PRISZNYÁK SZABOLCS

A TENYÉRVÉNA ALAPÚ AZONOSÍTÁS EGYES ALKALMAZÁSI LEHETŐSÉGEI

1. Bevezetés

Napjainkban egyre nagyobb igény van a biztonságra, ennek következtében egyre újabb és újabb módszerekkel védjük értékeinket. Egyre kiemelkedőbb szerepe van a személy-, a vagyon-, és az adatvédelemnek. A XXI. században az adatok döntő többségét számítógépeken, adatbázisokban tároljuk, így az adatok védelmét – a hagyományos papír alapú dokumentumok fizikai védelme mellett - egyre inkább információs rendszerek védelmével – a hozzáférés korlátozásával, ellenőrzésével - valósítjuk meg. A személyek, vagyoni értékek, adatok védelme során kiemelt jelentősége van a személyazonosításnak.

A különböző védelmi rendszerek kialakítása, ezzel párhuzamosan a személyek azonosítása évszázadokra, évezredekre nyúlik vissza, gyakorlatilag egyidős az emberiséggel. A különböző rendszerek fejlesztése, biztonságának fokozása megalkotásuktól folyamatos, és természetesen a tudás bővülésével sorra dolgoztak ki új megoldásokat, rendszereket is. A kezdeti módszerek fejlődése során megfigyelhető a tudás beépülése, így a fizikai védelmi módszerek mellett megjelentek a matematikai módszerek. Később a biometrikus módszerek is alkalmazásra kerültek. Az elektronika elterjedését követően egyre inkább ez a technológia is beépült a személyazonosításba, megújítva, kiegészítve a korábbi módszereket. Napjainkban az informatika robbanásszerű elterjedésével párhuzamosan a személyazonosításra szolgáló technológiák terén is hatalmas, gyors a fejlődés, egyre elterjedtebbek az informatikai alapokra épülő módszerek.

Ilyen módszer a cikkben bemutatásra kerülő tenyérvéna alapú azonosítás is. Itt mind a mintavételhez, annak tárolásához, mind a későbbi kereséshez, ellenőrzéshez, azonosításhoz informatikai háttér szükséges. A cikkben ismertetem a legelterjedtebb személyazonosítási módszereket, ezeket meghatározott szempontok szerint csoportokba sorolom. Ismertetem az egyes csoportokra vonatkozó legfőbb jellemzőket, illetve a gyakorlati használati lehetőségeket, előnyöket, hátrányokat. Ismertetem, hogy a fenti csoportosításon alapuló rendszerben hol helyezkedik el a biometrikus azonosítás, illetve, hogy hova sorolhatjuk a tenyérvéna alapú azonosítást. Részletesen ismertetem a tenyérvéna alapú azonosítás módszerét, fizikai, biológiai alapjait. Bemutatom az ipar által kialakított technológiát, bemutatom az alkalmazás lehetőségeit, mind az alkalmazott eszközök, mind a módszerekre vonatkozóan. Javaslatokat teszek a gyakorlati alkalmazásra a rendvédelmet érintően, elsősorban saját szakterületemre – a büntetés-végrehajtásra – fókuszálva. A javaslatok között megemlítem mind a fogvatartottak, mind a személyi állomány körében felmerülő alkalmazási lehetőségeket. Bemutatom a rendvédelem további területein alkalmazható megoldásokat, érintve a bűnüldözést, az idegenrendészetet, ideértve a - schengeni térség – határellenőrzését is. A hazai alkalmazás lehetőségének vizsgálata során ismertetem az egyes területeket érintő jogszabályi korlátozásokat, lehetőségeket. Egy esettanulmány feldolgozásán keresztül bemutatom a tenyérvéna alapú azonosítás egy megvalósult rendszerét a török egészségbiztosításban alkalmazott rendszer ismertetésével.

Az összegzésben az új megoldás nyilvánvaló előnyeinek felsorolása mellett felvázolom az esetleges rendvédelemi alkalmazásban jelentkező előnyöket is. Publikációm elkészítése során feldolgoztam a témához kapcsolódó hazai és nemzetközi szakirodalmat, jogszabályokat, valamint az ipari szabványokat, gyártói ismertetőket, ajánlásokat. Tanulmányoztam több külföldön megvalósult rendszer tervezésének, kialakításának, bevezetésének tapasztalatait összegző esettanulmányt.

