Magyar Rendészet 2015/3. 37–48.

Paradigmaváltás a biztonságtechnikában – miért alkalmazzunk biometrikus rendszert?

FÖLDESI Krisztina

A bűnözési statisztikák és a társadalmi változások egyénekre gyakorolt hatása egyértelművé tette a társadalom minden rétege számára, hogy a klasszikus bűnüldözési technikák, erők, eszközök már nem elégségesek a kielégítő magán- és közbiztonság megteremtéséhez. Innovációra tehát mind a rendőri, mind a civil társadalom biztonságteremtő tevékenységében szükség van. A tapasztalati és kutatási eredmények igazolják, hogy ebben a biometrikus azonosítási eljárások jelenthetik az egyik nagyon hatékony megoldást.

Mindennapjaink teljesen elfogadott eleme a személyazonosító rendszerek[1] használata, amelyek nélkül szinte már működésképtelenné válna társadalmunk. Ilyen rendszert használunk, amikor plasztikkártyánkkal fizetünk, ezt alkalmazzuk, amikor chipes kártyánkkal reggel bejelentkezünk a munkahelyünkön, vagy a direktnet szolgáltatást vesszük igénybe bankunknál. Ezen rendszerek közös jellemzője, hogy az egyén mellett valamilyen plusztudást vagy pluszeszközt igényel a használatuk. Ez a tudás, eszköz kerül összekapcsolásra a konkrét személlyel, aki számára az a szolgáltatás, belépés engedélyezetté, támogatottá válik. Elméletileg ezekkel csak ő kaphat készpénzt az automatából, csak ő léphet be a munkahelyre, csak ő indíthat tranzakciót az internetes felületen. Ez az „elméletileg" meghatározás azonban a valóságban, a gyakorlat szintjén egyáltalán nem így van. Mit is jelent ez az alkalmazás terén?

Hagyományos alapú személyazonosító technikák

Ezeket az ún. hagyományos személyazonosító technikákat egy konkrét személy meghatározására, azonosítására használjuk. Két típusa: a tudásalapú és a tárgyi[2] alapú rendszerek.[3] A tudásalapú azonosítás nem igényel pluszeszközt, ilyenkor valamilyen azonosító kód, jelszó, név ismerete ruház fel bennünket a joggal a szolgáltatásra, belépésre, tevékenységre. Tipikus alkalmazási területe a banki szektor, internetbank-szolgáltatás vagy akár egy vállalati belső számítógépes rendszer. A tárgyi alapú rendszerek értelemszerűen valamiféle eszközt használnak fel erre: ilyen a legegyszerűbb kulcs,

1 Ezen rendszerek segítségével egy konkrét személy kiléte hitelt érdemlően megállapítható.

2 Nevezik tulajdonalapú technikának is, mivel a legtöbb esetben valamely tárgynak, tudásnak a birtoklása kell ahhoz, hogy jogosultak legyünk a használatra, például kulcs, mágneskártya stb.

3 Kovács (2014)

pecsét, esetleg chipes támogatottsággal ellátott kitűző, igazolvány, mágnescsík, okoskártya, rádiófrekvenciás chip.

Tapasztalataim szerint a különböző létesítményekben telepített, hagyományos biztonságtechnikai rendszerek biztonsági kockázatait tekintve elhanyagolható százalékot képviselnek a műszaki problémák, technikai hiányosságok, eszközbéli hibakódok, háttértár-meghibásodások. Ezek legnagyobb részben a rendszereket használó személyek helytelen, szabályoknak ellentmondó viselkedéséből eredeztethetők, tehát emberi, felhasználói mulasztásra vezethetők vissza. A hagyományos, tudásalapú biztonsági rendszerek esetében a konspirációs szabályok figyelmen kívül hagyása, a jelszó elfelejtése, illetéktelen kezekbe jutása egyértelműen felelőtlen felhasználói magatartás, emberi mulasztás eredménye.

