú személyazonosító integrálást nehezen vagy csak nem biztonságosan tudják megtenni.

### **2.3.2 Biometriai technikák**

Minden olyan biológiai jellemző használható azonosítónak, amely egyedi az embernél, az idő előrehaladásával keveset változik, valamennyire mérhető, az információt tárolható.

#### Ujjlenyomat felhasználása

*Az ujjlenyomat egyedi karakterisztikával bír, egész életen át megmarad és jellegzetességei szisztematikusan osztályozhatók; mindezért lehet biometriai személyazonosító,*

Ujjlenyomatokat lehet lágú anyagba (pl. csokoládéba, viaszba) nyomni, kirajzolhatja egy színes közvetítő anyag (pl. szennyeződés, festék, grafitpor), vagy lehet rejtett is az ujjlenyomat, ilyenkor az ujj saját zsiradék vagy kisebb szennyeződések által képződik a felületen. A lágú anyagba készült és az idegen anyag által közvetített ujjlenyomat szabad szemmel is látható. A legtöbbször rejtett ujjlenyomatot valamilyen anyaggal megszínesítik, lézerrel megvilágítják, és ezután a kép digitális fotóra kerül. A tipikus ujjlenyomatnak kb. 150 megkülönböztető jegye, ún. „minutia” lehetséges, ezek közül legjellegzetesebbek a rajzolat forduló-és elágazási pontjai, ezeket szkennelés után géppel dolgozzák fel. A rajzolat mérete (az ujj mérete) változhat, de az elemek egymáshoz viszonyított helyzete állandó, és ez adja az egyedi azonosítás alapját. Régebben ezt szakértők hasonlították össze. A gépi feldolgozásban a szkennelt képet digitálisan tárolják, és elkészül egy „digitális térkép” a rajzolat jellegzetes pontjairól, és a gép összeveti a memóriájában tárolt összes ujjlenyomat rajzolatával. Az ujjlenyomat a legrégebbi biometriai azonosító, amit használnak, de sokáig csak a kriminalisztikában terjedt el. Szélesebb körű és üzleti típusú felhasználása mostanában gyorsult fel. Ha az ujjlenyomat bekerül a személyi okmányokba, akkor mindenkitől kell tudni mintát venni az újszülöttről az öregekig, egészen finom felbontásban. Az általánosan használt szkennel felbontása, amely 500 pixel négyzet-hüvelykenként (ppi) nem elég pontos

<sup>3</sup> Vö. *Rádiófrekvenciás azonosítás (és ami utána következik)* elemzés.

minőségű. 1000 ppi szükséges a gyermekek ujjának szkenneléséhez, és a jellegzetességek beazonosításához. Szinte minden embertől jó minta vehető ilyen pontossággal. Az 1000 ppi sűrűségű minta azonban négyszer nagyobb memóriakapacitást igényel. Emiatt, a szkennelt ujjlenyomat képet tömörítik többféle képformátumokba (pl. JPEG-be is.) Jelenleg folyik az ujjlenyomat adatok tárolási formátumának önálló kép-típuskenti szabványosítása.

A kockázat az ujjlenyomatonál az, hogy viszonylag könnyű duplikálni: egy kis ragasztó vagy gipsz, és az ujjlenyomat alacsony költségen másolható. Ugyanakkor, a nem élő anyagból készült ujj-másolat egészen más hullám-visszaverődést ad, mint egy valóban élő szövetekből álló emberi ujj. Ezt nevezik „élőség detekciónak”, amelyet egy biztonságos rendszerben ma már megkövetelnek. Többszínű fényvel, ún. „multispektrális” optikai technológiával lenyomatot tudnak venni akkor is, ha sérült, nedves, nagyon száraz vagy piszkos ujjról van szó. Ha ezt a technológiát kombinálják a nagyobb pontosságú szkenneléssel, akkor felügyelet nélküli alkalmazások is lehetségesek, alkalmas lehet az önkiszolgálásra is, és a csalások is kivédhetők.

#### Arcfelismerés

A hagyományos fényképeken az arcról egy síkbeli kép készült. Az elektronizált fényképek valójában ezt a kétdimenziós technológiát teszik át digitális formába. az új e-útlevelekbe az egész világon.

A legtöbb arcfelismerő az arc általános geometriájából indul ki, ez a különböző részek (orr, szájzug stb.) helyzetét elemzi egymáshoz viszonyítva. Nagykapacitású kamerával már a bőr textúrája is láthatóvá válik. Ez a bőrelemzés a bőr jellemzőire épül, mint például az apró bőrhibák, fény-elnyelés stb.

A digitális ábrázolás azonban lehetőséget ad háromdimenziós képek tárolására is. Az erre épülő arcfelismerési technikával a pontosságot növelhetjük valamennyire, mivel három dimenzióban a személyek azonossága vagy különbözősége<sup>4</sup> jobban felismerhető. A jelenlegi szabványokat úgy fejlesztik, hogy a 3D arcok bekerüljenek az elektronikus útlevelekbe.