2. Személyazonosítási lehetőségek

A személyek azonosításának egyre nagyobb jelentősége van napjainkban, hiszen azonosítanunk kell magunkat – a teljesség igénye nélkül – hivatali vagy akár közszolgáltatónál történő ügyintézésnél, készpénz nélküli fizetésnél, informatikai rendszerekhez történő hozzáférésnél, legyen az akár munkahelyi, akár otthoni, akár szolgáltatásként igénybevett alkalmazás. Fentieken túl szintén szükséges személyazonosságunk igazolása különböző épületekbe, építményekbe, magánterületre vagy akár meghatározott időszakra és célra körülhatárolt közterületre, rendezvények helyszínére történő belépéskor.

A biztonság ilyen mértékű fokozásával felértékelődött a személyazonosításra szolgáló technikák, módszerek szerepe is. A személyek azonosításának módszerei nagyon sokrétűek, ezért meghatározott szempontrendszer szerint célszerű csoportosítani őket.[466]

Tudás alapú azonosítás: ez a legrégebbi azonosítási módszer, nem áll rendelkezésre sem tárgy, sem más segédeszköz az azonosítás valamilyen információ tudásán alapul. Ide tartozik a név, jelszó, valamilyen azonosító kód, pl. a PIN-kód. Hátránya, hogy amennyiben az azonosításhoz szükséges információ kompromittálódik, úgy a módszer elveszti hitelességét.

Tárgyi alapú azonosítás: az egyik legelterjedtebb módszer, az azonosítás valamilyen tárgy birtoklásán – és egyes esetekben a tárgyon vagy tárgyban tárolt ember vagy gép által olvasható információn – alapul. Ebbe a kategóriába tartoznak a kulcsok, pecsétek, jelvények, kitűzők, igazolványok, mágneskártyák, chip kártyák, RFID-k. Jellemző a széleskörű elterjedtség, illetve az alkalmazott eszközök és technológiák folyamatos fejlesztése. Ezek a fejlesztések az egyre nagyobb biztonságra irányulnak. A felsorolásban szereplő jelvényhez, vagy kitűzőhöz képest egy biztonsági jeggyel ellátott igazolvány, vagy még inkább az elektronikus technológiával olvasható információkat tároló mágneskártya vagy RFID alkalmazása nagyobb biztonsági szint elérését teszi lehetővé. A tárgyi alapú azonosítás hátránya, hogy a tárgy elvesztésekor, sérülésekor, megsemmisülésekor vagy ellopása esetén nem lehetséges az azonosítás. Egyes esetekben pedig – a talált vagy lopott azonosításra szolgáló tárgyakat – arra nem jogosult személyek rosszindulatúan, bűnös szándékkal felhasználhatják.

Biológiai alapú azonosítás: az ember biológiai jellemzőire épülő azonosítási módszer. Ehhez a csoporthoz tartoznak az ujjnyomatot, kéznyomatot, kézgeometriát, arc információt (arckép, fénykép), termogrammot, szem információt (írisz, retina), illatot, DNS jellemzőket használó rendszerek. Ebbe a kategóriába tartozik az egyik legújabb módszer a tenyérvéna alapú azonosítás is. A biológiai alapú azonosítás a korábban ismertetett módszerekhez képest nagyobb biztonságú azonosítást eredményez. Előnye, hogy sem tudás, sem tárgy nem szükséges hozzá, így – a tudás alapú információ – nem kompromittálódhat,

[466] Kondás Katalin: A biometria jelenlegi megítélése. Hadmérnök 2013/1. sz. 24-25. o.

azonosításra szolgáló tárgy birtoklása nem szükséges. További előny, hogy – az esetek többségében – az azonosításhoz szükséges az érintett személy fizikai jelenléte, amely a biztonságot fokozza. A módszerek hátránya lehet, hogy bizonyos jellemzők az életkor előrehaladtával változhatnak. Ugyancsak változhatnak a jellemzők – esetenként ideiglenesen - a személyek speciális helyzetében, ilyen lehet pl. egy egyszerű betegség, amely következtében változhat az írisz, vagy egy kézsérülés, amely okán megváltozhat az ujjlenyomat. Bizonyos esetekben bonyolult, esetenként pedig költséges a mintavétel és azonosítás.

Viselkedési minta alapú azonosítás: az emberek bizonyos viselkedési minták alapján is azonosíthatóak. Ebben a csoportban a legismertebb a kézírás, de ide tartozik még a beszédhang, a gépelési ritmus, a járási mód, a szóhasználat, a testbeszéd és az arcmimika is. A felsoroltak közül a kézírás – aláírás – nagyon gyakran használt, ellenben a többi módszer a gyakorlatban rendkívül ritkán alkalmazott. A viselkedés alapú azonosítás egyes elemeinek hátránya, hogy gépi módszerek alkalmazásával nehezen kezelhető, problémás a mintavétel és a gyors, pontos azonosítás, ellenőrzés is.