Tipikus esete ennek a bankautomaták chipkártyái, illetőleg az ezekhez rendelt PIN-kód felhasználása. Egyértelmű ajánlás a bankok részéről, hogy a kártyát és a hozzá tartozó PIN-kódot soha ne tárolják a tulajdonosok azonos helyen. Ugyanakkor még mind a mai napig regisztrálnak olyan eseteket, hogy az elveszett, ellopott kártyára a tulajdonos alkoholos filccel ráírta a PIN-kódot is, hogy el ne felejtse.[4]

Számos helyen a munkaidő-nyilvántartás mágnes- vagy chipkártyás adatkezeléssel történik. Ezeken a helyeken lehet szembesülni többek között azzal, hogy valaki megkéri munkatársát, húzza le helyette a beléptetésnél a kártyáját, mivel valami oknál fogva késni fog. Emellett számos esetben fordul elő a kártya elvesztése, ellopása vagy egyszerűen otthon felejtése.

Az egyéni munkaállomások számítógépes belépési kódjai esetében megesik, hogy egymás jelszavaival lépnek be a dolgozók, illetőleg a számítógépből nem lép ki a felhasználó, így az utána belépni szándékozó az ő adataival használja az adatbázisokat. Felmérések bizonyítják,[5] hogy egy átlagos felhasználó 18 jelszóval rendelkezik, amelyek biztonságos használata, megjegyzése nem egyszerű. Ennek folytán sok esetben ugyanazon jelszót adják meg a különböző rendszerekbe való belépéshez, holott ez nagy biztonsági kockázatot jelent.

A hagyományos biztonsági rendszerek kiemelkedő kriminalizáló kockázata

Mivel ezeknek a rendszereknek, illetve a rendszerekbe történő bejutásnak csupán néhány adat a feltétele, bűnözői részről is nagy érdeklődésre tartanak számot, hiszen kis befektetéssel nagy nyereséget eredményeznek. Az egyszerű beléptetőkártyák, kulcsok, kódok ellopásán túl ezért specializálódtak sokan bankautomaták használóinak adatlopására. Ekkor különböző ATM-manipulációkkal, bankkártyakockázatok kihasználásával kerül illetéktelen kezekbe a rendszerhasználatra jogosító adat. Ezekben az esetekben speciális kamerákkal, rádiófrekvenciás továbbítással megszerzik a kártya adatait, illetve a közvetlenül beütött PIN-kódokat, és elkészítik az adott kártya klónját, tehát duplikálják azt.

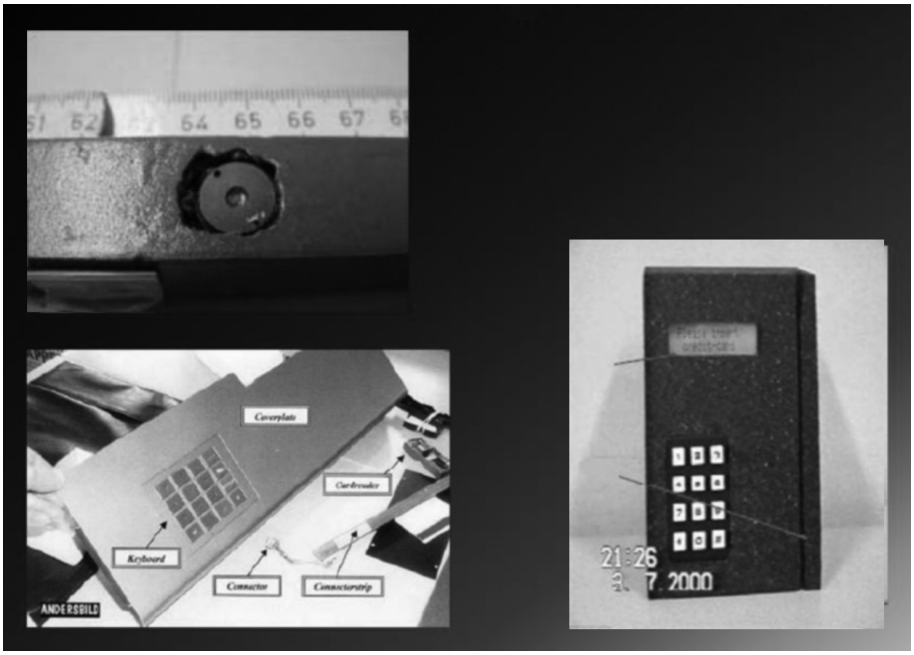
4 Az adatok a Fejér Megyei Rendőr-főkapitányság Elemző-értékelő Osztályától származnak.
5 Kiss (2014)

Erre mutat példát az *1. ábra,* amelyen azt láthatjuk, hogy az elkövetők felszerelik az automatákat olyan, az eredetihez tökéletesen hasonlító felületekkel (pl. kártyanyílás), amelyek az ún. skimmereken átfuttatva azonnal lemásolják annak adatait, és ezzel a duplikáció lehetősége adott is az elkövetőknek.