#### Hangfelismerés

A hangfelismerés a hangminta alapján a beszélő beazonosítását jelenti. A beszédanalízisen belül két nagy irányról beszélhetünk: a jelentés felismeréséről és a hangszín, hanghordozás alapján a beszélő beazonosításáról. Itt az utóbbiról van szó, függetlenül a jelentéstől. Tárolt hangmintákban választják szét a beszélő és a háttérzaj információit, és a hanghordozásbeli azonosságokat keresnek a beszélők között.

#### Írisz- és retina-felismerés

A szem szintén egyedi azonosításra alkalmas biológiai jellemzőket tartalmaz. Az írisz minta felismerés nagyon megbízható, és nagyobb repülőtereken alkalmazzák is. Az írisz 266 megkülönböztető jellegzetességgel bír, ezek a variációival már az egész ma élő emberiség megkülönböztethető. A felismerési folyamat elég megbízható, amit több projekt is igazol. A korábban elterjedt íriszfelismerést újabban kiegészítik retina-felismeréssel is. A szem-alapú azonosító eljárások előnye, hogy nem alakul ki érintkezés a vizsgálóponttal. Ez egyben a hátránya is, mivel az adatfelvétel lassabb, és hosszabb adat-ellenőrzésre is kell számítani.

#### További biometriai technológiák

Az érrajzolat módszer is biztos felismerést nyújt. A számítógépes algoritmusok

---

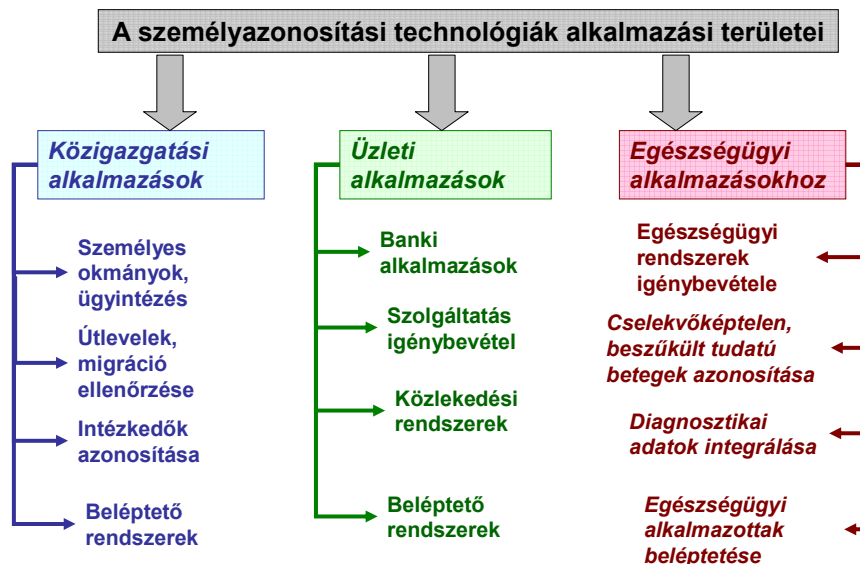
<sup>4</sup> Pl. egyetjű ikreket is meg kell tudni különböztetni.

megkönnyítik a minták elkülönítését. Infravörös lámpával és CDC kamerával veszik fel az érrajzolatot. Az algoritmus összeveti a véredény rajzolatát az ujjakon. A kulcselem, hogy ez a rajzolat nem változik a korról, és nem igényel érintkező felületet. 3D-s fül-felismerés, DNS, termográfiai arcfelismerés, retina, ajakrajzolat felismerése már használatos valamilyen formában. További technológiák is léteznek: szag, online aláírás, billentyűzet nyomás ereje, bőr kémiai összetételének vizsgálata. Ezek fontosabbá válhatnak a jövőben.

DNS-mintát ma már lehet venni mindenkitől, de még nem alakultak ki az országos DNS-minta táruk. A jövőben a DNS-minta előkészítése és felismerése percek alatt elvégezhető lesz. Ennek alapján a DNS személyi azonosításra is használhatóvá válik.

## 2.4. Személyazonosítás alkalmazási területei

A 2.1. fejezetben már tárgyaltuk, hogy milyen szituációkban lehet és kell a (lehetőleg gépi) személyazonosításokat megtenni. Most egy másik vetületből tekintjük át az alkalmazásokat: mely felhasználási területen épülnek be a folyamatokba a személyazonosítások. A választandó technika a felhasználási terület elvárt biztonsági szintjétől függ. A felhasználási területeket három nagy csoportban tárgyalhatjuk: közigazgatási alkalmazások, üzleti alkalmazások és egészségügyi alkalmazások. A közigazgatásban kiadott okmányokat másodlagos felhasználásként a többi alkalmazás is használhatja.<sup>5</sup> A 2. ábra áttekintést ad az alkalmazási területekről.



2. ábra: Személyazonosítási technikák alkalmazási területei

<sup>5</sup> A fordított irányú felhasználás ritka és esetleges: pl. egy balesetet szenvedett embert a bankkártyáján szereplő név alapján be lehet azonosítani, de ez rendkívüli eset.

