DOI: 10.38146/BSZ.2023.8.7

A biometria elterjedésének elemzése

Analysis of the spread of biometrics

Ujhegyi Péter
doktorandusz, műszaki vezető
Óbudai Egyetem
ujhegyi.peter@uni-obuda.hu

Absztrakt
Cél: A cikk rövid bevezetése áttekintést ad az azonosítási megoldások fő paramétereiről és a legelterjedtebb biometrikus azonosítási megoldásokról. Ezt követően a cikk az EU-ban a határrendészetnél használt biometrikus azonosítási megoldásokat mutatja be, illetve rövid összehasonlítást ad a jelenlegi megoldások és az érhálózat-alapú megoldások között, kiemelve az érhálózat-alapú megoldások előnyeit a korábbi megoldásokhoz képest. A cikk a továbbiakban a korábbi, biometrikus megoldások elterjedésével összefüggő kutatásokat foglalja össze egy új kutatás eredményeinek bemutatásával.
Módszertan: A biometria elterjedésével összefüggő korábbi, Óbudai Egyetemen végzett kutatás elemző összehasonlítása egy 2022-es friss kutatás eredményeivel.
Megállapítások: A biometriával összefüggő oktatás mélyítheti a megoldásokkal kapcsolatos kockázatok ismeretét, ami növelheti az elutasítottságát és a legerősebb félelem kialakulását, ami a biometrikus adatok kezelésével és biztonságával kapcsolatos.
Érték: A cikk felhívja a figyelmet, hogy a kockázatokat a biometrikus megoldások felhasználásának erősebb szabályozásával és az adatkezelési, adatvédelmi megoldások biometriára kialakított szabványosításával és elterjedésével lehetne csökkenteni.

Kulcsszavak: biometrikus azonosítás, biometria elterjedése, biometria kockázatai, személyes adatok védelme

Abstract
Aim: A brief introduction to this article gives an overview of the main parameters of identification solutions and the most common biometric identification solutions.

The article then describes the biometric identification solutions used by border police in the EU and gives a brief comparison between current solutions and the vascular network-based solutions, highlighting the advantages of the vascular network-based solutions compared to the previous solutions. Next, the article summarises previous research related to the uptake of biometric solutions by presenting the results of a recent research.
Methodology: An analytical comparison of previous research on the uptake of biometrics at Óbuda University with the results with a recent study from 2022.
Findings: Education about biometrics can deepen awareness of the risks associated with the solutions, which can increase the risk of rejection and fear of the most powerful fears related to the handling and security of biometric data.
Value: The article points out that the risks could be reduced by stronger regulation of the use of biometrics and by standardisation and diffusion of data management and privacy solutions designed for biometrics.

Keywords: biometric identification, uptake of biometrics, risks of biometrics, protection of personal data

Bevezetés

Modern és gyorsan fejlődő, de nagyon sérülékeny világban élünk, amit csak megfelelő és alapos körültekintéssel lehet érteni. Több hírforrásra támaszkodva, tudatos hírolvasási szokásokkal szinte minden nap olvasható valami „goodnews" egy ígéretes rákgyógyítási lehetőségről, egy újabb kísérleti akkumulátortechnológiáról, de gyakran jön szembe nagyobb hatékonyságot ígérő energiatermelési megoldás friss kutatási híre is. Sajnos, a hírolvasási tendenciákat látva egyre inkább csak a rossz hír a hír, és ezekből, korunkra jellemzően van bőven. Így nyersanyag és energia éhínség, környezeti katasztrófák, a bolygónkat kizsákmányoló életmódunk miatt a globális felmelegedés okozta csapadék- és ivóvízhiányok, és a COVID hírek mellett az elmúlt félévben az orosz–ukrán háború, Észak-Korea nukleáris fegyverkezése, a török–görög konfliktus éleződése a leginkább aggodalomra okot adó vezető hírek. Ezek a történések a nem igazán tudatos vagy kellően óvatos hírolvasóknak különféle narratívában, általában a médiát uraló globális trendek mentén tűnnek fel a közösségi médiát uraló átláthatatlan algoritmusok által, nemegyszer az olvasó politikai preferenciájának megfelelően kialakítva.

A válságok és a háborúk velejárója a zűrzavar és a káosz, amelyek hatására az elégedetlenek elkezdik keresni a kiutat, amely legtöbbször népvándorlásban,

menekültekben, migrációban mutatkozik meg. Ahogy számtalan probléma kezelésére közös összefogással az Európai Unió egységes megoldást alakított ki, előremutató lenne a háborús időkben a biztonságot növelő biometrikus azonosítási megoldások területén is a tagországokkal közös jogi, adatkezelési és technológiai megoldást kidolgozni. A cikkben az azonosítási megoldások elterjedésének hazai vonatkozásait elemzi a szerző egy friss kutatás és a korábbi kutatások összevetésével.