1. ábra: Példa ATM-preparációra[6]

Ehhez már csak a PIN-kód megszerzése szükséges, erre láthatunk példát a *2.* és a *3. ábrán,* amelyek különböző preparált felületek, másolt klaviatúrák és mikrokamerák elhelyezését szemléltetik.

6 Forrás: RVKI Bűnmegelőzési Akadémia Vagyonvédelmi Továbbképzés, Jakab Péter előadása



2. ábra: Példa PIN-kód megszerzésére irányuló eszközökre[7]

3. ábra: Példa ATM-preparációra[8]

7 Forrás: RVKI Bűnmegelőzési Akadémia Vagyonvédelmi Továbbképzés, Jakab Péter előadása
8 Forrás: RVKI Bűnmegelőzési Akadémia Vagyonvédelmi Továbbképzés, Jakab Péter előadása

Ezzel egy időben egy miniatűr rádióadó segítségével azonnal továbbítják a megszerzett adatokat az elkövetőknek, akik így már másolhatják is a kártyát, amelyet a PIN-kóddal használni is tudnak. Ugyanez a helyzet a tárgyi alapú rendszerek egyéb eseteinél, a kulcsok, kártyák és más szükséges eszközök alkalmazásakor is: elveszthetők, ellophatók, nagy alkalmazási kockázatot hordoznak.

Mi is lehetne ezekre a hibaforrásokra a megfelelő megoldás? Mit tehet egy felelős tulajdonos értékei, adatai tökéletesebb, megbízhatóbb, hatékonyabb védelme érdekében? Erre jelent megoldást az objektív, megtéveszthetetlen, eltulajdoníthatatlan adatokkal dolgozó személyazonosítási metodikák alkalmazása: a biometria. Nézzük, mi a biometria valójában!

Biometrikus személyazonosítási technikák[9]

A *biometrikus* kifejezés görög eredetű, és két részből tevődik össze: a *bios,* vagyis az 'élet' és a *metrein,* vagyis a 'megmér, összemér' szóból. Ezen értelemben használva: egy ember fizikai paramétereinek mérése. A biometrikus adatfelvétel lehetőségét általában két nagy csoportra osztják, amelyekben a biológiai és a viselkedésbeli tényezők szerepelnek.[10] Biológiai alapú biometrikus adatok:[11]

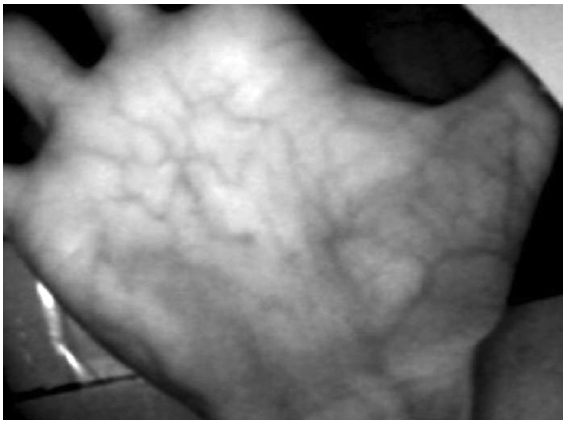
- bőrmintázat (ujjnyomat, ujjlenyomat, ujjnyom,[12] tenyérnyomat, talplenyomat);
- kézgeometria;
- érhálózat (tenyérerezet, ujjerezet);
- arc (2D, 3D, hőkép);
- szem (írisz, retina);
- DNS.

9 Kovács (2014)

10 Kovács et al. (2012) 486.

11 Jain et al. (2008)

12 Mivel a mai magyar kriminalisztikai gyakorlatban nincs példa az ujjnyom, az ujjnyomat és az ujjlenyomat funkcionális elkülönítésére, szükségesnek tartom ezen fogalomértelmezések tisztázását. *Ujjnyomat* (fingerprint): az ujj(begy) természetes módon (nyomás nélkül) sík felületre helyezett, ott maradó, egybefüggő rajzolata. *Ujjlenyomat* (finger roll): az ujj természetes módon (nyomás nélkül) sík felületre helyezett, balról jobbra (jobbról balra), 180 fokkal történő átforgatásakor keletkező, egybefüggő rajzolata. *Ujjnyom* (fragments of fingerprint or finger roll): az ujjlenyomat vagy ujjnyomat egybefüggő részlete.