### 2.4.1 Közigazgatási alkalmazások

A személyazonosítási technikák, ezen belül a *személyazonosító okmányok* elsődleges felhasználása a közigazgatási szolgáltatások és a közszolgáltatások igénybevételénél tapasztalható. Amikor a közigazgatás kapcsolatba lép az egyénnel, mindig ellenőrizni kell az egyén személyazonosságát, és ennek alapján intézik az ügyeit. Valójában a személyazonosság ellenőrzése egyfajta jogosultság ellenőrzés is, amelyben az állampolgárságot (vagy letelepedettséget) ellenőrzik, és a lakcímkártyával meg a helyi közigazgatási szolgáltatásokra való jogos igényt.

Az államok együttműködése befolyásolja az *útlevelekben és vízumokban* alkalmazott személyazonosítási technológiákat. A biometriai azonosítók kötik össze az útiokmányokat és a hordozó személyt. Az Európai Bizottság 2252/2004/EC számú szabályozása 2005-ben lépett hatályba, és előírta a tagállamok útiokmányaiban (a biztonság érdekében minimálisan) alkalmazandó biometriai azonosítók szabványait. Az útlevelekben el kell helyezni egy memóriaegységet, és abban kell tárolni egy digitális arcképet. Ezen kívül egy ujjlenyomat is elhelyezendő kezelhető formában. Az adatokat biztonságosan kell tárolni, hogy biztosítsa bizalmasságukat és a jogosultságok helyes kezelését.

Megjelent egy új hordozó technológia is: a rádiófrekvenciás azonosító chipek.<sup>6</sup> Az útlevelekben használatos kártyák körképe elég változatos. RFID-chip alapú kártyákat használnak már: Dániában 2003-tól, Ausztriában 2006-tól, Belgiumban 2006-tól, Németországban 2006-tól, Finnországban, Litvániában 2007-től.

A közigazgatásban az *intézkedők* (pl. köztisztviselők, rendőrök) *azonosítása* a következő feladat. Az intézkedő személy beazonosítása azért szükséges, hogy az intézkedési jogosultságát ellenőrizni lehessen, és neki személyes felelősséget kell vállalnia az intézkedésért. Ez a rendőröknél egy azonosító jelvény kötelező viselésével történik; egyéb esetekben az ügyiratokon megjelölik az ügyintéző nevét. A jövőben az intézkedő ügyintéző elektronikusan aláírhatná az elektronikus dokumentumot.<sup>7</sup>

Végül, de nem utolsósorban a *beléptető rendszerekben* kell a személyazonosító rendszereket alkalmazni: az alkalmazottak és az ügyfelek számára más-más szinten; valamint a kiemelt biztonságú területeken (pl. börtönlátogatásnál) erősebben.

### 2.4.2. Üzleti alkalmazások

A szolgáltatások nagy része ma már elérhető vagy megrendelhető hálózatokon keresztül, és ott szükség van a megrendelő ill. igénybevevő beazonosítására

A szolgáltatásokon belül, a legnagyobb biztonságú azonosítást az üzleti életben a *pénzügyi szolgáltatások* igénylik, amikor a bankjához, biztosításához, különböző pénztárakban gyűjtött pénzéhez kíván hozzájutni az ügyfél. A pénzügyi szolgáltatók ma a szerződéskötéskor (az elsődleges személyazonosításkor) személyi okmányokat és aláírás-mintát kérnek, erre adják ki a saját azonosító kártyájukat, amire az aláírás-képet is ráviszik, vagy aláírattják az ügyféllel. Az online pénzügyi szolgáltatás igénybevételénél egy szigorú autentikációs folyamatot írnak elő, amelyben az első lépés a személyazonosítás és jogosultság ellenőrzés a bankok által kiadott eszközökkel. Egyéb szolgáltatás-megrendelésnél a bejelentkezési folyamat egyszerűbb, sokszor az IP

<sup>6</sup> Vö. *Rádiófrekvenciás azonosítás (és ami utána következik)* elemzés.

<sup>7</sup> Az elektronikus aláírás elterjesztése a közigazgatásban logikus és várható lépés, a technikai előfeltételei már megvannak.

címre támaszkodik, amely alapján elvben mindig be lehet azonosítani a felhasználót. Az IP cím alapú azonosítás valójában nem a személy, hanem a hálózati kapcsolódási pontjának beazonosítása, és csak közvetve utal a személyre. Ez sok esetben elegendő ahhoz, hogy a felhasználót beazonosítsák. Sok esetben azonban nem eléggé egyértelmű, mert vannak olyan IP-alapú rendszerek, amelyek időszakos IP-cím kiosztással működnek, ilyenkor a címkiosztási naplót is ki kell nyerni a rendszerből, és össze kell vetni az időpont adattal.

