DATA MANAGEMENT ON MASTERS LEVEL: BIOMETRICS AND THE LEGAL BACKGROUND

ADATKEZELÉS MESTERFOKON: A BIOMETRIKUS AZONOSÍTÁS ÉS A JOGSZABÁLYI HÁTTÉR

UJHEGYI Péter[1], KUN Tamás[2]

Abstract

This article aims to provide a brief overview of the development of biometric identification solutions over the past decade. At the same time, the development of the legal environment is typically presented in the European Union and Hungary, but the international regulatory framework is also mentioned. Authentication has become a key area in the issue of applying IT technologies, which demanded procedures of the development side of processes, that could use most likely unique identifiers and could be use without difficulty. However, these solutions still give rise to public concern about the conditions under which companies and institutions using biometric procedures are entitled to collect data, and in many cases only years later it became clear that data collection proved to be unauthorized. At state-of-the-art procedures and technologies regulatory that influencing processes and societal attitudes has been reviewed, which could hinder or support diffusion.

Keywords

security, biometric identification, biometrics development, biometrics legal environment, authentication trends

Absztrakt

Jelen cikk rövid áttekintést kíván nyújtani az elmúlt évtized biometriai azonosítási megoldásainak fejlődéséről. Ezzel párhuzamosan bemutatásra kerül a jogi környezet fejlődése, jellemzően az Európai Unióban és Magyarországon, de említésre kerülnek a nemzetközi szabályozási keretek is. Az informatikai alkalmazások térnyerésével az azonosítás kulcsfontosságú területté vált, és olyan eljárások alkalmazását követelik meg a fejlesztői oldalon, amelyek többnyire egyediek, valamint könnyedén használhatók. Azonban ezek a megoldások a társadalomban aggályokat eredményeznek ma is, hogy milyen körülmények között jogosultak adatok gyűjtésére a biometriai eljárásokat alkalmazó vállalatok, intézmények, számos esetben csak évekkel később derült fény arra, hogy az adatgyűjtés jogosulatlannak bizonyult. Áttekintésre kerülnek a legmodernebb eljárások és technológiák, a szabályozásokat befolyásoló folyamatok és azok a társadalmi attitűdök, amelyek gátolják vagy támogatják az elterjedést.

Kulcsszavak

biztonság, biometrikus azonosítás, biometria fejlődése, biometria jogi környezet, azonosítási trendek

[1] ujhegyi.peter@phd.uni-obuda.hu | ORCID: 0000-0001-9143-6712| PhD Student/doktorandusz | Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] kun.tamas@phd.uni-obuda.hu | ORCID: 0000-0002-6620-7157| PhD Student/doktorandusz | Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az elmúlt évszázadok biometriával kapcsolatos fejlődését nagyobb részben az egyértelmű személyazonosítás területén megnövekedett igények alakították. Biometrikus azonosítás során mérjük és rögzítjük, lehetőleg automatikus technikákkal és eljárásokkal egy személy egyedi fizikai, testi jellemzőit, viselkedésbeli jellemvonásait és ezeket azonosítási és hitelesítési célra használjuk. A megoldást lehet személyazonosítás (identification) céljára használni, amikor egy adatbázis állományából keressük a megegyező mintát és azonosítjuk a személyt a csoport valamelyik tagjával. Vagy lehet használni ellenőrzésre, hitelesítésre (verification), amikor a rendszer hitelesít egy személyt az előzőleg felvett minta alapján és megállapítjuk, hogy a személy az e, akinek vallja magát. Hosszú út vezetett el az azonosítási megoldások tekintetében a mai sokrétű megoldásokig

A személyazonosítás a korai kezdetektől megjelenik történelmünkben. A becslések szerint is legalább 31 000 évvel ezelőtti Pech Merle barlangrajzokon olyan kézlenyomatokat találtak, melyek feltételezhetően a készítők azonosítása céljából aláírásként szolgáltak. [1] Hammurapi babilóniai király [2] törvénygyűjteményében a szerződéseket hitelesítő eljárásként ujjnyomatot használtak. Marcello Malpighi [3] 1684-ben az ujjak bőrléc-mintázatainak különbözőségeit tanulmányozta. Innen ered a Malpigi réteg elnevezés, ami a bőrfelület felső rétegére utal, ahol a fodorszálszerkezet található. 1685-ben az ujjnyom dermatoglífiai mintázatának elemzésével egy holland orvos, Bidloo foglalkozott behatóan és eredményei meghatározók a biometria tudományában.

A modern korban a népesség erőteljes növekedésének folyamata megkövetelte, hogy a bűnügyi nyomozati eljárások is haladjanak a korral, és olyan módszerek kerüljenek kidolgozásra, amelyekkel a bűnüldöző szervek egyértelműen beazonosíthatják az elkövetőket. Ebben az időben a migrációs folyamatok is adtak egy erőteljes lendületet a szakterületnek. Az 1800-as évek közepére, ahogy a városok népessége és az ipar fejlődött, egyre nagyobb igény merült fel az emberek pontosabb és gyorsabb azonosítására. A városok népességének bővülése magával hozta az emberek nagyobb mobilitását, a hatóságok már nem támaszkodhattak saját tapasztalataikra és helyi ismereteikre. Tudatosabb és kodifikáltabb lett az igazságszolgáltatás, ami egyre jobban igényelte az elkövetőkkel szembeni hatékonyabb fellépést és ezzel az egyértelmű azonosítási eljárások szükségszerűségét. Olyan formális rendszerek kidolgozására lett igény, mely nyilvántartja a bűncselekmények és elkövetők személyi jellemzőit. Az első rendszer a különböző testméretek mérésén és összehasonlításán alapuló Bertillon-rendszer volt, mely Franciaországból származott. A második módszer is a bűnüldözés területén indult fejlődének. Hivatalos eljárásokban a rendőri szervek az elkövetők azonosításában az ujjlenyomatokat kezdték használni.

Hazánkban a kriminalisztikai szakirodalom egységes abban, hogy a személyazonosítás új módszerének a magyar gyakorlatba történő bevezetése dr. Pekáry Ferenc kerületi rendőrkapitánynak (későbbi budapesti főkapitány-helyettesnek) köszönhető. [4] Vélhetően az 1902-ben Londonban töltött szabadsága alatt látottakat összegezve és az akkori szakirodalom (pl. Endrődy 1989-es nyomozati tankönyve) nyomon követésének hatására azt a következtetést vonta le, hogy az ujjnyomat alapú biometrikus azonosítási eljárás a gyakorlatban jobban alkalmazható és megbízhatóbb, mint az akkori korban inkább elterjedtebbnek számító Bertillon módszer. A Budapesti Rendőrfőkapitányságon kidolgozásra került az ujjnyomat alapú azonosítási módszertan [5] és 1904-ben bevezetésre került a daktiloszkópia. 1909. január 1. napján pedig megalakult az Országos Bűnügyi Nyilvántartó Hivatal és a

daktiloszkópiai részlege is, köszönhetően annak, hogy a dánosi rablógyilkosság felderítésénél az ujjnyomat azonosítás módszerével sikerült egyértelmű bizonyítékot szolgáltatni és az ügyet sikeresen lezárni.

Az 1900-as években a migrációs folyamatok indukálták az azonosítási módszerek fejlődését a bűnüldözési módszerekre fókuszálva és ahogy az törvényszerű, ezt lekövetve pedig az évezred végére a kereskedelmi forgalomban is egyre jobban elkezdtek terjedni a különféle biometrikus azonosításon alapuló megoldások. A továbbiakban kitérek az elmúlt évtizedben a biometrikus azonosítási technológiáinak fejlődésére és bemutatom a legújabb technológiák és tendenciák elterjedésének körülményeit.