4. ábra: Kézérhálózat-alapú azonosítás[13]

Viselkedési alapú biometrikus adatok: kézírás (íráskép, dinamika), beszédhang, gépelési ritmus, járási mód, mozgás. Ugyanakkor itt jegyezzük meg, hogy az egzakt mérési, algoritmizálási, értékelési mód kizárólag a biológiai (morfológiai, fiziológiai) csoport tekintetében szolgál egyértelmű, értékelhető és rendvédelmi szempontból is releváns eredménnyel. Emiatt az értelmezésünkben kizárólag a biológiai-fiziológiai egyedsajátosságok képezhetik a társadalmasítás, közösségi bevezetés, alkalmazhatóság alapját.

5. ábra: Íriszanalízisen és ujjnyomaton alapuló azonosítás[14]

13 Forrás: MEB 2014, 12th International Conference on Management, Enterprise and Benchmarking, Őszi Arnold előadása

14 Forrás: http://idegenszovet.blogspot.hu/2011/02/szivarvanyhartya-portrek-suren.html (2013. 04. 25.)

A biometrikus azonosító rendszerek között tehát a személy fiziológiai tulajdonságait alapul vevő technológiák képezik az opcionálisan legmegbízhatóbb kört, így az ujjnyomat-azonosítás, az íriszvizsgálat, a retinaanalízis, az arcfelismerés,[15] a kézgeometria-vizsgálat, az érhálózat-vizsgálat, a hangfelismerés és a DNS-analízis. Nézzük, milyen előnyöket nyerhetünk a biometrikus rendszerek alkalmazásával!

Biometria: költséghatékonyság

Természetesen a biztonságtechnikai rendszereket tekintve is elvárás a költséghatékony működés. E tekintetben a hagyományos, tulajdonalapú rendszerekkel összevetve a működés megkezdése magasabb költségekkel jár. Ugyanakkor, mivel a tulajdonalapú rendszerek üzemeltetésénél a személyek mozgása, a fluktuáció, a kártyák stb. amortizációja folyamatos pótlást, új és új költségeket követel meg, kb. háromévi használat múlva[16] egyértelműen olcsóbb működést fog eredményezni a biometrikus azonosítót alkalmazó metodika.

Biometria: megbízhatóság, tökéletesített rendszerműködés

A biometriai adatok megbízhatóságát, univerzális alkalmazhatóságát két elem garantálja: egyrészt ilyen adatai mindenkinek vannak, és ezen adatok dekonspirációjának, illetéktelen kezekbe jutásának százalékos esélye elenyésző; másrészt ezen adatok ténylegesen személyspecifikusak, egyediek és mint ilyenek originálisan csakis egyetlen személyhez köthetők.[17] Tehát az ujjnyomataink, íriszmintánk, kézgeometriánk, érhálózatunk nem elveszthető, nem ellopható, nem kölcsönadható, és duplikációjának lehetősége jelen technikai lehetőségek alapján gyakorlatilag elenyésző.

A biometriai azonosítás mindkét alapszegmens esetében tökéletes megbízhatósággal alkalmazható: a személyigazoló (SZI) és a személyazonosító (SZA) rendszereknél is. A személyazonosító rendszerek (SZA) esetében egy a sokhoz keresés zajlik. A biometrikus minta paramétereit hasonlítják össze a biometrikus adatbázisban már előzőleg azonosított személyek mintáival. A személyigazoló rendszerek esetében az azonosítás, keresés az egy az egyhez metodikát követi. A biometrikus azonosítási módszerek tulajdonképpen mintaillesztő algoritmuson alapulnak.[18] Az azonosításra váró egyén előzőleg eltárolt biometrikus adatait (ez történhet adatbázis használatával és beléptető-

15 Például ez a biometrikus azonosítási rendszer optimális lenne, és a lehető legnagyobb működési biztonságot nyújtaná a rendőrségi objektumokba való beléptetés, az egyes szolgálati feladatokat ellátó egységek közötti mozgás, információáramlás és természetesen a speciális, fedett feladatokat ellátó rendőri erők tevékenységi köre tekintetében. Ugyanakkor e metodika a felhasználók ontogenetikus (egyéni fejlődéssel kapcsolatos) változásai folytán éppen a statikusság alapelvét gyengíti. Ugyanis az arc arányainak lehetséges változásával fals eredmények lehetőségét is magában rejti.