A biológiai és viselkedési csoportot együttesen biometrikus azonosítóknak is nevezik. A biometria görög eredetű szó, ahol a bio az életet, a metric a mérést jelenti. Mai értelemben véve élettudományi jelenségeket ismert matematikai módszerek alkalmazásával vizsgáló interdiszciplináris tudomány, vagyis egyedi vonások meghatározására szolgáló eljárások összessége. A biometria méri és rögzíti az emberek egyedi – többségében – megváltoztathatatlan fizikai, testi jellemzőit.[467] A biometrikus azonosítás alkalmazható személyazonosításra (a rendszer azonosítja a személyt, a teljes adatbázisból kikeresve a megegyezőt), illetve ellenőrzésre (a rendszer hitelesít egy személyt az előzőleg bejegyzett mintái alapján).[468]

A tényleges alkalmazás során nagyon gyakori több különböző módszer kombinálása, együttes alkalmazása. Ilyen lehet a tudás és a tárgyi alapú módszer kombinálása pl. egy kártya és egy hozzá szükséges kód együttes alkalmazása, de ilyen a tenyérvéna és a hozzá szükséges kód együttes alkalmazása is. Több különböző módszer kombinálásának kettős célja lehet, egyik egyértelműen a biztonság fokozása. A két módszer együttes alkalmazásának másik oka az egyszerűbb, gyorsabb azonosítás, ez főleg a nagy háttéradatbázis esetén előnyös, pl. ha a tenyérvénát egy – felhasználónként egyedi - kóddal együttesen alkalmazzuk, akkor adott esetben nem szükséges az akár több millió rekordot tartalmazó adatbázis valamennyi elemét vizsgálnunk, hanem az egyedi kódhoz kötött – korábban rögzített – mintát kell az aktuális információval hasonlítani azonosítás céljából.

3. A tenyéralapú azonosítás

A Fujitsu az eddigi biometrikus és felületen alapuló azonosítási lehetőségeken túllépve megalkotta a tenyérvéna alapú azonosítás technológiáját, amelyet PalmSecure-nak nevezett el.[469] Az azonosítás a vénamintázat felismerésével történik. Az egyénre jellemző vénamintázat rögzítéséhez a PalmSecure infravörös-közeli sugarakat bocsát ki, amelyeket az ember tenyerének ereiben áramló vérben található oxigénmentes hemoglobin elnyel. Ily

[467] Nyári Éva: A határellenőrzési tevékenységek során alkalmazott technológiák, technikai eszközök és berendezések, fejlesztésének irányai a Schengen térségben. Hadtudományi Szemle 2014/1. sz. 201. o.
[468] Sikos László: Biometrikus azonosítók harca, Információ és biztonság http://iesb.hu/fizikai-biztonsag/biometrikus-azonositok-harca/ (letöltés ideje: 2014. 06. 20.)
[469] http://globalsp.ts.fujitsu.com/dmsp/Publications/public/ds-PalmSecure-eu-hu.pdf (letöltés ideje: 2014. 07. 22.)

módon a tenyér képe vénamintázatként rögzíthető, és – pl. a fizikai helyszín vagy a számítógépes hálózat elérésének engedélyezése vagy megtagadása, stb. céljából – a felhasználó korábban rögzített mintájával összehasonlítható. A rendszer – a minta rögzítése és későbbi ellenőrzése során - több mint 5 millió referencia pontot vizsgál.

A PalmSecure érintkezésmentes beolvasást alkalmaz, ami higiénikus módszer és feloldja azt az ellenérzést, ami egyes felhasználóknál a – más biometrikus módszereknél alkalmazott - érintkezők megérintése miatt jelentkezhet. Az érintkezésmentes megoldás kidolgozása – többek között – a japán társadalmi, kulturális szokásokra, hagyományokra vezethető vissza. A nyitott tenyér (ujjak nélkül) komplex vénamintázatának leolvasása 4-6 cm-ről történik, tehát a technológia nem invazív, így nyilvános helyen történő használat esetén is stressz mentesen alkalmazható módszer. Ezek a tulajdonságok összességében nagyobb felhasználói elfogadottságot eredményeznek.

Mivel az erek a testen belül találhatók, a személyazonosság hamisítása rendkívül nehéz, így garantált a nagyfokú biztonság. Fontos tény, hogy az azonosítás – ellentétben pl. az ujjlenyomattal – csak élő szervezet esetében lehetséges, hiszen a szervezet belsejéből nyert információhoz aktív vérkeringésre van szükség. Az egyedi mintázat 5-6 éves korra kialakul, és az életkor előrehaladtával már nem változik. A tenyérvéna mintázata egypetéjű ikrek esetén is különböző. Rendkívül könnyen kezelhető módszer, amely kihasználja a kéz természetes pozícióját, így az azonosítás folyamata kényelmesebb, mint pl. az írisz vagy a retina alapú azonosítás alkalmazása esetén.