A TECHNOLÓGIÁK FEJLŐDÉSE

Visszatekintve az alapokhoz, a biometria egy görög eredetű kifejezés, a bio, mint élet és a metron, mint mérés szavakból tevődik össze. [6] Általánosságban, valamilyen élőlény valamilyen élettani jellemzőjét mérjük. A biometrikus azonosítás esetében az élőlény általában egy adott ember. A biometrikus jellemzői pedig az ember saját személyi jellemzőinek tekinthető, amelyek alapját képezik a személyazonosságának és velük együtt a jogosultságai meghatározásának. „Definíciószerű megfogalmazással a biometrikus azonosítás olyan automatikus technikát igénylő eljárás, amely „méri és rögzíti egy személy egyedi fizikai, testi jellemzőit, viselkedésbeli jellemvonásait, és ezeket azonosítás és hitelesítés céljára használja fel. A biometrikus felismerés alkalmazható személyazonosítás céljára, amikor a biometrikus rendszer azonosítja a személyt, az egész lajstromozott adatállományból kikeresve a megegyezőt, valamint használható ellenőrzés céljából, amikor a rendszer hitelesít egy személyt az előzőleg róla felvett és eltárolt minták alapján.” [7]

A biometrikus azonosítási technikákat az általuk vizsgált jellemzők alapján két nagyobb csoportba sorolhatjuk. Egyik a fizikai, fiziológiai alapú vizsgálatokon alapuló technikák csoportja, ide tartoznak az ujjnyomat, tenyérnyomat alapú azonosítások, az íriszazonosítás, a retinaelemzés, az arcfelismerés alapú megoldások, a geometriai felismerésen alapuló technikák, mint a kézkörvonal és a fülforma felismerés. Ide sorolható még a testszagészlelés, a hangazonosítás, a verejtékpórus-elemzés és a DNS mintázat elemzés. A másik csoportba a viselkedési minta elemzésén alapuló azonosítási megoldások tartoznak, mint a gépelési ritmus és kézírás elemzés, valamint a járás és mozgás elemzés. Elterjedőben vannak a pszichológiai alapú technikák ma még gyerekcipőben járó területei. Ahogy a profilozási megoldások, az összekapcsolt adatbázisok és az AI (mesterséges intelligencia alapú) technológiák egyre jobban teret nyernek, úgy ezek egyre jobb hátteret adnak az új irányzatok térhódításának.

Multimodális rendszereknek nevezzük a fenti technikák megoldásainak összevonását és integrálását. Ezekkel olyan komplex megoldásokat kapunk, melyek során többféle cél is teljesülni tud. Ezek a rendszerek több biometrikus adatot használnak párhuzamosan (például többféle mozgási jellemzőt mérnek), ezzel csökkentve a biometrikus rendszerek hibás elfogadási arányát, illetve növelik a kényelmet, a biztonságot és a hatékonyságot. Képesek arra, hogy nagyobb távolságról, az egyén hozzájárulása vagy célirányos tevőleges cselekedete nélkül is adatot gyűjtsenek, és ezzel nagyon jó lehetőséget biztosítanak másodlagos felhasználási területeknek, ahol már nem csak az azonosítás a fő cél. A többféle biometrikus jellemző összetettsége miatt, az ilyen rendszerek nagyobb tömegekkel kapcsolatos azonosítási igények kiszolgálására is alkalmas, mert nem csak azonosítani, hanem követni is lehet

az egyéneket. Az azonosítás megtörténhet egy arcfelismerő kamera által, de a tömegben való mozgás is (elvegyülési szándék esetén) követhető az alany járásképének elemzésével, de ha a megfigyelt személy esetleg napszemüveg mögé rejtőzik, fülformája alapján is azonosítható. Speciális esetben, például éjszaka, azonosítható a személy hőkép alapján is. Az ilyen rendszerek megtévesztése nagy felkészültséget igényel és a visszaélések során is több biometrikus jellemzőt kellene megszereznie, vagy korrumpálnia egy támadónak. A jobb megértéshez érdemes pontosan megismerni, hogy zajlik egy azonosítási folyamat.

A biometrikus azonosítási folyamat az egyén biometrikus adataiból képzett kód, a sablon létrehozásával kezdődik, mely a regisztrációhoz szükséges. A sablont jogi értelmezésben személyes adatnak kell tekinteni és a biometrikus adatok kezelésére vonatkozó előírások betartása kötelező érvényű rá. A sablon létrehozásakor egyirányú kódolással, nem visszafejthető módon, automatizált felhasználás céljára az egyén személyes mérhető adatait és jellegzetességeit dolgozzák fel olyan módon, hogy a sablonból a korábbi adattartalom nem állítható vissza semmilyen módszerrel. Erre a személyes adatok célhoz kötött kezelése érdekében, illetve az osztott információs rendszerekre vonatkozó adatvédelmi követelmények miatt van szükség. Fontos az is, hogy a sablon létrehozása után már nem lehet leválogatni az adatbázisból valamilyen speciális tulajdonságnak megfelelő jellemzőkkel rendelkező egyéneket, de az adatbázis ugyanakkor alkalmas arra, hogy referencia adatforrásként összehasonlító eljárásokkal személyazonosítást végezzenek vele. Az azonosítási módszerek sokfélesége a felhasználási területek fejlődésében mutatkozik meg igazán, mely módszerek az utóbbi 20 évben a kriminalisztikai felhasználási területeken kívül is rengeteget fejlődtek.

Testalkat alapú azonosítás

Az antropomorf jellemzők, azaz az emberi testi méretek különbözőségét mérő eljárások adják az alapját a testalkat alapú azonosítási megoldásoknak. A mai felhasználási megoldásokban ezek az eljárások önállóan nem, vagy csak nagyon speciális esetekben alkalmasak egyértelmű azonosításra. Ezért is szorult háttérbe a Bertillon módszer az elmúlt 100 évben, de kiegészítve egyéb távoli azonosítási eljárásokkal pontosítható az azonosítás eredménye. Minél több testalkattal összefüggő paramétert mérünk, annál pontosabb az azonosítás. Példaként említve a testmagasság adatokból még nem tehetünk egyértelmű becslést az alany származására, hiába tudjuk, hogy az ázsiaiak átlagosan alacsonyabbak az európai embereknél. De ha ezeket az adatokat kiegészítjük fejforma adatokkal és végtagokra vonatkozó adatokkal, akkor arányaiban máris pontosabb eredményt kapunk.

Járás alapú azonosítás

A járás alapú azonosítás (gait recognition) az egyik legígéretesebb kiegészítő azonosítási megoldás, hiszem távolról is végezhető, tömegek ellenőrzésére is alkalmazható és viszonylag kevés dolog befolyásolja az eljárás hatékonyságát. Már az 1900-as években is végeztek kísérleteket (gait-humact), amikor az emberi testekre csatolt fényforrások mozgását mérték és elemezték különböző testmozgások közben. A képfeldolgozáson alapuló technológia két modell alapján működik, az egyik a holisztikus, mely során a körvonalakat vizsgáljuk statisztikai módszerekkel, a másik a modell alapú parametrikus módszer, mely során fiziológiai paramétereket hasonlítunk össze. [8]

A hazai kutatások közül szeretném kiemelni Gálai Bence és Benedek Csaba 2017-ben végzett kutatását, többszenzoros LiDAR rendszerrel végzett, járás alapú személyazonosítás és cselekvésfelismerés témában. Eljárásuk többszereplős kültéri jelenetekből nyeri ki a felismeréshez szükséges jellemzőket, a személyek egyidejű mozgása mellett. Kölcsönös kitakarások és egyéb háttérmozgások zaja mellett sikeres, nagy hatékonyságú azonosításokat végeztek, mely a technológia további felhasználhatóságát támasztja alá. [9] Nemzetközi porondon a kínai Watrix cég megoldása 50 méteres távolságon belül képes nagy (94%-os) hatékonysággal az azonosításra, és a rendszerrel nem szükséges az alanynak együttműködni. Nagy tömegben, eltakart arccal, hátat fordítva, szándékosan sántikálva, görnyedt tartással sem téveszthető meg a rendszerük, mely természetesen AI támogatással működik. A technológia egyelőre nem real-time, azaz nem valós időben azonosítja a személyeket. [10]