16 Otti (2012)

17 Tekintsünk el ehelyütt a kisebb mértékben megbízható, viselkedésalapú biometrikus azonosítástól, amelybe beleértendő például az aláírásminta vizsgálata, a billentyűleütés-vizsgálat és a járáselemzés!

18 Az egyes biometrikus azonosítók teljesítőképességének meghatározására a Zephyr-analízist használják. A Zephyr-analízis az azonosítókat négy fő szempont szerint vizsgálja: pontosság, költség, a működtetés egyszerűsége, használati zavar.

kártyán) vetik össze az aktuálisan adott mintával. Tehát tulajdonképpen azt ellenőrzik, hogy az adott személy azonos-e önmagával, vagyis a tevékenység folytatására, belépésre stb. jogosult-e.

Biometria: nagyobb hatékonyság

A felvázolt hibalehetőségek figyelembevételével a biometrikus azonosítási eljárások hatékonysága a legmagasabb az eddig alkalmazott technikák közül. Eleve kiiktatjuk az egyéb használati veszélyeket, például a jelszó elfelejtése, kártya elvesztése, ezért teljes mértékben megbízható, mert a használt „adat" (ujjnyomat, íriszminta stb.) közvetlenül a személyhez kötődik. Mivel pedig minden pillanatban az egyén rendelkezésére áll, használata kényelmes. Az aktuális adatbankban kezelt populáció egyedszámának megnövekedésével együtt járó feldolgozási lassúság pedig egy megfelelő algoritmus, speciális adatbázis használatával kiküszöbölhető. Az alkalmazhatóság elsődleges alapeleme tehát, hogy bármekkora populáció esetében gyors válaszreakciót produkáljon, és többezres mintaszámmal operálva is megbízhatóan, másodpercek töredéke alatt végezze el az azonosság megállapítását, illetőleg kizárását.

Nagy dilemma ezen esetekben a megbízhatóság fokának növelése és ezzel egyenes arányban a téves jogosultsági visszautasítások számának növekedése, amely az alkalmazás hatásfokát ronthatja.[19] Ezekben az esetekben a rendszer jogosulatlannak értékeli, tehát például nem engedélyezi a belépést olyan személynek, aki pedig jogosult lenne rá, illetve jogosultnak értékel olyan személyt, aki nem lenne az. Ennek a hibalehetőségnek a minimálisra csökkentése azonban már pusztán technológiai, fejlesztési kérdés.

Gyakori kérdés például egy ujjnyomat-azonosító rendszer esetében, hogy egy előzőleg rögzített ujjnyomattal vagy egy speciális, preparált ujjal, amelyre felviszik az ujjnyomatot, megtéveszthető-e a szerkezet. Megfelelő eszköz, illetve technológia alkalmazásával azonban meg lehet győződni arról, hogy a mintavételezés valós, élő személytől származik-e, ezzel az ún. élőminta-ellenőrzéssel kiiktatva a megtévesztés lehetőségét.

Fontos szempont a mérhetőség, egyben könnyű elérhetőség. Tehát hiába van meg a bőrfodorszálak egyedi mintázata az emberek talpán is, alkalmassá téve azt az egyedi azonosításra, ez a biometrikus adat mégsem lesz soha egy beléptetőrendszer adatbázisának alapja. Ezt egészségügyi és egyéb praktikus megfontolások nem teszik lehetővé. Az ujjnyomatok levételéhez ugyanis közvetlen kontaktust kell teremteni az eszközzel, tehát az ujjat rá kell tenni az ujjnyomat-azonosító felületére, ez pedig többezres egyedszám esetén is generálhat ellenérzéseket. A gyakorlatban tapasztalható infektológiai, fertőzésmegelőzési szempontok miatt tehát az emberek részéről jogos az az igény, hogy fizikai kontaktus nélkül történjen az azonosítás. E feltételnek a biometrikus azonosítási módok közül több teljes mértékben megfelel. Ilyen például az egyik legmegbízhatóbb technológia, az íriszazonosítás.

19 A különféle biometrikus rendszerek biztonságának mérésére az alábbi mutatók használatosak: téves elfogadási hányad, FAR (jogosultként ismer fel nem jogosult személyt) és téves visszautasítási hányad, FRR (nem jogosultként ismer fel jogosult személyt).