Az Internet kultúrája igényli az anonimitás lehetőségét, a névtelen email küldést is, mint ahogy postai levelet is fel lehet adni a feladó megjelölése nélkül. A kéretlen email küldemények és egyéb informatikai támadások oda vezettek, hogy a rendszerek különféle szűrőkkel védekeznek a névtelen kapcsolatfelvétel ellen, pl. ellenőrzik, hogy érvényesen regisztrált Internet felhasználó küldte-e a levelet, stb. Egyes igényesebb csoportok privát szférát erősítő technológiaként csoportos IP-címkiosztással dolgoznak, amelynek során kifelé csak a csoport látszik. Ezeket az ún. PET-technológiákat<sup>8</sup> azonban úgy kell létrehozni, hogy jogilag felhatalmazott igényre ki kell tudni adni a valódi IP-címet. A közlekedési rendszerekben valódi személyazonosítással ott találkozunk, ahol a szolgáltatási viszony ellenőrzésén túlmenően a vevők személyét is regisztrálni kell, pl. a repülésben. Több repülőtéren bevezették már az írisz-felismerésekre épülő személyazonosítást, ami eléggé lassítja az átengedési időket. Ugyanakkor, néhány nagy repülőtér (például a frankfurti is) bevezette a regisztrált légiutasok rendszerét, elsősorban törzsutasok számára. A rendszer megengedi a megbízható egyéneknek, hogy ne kelljen az íriszfelismerésen átmenniük, és így jelentős időt takaríthatnak meg a beszálláskor. Egy sor tanulmány és összehasonlító adat mutatja be, milyen hasznokkal és fenyegetésekkel jár az ilyen, előzetes szelekció.

Az ügyfélre vonatkozó, személyazonosítási technikákra épülő beléptető rendszereket ott célszerű alkalmazni, ahol jelentősebb biztonsági kockázatot tapasztalnak: tömegrendezvényeken (futballstadionban, fesztiválokon), vagy bírósági tárgyalásokon, kiemelt középületek látogatóinál, stb. A futball-huliganizmus elleni harcban is kipróbálják a biometriát: az Egyesült Királyságban hangfelismerő rendszereket tesztelnek, hogy a renitens elemek ne jussanak be olyan meccsre, amelyekre nincsenek beengedve. Svájcban a Bern klub egy arcfelismerő rendszert próbál ki, a huligánok beazonosítására.

#### **2.4.5 Egészségügyi szektor**

*Az egészségügyi rendszerek igénybevételéhez* azonosító kártyákat használnak, legyenek ezek társadalombiztosítási azonosító kódok, vagy egészségpénztári kártyák. Ez utóbbiak kombinálják a személyazonosítást, a pénztári szolgáltatások pénzügyi kártyáját, és lehetséges egészségi állapotra vonatkozó adat tárolása is a segítségükkel<sup>9</sup>.

Az egészségügyi szektorban a személyazonosításra olyan esetben is szükség lehet, amikor a személy időlegesen vagy tartósan *cselekvőképtelen vagy beszűkült tudatú* állapotban van, és kizárólag biológiai minták állnak rendelkezésre. Például olyan alkalmazásokban, ahol a gyógyszereket nem lenne szabad duplán bevenni, de a beteg ezt

---

<sup>8</sup> Lásd a *Privátszférát erősítő technológiák* című elemzésben.

<sup>9</sup> Ma még csak a háttér adatbázisban, de később valószínűleg magán a kártyán is lehetséges lesz pl. a cukorbetegség vagy epilepszia megjelölése.

nem képes kontrollálni (például drog-leszoktatási programokban), lehet alkalmazni a biometriai azonosítást a dupla használat észlelésére vagy megakadályozására is. Szükség van a személyhez kapcsolható *diagnosztikai adatok integrálására* egy-egy bonyolultabb esetben. A biometrikus információk ugyanakkor önmagukban is orvosi információforrások is lehetnek: néhány jellemzőből megállapítható, hogy a személy iszik-e, drogozik-e, terhes-e, öreg-e, érzelmi hatások alatt áll-e. Az egészségügyi személyzet azonosítása kiemelten fontos, mivel személyes felelősséggel tartoznak a paciens életéért és a paciensek érzékeny adatainak kezeléséért is. Korlátozni kell a kórházi épületekbe való bemenetet, és igazolni kell az orvosi és ápolószemélyzet bejutását, hogy az érzékeny (orvosi, genetikai stb.) adatokhoz korlátozottan jussanak hozzá. Biztonsági célból korlátozni kell a (biológiai fegyver és orvosság előállítására egyaránt alkalmas) technológiák kettős használatát – hogy az adatokhoz ne lehessen hozzáférni.

### 3. Folyamatban lévő kutatások, fejlesztések

#### 3.1. Európa

Európa nagy hangsúlyt fektet a közös fejlesztésekre és az igazgatási felhasználásokra. **Európai Biometriai Fórum** (<http://www.eubiometricsforum.com>): független európai szervezet, amelyet az Európai Bizottság támogat. Célja, hogy az EU vezető legyen a biometriában. Az érintett cégeket, kutatókat, hatóságokat és a felhasználói csoportokat is tömöríti.