Hőkép alapú azonosítás

Az amerikai hadsereg harci képességeinek fejlesztéséért felelős részlege, a Hadseregkutató Laboratórium tudósai együttműködtek a Polaris Sensor Technologies céggel, hogy kifejlesszenek egy speciális infravörös kamerát. Az elektromágneses sugárzás által kibocsátott fény tulajdonságai alapján minden tárgy sajátos polarizációs jelzéssel rendelkezik, az objektum felületének tulajdonságaitól és alakjától függően. Az IR polarimetrikus kamera, az úgynevezett Pyxis, képes megkülönböztetni az ember alkotta tárgyak polarizációs jelét a természetes háttérétől. A hő polarimetria lehetővé tette a kutatók számára az emberi azonosítás és arcfelismerés teljes sötétségben történő elvégzését, ahogy a kapott adatokat összevetették más biometrikus adatbázisokkal. Ezt kihasználva a katonaság számára olyan AI-val támogatott arcfelismerési megoldást fejlesztettek, mely teljes sötétben, hőkép alapján képes személyek azonosítására, vagy speciális felhasználási területen könnyűszerrel végzi személyek követését. A Polaris által kifejlesztett polarimetrikus IR kamera drónokra szerelve már bizonyított, de a katonáságon kívüli egyéb kereskedelmi felhasználási területen is eredményeket hozott. Kikötők, kereskedelmi vízi útvonalak, olajfúró platformok megfigyelésére és az olajszennyezett területek észlelésére is alkalmazható. [11]

Viselkedésalapú megoldások (behavioral biometric)

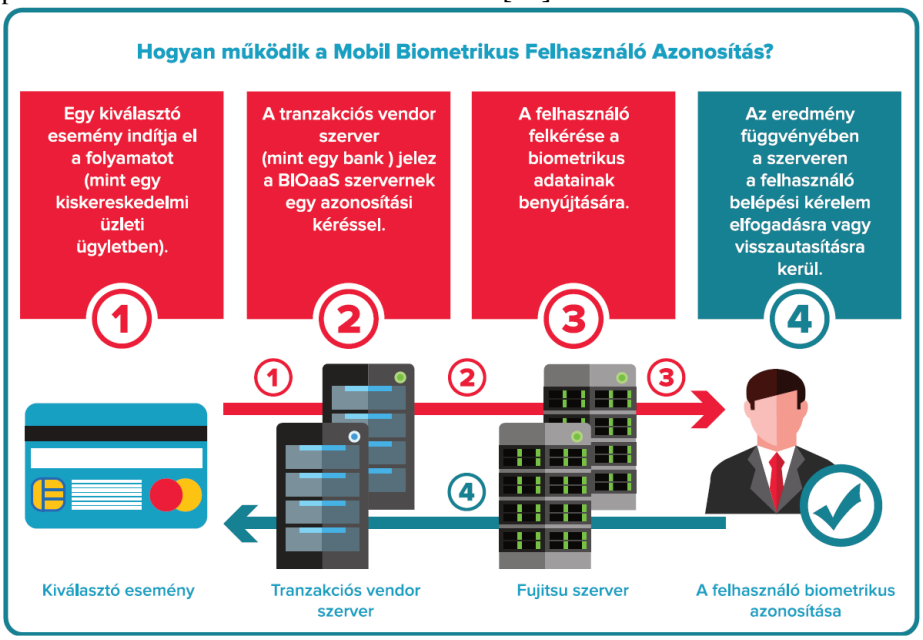
A viselkedés alapú biometria olyan emberi tulajdonságokkal kapcsolatos azonosítási megoldás, mely az egyedi képességek, stílus vagy motorikus képességek napi, rutinszerű feladatvégzés közbeni mérésén, összehasonlításán alapul. Ilyen lehet például minden számítógép használattal összefüggő tevékenység, mint a jellemző gépelési szokások, vagy az egér használattal összefüggő jellemző minták. De akár a telefonálás, az autóvezetés mintái, vagy a beszéd, sőt még a járás dinamikája és módja is ide tartozik.

„Az emberi viselkedésben rejlő különbözőségek elemzésére eddig is léteztek módszerek, melyek nem igényeltek gépi analízist: írásdinamika elemzése, beszédelemzés stb. Nagyon jó példa erre, hogy a második világháború során a Brit hírszerzés operátorai, a német Morse-kódok küldőiről képesek voltak anonim profilokat kialakítani, a gépelési sebesség és a vétett hibák alapján." [12] Ezek a megoldások, vagyis inkább adatok, nem használhatók egy beléptetés során elvégzendő hitelesítésre, de kiválóan alkalmasak profil alkotásra és a háttérben futó algoritmusok segítségével a folyamatos azonosításra, valamint a referen-

cia mintától való eltérés esetén riasztás életbe léptésére. A technológia természetesen alkalmas rejtett feltérképezésre és titkos profilozásra, hiszen interneten keresztül gépelési szokásainkat észrevétlenül rögzíthetik, vagy éppen rejtett kamerákkal és az arcfelismerés kombinálásával, járásunk módja egy adatbázisban összerendelhető.

Legújabb technológiák

Zártan működő és védett rendszer felhasználóinak védelmére fejlesztett proaktív, végponti viselkedéselemző megoldást a BlackBerry Cylance. A Cylance Persona folyamatosan figyeli és elemzi a védett rendszer felhasználóinak viselkedését, azaz a beviteli perifériák használatát, mely során észleli a korábban felvett referencia adatoktól való eltérést és életbe lépteti az előre definiált cselekvési terveket. [13]

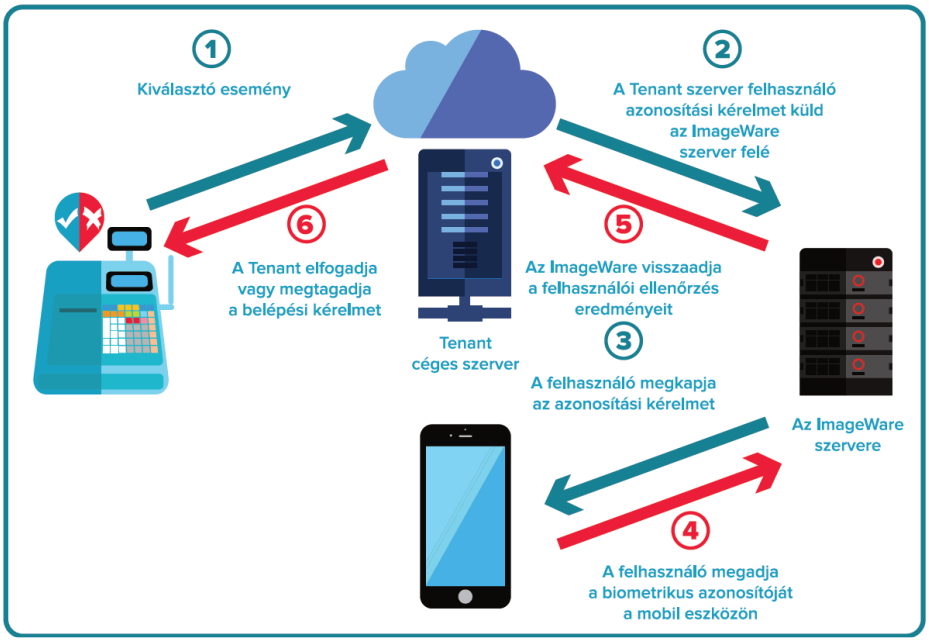


1. ábra: Mobil biometrikus felhasználói hitelesítés [14]

Biometric as a Service (BIOaaS)

Vezető ICT szolgáltatóként a Fujitsu egy felhőalapú biometrikus platform kifejlesztését tervezi az ImageWare® Systems (IWS)-el kötött partnerség keretein belül. Az IWS a mobil és felhő alapú multimodális, biometrikus identitáskezelő megoldások egyik élenjáró szakértője, a Fujitsu pedig felhőalapú infrastruktúra szolgáltatásaival (IaaS) és szoftver szolgáltatásaival (SaaS) piacvezető. A Fujitsu a megoldásaival már régóta előkészíti a terepet a BYOD (Bring Your Own Device) jellegű környezetekhez és az ilyen üzleti igények kiszolgálásához. A szolgáltatásuk középpontjában a GoCloudID® áll, az IWS felhőalapú, biometrikus kezelési és azonosítási szolgáltatása. Ezt a Fujitsu felhőjéből igénybe véve, viszonylag gyorsan integrálni lehet az üzleti alkalmazásokkal, a pay-as-you-go modellen működő plug-n-play biometria segítségével. Az IWS GoCloudID® által a felhasználó személye gyorsan azonosítható, és így hozzáférés nyerhető a biztonságos digitális tartalmakhoz. Természetesen, mindezekhez szükséges a szolgáltató biztonságos alkalmazáskiszolgálója a

GoMobileInteraktiv®, mely a gyors és pontos személyazonosság ellenőrzést végzi. [14] Amikor a GoVerifyID alkalmazás rögzíti a felhasználó biometrikus adatait, azt továbbítja az IWS GoCloudID® platformjára, átalakítja digitális biometrikus sablonokba, és névtelenül tárolja a Fujitsu felhőalapú, Software-as-a-Service (SaaS) rendszerén keresztül.