Az innováció műszaki alapja egy kisméretű (35x35x27 mm) és kis súlyú (50 g) egység, ami integrálható multimodális – más funkciókat is ellátó – eszközökbe, így pl. egérbe, billentyűzetbe, laptopba, de beléptető rendszerekbe, bank automatákba is.[470] A gyártó az eszközhöz szoftver fejlesztői környezetet (SDK) biztosít, amely lehetővé teszi a más technológiákkal – akár több tényezős azonosítást végző rendszerekkel - történő integrációt. A műszaki paraméterek között meg kell említeni – az integrálhatóság mellett - a széles körű csatlakoztatási lehetőséget is, hiszen az eszközön megtalálható az USB és az RJ45 szabványú csatlakozó is. A széles működési tartomány a hőmérséklet (0-60°C) és a páratartalom (10-90%) vonatkozásában, amely lehetővé teszi a szabad téri alkalmazást is. A PalmSecure vénaszkenner érzékelő egységének felülete cseppálló – megfelelés az IP41 (ingress protection[471]) szabványnak – a vénaadatok regisztrációja vagy azonosítása azonban nem ajánlott akkor, ha az érzékelő felületén vízcseppek vannak. Az azonosítási idők az alábbi táblázatban foglaltak szerint alakulnak.

[470] http://www.pcpro.co.uk/reviews/mice/246581/fujitsu-palmsecure (Letöltés ideje: 2014. 07. 22.)
[471] http://megaohm.hu/index.php/erintesvedelem/ip-vedettseg (Letöltés ideje: 2014. 07. 23.)

Azonosítási idő			
Ellenőrzés (1:1)		Kéz érzékelése	0,2 másodperc
		Rögzítés	0,4 másodperc
		Ellenőrzés	0,2 másodperc
		összesen:	**0,8 másodperc**
Azonosítás (1:N)	S-módszer N = 10 fő (20 kéz)	Kéz érzékelése	0,2 másodperc
		Rögzítés	0,4 másodperc
		Ellenőrzés	0,9 másodperc
		összesen:	**1,5 másodperc**
	F27-módszer N = 500 fő (1000 kéz)	Kéz érzékelése	0,2 másodperc
		Rögzítés	0,4 másodperc
		Ellenőrzés	2,4 másodperc
		összesen:	**3,0 másodperc**

A biometrikus rendszerek esetében a gyártók valamint az üzemeltetők és felhasználók szempontjából különlegesen fontos jelentősége van két valószínűségi jellemzőnek.[472] Az egyik a téves elfogadási arány (FAR=False Accept Rate), amely arról ad felvilágosítást, hogy illetéktelen, tehát nem regisztrált mintát milyen eséllyel fogad el a rendszer, ez a PalmSecure-nál 0,00008%. A másik a téves elutasítási arány (FRR = False Reject Rate), amely arra vonatkozólag ad információt, hogy a regisztrált felhasználók esetében milyen eséllyel következik be elutasítás, tehát mi a valószínűsége annak, hogy egy jogosult személyt a rendszer nem ismer fel, ez a PalmSecure esetében 0,01%. Mindkét érték nagyon magas megbízhatóságúnak számít a biometrikus azonosítási módszerek között.

A PalmSecure az első tenyérvéna-alapú azonosító rendszer és a harmadik nemzetközi szabvány szerint tanúsított biometrikus azonosító rendszer a világon. Az utóbbi években sokféle alkalmazási területen elterjedtek az erekre, ujjlenyomatokra és íriszmintázatra épülő azonosító rendszerek (pl. PC-k vagy üzleti alkalmazások hozzáférése, személyazonosítás ATM-eknél és beléptető rendszereknél). Amikor a Fujitsu Csoport bevezette a tenyérvéna-alapú azonosítást a közösségi infrastruktúra területén, pl. a bankszektorban, az egészségügyben és a felsőoktatási vizsgáztatásban, ügyfelei (pl. a Japánon kívüli kormányzati intézmények és pénzintézetek) megkérték, hogy vesse alá a megoldást független biztonsági tanúsításnak. A Fujitsu erre a kérésre reagálva tanúsította azonosító megoldását az informatikai biztonság közös követelményei – Common Criteria1 for Information Technology Security Evaluation (ISO15408) – szerint EAL2-es megfelelési szintre. A közös követelményeken belül hét, egyre szigorodó megfelelési szint létezik. A magasabb megfelelési szint azt jelenti, hogy szélesebb körben tesztelték az értékelési cél (Target of Evaluation, TOE) biztonsági minőségét, bár ez nem feltétlenül jelez magasabb szintű biztonságot. A PalmSecure esetében a 2-es megfelelési szint a strukturális tesztelés elvégzését bizonyítja.