A biometrikus azonosítás lehetőségei és mérőszámai

Fontos különbséget tenni az azonosítás és a hitelesítés között. „1:n" típusú azonosításról beszélünk, amikor az aktuálisan mért biometrikus mintát („1") összevetjük egy adatbázisban tárolt összes mintával („n"), és ha van egyezés, akkor megállapításra kerül a jogosultságot kérő személye, és megtörténik, mondjuk egy beléptetés. Tehát egy mintát vetettünk össze sok ember adatát tartalmazó halmazzal. Kiemelt része ennek a folyamatnak, hogy a biometrikus sablonok, minták tárolása jogi feltételeinek is teljesülnie kell, hiszen a biometrikus sablon személyes adatnak minősül, és erre a személyes adatok védelme érdekében megfelelő szabályozás vonatkozik (Kovács & Ujhegyi, 2021).

Hitelesítés („1:1") során egy sablon („1"), azaz egy biometrikus adat kerül letárolásra és az éppen levett mintázattal („1") kerül összevetésre. Ennél a módszernél azt vizsgáljuk, hogy az adott és tárolt mintához tartozó személy van-e éppen ott, és az azonosítás pillanatában ő adja-e a biometrikus mintát. Ezt a hitelesítési eljárást alkalmazza a mobiltelefonunk a biometrikus ellenőrzésnél, ha belépünk a készülékbe vagy bankolni, esetleg épp fizetni akarunk, de a folyamat szempontjából ide tartozik az útlevelünk által tárolt biometrikus adat felhasználásának módja is. Tehát a frissen levett és a korábban tárolt minta egyezőségét vizsgálja az adott metodika (Kovács & Ujhegyi, 2021).

A hitelesítési eljárásnak a folyamata általában sokkal gyorsabb, ugyanis nem kell több száz, ezer vagy akár milliós nagyságú adatbázisrekordban elvégezni az összehasonlítást, valamint a sok érzékeny adatot tartalmazó adatbázis védelme sem jelent nagy kockázatot, hiszen az adatokat nem így tároljuk.

Az azonosítási folyamat és a használt biometrikus mérési megoldás fontos jellemzője még a FAR és a FRR érték. A FAR (False Acceptance Rate, azaz téves elfogadási arány) érték azt mutatja meg, hogy a beléptetés során mennyi esetben történik jogosulatlan felhasználó jogosultként történő azonosítása. Ennél a mutatónál kevésbé problémásnak tűnik az FRR (False Rejection Rate, azaz téves visszautasítási arány), tehát a jogosult felhasználók visszautasítása.

Azonosítási megoldásoknál jellemző szempont még, hogy a használt technológia mennyi biometrikus jellemzőt rögzít. Nagyon széles skálán mozog a rögzített adatok száma, egy ujjnyomat esetén 15–35 pontról beszélünk, de egy tenyérérhálózat alapú megoldás ötmillió referenciapontot is képes rögzíteni. A biometrikus megoldásokat fejlesztő cégek saját szakmai „know-how"-ja, hogy mennyi felvett adatból mennyi egyezőséget fogad el sikeres azonosítás során, és mennyinél van a határ, ahol visszautasítja a folyamatot a rendszer. A 2020-as, 2021-es évekre jellemző pandémiás helyzet erre még ráerősíteni látszott, mert számos zavaró körülmény befolyásolhatja a sikeres minta adását. Mielőtt ennek kifejtésére rátérnénk, nézzük meg az azonosítási módszereket, illetve, hogy a kritikus infrastruktúráknál, vagy az objektumbiztonságban, azon belül is a speciális objektumok esetében milyen kapcsolódási pontok lehetnek a biometrikus azonosítással, és ez hogyan változik a pandémiás helyzetben.

Ujjnyomat-, tenyérnyomat-alapú biometrikus azonosítás

Az ujj vagy tenyér felületén lévő bőr barázdáltságát az úgynevezett fodorszálak és fodorvonalak alkotják. Ezek rögzítése gyors és hatásos azonosítási eljárás, amely a bűnüldözés korai szakaszának szinte egyeduralkodó megoldása volt. Bár az egyik legősibb biometrikus technológiaként tartjuk számon, mind a mai napig a leginkább elfogadott és elterjedt módszer. A folyamat során nagyságrendileg 15–50 külső jellemzőt mérünk, de általában nem érintésmentes technológia, ezért a detektort bizonyos helyzetekben fertőtleníteni szükséges. A minta könnyen másolható, mert akár akaratlanul is ott marad az arra alkalmas felületen (például ilyen az üvegpohár). Az emberiség 3–5%-a esetében nem alkalmazható, mert nem rendelkeznek elektronikus mintavételre alkalmas ujjnyomattal. Két tenyér vagy akár tíz ujj mintája áll rendelkezésre, de a vegyszerekkel végzett munka, vagy az építőipar bizonyos területein végzett fizikai tevékenység hatására a tenyerek vagy az ujjak bőrredőzete könnyen roncsolódik, ami az ilyen jellegű azonosítást lehetetlenné teszi. Előfordul, hogy határátlépésnél az ujj(le) nyomatalapú azonosítás sikertelensége „érdekében" erős savakkal roncsolják a felső hámréteket, ezzel elkerülve az egyértelmű azonosíthatóságot. 18 hetes kortól már kialakul a minta és az évek során nem változik. Az egyészségügyi területen történő felhasználás esetén az orvosi gumikesztyű használata kizáró ok lehet.