A biometrikus technikák alkalmazásával az adatvédelmi szempontok is maximálisan érvényesülnek. A biometriai adatok személyes, különösen szenzitív adatnak minősülnek, hiszen egy ujjnyomatnál, íriszmintánál jobban semmi nem azonosítja az egyént.[20] Mivel azonban a mintából generált algoritmus már független magától a személytől, és a későbbiekben nem alkalmas arra, hogy a konkrét mintát visszaalakítsák belőle, így a konkrét személyhez köthető legyen, ezért tökéletesen megfelel az adatvédelmi előírásoknak.

Napjaink biometriája és a jövő

Az ujjnyomat-azonosítást a bűnügyi nyomozások, rendvédelem területén már a múlt évszázad óta megbízhatóan alkalmazzák.[21] A bűnelkövetkők ujjnyomatainak nyilvántartása, illetve az elkövetés helyén fellelt, eddig még nem azonosított ujjnyomok, ujjnyomtöredékek, tenyérnyomok és tenyérnyomtöredékek nyilvántartása már jól működő rendszer. E technológiának társadalmasodása, magáncélú alkalmazása egyre gyakoribb a civil életben. Már tudjuk technikai eszközeinket ujjnyomatunkkal titkosítani (pl.: okostelefon, laptop, tablet). Az Apple Pay mobilfizetési mód például a felhasználó ujjnyomatával hitelesíti az iPhone telefonnal vagy iPad tablettel kezdeményezett bankkártyás tranzakciókat. De kifejlesztették már a kézmozdulat, arcvonások, illetve hangfelismerés alapján történő azonosítási technikákat is.[22] Ezeknek a nagyvállalati beléptetőrendszerekbe illesztett alkalmazása mellett elkezdődött a magáncélú, magánlakásokba történő egyéni felhasználása is, bár inkább még egyedi jelleggel. A nagy megbízhatóság, az alkalmazási kényelem, illetve a bizonyos idő elteltével tapasztalható rentábilis működés támasztja alá a biometrikák alkalmazásának elkerülhetetlenségét, központi szerepét.

Az egyik prominens autógyártó[23] azt a bejelentést tette, hogy arcfelismerő rendszert telepített autóiba. Ez esetben nem az autó kizárólagos indításának jogát foglalja magában a rendszer, hanem a menetbiztonság növelését. A műszerfalba épített szenzorok, infra LED-ek és kamera segítségével a Driver State Estimation képes eldönteni, hogy a vezető helyes irányba néz-e, merre fordítja a fejét, és nyitva van-e a szeme, tehát hogy az utat nézi-e egyáltalán vagy ébren van-e. A kapott eredmények tükrében képes felébreszteni a sofőrt, eredménytelenség esetén pedig biztonsággal meg is állítja az autót. A biometria biztonsági szektorban történő alkalmazási lehetősége óriási, megbízhatósága kiemelkedő.

---

20 Meg kell azonban jegyeznünk, hogy míg egy ujjnyomat-azonosító FAR értéke 1 000 000:1, addig az íriszazonosítóé 12 000 000:1. Illetve az a tény is az íriszazonosítás alkalmazása mellett szól, miszerint az emberiség 3–5 százalékának nincs értékelhető ujjnyomata (pl. elkopott ujjnyomat fizikai munkát végzőknél vagy a kisgyermekek és idősek esetén a nehézségekbe ütköző levétel miatt). Ugyancsak nehezítő körülmény az ujjnyomatvétel esetében az extrém hosszú körmök vagy a szennyezett kéz is.

21 A Bűnügyi Szakértői és Kutató Intézetén belül működik a Daktiloszkópiai Szakértői Laboratórium, amely a bűnügyi szempontú ujj- és tenyérnyomatok vizsgálatával foglalkozik.

22 Például az Intel által 2014-ben kiadott Perceptual Computing SDK is, amellyel az alkalmazások többek között arc- és hangfelismeréssel vértezhetők fel.