[472] http://www.securinfo.hu/termekek/biometria/1016-matematikai-modszerek-a-biometriaban-1.html (Letöltés ideje: 2014.07.23.)

4. Alkalmazási lehetőségek

A tenyérvéna mintázaton alapuló azonosítást minden olyan helyen alkalmazhatjuk, ahol más személyazonosítási módszereket alkalmazunk. Ennek a biometrikus azonosításnak azonban megvan az – a korábban ismertetett - előnye, hogy nem szükséges hozzá tárgy pl. mágneskártya, chipkártya, stb. illetve valamilyen információ tudása sem. Egyes esetekben azonban a tenyérvéna azonosításhoz is alkalmaznak tudás alapú azonosítási technikát is (pl. PIN kód), ahogy azt a Személyazonosítási lehetőségek fejezet végén ismertettem. Ennek alapján a technológia alkalmazható beléptető rendszerek, munkaidő nyilvántartó rendszerek esetében. Kiemelt alkalmazási terület az informatikai eszközökhöz, rendszerekhez, így adatokhoz, információkhoz történő hozzáférés szabályozása, ellenőrzése.

Napjainkban egyre nagyobb a jelentősége a biztonságnak, ezért fontos alkalmazási terület a különböző okok miatt körülhatárolt, lezárt területekre történő be- és kilépés, így pl. ipari létesítmények, konferenciák, sportesemények látogatása esetén alkalmazható a technológia. A biztonság igénye fokozottan érvényesül a repülőtereken, ezért ez is egy fontos alkalmazási terület lehet.

Szintén fontos terület a banki, közigazgatási ügyintézés, az egészségügyi szolgáltatásokhoz való hozzáférés során történő személyazonosítás. A bankokkal kapcsolatban nem csak az ügyfélszolgálaton történő ügyintézés lehet alkalmazási terület, hanem fizetési rendszerek is kialakíthatók a tenyérvéna alapú azonosítás nyújtotta biztonság alapjaira építve, így lehetségessé válik, hogy nem a bankkártyánkkal fizetünk, hanem a „tenyerünkkel". A tenyérrel fizetés nem csak a jövő, hanem a közelmúlt és a jelen is. A Nyugat- és Észak-európai országokban több példa is van tenyérvéna alapú fizetési rendszerekre. Ezek a rendszerek – a teljes infrastruktúra kiépítésének magas költsége miatt – jellemzően kisebb területen, egy-egy városban, szervezetnél valósultak meg. Az egyik legújabb ilyen rendszert a svédországi Lund városában alakították ki. Lund Svédország déli részén fekszik Malmö közelében, egy kb. 80 ezer lakosú város, de itt működik a Lund Egyetem, amely Svédország legnagyobb egyeteme. Az egyetemre mintegy 46 000 diák a jár világ kb. 150 országából. Az egyetem több elismert nemzetközi rangsorolási listán is benne szerepel a világ 100 legjobb egyetemében.[473] Ebben az innovatív környezetben 2014 tavaszán vezették be a tenyérvéna alapú fizetési rendszert[474], amellyel kapcsolatosan az egyetem polgárainak első tapasztalatai pozitívak.[475]

Külön terület a rendvédelemben történő alkalmazás lehetősége. Itt egyrészt a rendvédelemi alkalmazottak oldalán merülnek fel alkalmazási lehetőségek, másrészt a rendvédelemmel valamilyen módon kapcsolatba kerülő személyek (pl.: ügyfelek, gyanúsítottak, fogvatartottak, stb.) esetében.

A rendvédelmi alkalmazottak a legtöbb esetben azonos élethelyzetekben használhatják eredményesen a rendszert, mint a fent említett civil szféra. Így a munkahelyükre, rendvédelmi objektumokba történő be- és kilépés céljából, egyes objektumokban a különböző zónák közti mozgások biztosítására, a speciálisan védett területekre (pl.: biztonsági területek, informatikai központok, stb.) történő belépés céljából, a munkaidő nyilvántartás okán, informatikai rendszerekhez történő hozzáféréshez alkalmazható hatékonyan a tenyérvéna alapú azonosítás. Ezen lehetőségek szinte

[473] http://www.lunduniversity.lu.se/about-lund-university (Letöltés ideje: 2014. 07. 30.)
[474] http://www.lth.se/english/about_lth/news/news/article/buy-lunch-pay-with-your-hand/ (Letöltés ideje: 2014. 07. 30.)
[475] http://www.youtube.com/watch?v=4g_YL7O9wsU&feature=youtu.be letöltve: 2014. július 30.

mindegyike esetében a hatékony működéshez szükséges lehet más informatikai rendszerekkel, adatbázisokkal történő adatcsere, integráció. Ezeket a rendszerintegrációkat minden esetben meg kell, hogy előzze a jogi, adatvédelmi vizsgálat.