Kézgeometria-alapú biometrikus azonosítás

Gyakran alkalmazott technológia, amely a kéz formáját és fizikai dimenzióit, arányait veszi figyelembe. Az újabb technológiák már pozicionáló tüskék nélkül is (érintésmentesen) elvégzik az azonosítást. Népesség tekintetében széles körben alkalmazható, nincs jelentős kizáró tényező, és a néhány másodperces azonosítási idő sem jelentős. A felhasználók által elfogadható az azonosítás folyamata, nem vált ki ellenérzést az azonosítás menete és technológiája, és nem túl magas az eszközzel való együttműködési igény. Külső paramétert mér és ezekből megközelítőleg 30 alapján történik az azonosítás (Gulyás & Kovács, 2021). Hízás, ízületi betegség hatására megváltozott kézgeometria okozhat azonosítási problémát, erre érzékeny a technológia. Egészségügyi területen, vagy a pandémiás védekezés miatt sok szakmában és esetben szükséges a gumikesztyű, amely gátolja az azonosítást.

Arcfelismerés-alapú biometrikus azonosítás

Az egyik legismertebb technológia és a mindennapi életünkben a legtöbbet használt megoldás. A telefonok, tabletek, notebookok zárolásának feloldására a legtöbb esetben használt biometrikus azonosítási módszer, amely közkedvelt kényelmi megoldás lett, és közel mindenkihez eljutott már. Ma már szinte a legtöbb kamerás rendszer ajánl valamilyen arc alapján történő azonosítási megoldást. A technológia elfogadottsága tehát magas, külső paraméterek alapján történik a hitelesítés, a mérés során nem igényel fizikai kontaktot, de a kamera és a személy helyzete és még számos külső tényező (például megvilágítás) jelentősen befolyásolja a sikerességet.

Nem kell a személy beleegyezése vagy együttműködése a sikeres azonosításhoz, ami alkalmassá teszi a megoldást többcélú és rejtett felhasználásra. Az azonosítás során a minták összehasonlítása nem feltétlenül az adatkezelés céljához hozzájárult felhasználók regisztrált adatbázisával történhet. Mozgóképből kivett vagy letöltött kép alapján is működhet az azonosítás, és mesterséges intelligenciával támogatott megoldások esetén még a kamerába nézni sem szükséges, meglepően kevés paraméter alapján is lehet sikeres az azonosítás (URL1).

A technológia az arc jellegzetes pontjait, azok távolságát, arányát méri. Anyajegyek és más jellegzetes azonosítók keresése (forradások, tetoválások) segítik a folyamatot, a ráncok és bőrpólus vizsgálat alapján akár az illető korának meghatározása is lehetséges. Ide tartozik a fülforma alapján történő személymeghatározás, illetve az új megoldások között léteznek olyan technológiák, melyek

kiegészítő jelleggel, profilból is képesek fejforma és a fül formája alapján azonosítást végezni.

A technológia pontossága alacsony, sérülékenysége igen magas (URL2; Sharan, Gordon & Florescu 2021), könnyen elérhető, hogy jó minőségű, nagy felbontású képek alapján, maszkok használatával fizetési vagy azonosítási szolgáltatások sérülékenységét kihasználják. A rendszerek általában nem tartalmaznak élőminta felismerést segítő hardver-szoftver megoldásokat.

Íriszalapú biometrikus azonosítás

A szem szivárványhártyájának mintázatát dolgozzuk fel. Az íriszkép a magzati lét nyolcadik hónapjától a halál pillanatáig változatlan, széles körben alkalmazható és két eltérő személy mintája egyezőségének 10^{70} az esélye (Tajti, 2012). Belső biometrikus jellemző, a technológia érintésmentes. Aktív megoldás esetén közelről az érzékelőbe kell nézni, emiatt magas az együttműködési igénye az azonosítási folyamat végrehajtásának, és alacsony az elfogadottsága a nem megalapozott egészségkárosító félelmek miatt. Nagyjából 400 jellemzőt vesz figyelembe az azonosítás során, az egyik legpontosabb technika, de különféle szembetegségekre érzékenyek ezek a megoldások.

Retinaalapú biometrikus azonosítás

A szem hátsó falán futó érhálózat mérésével a retinahártya véredény struktúrája alapján azonosít az eszköz, mely során infrafényalapú megvilágítást használ a technológia. Nagyon nagy pontosságú megoldás és a retina egyedisége biztosítja, hogy széles körben használható legyen. Az eljárás elfogadottsága alacsony, mert a technológiát nem ismerők idegenkednek a szem „megvilágításától". A retinaalapú azonosítás a biometrikus módszerek közül az egyik legjobb teljesítményt nyújtja, alacsony FRR és közel nulla százalékos FAR értékekkel. Az azonosításhoz a fej pozicionálási igénye szintén nem kedvező, tömeges gyors leolvasási igénynél hátrányban van a megoldás, és higiéniai szempontból sem előnyös. A hátrányai miatt ez az eljárás tömeges használatra nem terjedt el.