Az EU által finanszírozott **BITE** projekt (<http://www.biteproject.org>) célja a biometriai témák bioetikai megközelítése. Egyedülálló ötvözet a tudományos centrumoknak, az ipari és nemzetközi szervezeteknek.

**BIOSEC** (<http://www.biosec.org>): az EU hatodik keretprogramban indult, biometriai biztonság témakörű program keretében biztonsági alkalmazásokat fejlesztenek.

Az **EJustice** (<http://www.ejustice.eu.com>) kutatási program igazságügyi alkalmazásokban fejleszt személyazonosításokat. Négy ország (Belgium, Franciaország, Spanyolország és Németország) részvételével 2006-tól folyik a pilot projekt, amelyben a bíróságokon és a büntetés-végrehajtásban próbálják megteremteni a bűnügyi regiszterek közötti együttműködést. Egyik kulcskérdés, hogyan lehet szabványosítani a személyazonosítást az EU tagállamaiban, hiszen a dokumentumok követhetősége más és más a kiállítók és a helyi végrehajtás között a különböző tagállamokban. Az Eurojust és az Eurojust hálózat közös biometrikus smart kártyákra épülhet.

**PRIME** (<http://www.prime-project.eu.org>): az „Adatvédelem és személyazonosság menedzsment Európa számára” projekt célja a felhasználó által – személyazonosságát menedzselendő – kontrollálható rendszer. A technológiai platform az adatvédelmi szabályok technológiai megvalósításán dolgozik.

**GUIDE** (<http://istrg.som.surrey.ac.uk/projects/guide>): az „Európai identitás-menedzselő rendszer az elektronikus kormányzás számára” projekt kutatást és technológiafejlesztést végez az elektronikus kormányzati hálózatok együttműködéséért. Tizenhárom ország huszonhárom szervezete vesz részt benne. Technológiával, folyamatokkal és szabályozással is foglalkozik, egy nyílt architektúrát hoz létre az identitások ellenőrzéséhez.

#### 3.2. USA

Az USA-ban az ipari csoportok erősek, az üzleti alkalmazások gyorsan terjednek. A **Nemzetközi Biometriai Csoport** (<http://www.biometricgroup.com>) az előállítókat és az alkalmazókat is tömörítő ipari csoport.

**Nemzeti Biometriai Biztonsági** (<http://www.nationalbiometric.org>) projekt USA alapítású nemzetközi nonprofit szervezet, a terrorizmus ellen küzd, amihez biometriai technológiákat is használ.

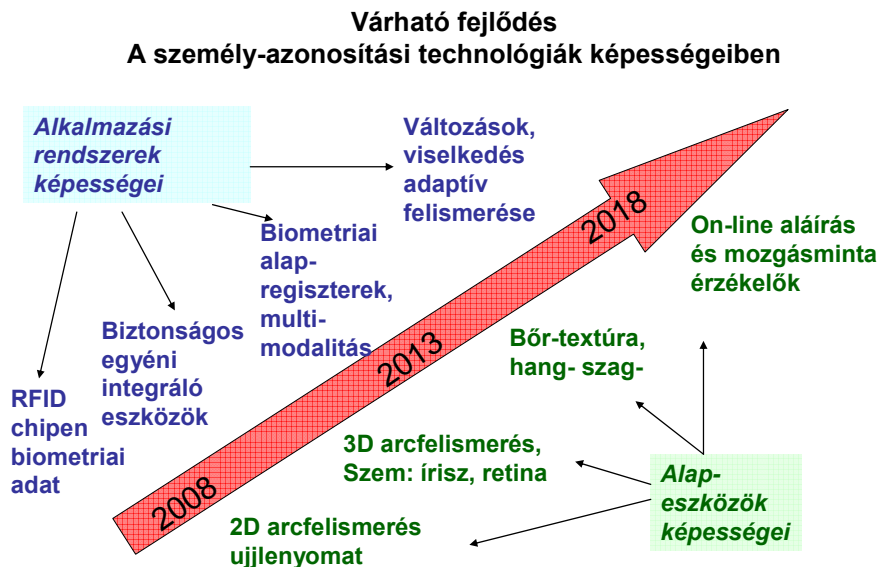
**Nemzetközi Biometriai Ipari Szövetség** (International Biometric Industry Association, IBIA, <http://66.148.3.250/aboutibia>): USA alapítású, technológiák és alkalmazások fejlesztésével, terjesztésével foglalkozó nemzetközi ipari csoport.

### 3.3. Ázsia, Ausztrália, Óceánia

Ázsiában a személyazonosítási technikák közül a tárgyalapú, RFID chipekre épülő azonosítások vannak elterjedőben. Ezeket gyakran kombinálják biometriai adatokkal, hordozóként használják biometriai adatok tárolására. A csendes-óceáni térségben nemzetközi összefogással dolgozik a **Biometriai Intézet** ([www.biometricsinstitute.org](http://www.biometricsinstitute.org)), egy független, nonprofit, tagságra épülő szervezet. Ausztrália és Új-Zéland alapította 2001-ben, elsődleges tagjai állami és ipari felhasználók, de gyártók is lehetnek benne. A biometria térségbeli általános fóruma kíván lenni.