A rendvédelmi feladatok végrehajtása során is sok alkalmazási terület lehet. A bűnüldözési tevékenység során meg kell említeni a tenyérvéna alapú azonosítás egyik hátrányát. Problémát jelent, hogy a tenyérvéna nem marad ott a helyszínen, azaz egy cselekmény után utólagosan nem alkalmas személyazonosításra, ellentétben pl.: az ujjlenyomattal, fogmintázattal, DNS-sel stb. A bűnüldözésben is csak személyazonosításra használható korábban rögzített minta alapján.

A büntetés-végrehajtásban azonban több alkalmazási lehetőség is létezik. Az egyik legfontosabb a bérrabság kiszűrése, vagyis azoknak a helyzeteknek a felismerése, amikor az elítélt helyett egy másik személy jelentkezik a büntetés letöltésére. Természetesen ebben az esetben is szükséges az előzetesen rögzített minta. A tenyérvéna alapú azonosítás alkalmazható lenne a fogvatartottak telefonálása[476] során, ahol fontos, hogy ténylegesen a jogosult fogvatartott telefonáljon és csak a számára engedélyezett személyekkel létesítsen kapcsolatot. Szintén alkalmazható a rendszer a fogvatartottak bolti vásárlása, az úgynevezett kiétkeztetés során, ahol szintén fontos a személyek egyértelmű azonosítása. Jelenleg a telefonálás és a kiétkeztetés során az azonosítás egy biztonsági jegyeket nem tartalmazó, így egyszerűen másolható kártyával – egyes szolgáltatások esetében vonalkóddal, egyes szolgáltatások esetében QR-kóddal – történik. A büntetés-végrehajtási intézetekben – a fogvatartottak magatartásából következően – gyakori a kártyák elvesztése, ellopása, megsemmisítése, stb. A tenyérvéna alapú ellenőrzés alkalmazásával ennek kockázata kiküszöbölhető.

A tenyérvéna alapú személyazonosítás alkalmazása előrelépést jelentene a schengeni térségbe történő belépés, az ott tartózkodás jogszerűségének ellenőrzésére is. További határrendészethez kapcsolódó alkalmazási lehetőség az intelligens repülőtéri rendszerekkel történő integráció.

5. Jogi háttér

Az információs önrendelkezési jogról és az információszabadságról szóló törvény[477] mások mellett a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítését adatkezelésnek tekinti. A törvényben nincs kifejezetten megemlítve a tenyérvéna rögzítése, ennek oka valószínűsíthetően az, hogy a jogszabály megalkotásakor, elfogadásakor még nem volt széles körben ismert a módszer. Azonban a szöveg értelmezéséből következően a tenyérvéna információ rögzítése is nyilvánvalóan adatkezelésnek tekinthető. Fentiek értelmében a tenyérvéna információk rögzítésekor fenn kell állni a jogszabályban meghatározott feltételeknek, így az érintett hozzájárulásának – amely nem kikényszeríthető – vagy a törvényi felhatalmazásnak (jogos érdek), illetve a célhoz kötöttségnek. A jogszabály meghatározza, hogy az adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.[478]

[476] 1979. évi 11. törvényerejű rendelet a büntetések és az intézkedések végrehajtásáról 36.§ (5) bekezdés e.) pont
[477] 2011. évi CXII. törvény
[478] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról II. fejezet A személyes adatok védelme

A munka törvénykönyve[479] nem köti a dolgozók előzetes beleegyezéséhez a technikai eszközzel történő azonosítás bevezetését. A 11. § (1) bekezdése szerint a munkáltató a munkavállalót csak a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A 11. § (2) bekezdés szerint a munkáltató előzetesen tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak. Ennek alapján pl. a munkahelyre történő be-, és kilépés tényének, időpontjának, a munkaidő betartásának, továbbá adott helyen való tartózkodás ellenőrzéséhez technikai eszközök alkalmazhatók. A technikai eszközök alkalmazása azonban nem jelent felhatalmazás a biometrikus azonosító alapján történő ellenőrzésre. Tehát amíg a tudás vagy tárgyi alapú azonosítási lehetőségeknek a jogszabály gyakorlatilag zöld utat ad, addig a biometrikus azonosításhoz – valószínűsíthetően – jogszabály módosítás szükséges.