Érhálózat-alapú biometrikus azonosítás

Ujj- vagy tenyérérhálózat azonosítás során belső adatokat mérünk. A szenzor az infravörös fény által megvilágított, széndioxiddal dúsult vér áramlását

érzékeli a vénás erekben, tehát csak élő minta mérésére alkalmas. A mért referencia pontok milliós nagyságrendűek, nagy pontosságú és gyors megoldás. A legújabb technológiák nem igényelnek különösebb együttműködést, az ujjat vagy a kézfejet elhúzva egy felület felett, pár másodpercen belül, érintésmentesen megtörténik az azonosítás. Nem befolyásolja az azonosítást a szennyezett bőr vagy a felületi sérülések. A népesség legszélesebb körében alkalmazható, kevés a kizáró ok. 12 éves kor alatt a gyermekek növekedésével járó változások miatt évenkénti mintafelvétel javasolt. Pandémiás időszakban, az egyészségügyi területen történő felhasználás esetén az orvosi gumikesztyű használata több területen kizáró ok lehet.

Hangalapú biometrikus azonosítás

Hang azonosítás során először a hang frekvenciáját azonosítják, majd a későbbi fázisban a hang egyéb tulajdonságait: a hangszínt, hanglejtést, ritmust. Jelentős különbség van két módszer között, az úgynevezett „speech recognition" esetén a beszédet ismeri fel a rendszer, míg „speaker recognition" módszer során magát a hangot és a kibocsátójának egyedi jellemzőit. A mért hang nemcsak az átvivő közegtől, távolságtól és a rögzítés módjától függ, hanem az egyén hangképző szerveinek biológiai jellemzőitől is, illetve a személyiségétől, szociokulturális környezetétől, intelligenciájától és még számos tényezőtől. Rendkívül egyedi minden minta (Fejes, 2018). Általában nem szükséges az egyén beleegyezése a mintavételhez vagy az azonosításhoz. Belső azonosítónak számít, elfogadott technológia. Gyenge pontja, hogy betegségekre, de akár érzelmi vagy fizikai megterhelés hatására is változik a hang, ami befolyásolja a mintaadást és az azonosítás sikerességét. Ideális körülmények között nagy pontosságú a technológia, de az általános felhasználási területekben nincs élőminta-azonosítás és az ideális körülmények is ritkák, így inkább másodlagos megoldásként jelent nagy potenciált.

Rendészeti célú személyazonosítás

„Az ellenőrzés alá vont személy és az általa személyazonosításra átadott okmány közötti közvetlen kapcsolat megállapítása az arckép/fénykép, a személyes adatok és a rögzített biometrikus azonosító által az ellenőrzés helyszínén, az ellenőrzés folyamatába építetten és azonnali válaszadással az azonosságra vagy eltérésre. A személyazonosítás célja annak megállapítása, hogy a személyazonosító

okmányt felmutató személy azonos-e azzal, aki részére az okmányt kiállították." (Balla, 2019).

Az Európai Unióban – így Magyarországon is – az egy évnél hosszabb érvényességi idővel kiállított útlevelek kötelező jelleggel elsődleges biometrikus azonosítóként arcképet, másodlagos biometrikus azonosítóként ujjnyomatot tartalmaznak a chipen. Ha a kiállításkor állandó vagy ideiglenes jelleggel nem lehetséges ujjnyomatot rögzíteni/venni, akkor az útlevél érvényességi ideje maximum egy év lehet. A jelenlegi szabályozás szerint a 12 év alattiaktól sem kell biometrikus ujjnyomat mintát tárolni (URL3). Ez sérülékenységi pontot jelent a jelenlegi rendszerben, mert nincs lehetőség más jellegű biometrikus megoldást alkalmazni, vagy egyértelmű azonosítással meggyőződni a személy kilétéről, vagyis megállapítani az okmány és az azt ellenőrzésre átadó személy közötti közvetlen kapcsolatot. Gondoljunk csak bele, hogy milyen biztonsági kockázatot rejt magában, ha például egy tíz hónapos csecsemőt ötnapos korában kiállított úti okmánya alapján kell azonosítani, ráadásul a szülőkkel való kapcsolatának megállapítása is kétséges, mert az úti okmány nem támogatja azt.

Az ujjnyomat az útlevélben már egy bővített védelemmel ellátott személyes adat, amelyet a jogszabályi környezet – személyes adatok kezelése – miatt nem lehet nem célhoz kötötten tárolni, illetve ellenőrizni, vagyis kiolvasni az elektronikus adattárolóról. Ez azt jelenti, hogy az ellenőrzésnél a hatóság is szigorú szabályokhoz van kötve, mert az útlevélből a biometrikus adat lekérdezéséhez tanúsítvány szükséges. A magyar rendőr a magyar okmányból le tudja kérdezni az adatot és el tudja végezni a biometrikus azonosítást, mert rendelkezik a szükséges tanúsítvánnyal, de – a példa kedvéért – az osztrák útlevélből már csak akkor, ha rendelkezik az adott okmányhoz szükséges tanúsítvánnyal. A határon túl, például az osztrák rendőrnek is hasonló háttéradattal, tanúsítvánnyal kell rendelkeznie ahhoz, hogy a magyar okmányból elektronikusan tárolt biometrikus adatot tudjon a személyazonosítás biztonságos végrehajtásához felhasználni.