## 4. A várható fejlődés

A várható fejlődés egyrészt az alap-eszközök képességeinek fejlődésében, másrészt az alkalmazási rendszerek komplexitásában figyelhető meg.



3. ábra: Várható fejlődés a személyazonosítási képességekben

## 4.1. Személyazonosító eszközök képességeinek fejlődése

A személyazonosító eszközök közül a biometriai technológiák gyors fejlődési folyamatban vannak, ezen belül különböző fázisban tartanak, egymással is versenyeznek, de kombinálhatók is. Kiforrott technikának mondható az arc- és az ujjlenyomat-felismerés; ehhez a háromdimenziós ábrázolás terjed a gépi rendszerekben. Gyors fejlődésben van a szem felismerése, ezen belül az írisz mintáé kiforrottabb, a retina mintázata újabb. Még kísérleti fázisban van, de már megjelent a bőrtextúra, a hang és a szagminta felismerése. A mozgásmintáé általában szintén kísérleti fázisban jár, ezen belül az online aláírás érzékelése a kiforrottabb. Léteznek már arckontúr-felismerő rendszerek is, amelyek elmaszkírozott körözött személyeket is felismerhetnek arcvonásaik és mozgásuk alapján. Várható, hogy a biometriai technológiák stabilizálódnak, alkalmazásuk nemcsak megbízható, de gyors is lesz, és alacsony lesz a fertőzési, vagy a környezetszennyezési kockázat.

A tárgyi eszközök is fejlődnek, egyre kódoltabban tárolják az információkat, beleértve a biometriai információkat is. Az elektronikus tárgyi személyazonosító eszközöknél a hosszú távú technológiai migrációt meg kell oldani, mivel egy-egy személy azonosításának használhatónak kell lennie kb. 100-120 évig, de a leszármazottak számára több (átlagosan 3-4) generáció adatára is szükség lehet.

## 4.2. Személyazonosító alkalmazások fejlődése

Az egyén számára a biometriai alkalmazások új biztonságos technológiákat kínálnak a különböző azonosítási funkcióinak *integrálására*. Ez történhet a jelenlegi kódok biztonságos és könnyen visszakereshető tárolásával is, de önálló integráló eszközzel is. Az integrálási technológiában is számolni kell a biztonsági másolatokkal és a felhasználó sérült, cselekvőképtelen vagy öntudatlan állapotával.

Az új személyazonosító technikák általánossá válásához ki kell épülniük a *biometriai* adatokat is tartalmazó *alapregisztereknek* (például ujjlenyomatot is tartalmazó anyakönyvezésnek). A nagyobb megbízhatóság érdekében *multimodális biometriai* jellemzőket használnak, azaz egyidejűleg többféle biometriai mintát, például ujjlenyomatot, íriszképet és 3D-s arcábrázolást vetnek össze.

Komoly fejlődési irány a *változások* modellezése és érzékelése. Az emberi test idővel, sérülések, betegségek következtében megváltozik, amit a rendszereknek intelligens hasonlóság-érzékeléssel kell kiszűrniük. Egyes emberek (például plasztikai sebészettel) el is változtathatják a külsejüket, és ezt a rendszereknek fel kell ismerni, valamint kezelni is kell. A *viselkedési minta* alapú azonosítások terjedéséhez szenzorokkal és *adaptív* mechanizmusokkal meg lehet tanítani a rendszereket arra, hogy egy korábban már azonosított személy vonásait, viselkedését, hanghordozását, szóhasználatát, mozgását megjegyezzék, és ezek alapján felismerjék, ha tőle nem elvárható, szokatlan viselkedést tanúsít. Ilyenkor felmerül a gyanú, hogy befolyásolás alatt lévő vagy egészen más, valakinek az identitását bitorló személyről van szó.

## 5. Befolyásoló tényezők

### 5.1. Technológia

A tárgyi alapú technológiák kidolgozottak, a biometriai azonosítás gyorsan fejlődik. Utóbbihoz elsősorban a mintatárolási kapacitásokat kell megsokszorozni. Az ujjlenyomat alapú adatintegráláshoz olcsó, megbízható és kis helyigényű – mobiltelefonban vagy

bankkártyán is elférő – szkennelés kell. A viselkedési minta megbízható felismeréséhez hatékony adaptív algoritmusok fejlesztése, megbízhatóságuk mérése szükséges.

## **5.2. Társadalom**

Az új személyazonosítási technológiák használatára vonatkozóan új szabályozásnak kell létrejönnie. A biometriai azonosság személyes adatnak számít, a nemzeti adatvédelmi hatóságok nagy szerepet kapnak abban, hogy engedélyezik vagy nem a biometriai módszerek szükséges és arányos alkalmazását. A hatóságok nagy reményeket fűznek a biometriához, a határvédelem, a személyazonosító okmányok és a közösségi terek védelme érdekében.