2. ábra: Felhő alapú azonosítás és hitelesítés folyamata [16]

Viselkedés alapú azonosítás

A Fujitsu nem csak az egyike a felhő infrastruktúrában élen járóknak, de az ő nevéhez fűződik az első, tenyér érhálózat alapú, biometrikus azonosító szenzor, a PalmSecure szenzortechnológiája is. Erre az eszközre épül a Groupama Arénában bevezetett, „véna-szenzor" néven elhíresült, tenyérérhálózat alapú azonosító megoldás is. De a gyártónál az évek alatt nem álltak meg a fejlesztéssel, mert az új trendeknek megfelelően, olyan mesterséges intelligencia alapú –rögzített video tartalomban az emberi viselkedést elemző – eljárást fejlesztett ki, mely egyaránt képes a szinte alig észrevehető gesztusok és a komplex viselkedés arzenál felismerésére. „A szoftver mintegy 100 alap „cselekvés" segítségével képes modulárisan azonosítani összetettebb viselkedésmintákat, mint pl. a vásárláson való rágódás, vagy bűncselekményre készülődés. Mint azt a fejlesztő kifejtette, a „hagyományos", mélytanuláson alapuló eljárások jelentős méretű tanító adatbázisok segítségével, több hónapos munkával készíthetők fel az éles tevékenységre, melyet a Fujitsu megoldása szükségtelenné tehet. A szoftverbe alapként integrált 100 cselekvést/gesztust a rendszer 90% feletti hatékonysággal ismeri fel a fejlesztők állítása szerint. A cég tervei szerint, az Actlyzer a japán piacon debütál még az idén, majd az így beszerzett tapasztalatokra építve fejlesztik, mielőtt a Fujitsu Human Centric AI Zinrai termékcsomag részeként a globális piac számára is elérhetővé válik." [16]

Érintés nélküli, ujjlenyomat alapú azonosítás

Nedves vagy sérült ujjlenyomat azonosítására képes eszközök és megoldások, melyek érintés nélkül végzik el nagy sebességgel az azonosítást. Jellemzőjük a nagy pontosság és a nagy sebesség. Érintés nélküli technológiát használ, tehát higiénikus, egy másodpercen belüli gyors azonosítást tesz lehetővé, négy ujj menet közbeni azonosításával. Az azonosítás során a mintavétel folyamat így nem igényel külön időt, és az azonosítási eljárás elfogadásának cselekedete sem szükségszerű többé, hiszen a folyamat nem igényel a felhasználótól ráutaló magatartást. Az ilyen, rejtett azonosításon alapuló megoldások, a felhasználó hozzájárulását nem igénylő, vagy észrevétlenül kikényszerített azonosítást igénylő megoldások egyre jobban terjednek és ilyen eljárás egyre több várható a világban. 2020-ban a londoni Metropolitan Rendőrség nagy számban fog arcfelismerő kamerákat beüzemelni a kedvelt turistahelyszíneken és a bevásárló központokban. [17] Eddig az arcfelismerést Angliában csak sporteseményeken és koncerteken használták, de viszonylag magas számú téves azonosítással. Az új módszer szerint a rendszer csak megjelöli a gyanús egyéneket és a járőröző rendőrök pedig igazoltatják. Ugyanakkor az adatvédelmi szakemberek a polgári szabadságjogok elleni támadásnak veszik a bejelentést és felhívják a figyelmet, hogy könnyű a rendszerrel visszaélni.

Közösségi médiából gyűjtött képek elemzése

A Clearview AI, amerikai startup cég azzal került a figyelem központjába, hogy olyan szolgáltatóktól gyűjtött be publikusan elérhető képeket, mint a Facebook, a Youtube, az Instagram vagy a Twitter. Adatbázisában 3 milliárd kép található. [18] Maga a technológia ugyanúgy működik, mint bármilyen másik arcfelismerő algoritmus: az arcvonások elemzésével az adatbázisukban szereplő minden arcot matematikailag értelmezhető vektorokká alakítanak és a hasonló értékek alapján csoportokba rendezik őket. Amikor a rendszer egy azonosítandó arcot lát, azt is átalakítja, és összeveti a már tárolt értékekkel, majd kidobja a leginkább hasonló találatokat, azaz minden keresett személy képe mellé a leginkább releváns Facebook, Instagram vagy egyéb közösségi média találatokat párosítja. Ez a mélymerítés olyan széleskörű azonosítást tesz lehetővé, amelyhez foghatót nemcsak egyetlen másik technológiai vállalat, de az amerikai kormány se rakott még össze soha, legalább is mai ismereteink szerint. A cég megoldását több mint 600 bűnüldöző szerv használja. A szoftvercég nagyon sok ellenséget gyűjtött, és ezzel az arcfelismerés technológiára is rányomta a bélyeget. A megoldást úgy használja hatóságok sora, hogy az nem esett át független ellenőrzésen, például a technológiai sztenderdekre ajánlásokat megfogalmazó kormányzati ügynökség, a NIST vizsgálatán, illetve magát a céget és adatkezelési szabályzatait és azok betartását sem auditálta senki.

A hírek alapján a cég az adatbázist engedély nélkül állította össze. A közösségi médiában megtalálható képek tömeges leszűrését minden érintett cég saját adatkezelési szabályzatában tiltja. Valamint a bűnüldöző és állami szervek eddig csak hivatalos, hatósági forrásból származó képeket használhattak, nem pedig a polgárok közösségi médiában megosztott magánfotóit. Technológiailag úttörő, de jogi és adatkezelési szempontból kifejezetten aggályos, hogy a Clearview AI technológiája úgy képes azonosításra, hogy nem profilképeket használ, hanem bármilyen szögben készült kép, vagy apró képrészlet alapján képes azonosítani. Fő probléma, hogy nem ismert a cég adatkezelési szabályzata, az adatbázisok

védelmi szintje és a harmadik fél hozzáférésének lehetősége, kockázata sem. Mindez egyébként azért is problémás, mert az arc alapján történő biometrikus azonosítás több nagy technológiai cégnél is már évekkel ezelőtt kikutatott és elkészült technológia. A Facebook is készített arcfelismerő alkalmazást, a Google is kész már a technológiával (pl. GoogleGlass), de végül nem, vagy nem úgy dobták piacra a terméket ahogy eredetileg tervezték. A hírek szerint azért, mert az átfogó, nemzetközi szabályozási irányelvek még nem készültek el és nem akarták a technológiát ideje korán úgy bevetni, hogy az komoly ellenérzést vált ki a nagy tömegekből, vagy azért, hogy az esetleges visszaélések miatt a technológia ne szenvedjen hátrányt. [19]

A biometria elterjedésének összefüggései

Az elsietett megoldások piacra dobása nagyban rontja a technológia megítélését és elfogadottságát. Olyannyira, hogy az EU átmenetileg betiltaná pár évre az arcfelismerő rendszerek publikus helyeken való használatát az EU-n belül, hogy megelőzzék a lakosság megfigyelését és az ezzel járó ellenállás növekedését. Az egyelőre vázlat formájában létező, várhatóan a 2020-as év elején megszilárduló javaslat a GDPR adatvédelmi szabályozásból indul ki, melynek fő célja, hogy az EU polgárai ne legyenek kitéve a személyes profilt alkotó, automatizált rendszerek döntéseinek. A kamerákra azért vezetnék be az ideiglenes tiltást, hogy legyen idő mérlegelni a mesterséges intelligencián alapuló automatikus személyazonosítás kockázatait, és kidolgozni a szükséges finomhangolásokat és szabályozásokat. [20]