A EU-s állampolgárok, pontosabban a szabad mozgás uniós jogával rendelkező személyek esetében az okmány kötelező eleme a biometria, de miután zöldhatárok vannak, így a tagállamok belső határain határátlépésről csak elvi értelemben beszélhetünk. A schengeni külső határon ebben az utaskategóriában is biztosítani kell a biometrikus adatok alapján történő személyazonosítás lehetőségét, amihez az említett tanúsítványok szükségesek. A vízumkötelezett harmadik ország állampolgárai esetében nincs kötelezően biometrikus adat az útlevélben (bár lehet benne) (Balla, 2017), de a Vízuminformációs Rendszerben (VIS) – az Európai Parlament és a Tanács 767/2008/EK számú, a vízuminformációs rendszerről és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről rendelete alapján – rögzítésre

kerül az ujjnyomatadatunk, amit minden egyes schengeni térségbe történő belépésnél alkalmazni kell a személyazonosításhoz. Ez az 1. számú táblázatban látható. A vízummentes harmadik országok állampolgárai jelenleg még „kiesnek" a biometrikus adataik alapján történő személyazonosítás lehetőségéből.

1. számú táblázat
Az okmányok biometrikus adattartalma

Kategória	Az okmánynak kell-e kötelezően tartalmaznia biometriát	Magyarországra belépéskor kell-e biometrikusan azonosítani a személyt	Az EU tagállamaiban közúti igazoltatáskor lehet-e, illetve tudja-e a hatóság biometrikus azonosítással igazoltatni az állampolgárt
Európai Unió tagállamai	Igen	Nem	Saját országának állampolgárát igen, a többi tagállamét hozzáférés biztosításnak függvényében
Vízummentes harmadik országbeli	Nem (de az úti okmányok elfogadásának szempontja lehet)	Nem	Hozzáférés biztosításnak függvényében
Vízumkötelezett harmadik országbeli	Vízumhoz igen (az úti okmányok elfogadásának szempontja lehet)	Igen	Igen

Forrás: A táblázat a szerző saját szerkesztése.

Az ujjnyomatalapú azonosítás a rendészeti célú berögződések és megszokások miatt a legelterjedtebb azonosítási megoldás, de egyben ezáltal a módszerek fejlődésének egyik gátja is. Az eszköz- és módszerspecifikus követelmények szempontjából vizsgálva lehetne újabb megoldásokat bevonni, de mivel 27 tagállam használja kötelező jelleggel, így nehéz lenne kiváltani más biometrikus adattal. *„A biometrikus adatok alapján történő személyazonosításnak legalább 10–15 lehetséges változata van, amelyek a kétséget kizáró azonosság megállapítására alkalmazhatók. Ezek eltérő azonosítási eljárásokat, technikai infrastruktúrát és szakértelmet feltételeznek, továbbá igényelnek. Ebből adódóan a rendészeti célú személyazonosításban jelenleg három olyan alkalmazott eljárás van, amelyek alapvetően megfelelnek a biometrikus személyazonosítással szemben támasztott szakmai követelményeknek is. Ezen eljárásokat az ICAO és az Európai Határ- és Partvédelmi Ügynökség (Frontex) is preferálja és támogatja [az Európai Parlament és a Tanács (EU) 2019/1896 rendelete (2019. november 13.) az Európai Határ- és Parti Őrségről, valamint az 1052/2013/EU és az (EU) 2016/1624 rendelet hatályon kívül helyezéséről], illetve a személyazonosítás során már az EU-ban alkalmazandó vagy jogi norma alapján alkalmazni kell a jövőben. Az ICAO számos biometrikus azonosítási technológiát is vizsgált, amelyek közül már a 2001-es értékelése során az arcfelismerésen, az*

íriszen, az ujjnyomaton, a kézgeometrián, a hangon, illetve az aláíráson alapuló azonosítási eljárásokat tartotta az okmányvizsgálatok során alkalmazhatónak, és ezek közül az arcfelismerésen, az íriszen, továbbá az ujjnyomaton alapuló személyazonosítást támogatja (ICAO 2007). A Frontex a biometrikus azonosítókkal összefüggésben szintén ezen három azonosítási eljárást támogatja, viszont az Automatizált Határellenőrző Rendszer (ABC-rendszer) és a Regisztráltutas-program (RTP-rendszer) esetében azt mondja, hogy amennyiben a rendszer nem támaszkodik a biometrikus elemeket tartalmazó úti okmány alkalmazására, akkor külön mintavételezés alapján más biometrikus azonosító is szolgálhat személyazonosításként" (Balla, 2019).