## **5.3. Gazdaság**

Az új technológia valódi haszna, hogy szabványosítja az utazások és betelepülések ellenőrzési folyamatát, egy sor üzleti- és állami szolgáltatást, ez csökkentheti a családok kockázatát. Világossá tehető és elmagyarázható a polgároknak, hogy a magánélet zavartalanságából mennyit kell feláldozniuk a szolgálatokból származó haszonért.

# **6. Várható hatások**

## **6.1. Technológia**

*A biometriai azonosítás technológiai hatása a kapcsolódó orvos-diagnosztikai területek fejlődése, például íriszfelismerésből írisz-diagnosztika, géntérképéből örökletes betegségek és kezdődő rákbetegség szűrése.*

A viselkedésminta-alapú azonosítás várható technológiai hatása a viselkedési felismerők, analízátorok és szintetizátorok, szimulátorok fejlődése, amelyeket oktatásban, fogyatékos emberek kiszolgálásában alkalmazhatnak. Távlabbi alkalmazási módja lehet a valószínűleg a bűnüldözésben és a védelem egyes területein alkalmazható „virtuális személyiségprofil” kialakítása.

## **6.2. Társadalom**

A modern személyazonosítási technikák használatának társadalmi hatása, hogy növeli a biztonságot, a bizalmat, a szabálykövető magatartást.

A személyek használnak egy sor tárgyat, amelyek alkalmasak a beazonosításukra. A személy tudtán kívüli azonosítása, nyomon követése, magatartásának megfigyelése lehetséges technikailag. A jogszabályok védik ugyan, de csak a tudatos és viszonylag képzett személyek tudják valójában érvényesíteni ilyen irányú jogait. A hátrányos helyzetűek, képzetlenek, nem tudatosan gondolkodók többnyire fel sem ismerik a megfigyelhetőségükből adódó kockázatokat. Emiatt, igény merülhet fel az azonosítással foglalkozók feletti társadalmi kontroll növelésére.

Olyan emberek azonosítására is használhatók a modern személyazonosítási eszközök, akik nem képesek magukat azonosítani, vagy más sajátos csoportok; és ez kritikus lehet, etikai szempontból, mert az ilyen csoportok nem, vagy korlátozott belátással rendelkeznek a témáról. Lehetnek olyan politikai csoportok is, amelyek radikálisabb eszméket hangoztatva elutasítják az új személyi azonosítási technológiákat. Egyesek viszont éppen a társadalmi kontroll kiépítésére akarják majd széleskörűen felhasználni.

### **6.3. Gazdaság**

A technológiai fejlődés együtt jár új cégek megjelenésével, összeolvadásával és felvásárlásával. A széttöredezetttség mind a cégeknél, mind a technológiáknál, éretlenségre utal. Optimista becslések szerint, a biometriai alkalmazások, amelyek a személyazonosítási alkalmazásoknak csak egy részét teszik ki, piacának éves átlagos növekedése 39%; és ennek kb. a felét az USA, egynegyedét Európa állítja elő. Az európai piac mérete gyorsan növekedik: 2000-ben 7,3 millió euró, 2004-ben 46,3 millió euró 2007-ben már 360 millió euró volt, míg 2010-re 614 millió eurót becsülnek.

## **7. Hazai helyzet**

### **7.1. Jelenlegi helyzet**

Az ujjlenyomat használata a nagybiztonságú terek beléptető rendszereinél már előfordul, vagy nemsokára elkezdődik. A géntérkép ma még elsősorban az orvosi gyakorlatban létezik, és nem személyazonosításra használják..

Az Európai Unió 13/12/2004 határozatával bevezette az európai uniós útlevélek új szabványát, amelyben biometriai jellemzőket is el kell helyezni. Az útlevélekbe kötelezően be kell tenni az arckép és az ujjlenyomat biometriai adatait. Ezen túlmenően, az adott tagállam döntése szerint el lehet helyezni más biometriai azonosítót is. A Miniszterek Tanácsa 2004-ben a tagállamok figyelmét szorosabb adatmegosztási és határbiztonsági együttműködésre hívta fel, a nemzetközi terrorizmus és szervezett bűnözés elleni harc érdekében.

### **7.2. Kutatások, fejlesztések és a várható fejlődés**

A személyazonosítási technikák esetében Magyarország követő átvételt valósít meg. Nemrég zárult le a „Jogügyletek biztonsága” c. EU-s projekt, amely az ingatlanforgalmazásban résztvevő közjegyzők és ügyvédek számára online szolgáltatásként nyújtja az ügyfelek személyi okmányainak ellenőrzését.

Hazánk az EU által előírt technikákat alkalmazza a személyi okmányokban, így az újonnan kiadott útlevélekben is.

Viselkedési minta alapú azonosítás ma még kutatási fázisban hazánkban is, de a repülőterek és bankfiókok biztonsági kamerái mögött nemsokára várható.