Eközben az USA kormányzata nyilvánosságra hozta saját, AI szabályozási irányelveit, amelyeknek célja a hatóságok túlzott mértékű korlátozására vonatkozik, és sürgette az EU-t, hogy kerülje el az agresszív megközelítéseket. [21]

Az arcfelismerő technológiák ellentmondásosak a világ többi részén is. Magyarországon a Parlament 2019. december 10-én megszavazta az "egyes eljárások egyszerűsítése és elektronizálása érdekében szükséges" salátatörvényben a rendőrségi törvény módosítását, aminek egyik pontja a biometrikus arcfelismerést szabályozza. [22] Eszerint az olyan esetekben, ahol a rendőr az igazoltatás során nem tudja hitelt érdemlően azonosítani a személyt, ott lehetséges az arcfelismerő szoftver használata. Sőt, további lehetőségként a rendőr ujjnyomtatot vehet a személytől és más biometrikus adatát is rögzítheti, melyek segítségével ott a helyszínen biometrikus azonosítást végezhet a megfelelő rendszerben. [23]

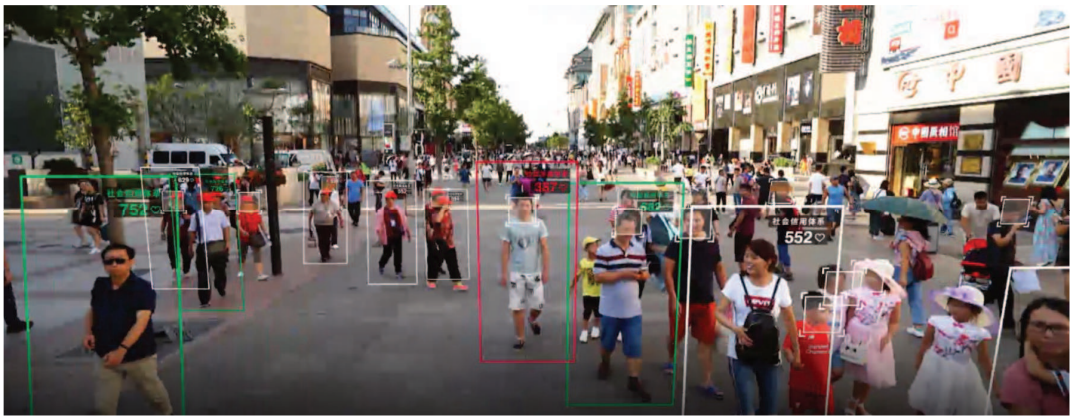
Megoldások szempontjából a kormányzati szektor mindig is a biometria korai alkalmazói közé tartozott, ideértve a határellenőrzésben használt technológiákat, a nemzeti azonosító megoldásokat vagy a bűnüldöző szervek által bevett eljárásokat. A mobil eszközök és alkalmazások növekvő elterjedésével várható, hogy az iparágakban egyre növekszik a biometrikus alkalmazások iránti igény az identitások hitelesítésére az online tranzakciókban. A magas kockázatú iparágak, mint a bankszektor is, jelentős beruházásokat végeznek a biometria területén. Csak a hangbiometria felhasználására már 2015-ben is 350 millió dollárt költött a szektor, aminek a következő időszakra a többszörözését várhatjuk, bár ebben a statisztikában majd érdekes lesz megfigyelni a koronavírus okozta, egyelőre ismeretlen mértékű hatásokat. Globális értelemben a közepes méretű biztosítótársaságok 70-80%-a már elfogadja a BYOD stratégiát, és ennek eredményeképpen a biztosítási üzletág jövőbeli kiadásai várhatóan mobilitási megoldásokat, biztonsági és vállalati alkalmazásokat céloznak meg. Különösen igaz lehet ez abban az esetben, ha a koronavírus okozta otthoni

munkavégzés megszokottá válik, mert ez lökést ad a távoli azonosítási megoldások fejlődésének.

A viselkedési minták integrálása biometrikus adatokkal, már napi szinten jelen van életünkben, amikor személyre szabott hirdetéseket kapunk. Ezeket hitelesítési eljárásokkal összekapcsolva sokkal magasabb szintre lehet emelni a biztonságot. Azonban nem szabad elfelejtkezni arról, hogy a nagyobb biztonság minden esetben a nagyobb szabadság rovására megy.

A pekingi Normal Egyetem kampuszán már évek óta arcfelismeréssel és kártya használatával lehet bejutni, amit nemcsak a diákok azonosítására használnak, de a viselkedési szokásaikat (éjszakai kimaradás) is elemzik. [24] Hangcsou 11. számú középiskolájában pedig a teremben tanuló diákokat figyelik meg arcfelismerő kamerákkal, melyek képesek az emberi arckifejezéseket értékelni. Így, ha egy diák tekintete sokáig elkalandozik, vagy ásítozik, azt a rendszer észleli. A tapasztalati visszajelzések alapján a tanulmányi teljesítmény javult, persze, ki merné az asztalra hajtani a fejét, ha közben tudja, hogy több kamera folyamatosan figyeli és értékeli. A rendszer egyébként nem rögzíti a képeket és nem tölt fel adatokat a felhőbe, csak a belső rendszer számára készít statisztikákat. [25]

Mindemellett, Kínában a digitális diktatúra csúcsra járatása történik éppen. [15] A Kínai kreditrendszer alapja a több százmillió arcfelismerést támogató kamera, mely segítségével totális megfigyelést hajt végre a kormány. A megfigyelésből gyűjtött adatok segítségével az embereket állami pontrendszerben pontozzák. A fizetési megoldásokat összekötik arcfelismerést használó mobil alkalmazásokkal. A bolti vásárlási szokásokat elemzik, a túl sok alkohol vásárlása pontlevonással jár, pelenka, vagy trendi és egészséges termékek vásárlásért plusz pontokat lehet szerezni. Az állam által kívánatos szolgáltatások igénybevételéért, vagy magán adatok megadásáért szintén plusz pontok járnak, akárcsak, ha valaki pontosan fizeti a hiteleit. De egy bebukott hitel akár le is nullázhatja a társadalmi kreditpontokat, amivel az illető egzisztenciája is semmivé foszlik, legvégső esetben a rendszer peremére sodródik. Nem ér el szolgáltatásokat, nem utazhat szabadon, nem vehet meg bármit, mert a társadalmon kívülre került. A népnevelés ilyen formája könnyen megy az autoriter rezsim állami propagandájának nyomása alatt, a közbiztonság igénye mögé bújva elveszi a magánszférát és digitalizálja a diktatúrát.



3. ábra: Kínai megfigyelőrendszer. Forrás: HVG [26]

Kínában a rendszer segítségével, algoritmusokkal kormányoznak. A laza, csak a központi állami szervek igényeire kialakított adatkezelési szabályzatok teljes mértékben támogatják a személyes adatok gyűjtését, profilozást és ezzel a magánszféra durva megsértését. Itt vissza is jutottunk a technológia fejlődéséhez és annak fontosságához, hogy a technikai fejlődéssel szorosan együtt kell, hogy járjon a jogi szabályozás fejlődése és a felhasználók megfelelő oktatása. A következőkben a nemzetközi jogszabályi környezetet vizsgáljuk.