Az EU-ban létezik több, biometrikus adatokat tartalmazó központi adatbázis is, ezekből az egyik az EURODAC, amely ujjlenyomatokat tartalmazó rendszer és a menedékkérelmek elbírálását segíti elő. Ennek a rendszernek a jogi alapját a dublini egyezmény, vagy más néven dublini rendelet adja, amelyet 2003-ban fogadott el 12 aláíró állam (Belgium, Dánia, Franciaország, Németország, Görögország, Írország, Olaszország, Luxemburg, Hollandia, Portugália, Spanyolország és az Egyesült Királyság). A jelenlegi határvédelmi szabályok alapján két biometrikus adat kerül letárolásra az útlevélben, amelyek a fénykép és az ujjlenyomat, ezek kerülnek rögzítésre az európai uniós útlevélben annak érdekében, hogy az okmány és annak birtokosa között a kapcsolat egyértelműen megállapítható legyen, és ez vonatkozik az illegális határátlépőkre is. A bűnügyi azonosításban is több mint százéves hagyománya van az ujjnyomatalapú azonosításnak.

A jelenlegi EURODAC-rendelet kizárólag ujjnyomatadatok összehasonlítását teszi lehetővé. 2015-ben az európai migrációs stratégia javasolta, hogy az EURODAC-ot egészítsék ki más biometrikus azonosítókkal, ezáltal valamelyest csökkentve azokat a nehézségeket, amelyekkel a tagállamok gyakran szembesülnek a sérült ujjbegyek vagy az ujjnyomatvételi eljárás megtagadása miatt. Ez a javaslat előírja a tagállamok számára, hogy készítsenek arcképmást az érintettről a központi rendszerbe való továbbítás céljára, valamint rendelkezéseket tartalmaz az ujjnyomatok és az arcképmások együttes összehasonlítására, illetve az arcképmások külön, bizonyos meghatározott feltételek mellett történő összehasonlítására. Az arcképmások központi rendszerbe való integrálásának köszönhetően a jövőben arcfelismerő szoftverrel végzett lekérdezésekre is mód nyílik [Regulation Of The European Parliament And Of The Council, Brussel, 2016.5.4, Com(2016) 272].

2020-ig az eu-LISA tanulmányt végez a központi rendszer további olyan arcképfelismerő szoftverrel való kiegészítésének technikai megvalósíthatóságáról, amely megbízható és pontos eredményeket biztosít az arcképmásadatok

összehasonlítását követően [Regulation Of The European Parliament And Of The Council, Brussel, 2016.5.4, Com(2016) 272].

Az Egyesült Államokban ennél lazább a szabályozás, nincs két biometrikus adat felvétele előírva. Felmerülhet persze a kérdés, hogy a szükségesség-arányosság elve alapján ez sérti-e a közösségi jogot és a közösségi jog által deklarált magánszférához való jogot? Mindig el kell kerülni a biometrikus adatbázisok kombinálást, a profilozást, a totális ellenőrzést, az automatizálást a megfigyelések terén. Az alkotmányos jogokat legkevésbé korlátozó megoldások jöhetnek számításba.

Ujjnyomat helyett érhálózat-alapú megoldás

A jelenleg két használatban lévő azonosítási megoldás a fénykép és az ujjnyomat. Mindkettő külső ismérvet vesz alapul az azonosítási eljárás során.

Az ujjnyomatnak a bűnüldözési gyakorlatban bizonyított több évtizedes sikere miatt nagy az előnye, elterjedt megoldás, az ujjlenyomat ott marad minden felületen, tíz ujjról levehető, egyedisége magas, az ujjvégen lévő bőrredők roncsolása viszont nagyon könnyű, a minta hamisíthatósága magas. Ezt ki is használják a menekültek, mert ha az egyik tagállamban történt regisztráció és azonosítás során nem kapnak menedékjogot, és kiutasításra kerülnek, akkor az ujjnyomatuk roncsolásával megakadályozzák, hogy egy másik tagállam egyértelműen azonosítsa őket. Több olyan terrortámadás történt, amit olyan személyek követtek el, akiket korábban kiutasítottak más államokból, de az azonosítási rendszereket kijátszva bejutottak más európai országokba, és ott minimális „befektetéssel" és eszközökkel terrortámadást hajtottak végre (Besenyő, 2017).

Egy rendészeti szakember fénykép, digitális arckép alapján egy igazolvány ellenőrzése során is azonosítást végezhet, az arcfelismerési technológia nagyot fejlődött. Elemző és képanalizáló szoftverek tudják segíteni az azonosítást, akár fénykép alapján, vagy akár egy korábbi képből egy idősebb kori állapotot is könnyen meg lehet alkotni. Az alany tudta nélkül távolról is elvégezhető az azonosítás. Az azonosítás sikeressége könnyen befolyásolható vagy akadályozható smink, sapka, paróka, napszemüveg, arcplasztika megoldásokkal.