23 *Fejlett arcfelismerés kerülhet a Volvókba.*

Napjainkra a biometrikus azonosítási eljárások egyre elterjedtebbekké, a megbízhatóság és biztonság zálogává avanzsáltak. Az azonosítási eljárások jövőjét a legelismertebb biztonságtechnikai cégek is ebben látják.[24] A biometria térnyerése, egyre szélesebb körben való felhasználása megállíthatatlan a legegyszerűbb feladatoktól a legbonyolultabb rendszerekig. Egyre több munkahelyen, de például egyetemek[25] manuális jelenléti ívének helyettesítésére is alkalmazzák. Az elavult papíralapú vagy mágneskártyás, tudás- vagy tárgyi alapú beléptetőrendszereket ujjnyomat-, íriszkép-, esetleg érhálózatvizsgálat-alapú technikák váltják fel. Ezt támogatja a jogszabályi háttér is, például az a tény, hogy a 2012. július 1-jén hatályba lépő új munka törvénykönyve[26] rendelkezései alapján elegendő tájékoztatni a munkavállalót a rendszer alkalmazásáról, annak adatkezelést is érintő vetületeiről, de a munkavállalók hozzájárulása nem szükséges a rendszer bevezetéséhez.

Ugyanakkor azzal, hogy például születésünkkor rögzítik retina-, írisz-, erezet-, DNS-mintánkat vagy ujjnyomatunkat, önszántunkból lemondunk szabadságunk, önállóságunk, önrendelkezésünk egy részéről is. Az vitathatatlan tény, hogy ezen alternatívák alkalmazásával a legnagyobb nyeresége a bűnüldöző szerveknek lenne, mivel a rendőrségnek nem kellene nagy apparátust, erőt, eszközöket megmozgatnia annak érdekében, hogy egy beszerzett biometrikus minta esetében megtalálja a nyomhoz kizárólagosan köthető személyt. Az íriszazonosítók működtetéséhez a csúcstechnológiák vonatkozásában már ma sem kell közvetlen, néhány centiméteres kontaktus, méteres távolságról is azonosítanak. Maga az íriszazonosítás pedig a legmegbízhatóbb biometrikus módszer, hiszen amellett, hogy nincs két azonos íriszmintájú ember, az egyes emberek két szemének mintázata is különböző. Annak a valószínűsége pedig, hogy két azonos íriszminta megjelenik, $1{:}10^{78}$ (miközben a Föld jelenlegi népessége 10^{10} nagyságrendű). Egy arcazonosító rendszer alkalmas arra, hogy a bűnügyi nyilvántartások alapján jelzést küldjön, ha egy körözött vagy csak megfigyelt személy átlépi a kerület határát. Gyakorlatilag összeköttetést tud létrehozni a népesség-nyilvántartó adataival, ahol a személyes adatokat őrizve digitalizált fényképeinket is tárolják.

Akár a mindenkire kiterjedő ujjnyomat- és arcazonosításról (2D, 3D), az íriszazonosításról, akár az érhálózat-azonosításról legyen szó, azonnal biztonságosabbá válna a mindennapi élet, ellenőrizhetővé a visszaeső, veszélyes bűnözők, megelőzhetővé a későbbi bűnelkövetéseik, a körözött bűnözők néhány órán belül a hatóság kezére kerülhetnének. Az eltűnt gyerekeket sikerülne visszajuttatni szüleikhez. A tapasztalatok szerint az évente eltűnt – országos átlagban – 15 ezer gyermekből 90 százalék néhány napon belül megkerül, ám van 1–2 százalék, akiket csak nagyon hosszú idő elteltével találnak meg, illetőleg akad olyan kiskorú is, aki egyéb ellenőrzések kapcsán kerül elő, és nehézségekbe ütközik az azonosítása.[27] Ezen kiskorúak fiziológiája, külseje ugyanis olyan gyorsan változik, hogy néhány hónap elteltével kétséget kizáróan csak biometrikus adatok segítségével lehetséges az azonosításuk. A szülők nyugalma érdekében a

24 *Az Intel szélesebb körben használná a biometrikus azonosítást.*
25 Turóczy (2010)
26 2012. évi 1. törvény
27 Adatforrás: Police.hu

születéskor levett íriszminta nagy biztonságot jelenthet a gyermek esetleges elrablása, elvesztése, elkóborlása esetén.

Több tízezer eddig felderítetlen bűncselekmény elkövetője sikeresen azonosíthatóvá válna, ezzel nemcsak a felderítést, de a szekunder prevenciót is szolgálva, tehát a későbbi bűnelkövetőket is megakadályozhatnánk abban, hogy újra bűncselekményt kövessenek el. Bűnügyi statisztikáink javulnának, a sikeres felderítések visszatartó ereje azonnal érvényesülne, csökkenne a későbbi bűnelkövetések száma, amely alapjaiban javítaná a lakosság szubjektív biztonságérzetét. Végeredményben az emberek jóval nagyobb biztonságban éreznék magukat, emellett az egyes magánkézben lévő azonosító rendszerek is megbízhatóbbá, hatékonyabbá válnának. Az emberi mulasztások lehetősége csökkenne, a rendszerek működése optimálisabbá válna.