A BIOMETRIKUS AZONOSÍTÁS NEMZETKÖZI ÉS MAGYAR JOGSZABÁLYI HÁTTERÉNEK ÁTTEKINTÉSE

General Data Protection Regulation (GDPR)

A GDPR azon felül, hogy az Európai Unió tagállamaira vonatkozóan speciális adatkezelési szabályokat határoz meg, attól az érintettek körébe tartoznak az Unión kívüli országok is, ezáltal a rendelet hatálya globális, mert EU adattal kapcsolatos tárgykörben is folyik adatkezelés. A rendelet deklarálja, hogy az adatgyűjtés megkezdése előtt a hozzájárulásnak explicit módon meg kell lennie. Nagy volumenű sajátossága a rendeletnek az elfeledtetéshez való jog, amely a kezelt adatokra vonatkozó visszaállíthatatlan törlés lehetőségének megvalósítását szorgalmazza. [27]

Az Európai Adatvédelmi Testület ajánlása biometrikus adatkezelésre vonatkozólag

„A biometrikus adatok felhasználása és különösen az arcfelismerés fokozott kockázatot jelent az érintettek jogai szempontjából. Alapvető fontosságú, hogy az ilyen technológiák igénybevételére a GDPR-ben rögzített jogszerűség, szükségesség, arányosság és az adatok minimalizálása elveinek kellő tiszteletben tartásával kerüljön sor.” [28]

UK Data Protection Act

Az Egyesült Királyságban 2018-ban elfogadott adatvédelmi törvény számos alkalommal említi a biometrikus adat kifejezést, a jogos érdek és a törvényes eljáráson felül a „sensitive processing”, azaz érzékeny adatkezelés meghatározáson belül is definiálja. Az általános rendelkezésekről e téren a 205. szakasz rendelkezik részletesen. [29]

California Consumer Privacy Act (CCPA) módosítása AB-375

A törvénymódosító szerint a személyes adat kategóriájába a nyilvánosan elérhető információk nem tartoznak bele. Rögzíti továbbá, hogy a nyilvánosan elérhető adatok körébe kizárólag a törvényesen elérhető adatok tartoznak, amelyek a központi kormányzattól, az állami vagy helyi kormányzatok nyilvántartásaiból származnak. A biometrikus adatokra vonatkozólag úgy rendelkezik, hogy azok nem tartoznak nyilvánosan elérhető információk körébe és nem gyűjthetők a fogyasztó tudomása nélkül. [30]

Összegezve tehát elmondhatjuk, hogy a nemzetközi gyakorlatban a szabályozás arra törekszik, hogy legyen az állampolgár/magánszemély/fogyasztó besorolásokban egy olyan kapaszkodó pont, amely védi az egyéneket az akaratukon kívüli adatgyűjtéstől, valamint attól, hogy ha ezek mégis megtörténnének, legyen mozgásterük azoknak a kiküszöbölésére, módosítására, semmissé tételére. A különleges adatkategóriába tartozó biometrikus

adatok kezelése azért is kockázatos, mert olyan területeket képes kiszolgálni, mint a bűnüldözés, a személyre szabott marketing, politikai és vallási konfliktusok és számos más terület, ahol a személy pontos beazonosítása közel tökéletes azonosító jegyek alapján megvalósítható, az intézkedések és eljárások pedig személyre szabhatók. Ennek tudatában a szabályozás a jogos érdeket és a törvények szerinti eljárást különösképpen hangsúlyozza a jogszabályi keretekben.

A BIOMETRIAI AZONOSÍTÁS SZABÁLYOZÁSÁNAK NEMZETKÖZI PÉLDÁI

Iskolai keretek között rögzített ujjnyomatok miatt kiszabott bírság

A lengyelországi Gdańsk városában lévő 2.-es számú Általános Iskolában az iskolai ebédbefizetés ellenőrzése során alkalmazott ujjnyomatazonosítási eljárás miatt történt jogosulatlanul adatgyűjtés és adatkezelés. Ennek következtében a lengyel adatvédelmi hatóság bírságot szabott ki a tanintézmény számára, 20 000 lengyel zloty tételben (megközelítőleg 1,6 millió magyar forint). Az iskola 2015 áprilisa óta a 2019/2020-as tanévig 680 diák biometrikus adatát kezelte jogosulatlanul, és mindösszesen 4 tanuló választotta az alternatív megoldást az azonosításra. [31]

Növekvő jogi és szabályozási követelmények a biometrikus adatok gyűjtésével kapcsolatban

Az elmúlt években a biometrikus azonosítás az ujjnyomat-ellenőrzéstől az arcfelismerésig, széles körben került elterjedésre a mindennapi használatban, elég, ha a fizetési megoldásokra gondolunk, vagy a reptéri beléptetésre a csomagellenőrzésnél. Ezek a megoldások, bár egyszerűsített azonosítási módszereket jelenthetnek a felhasználói oldalon, azonban adatvédelmi szempontból (és védelmi szempontból is) komoly elvárásokat támasztanak az adatkezelők számára ezeknek az adatoknak a gyűjtése során. Az Egyesült Államokban 2008 óta érvényben lévő Biometric Information Privacy Act is az egyik megjelenési formája ezeknek. 2019 januárjában egy iskolai kirándulás során egy fiúnak felvették az ujjnyomatát, mellyel igénybe vette a szabadidős parkba a belépőkártyáját. Azonban az azonosítást végző vállalat nem kötött ki határozott időt a felvett különleges adat kezelésével kapcsolatban, ezzel jogosulatlan adatgyűjtés miatt megszegte a BIPA rendelkezéseit. A vállalat szándéka a biometrikus azonosítással az volt, ha netán egy vendég elveszíti a papír alapú belépőkártyáját, a csalási szándék ezáltal kizárható legyen, tehát csak az az egyedi azonosítóval együttesen rendelkező személy használhassa a belépőt, akinek a regisztrációkor azt rögzítették. Viszont a cég a jogos érdekét az adatkezelés időtartamát tekintve nem tudta igazolni, ezért a per során veszített. [32]

Biometrikus adat – a permanens személyes adat kockázatai

Néhány terület, ahol alkalmazásra kerülnek a biometrikus azonosítási eljárások:

- Munkaerőgazdálkodás
- Kórházak
- Bankszektor
- Kereskedelem
- Járműipar

Az Egyesült államokban az Illinois-i BIPA alapján 1000 dollártól 5000 dollárig terjedhet a bírság annak függvényében, hogy milyen természetű szabályszegés történt (szándékosság tényállása). Ezek a rendelkezések azonban 2018 februárjában módosítva lettek olyan kizáró tényezőkkel, mint hogy:

- az adott entitás a biometriai adatkezelést és adatgyűjtést biztonsági okokból, csalás megelőzés céljával vagy munkaerőgazdálkodási szempontból alkalmazza,
- nem folytat kereskedést ezekkel az adatokkal,
- illetve ezeknek az adatoknak a tárolása, cseréje, valamint védelme a magánszektorra jellemző alapvető módon vagy még hatékonyabb szinten történik, hasonlóan a bizalmas és érzékeny információkra tekintettel [33]

Biometrikus azonosítás a munkahelyen

A biometrikus azonosítás munkahelyi környezetben való alkalmazása világszerte elterjedőben van, a munkavállalóknak a vállalati eszközökhöz való hozzáférését, vagy elzárt területekre való bejutását szolgálhatja ki. A módszertan bevezetésével a csalások redukálhatók, a biztonsági szint számottevően emelkedik, amellett, hogy egyéb területek biztonsági költségein még spórolni is tudunk. Azonban fontos szem előtt tartani, mivel különleges adatok kezeléséről van szó, ezért adatvédelmi szempontból kellő gondoskodással kell eljárnunk mind a rendszerek, mind az adatok védelmével kapcsolatban. További fontos elemként jelenik meg, hogy a kezelt adat természetéből fakadóan jellemzően a tökéletesen egyedi felé tendál, azoknak esetleges kiszivárgása a rendszerekből, illetve egyéb okból jogosulatlan kézbe kerülésük esetén komoly gondokat okozhatnak. Ezeket még a bevezetés előtt célszerű felmérni, ezzel is elkerülve a kontraproduktív hatást. A jogszabályi háttér során két alapelvet mindig biztosítani kell, ez pedig az előzetes önkéntes hozzájárulás, valamint a jogos érdek biztosítása. Ezekről már a korábban említett GDPR részletesen rendelkezik. Fontos továbbá az is, hogy a biometrikus eljárások alkalmazása során kellő körültekintéssel rendelkezzenek a munkavállalók is, hiszen ők maguk is felelősek az általuk kezelt adatokért. [34]

Arcfelismerési szabályozás az Egyesült Királyságban, Kanadában és az Egyesült Államokban