A közalkalmazottak jogállásáról szóló törvény[480] 5. számú mellékletben meghatározott adatkört tarthatja nyilván a közalkalmazottakról. A törvény 83/B. § (1) bekezdése alapján az 5. számú mellékletben nem szereplő körben - törvény eltérő rendelkezésének hiányában - adatszerzés nem végezhető, ilyen adatot nyilvántartani nem lehet. Az 5. számú mellékeltben biometrikus adatok nyilvántartásának lehetősége nem szerepel. Az ún. Hszt.[481] – hasonlóan a közalkalmazottak jogállásáról szóló törvényhez – szintén a jogszabály mellékletében határozza meg a nyilvántartandó személyes adatok körét. A törvény 7. mellékletében felsorolt adatkör bővebb, mint a közalkalmazottak esetében, de szintén nem szerepelnek benne a biometrikus adatok, azonban a Hszt. kifejezett tiltást sem ír elő erre vonatkozóan. Fenti jogszabályokhoz illeszkedve a közszolgálati tisztviselők kódexe[482] sem tartalmazza a biometrikus azonosítók nyilvántartásának lehetőségét.

A jogszabályok áttekintése alapján levonható az a következtetés, hogy amennyiben a közszférában bármely biometrikus azonosító alapján terveznénk megvalósítani a munkavégzéssel kapcsolatos ellenőrzést, úgy ahhoz a jogi környezet szakértők általi felülvizsgálatára – szükség esetén jogszabályok módosítására – lenne szükség.

Magyarországon a biometrikus azonosítás bevezethetősége indukálta első törvénymódosítást 2014. június 23-án szavazta meg a Parlament[483]. A 2004. évi I. törvény a sportról módosítása 2014. július 15-én lépett hatályba. A jogszabály 72/A. § (2) bekezdése szerint a sportrendezvény szervezője jogosult – a klubkártya tulajdonosa személyazonosítása céljából – a klubkártya tizennegyedik életévét betöltött tulajdonosának képmásából, ujjnyomatából, íriszképéből vagy vénalenyomatából (biometrikus adat) generált, vissza nem fejthető alfanumerikus kódot (biometrikus sablon) kezelni. A vénanyomat hazai jogszabályban itt jelenik meg először. Várhatóan a jövőben ez több jogszabályban is nevesítésre kerül, hiszen a jogszabályoknak lépést kell tartaniuk a technikai lehetőségek fejlődésével. A tenyérvéna alapú azonosítás lehetőségétől – ebben az esetben - a jogalkotó a potenciális rendbontók hatékonyabb kiszűrését és ennek következtésben a sportrendezvényeken a rendbontások számának csökkenését várja, mint ahogy ez megfogalmazásra került a törvényjavaslat indoklásában (T/156)[484].

[479] 2012. évi I. törvény
[480] 1992. évi XXXIII. törvény
[481] A fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló 1996. évi XLIII. törvény
[482] 2011. évi CXCIX. törvény
[483] http://hvg.hu/sport/20140623_Biometrikusan_azonosithatjak_a_szurkoloka (Letöltés ideje: 2014. 07.27.)
[484] http://www.parlament.hu/irom40/00156/00156.pdf (Letöltés ideje: 2014. 07.29.)

6. Külföldi esettanulmány[485]

Az Európa és Ázsia határán fekvő több mint 71 millió lakosú Törökország a térség egyik legdinamikusabban fejlődő állama. 2001 és 2011 között 10 év alatt közel a négyszeresére növekedett az ország bruttó hazai terméke (GDP)[486]. A dinamikus fejlődés következtében jelentősen megnövekedett az igény az állam által nyújtott szociális szolgáltatások iránt is. Ennek következtében az állam egészségügyi kiadásai is dinamikus növekedést mutattak. A törökországi közegészségügyi ellátás finanszírozásáért felelős kormányzati szervezet a török Társadalombiztosítási Intézet (SSI: Social Security Institute) azonban olyan információkkal rendelkezett, hogy jelentős mértékű a jogtalanul igénybevett szolgáltatások aránya. Az egészségügyi szolgáltatók által elkövetett csalások komoly veszteséget okoznak az SSI éves költségvetésében. A jogosulatlan igénylések a 2010-es évben több mint 3 milliárd török líra (1 török líra = kb. 105 Ft) veszteséget okoztak.