Összefoglalás

Nyilvánvalóan változás szükséges a biztonsági piac területén. Mind a magánbiztonság, mind a közbiztonság terén megfogalmazódott az igény az új technikákra. Egyértelművé vált, hogy a hagyományos biztonsági rendszerek elérték hatékonyságuk maximumát, ezekkel már nem tudunk jobb, eredményesebb személy- és rendszerbiztonságot produkálni.

A paradigmaváltás meg is kezdődött, a hagyományos eszközök helyett megjelent az igény a biztonságosabb, megbízhatóbb technológiák alkalmazására.[28] Egyre egyértelműbben körvonalazódik, hogy ez a technológia a biometrikus azonosítás lehet, lesz.[29] Ezen rendszerek előnyei egyértelműek: megoldást jelenthetnek a saját és környezetünk nagyobb fokú biztonságának megteremtésére. Dilemma mégis megfogalmazódik: vajon megéri-e nekünk a szabadságunk egy nem kis szeletéről önként lemondani annak érdekében, hogy nyugodt, biztonságos életet tudjunk teremteni gyerekeinknek, unokáinknak, egész társadalmunknak? Egyetlen adat a magán- és a totális társadalmi élet jóval nagyobb biztonságáért – vajon megéri?

IRODALOMJEGYZÉK

2012. évi I. törvény a munka törvénykönyvéről

Jain, Anil – Flynn, Patrick – Ross, Arun A. (eds.) (2008): *Handbook of Biometrics.* New York, Springer Science + Business Media LLC.

Kovács Tibor (2014): *Biometrikus azonosítás.* Digitális jegyzet. Budapest, Óbudai Egyetem.

Kovács Tibor – Otti Csaba – Milák István (2012): *A biztonságtudomány biometriai aspektusai.* Forrás: www.pecshor.hu/periodika/XIII/kovacsti.pdf (2014. 09. 10.)

28 *Working document on biometrics.*

29 *Uo.*

Internetes források:

Az Intel szélesebb körben használná a biometrikus azonosítást. Forrás: http://m-shop.hu/index.php?option=com_content&view=article&id=20300:az-intel-szelesebb-korben-hasznalna-a-biometrikus-azonositast&catid=16&Itemid=174 (2014. 12. 01.)

Fejlett arcfelismerés kerülhet a Volvókba. Forrás: www.geeks.hu/hirek/140319_fejlett_arcfelismeres_kerulhet_a_volvokba (2014. 07. 14.)

http://idegenszovet.blogspot.hu/2011/02/szivarvanyhartya-portrek-suren.html (2013. 04. 25.)

Kiss Endre (2014): *Nyugdíjazná a jelszót az Intel.* Forrás: http://computerworld.hu/computerworld/nyugdijazna-a-jelszot-az-intel.html (2014. 11. 29.)

Kristóf Csaba (2014): *Az Intel kezébe került a PasswordBox.* http://biztonsagportal.hu/az-intel-kezebe-kerult-a-passwordbox.html (2014. 12. 12.)

Otti Csaba (2012): *A biometria biztonsága és sérülékenysége.* Forrás: www.youtube.com/watch?v=axiwyxXmKSQ (2014. 12. 20.)

Turóczy Zsófia (2010): *Biometriai ujjlenyomat-azonosítás: a jövő katalógusrendszere?* Forrás: www.mohaonline.hu/egyetem_guide/biometriai_ujjlenyomat_azonositas_a_jovo_katalogusrendszere (2014. 12. 10.)

Working document on biometrics. (2003) Forrás: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf (2014. 11. 23.)

SUMMARY

A Paradigm Change: Why Biometrics Should Be Applied?

FÖLDESI Krisztina

Social changes and criminal statistics have made it apparent for all layers of society that traditional law enforcement techniques, forces and equipment are no longer sufficient for providing adequate private and public security. There is a grave need for innovation arising on both the part of civil and police activity. Experimental and research findings justify that biometric recognition processes may be one of the most efficient solutions.