A döntéshozók szerte a világban vagy várakozási álláspontot, vagy védekezési módban állnak a technológiai megoldással kapcsolatban. A kanadai tartományok közül az atlanti térségben elhelyezkedő mind a négy tartományban közös nevezőn vannak a járművezetési engedély kiadásához kötődő arcfelismerési eljárások bevezetésében a szabályozást illetően. A közlekedésügyi miniszter megjegyezte, hogy 2007 óta már rendelkezésre áll a technológia és az engedély nélküli autóvezetés területén már volt néhány fogás annak alkalmazásával. Skóciában a liberális politikai erők azért emeltek szót, hogy a rendőrségi nyilvántartásban szereplő ártatlan emberek arcképmásai legyenek eltávolítva, mert nincs jogos érdek tárolásukra. Az Egyesült Államokban egy korábban a New York Police Department biztosaként dolgozó szakember, Bill Bratton szerint a szabályozásnak nem kellene tiltania a biometrikus eljárásokat. Álláspontját azzal igyekezett alátámasztani, hogy a magánszektor már régóta foglalkozik és fejleszti ezeket az eljárásokat, attól függetlenül, hogy

ezt a Szenátus szeretné vagy sem. Továbbá kiemelte, hogy a technológiai megoldás az ártatlan embereket igyekszik védeni a börtönbüntetéstől, szembe állítva ezt a szemtanúi vallomás alapján történő ítélkezési eljárással. [35]

2015-ben a skót parlamenti képviselők kritikával illették a szabályozási gyakorlatot, valamint a skót kormány által létrehozott biometriai biztosi pozíciót, melyről azt vélték, hogy nem lesz olyan hatékony, mint az elvárt lenne. Mathew Rice, az Open Right Group Scotland igazgatója a problémát a beszámolási kötelezettségekben találta, érvelésében az információügyi biztos pozíciójával vonta párhuzamba, ahol a probléma a tájékoztatás szűkösségében van, mert a biometriai biztos csak a parlament irányába szolgáltathat adatot. [36]

A magyar jogszabályi környezet fejlődésének vizsgálata a biometrikus azonosítás szabályozásának szemszögéből

A hazai szabályozás első körben a (1. táblázat) szereplő bűnügyi nyilvántartó rendszer (rendelkező jogszabály a bnytv). keretein belül rendelkezik a biometrikus azonosítás, mint eljárás és különleges adatgyűjtési módszerről, valamint annak meghatározott céljáról. Kiindulópontként az ujjnyomat felvételi eljárás, valamint annak (a) személyhez kötött eljárás rendjét definiálja.

Kihirdetés ideje	Jogszabály neve
2009. VI. 19.	2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről
2011. VII. 26.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
2013. IV. 25.	2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
2016. IV. 27.	AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE
2018. XI. 28.	AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/1860 RENDELETE AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/1861 RENDELETE AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/1862 RENDELETE
2018. XII. 12.	2018. évi CXXXV. törvény a sportról szóló 2004. évi I. törvény módosításáról
2018. XII. 20.	2018. évi CXXI. törvény egyes belügyi tárgyú és más kapcsolódó törvények módosításáról

1. táblázat: A jogszabályi háttér időrendi változása (Saját szerkesztés)

A növekvő igényre mind az azonosítás, mind az adatgyűjtés területén, szükség volt nemzeti szabályozási keret megteremtésére is, a már meglévő Uniós ajánlásokon és az akkor még hatályban lévő 95/46/EK irányelven felül, ennek következtében született meg a köznyelvben infotörvényként ismert jogszabály. Az infobiztonsági törvény (ibtv.) az állami és önkormányzati hatáskörben gyűjtött és kezelt adatokkal kapcsolatosan fogalmazott meg alapelveket, valamint eljárást ezeknek az adatoknak a kezeléséről. 2016-ban jelent meg ajánlás az Általános Adatvédelmi Rendelet (GDPR) tekintetében, amely egy 2 éves periódust kínált fel a tagállamok számára, hogy a jogharmonizációt érvényre juttassák a nemzeti jogszabályi keretrendszerükben. Az illegális migráció okozta közigazgatási nyomás következtében, 2018-ban az Európai Parlament és a Tanács rendeletben korlátozta a kiutasítás és a schengeni övezetben jogosulatlanul tartózkodó személyek mozgását, ezeknek a szemé-

lyeknek azonosítását részben biometrikus módszerek alkalmazásával is kiszolgálta (pl. ujjnyomat-, arcfelismerés alapú azonosítás). Sportrendezvényekre való könnyebb beléptetés gyanánt, valamint az ilyen eseményeken gyakran előforduló rendbontás következtében a 2004-es sporttörvény módosítására került sor, melynek során bevezetésre kerültek biometrikus azonosítási eljárások is.

KONKLÚZIÓ

Vészhelyzetben, vagy amikor biztosságérzetünk bármilyen szempontból gyengül, könnyen lemondunk bizonyos szabadságfokokról annak érdekében, hogy az életünk visszazökkenjen a megszokott kerékvágásba. A koronavírus idején (2020) könnyen indokolható közösségi érdekekkel, hogy a mobiltelefonunk lokációs információi alapján visszakövethető legyen, kikkel érintkeztünk az elmúlt időszakban, és ezzel gátoljuk a vírus terjedését. Vagy megosszuk utazási információinkat a hatóságokkal. Ehhez jó alapot ad a környező országok és hazánk kormánya által meghirdetett rendkívüli helyzet és különleges jogrend, ami itthon amúgy is igen széles lehetőségeket biztosít. De mi garantálja, hogy ezek az információk nem kerülnek illetéktelenek kezébe, vagy, hogy az állami szervek nem használják fel biometrikus azonosítóinkat, kapcsolati adatainkat, szokásainkat profilozásra és a kinyert adatokat később saját céljaikra? Szükség lenne egy ilyen helyzethez illeszkedő, kétharmados törvényekkel és rendkívüli helyzetekben sem felülírható szabályozásra, mely védi a polgárok személyes adatait és jogait, ugyanakkor a biztonság növelése mellett sem ad lehetőséget a visszaélésre. Ha hallgatunk a vészjósló hangokra, a jövőben is fel kell készülni a koronavírushoz hasonló, globális katasztrófahelyzetekre. Az ilyen helyzetekben a biztonság megnövelése mellett szólnak a fokozódó munkanélküliség miatt szaporodó bűnesetek, vagy az újra felerősödő terrortámadások. Mi történne, ha terrorszervezetek, kihasználva a zavaros időszakot támadást indítanának mondjuk közművek ellen? Erre idejében fel lehetne készülni, minden technológia adott, könnyen kialakítható lenne olyan AI-val támogatott arc és járás felismerő megoldás, amelyekkel automatizáltan védhetők lennének eddig nem fókuszban lévő közművek, például nagyobb települések vízbázisai, vagy víztisztító, vízellátást biztosító telepek. A jövő legnagyobb kincse a víz lesz, ezért ezek védelmére kiemelt figyelmet kellene fordítani! De könnyen belátható, hogy amíg nincs egységes, a demokratikus értékrendekhez jobban igazodó (pl. Európai Uniós) szabályozás és kontroll, addig azokban az országokban, ahol a biometrikus adatok gyűjtése és felhasználása elterjedőben van, ott a visszaélések száma is várhatóan magas lesz.

A koronavírushoz hasonló epidemiológiai események jó táptalajt adhatnak a biometria terjedésének, mely kihat majd más területekre is. Gondoljunk bele, milyen egyértelmű lehetőség lenne biometrikus azonosítási elven működő országgyűlési választási rendszert fejleszteni (online állampolgári azonosító elve), vagy az egészségügyben betegazonosításra, recept kiváltásra vagy távoli ügyintézésre használni az ilyen rendszereket. Persze a világ számos pontján már sziget megoldásként történtek ilyen területen fejlesztések, de ezek elterjedése és az egységes szabályozás még várat magára. A kockázatok figyelembevételével, ha magasabb szintű biztonságra van szükség vagy az elvárás nagyobb, akkor többféle azonosító faktor használata a megoldás a megfelelő szabályozás és kontroll mellett.