Az SSI biztosítja a forrásokat a közegészségügyi ellátást nyújtó állami és magánkórházak, klinikák, családorvosok, gyógyszertárak és optikusok számára. Az Intézetnek biztonságos, megbízható infrastruktúrára volt szüksége a visszaélések előfordulásának csökkentésére. Az SSI arra a következtetésre jutott, hogy a biometrikus módszerekkel jelentősen visszaszoríthatók a csalások, hiszen ilyenkor a beteg fizikai jelenlétére van szükség az igénylés elindításához. A projekt – az ország méretei és lakosainak száma okán – rendkívül nagy terjedelmű volt, 81 városban 1700 egészségügyi szolgáltatót érintett, és összesen 9000 tenyérvéna leolvasót működik a rendszerben. Az 5 évesre tervezett projektben a rendszer kialakítása 2011 márciusában kezdődött, a tervezési, majd tesztelési fázist folyamatos bevezetés követte, 2013 és 2014 voltak a kiteljesedés évei.

A megoldás lényege, hogy a társadalombiztosítással rendelkező állampolgároknak egy alkalommal regisztrálniuk kell a rendszerbe. A regisztráció során rögzítik a személyek tenyérvéna mintázatát, amelyet összepárosítanak a társadalombiztosítási azonosító jellel. Amennyiben ezt követően bármilyen – az SSI által finanszírozott - egészségügyi szolgáltatást szeretnének igénybe venni, a társadalombiztosítási azonosító jel rögzítését követően egy érzékelő leolvassa a személy tenyérvéna mintázatát és azt összehasonlítja a regisztráció során rögzített mintával. Amennyiben az adott személy jogosult az ellátásra, úgy adatai átkerülnek az SSI által alkalmazott egészségügyi rendszerbe (Medula), ellenkező esetben a szolgáltatás iránti igénye elutasításra kerül. Konkrét adatok még nem állnak rendelkezésre a finanszírozásra gyakorolt pozitív hatásra vonatkozóan, de a kialakított rendszer egy modern, előremutató megoldás.

7. Összegzés

Jelen publikációban bemutattam a személyazonosítási lehetőségeket, amelyeket meghatározott szempontok alapján csoportosítottam. Ismertettem, hogy ezek közül melyek a biometrikus azonosítási lehetőségek. A biometrikus módszerek közül kiemeltem egy új

[485] http://www.fujitsu.com/fts/about/resources/case-studies/SSI-Healthcare-in-Turkey.html (Letöltés ideje: 2014. 07.29.)

[486] Forrás: Világbank. https://www.google.hu/publicdata/explore?ds=d5bncppjof8f9_&ctype=l&met_y=ny_gdp_mktp_cd#!ctype=l&strail=false&bcs=d&nselm=h&met_y=ny_gdp_mktp_cd&scale_y=lin&ind_y=false&rdim=region&idim=country:TUR&ifdim=region&hl=hu&dl=hu&ind=false (Letöltés ideje:2014.08.28.)

lehetőséget a tenyérvéna alapú azonosítást. Részletesen bemutattam a jelenleg legbiztonságosabbnak tartott megoldás biológiai és műszaki hátterét is. Ismertettem az alkalmazható eszközöket, részletesen bemutattam ezek tulajdonságait. Áttekintettem az alkalmazási lehetőségeket, elsősorban a rendvédelmi területet vizsgálva. Érintettem mind a rendvédelem alkalmazottai, mind a rendvédelmi szervekkel kapcsolatba kerülő személyek azonosítási lehetőségeit. Érintőlegesen megvizsgáltam a hazai alkalmazhatóság jogi hátterét. Megállapítottam, hogy – mint a modern technikai fejlődés során az elmúlt évtizedekben már többször tapasztaltuk – a jogszabályok lassan követik az eszközök fejlődését, a rendelkezésünkre álló lehetőségeket. Ebben az esetben azonban alaposan meg kell vizsgálni az adatvédelmi kérdéseket is, hiszen a biometrikus azonosítás lehetőségei tekintetében jelenleg rendkívül szűk a mozgástér e vonatkozásban. Megállapítom, hogy a biometrikus azonosítás alkalmazásának jogi háttere önálló kutatási téma. Végül egy külföldi esettanulmányon keresztül bemutattam a gyakorlati alkalmazás egy lehetőségét.

Összegezve az eredményeket megállapítom, hogy a tenyérvéna alapú azonosításban rendkívül nagy lehetőségek rejlenek. A módszer megfelel a társadalmi elvárásoknak, hiszen gyors, higiénikus, ugyanakkor nagy biztonságot nyújtó megoldás. Tanulságos, hogy a jelenleg legmodernebbnek tartott megoldás kidolgozása során az ősi japán kulturális szokások milyen fontos szerepet játszottak. Kiváló példája ez annak, hogy a több ezer éves kultúra és a csúcstechnológia együttműködése milyen nagyszerű dolgokat adhat a világnak.