Az érhálózat-alapú azonosítás minimális együttműködést igényel az alanytól, elég elhúzni a kézfejet vagy az ujjat a szenzor felülete felett. Az azonosítás sikeressége nem vagy csak nehezen befolyásolható, nincs hatással a mintára a bőrfelület roncsolódása, szennyeződése, nem alkalmazható hamisított kéz- vagy érstruktúra, a mérés csak élő szöveten végezhető el, a szenzor a véráramlásból eredő változások alapján képezi le az érstruktúra mintázatát. Belső

ismérvet mér. Nem érzékeny a bőrszínre, minden embernek van legalább egy keze, kevés a kizáró tényező. Az azonosítás során felhasznált adat 12 éves kor felett állandó, halálunkig nem változik az érhálózat struktúrája. 12 éves kor alatt 1-2 évente, vagy az okmányok megújítási periódusával egyszerre új mintavétel javasolt. A megoldás nem érzékeny a betegségekre, de kettő kéz (tenyér) mintájának használatával minimalizálható ez a kizáró faktor. Lehet tenyér-, lehet ujjalapú, de akár alkaron is lehet érhálózatmintát venni. Lehet érintésmentes a technológia, nem kell a higiéniai problémákkal foglalkozni, viszont a mintavételnél a pozicionálás gyakorlatot igényel. A megoldás elutasítottsága kicsi, mert a mindennapi életben is számtalan dolgot a kezünkkel végzünk, így nem okoz kényelmetlenséget az azonosítási folyamathoz is igénybe venni, még fizikai kontaktus árán sem. Az azonosítási megoldásnak kicsi a kitettsége a fényviszonyokkal szemben, sötétben, terepen is elvégezhető, nem extrém hőmérsékleti időjárási viszonyok esetén kiválóan alkalmazható. Az azonosítási pontosság a többi biometrikus megoldáshoz képest nagy, a sebesség is megfelelő, de ezen paraméterek nyilván a háttérrendszerekkel is függőségben állnak. Talán az egyetlen negatív tényező, hogy a megoldás ára a biometrikus megoldások között közepesen magasnak mondható. Ez a probléma viszont nem áll fenn sokáig, ha sok gyártó jelenik meg a piacon és a tömeges felhasználás beindul.

Az érhálózat-alapú azonosítás nem használható távoli azonosítási megoldásként, szemben egy arcfelismerési megoldással, de így rejtett azonosítást sem tesz lehetővé, az alany hozzájárulása nélkül nem alkalmazható. Az érhálózat lenyomata nem marad ott egy üvegfelületen, mint az ujjlenyomat, vagy egy DNS-minta, így a bűnüldözésben használt ujjlenyomatot nem fogja kiváltani, cserébe a felhasználóknak megadja a védelmet, hogy a tudtuk nélkül nem történik azonosítás vagy rejtett célú felhasználása a személyes adatuknak.

A korábbi kutatások áttekintése

A biometrikus azonosítások elterjedése számos tényezőtől függ, a technológia újszerűségétől és egyszerűségétől, a felhasználási területtől és a biztonsági kihívásoktól, a nemzetközi és hazai jogi szabályozástól, az adatkezelések, személyes adatok védelmének megoldásaitól. De szintén fontos tényezők a felhasználók attitűdbeli változásai és a társadalmi és kognitív folyamatok, mert ezek elsődleges hatással vannak az innovatív technológiák gyakorlatban történő alkalmazására (URL4).

A biometria elterjedésének vizsgálata nem tekint vissza több tízéves múltra, de abban a szerencsés helyzetben vagyunk, hogy a területen már számos

kutatási eredmény látott napvilágot, és ezeknek az összehasonlítása az új kutatással megvalósítható. A korábbi kutatások az Óbudai Egyetem keretein belül kerültek lebonyolításra. A 2002-es vizsgálat még a jogelőd Budapesti Műszaki Főiskola Bánki Donát Gépészmérnöki Kar Gépszerkezettani és Biztonságtechnikai Intézetének Biztonságtechnikai Laboratóriumában, a 2014-es vizsgálat a Biztonságtudományi Doktori Iskola keretein belül került megvalósításra.

A jelenlegi kutatás elemzése/tanulságai

A 2022-es kutatás kérdőíve a korábbi kutatások kérdéseit felhasználva, illetve azokat kiegészítve a biometria elterjedését, az elterjedést gátló tényezőket és a felhasználók érzelmi és gondolati attitűdjét vizsgálja. A kérdőív anonim és önkéntes alapon került kitöltésre általános és véletlenszerű válaszadók által, amelyekben szerepeltek egyetemi hallgatók, illetve munkahely, lakóhely, érdeklődési kör, hobbival kapcsolatos szociál média csoportok válaszadói.

A teljes mintát – 500 fő – 139 nő és 361 férfi alkotta. Korcsoportok szerint viszonylag széles spektrumot ölel fel a minta, a legfiatalabb a Z generációba tartozik (1995 és 2009 között született), de van három fő, aki 1945 előtt született. A megkérdezettek többsége (42,2%) fővárosi, a második legnagyobb csoportot a városi lakosok alkotják (36,6%), a minta fennmaradó része megyeszékhelyen (7,8%), községben (7,6%) vagy falun (6,8%) lakik. A legtöbb megkérdezett jelenleg is a felsőoktatásban tanul (33%), 41,4% rendelkezik diplomával (BSc 22,0%, MSc 19,4%), érettségivel 17,8% rendelkezik, a maradék 7,8% vagy nagyon magas (PhD 2,4%, posztgraduális képzésben veszek részt 2,6%), vagy pedig alacsony (szakmunkásképző 1,4%, általános iskola 1,4%) iskolai végzettséggel rendelkezik. Lásd 2. számú táblázat.