HIVATKOZÁSOK

[1] J. Renaghan, „Etched in stone," The Zoogoer, 1997.
[2] 13 Kr. e. 1792-1750 vagy Kr. e. 1728-1686 között uralkodott.
[3] Marcello Malpighi a Bolognai Egyetem anatómiaprofesszora, (1628-1694).
[4] K. FÖLDESI, „A DAKTILOSZKÓPIA FUNKCIONÁLIS TÖRTÉNETE," [Online]. Available: hadmernok.hu/153_01_foldesik.pdf. [Hozzáférés dátuma: 16 december 2019].
[5] d. H. A. T. dr. GÁBOR Béla, Dactyloscopia, Budapest: Országos Központi Nyomda Részvénytársaság, 1905.
[6] M. I. O. C. KOVÁCS Tibor, „A biztonságtudomány biometria aspektusai," [Online]. Available: http://www.pecshor.hu/periodika/XIII/kovacsti.pdf. [Hozzáférés dátuma: 10 november 2019].
[7] G. KETSKEMÉTY, Biometrián alapuló személyazonosító rendszerek, Budapest: Budapest Műszaki Főiskola Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2008.
[8] GUARDWARESYSTEMS, „Távoli személyazonosítási technikák," [Online]. Available: http://oldweb.mit.bme.hu/eng/research/search/downloads/tst/Irodalomkutatas.pdf. [Hozzáférés dátuma: 21 február 2020].
[9] B. C. GÁLAI Bence, „Járás alapú személyazonosítás és cselekvés felismerés LIDAR szenzorokkal," [Online]. Available: https://eprints.sztaki.hu/9175/1/Galai_1_3239040_ny.pdf. [Hozzáférés dátuma: 10 március 2020].
[10] „Chinese 'gait recognition' tech IDs people by how they walk," [Online]. Available: https://apnews.com/bf75dd1c26c947b7826d270a16e2658a. [Hozzáférés dátuma: 5 március 2020].
[11] „US Army infrared drone camera," [Online]. Available: https://www.army.mil/article/230293/researchers_tackle_challenges_of_tomorrow_with_new_infrared_drone_camera. [Hozzáférés dátuma: 13 február 2020].
[12] Securinfo, „Viselkedés alapú biometria," [Online]. Available: https://www.securinfo.hu/termekek/biometria/3735-behavioral-biometrics-viselkedesalapu-biometria.html. [Hozzáférés dátuma: 29 január 2020].
[13] SecuriFocus, „BlackBerry viselkedés alapú biometria," [Online]. Available: https://www.securifocus.com/portal.php?pagename=hir_reszlet&hir_id=6965. [Hozzáférés dátuma: 11 Március 2020].
[14] „Fujitsu BIOaaS solution," [Online]. Available: https://www.fujitsu.com/ca/en/Images/Biometrics-as-a-Service_BIOaaS-Flyer.pdf. [Hozzáférés dátuma: 10 február 2020].
[15] F. &. Sullivan, „Biometric As a Service," [Online]. Available: https://www.fujitsu.com/caribbean/Images/Fujitsu-FrostSullivan_Cloud_WP_Biometrics-as-a-Service.pdf. [Hozzáférés dátuma: 11 március 2020].
[16] F. &. Sullival, „Cloud-based Identity and Authentication," [Online]. Available: https://www.fujitsu.com/caribbean/Images/Fujitsu-FrostSullivan_Cloud_WP_Biometrics-as-a-Service.pdf. [Hozzáférés dátuma: 16 január 2020].

[17] SecuriFocus, „Fujitsu viselkedés alapú biometria AI támogatással," [Online]. Available: https://www.securifocus.com/portal.php?pagename=hir_reszlet&hir_id=7786. [Hozzáférés dátuma: 17 február 2020].
[18] „Londoni arcfelismerés bevezetése," [Online]. Available: https://www.theverge.com/2020/1/24/21079919/facial-recognition-london-cctv-camera-deployment. [Hozzáférés dátuma: 20 március 2020].
[19] „Clearview közösségi média alapú arcfelismerési megoldása," [Online]. Available: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing. [Hozzáférés dátuma: 4 február 2020].
[20] „Google arcfelismerés," [Online]. Available: https://www.cnet.com/news/google-vows-not-to-sell-its-facial-recognition-technology-for-now/. [Hozzáférés dátuma: 22 február 2020].
[21] „EU drops idea of facial recognition ban in public areas," [Online]. Available: https://ca.reuters.com/article/idUSKBN1ZS37Q. [Hozzáférés dátuma: 14 március 2020].
[22] „Guidance for Regulation of Artificial Intelligence Applications," [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf. [Hozzáférés dátuma: 15 március 2020].
[23] MagyarországKormánya, „T/7690. számú törvényjavaslat," [Online]. Available: https://www.parlament.hu/irom41/07690/07690.pdf. [Hozzáférés dátuma: 26 február 2020].
[24] „Az igazoltató rendőr akár arcfelismerő szoftvert is használhat," [Online]. Available: https://index.hu/belfold/2019/12/10/az_igazoltato_rendor_akar_arcfelismero_szoftvert_is_hasznalhat/. [Hozzáférés dátuma: 24 február 2020].
[25] „Beijing Normal University facial scanner," [Online]. Available: http://www.xinhuanet.com//english/2017-09/12/c_136604144.htm. [Hozzáférés dátuma: 14 március 2020].
[26] Techjuice, „Intelligent Classroom Behavior Management System," [Online]. Available: https://www.techjuice.pk/this-school-scans-classrooms-every-30-seconds-through-facial-recognition-technology/. [Hozzáférés dátuma: 13 március 2020].
[27] „A Kínai kreditrendszer," [Online]. Available: www.independent.co.uk/news/world/asia/china-social-credit-system-flight-booking-blacklisted-beijing-points-a8646316.html?utm_source=reddit.com. [Hozzáférés dátuma: 20 február 2020].
[28] https://hvg.hu/tudomany/20180919_kina_tarsadalmi_kreditrendszer_hogyan_mukodik_pontszam_megfigyeles_digitalis_diktatura, A Kínai kreditrendszer, HVG, 2018.
[29] „Biometric data and data protection regulations (GDPR and CCPA)," 27 02 2020. [Online]. Available: https://www.gemalto.com/govt/biometrics/biometric-data. [Hozzáférés dátuma: 25 03 2020].
[30] European Data Protection Board, „Guidelines 3/2019 on processing of personal data," 10 07 2019. [Online]. Available: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf. [Hozzáférés dátuma: 01 04 2020].
[31] United Kingdom Parliament, „Data Protection Act," UK, 2018.
[32] H. S. Chau A., „n act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy.," California, 2018.
[33] Office for Personal Data Protection, „School with students' fingerprints," 05 03 2020. [Online]. Available: https://uodo.gov.pl/pl/138/1453. [Hozzáférés dátuma: 01 04 2020].

[34] Forrester Research, „The growing legal and regulatory implications of collecting biometric data," 17 05 2019. [Online]. Available: https://www.zdnet.com/article/the-growing-legal-and-regulatory-implications-of-collecting-biometric-data/. [Hozzáférés dátuma: 25 03 2020].
[35] A. S. Wernick, „Biometric Information – Permanent Personally Identifiable Information Risk," 14 02 2019. [Online]. Available: https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_8/. [Hozzáférés dátuma: 25 március 2020].
[36] P. Kovacsics, „Biometric Authentication at the Workplace: Risks and Legal Challenges," 28 08 2019. [Online]. Available: https://www.hrtechnologist.com/articles/hr-compliance/biometric-authentication-at-the-workplace-risks-and-legal-challenges/. [Hozzáférés dátuma: 25 03 2020].
[37] C. Burt, „Legal issues around facial biometrics use examined in U.S., Canada, and UK," 03 02 2020. [Online]. Available: https://www.biometricupdate.com/202002/legal-issues-around-facial-biometrics-use-examined-in-u-s-canada-and-uk. [Hozzáférés dátuma: 25 03 2020].
[38] A. Tibbitt, „Biometrics watchdog will lack powers, say critics," The Ferret, 23 07 2018. [Online]. Available: https://theferret.scot/scottish-biometrics-commissioner-enforcement-powers/. [Hozzáférés dátuma: 31 március 2020].