### **7.3. Befolyásoló tényezők és hatások**

Az állampolgárok elvárják az állam gondoskodását a személyi és vagyonbiztonság tekintetében. A kötelező társadalombiztosítási rendszer is hosszú távú, személyhez kapcsolódó adattárolást igényel. A közigazgatási szolgáltatások igénybevételéhez a tárgyi alapú adathordozóban előbb-utóbb biometriai adatokat is fognak tárolni. Az adatok elosztott tárolása esetén is lehetővé válik egyes igazgatási és közszolgáltatási adatbázisok állandó vagy ad hoc jellegű összekapcsolása. Két területen lehet gond: a munkavállalók, valamint a cselekvőképtelen és a korlátozottan cselekvőképes személyek beazonosítása biometriai adatok alapján. Ezek a csoportok kiszolgáltatott helyzetben vannak, lehetnek, és emiatt a személyazonosításuk körültekintő szabályozást igényel.

*Kelet-európai specialitás, hogy az állampolgárok bizalmatlanok a kötelező állami adatrendszerekkel és adattárolásokkal kapcsolatban. Történelmi tapasztalatok mutatják, hátrányos lehet, ha archiválják és nem az eredeti célra használják érzékeny adatainkat.*

## 8. Összegzés

A személyazonosság alapja az *identitás*, amely egyidejűleg elismer egy csoporthoz tartozást, pl. állampolgárságot, és ezen belül igazolja az egyediséget is. Hosszú távra a személyazonosítás alapja az *okmány*, amelyet egy *alapregiszter* alapján a hatóságok állítanak ki.

A személyazonosítás gyakorisága és biztonságossága iránti igény nőni fog. Az állam online szervezi a saját szolgáltatásait, távolabbi személyek lépnek egymással üzleti kapcsolatba, a kockázatosabb üzletágak is elérhetők hálózatokon. A gépi archiválás, jogosultság kezelése és egy sor gépi tevékenység is a személyazonosítási technikákra épül rá. A technológizálódás, a társadalmi-gazdasági rétegződés, a virtuális közösségek létrejötte együttesen növeli a személyi azonosítási igényeket.

A volumenében és biztonsági szintjében is növekvő igényekre válaszul, bevezetésre kerülnek a *magasabb biztonsági szintű azonosítási technikák*. Bővül az új, nagyobb hatékonyságú személyazonosítási megoldások választéka a kínálatban. Ezek az új technológiák nagyobb biztonsággal azonosítják a személyt. A *tárgyi és tudás alapú technikákat* leváltja egy *multimodális biometriai mintára épülő*, és az adatokat *elektronikusan tároló* technológia, amely egyesíti az eddigi és újabb eljárások előnyeit. Az *egyén* kontrollálni szeretné a többféle kapcsolódást a szolgáltatási rendszerekhez: *integrálni* kívánja saját azonosítási technikáit, és tudatosan benne, hogy több adatot tárolnak róla különböző helyeken, mint korábban. A személy tudta és beleegyezése nélkül is azonosító és nyomkövető technológiák növelhetik a személy feletti társadalmi kontrollt. A növekvő biztonság, bizalmat szerezhet az online rendszereknek. A növekvő vagy legalább szinten tartott biztonság is ára van.

Az igényesebb felhasználói körök várhatóan kikényszerítik, hogy a személyazonosítási technikák alkalmazását, a keletkező adatok felhasználhatóságát szabályozzák.

## Ajánlott irodalom

- BITE (Biometrics, Identification, Technology, Ethics) Project: *Ethics and Biometrics*. 2005-2007. (<http://www.biteproject.org>)
- Dessimoz, Damien – Richiardi, Jonas – Champod, Christophe – Drygajlo, Andrzej: *MBIOID: Multimodal Biometrics for Identity Documents – State-of-the-Art*. Université de Lausanne, École Polytechnique Fédérale de Lausanne, 2006. ([http://www.europeanbiometrics.info/images/resources/90\\_264\\_file.pdf](http://www.europeanbiometrics.info/images/resources/90_264_file.pdf))
- Goudarzi Pour, Babak – Adolfsson, Victor: *Reliability, Availability and Maintainability (RAM) in Biometric Applications – Delivering Quality of Service that customer wants*. Optimum Biometrics Labs, EBP (European Biometrics Portal), 2008. ([http://www.europeanbiometrics.info/images/resources/124\\_597\\_file.pdf](http://www.europeanbiometrics.info/images/resources/124_597_file.pdf))
- Schmitz, Patrice-Emmanuel – Huijgens, Ronald – Tavano, Roberto – Lodge, Juliet – Aisola, Kamini – Flammang, Marc: *Biometrics in Europe – Trend Report 2006*. Unisys, EBP (European Biometrics Portal), 2006. ([http://www.libertysecurity.org/IMG/pdf/Trend\\_Report\\_2006.pdf](http://www.libertysecurity.org/IMG/pdf/Trend_Report_2006.pdf))
- Schmitz, Patrice-Emmanuel – Huijgens, Ronald – Flammang, Marc – Schaffner, Ed – Tavano, Roberto: *Biometrics in Europe – Trend Report 2007*. Unisys, EBP (European Biometrics Portal), 2007. ([http://www.europeanbiometrics.info/images/resources/121\\_975\\_file.pdf](http://www.europeanbiometrics.info/images/resources/121_975_file.pdf))