2. számú táblázat
A minta megoszlása a demográfiai változók mentén

	Gyakoriság	Relatív gyakoriság
Nem		
Nő	139	27,8%
Férfi	361	72,2%
Mely generációba tartozik		
Z generáció (1995-2009)	220	44,0%
Y generáció (1980-1994)	146	29,2%
X generáció (1965-1979)	105	21,0%
Baby-boom (1946-1964)	26	5,2%
Veteránok (1945 előtt)	3	0,6%
Hol lakik		
Falu	34	6,8%
Község	38	7,6%
Város	178	35,6%
Megyeszékhely	39	7,8%
Főváros	211	42,2%
Legmagasabb iskolai végzettség		
Általános iskola	7	1,4%
Szakmunkásképző	7	1,4%
Érettségi	89	17,8%
Jelenleg a felsőoktatásban tanulok	165	33,0%
BSc (régi főiskolai végzettség)	110	22,0%
MSc (régi egyetemi végzettség)	97	19,4%
Posztgraduális képzésben veszek részt	13	2,6%
PhD	12	2,4%
Összesen	**500**	**100,0%**

Forrás: A táblázat a szerző saját készítése.

1. kérdés: Ha hallott már a biometrikus azonosításról, mi a jellemzőbb a megoldások ismerete kapcsán Önre?
Erre a kérdésre a következő arányban válaszoltak:

- 1% Egyáltalán nem ismerem a megoldásokat.
- 46% Felületes ismereteim vannak.
- 41% Követem az eseményeket és általánosan tájékozott vagyok.
- 12% Utánaolvasok, ismereteim naprakészek.

A válaszokból megállapítható, hogy a válaszadók alapvetően tudják, hogy mi az a biometrikus azonosítás. Fele-fele arányban oszlanak meg abból a szempontból, hogy csak felületes ismereteik vannak vagy tájékozottak. Van egy kiemelkedő 12% is, aki utánaolvas a témának, érdeklődik utána vagy ismeretei naprakészek.

A korábbi, az Óbudai Egyetemen végzett kutatásokra alapozva azt feltételeztem, hogy a biometrikus azonosítási módszerek elterjedésének legfőbb gátja a széles körű társadalmi elfogadás hiánya. A kérdőíves kérdések ennek vizsgálatára irányultak, amelyet a kérdőív egyik kérdése és egy általam létrehozott index közötti kapcsolat vizsgálatával végeztem el (Lumley, Thomas, Emerson & Chen, 2002; Norman, 2010).

A kérdőív dedikált kérdése arra vonatkozott, hogy a megkérdezetteknek tetszenek-e a biometrikus rendszerek. A biometrikus azonosítási módszerekkel kapcsolatos elfogadást hat kérdésre adott válasz alapján hoztam létre. A létrehozott index elméleti minimuma 1, elméleti maximuma pedig 5 lett. Az index átlaga 3,31, szórása pedig 0,83; megbízhatóságát teljes mértékben igazolja a Chronbach-alfa mutató magas értéke, amely 0,777 (0,7 alatt gyenge a mutató, felette jó). A biometrikus azonosítási módszerek elfogadását mérő index a következő kérdésekből jött létre átlagszámítás segítségével – lásd 3. számú táblázat. Megjegyzendő, hogy a 3., 4., 10. kérdések lehetséges válaszai az „igen” és a „nem” lehetett, ezért azokat átkódoltam rendre négyre és kettőre.

3. számú táblázat

A biometrikus azonosítási módszerekkel kapcsolatos elfogadást mérő index komponensei

Kérdés	n	Min	Max	Átlag	Szórás
3. Inkább ellenezné, vagy inkább támogatná a biometrikus adatainak rögzítését és szélesebb körű felhasználását a mindennapi élet megkönnyítése érdekében?	500	2	4	3,28	0,962
4. Inkább ellenezné, vagy inkább támogatná a biometrikus adatok rögzítését és szélesebb körű felhasználását mondjuk a gyermekek biztonsága, vagy általánosságban a mindennapok létbiztonságának növelése érdekében?	498	2	4	3,43	0,904
10. Tart-e Ön a biometrikus azonosítást végző rendszerek egészségkárosító hatásától? (Pl: retina, írisz, érhálózat azonosítás során)	497	2	4	3,84	0,545
12. Támogatom, hogy az elektronikusan rögzített ujj(le) nyomat nyilvántartást terjesszék ki minden állampolgárra.	497	1	5	3,22	1,504
12. Egyetértek azzal, hogy születéskor minden gyermek íriszmintáját rögzítsék és tárolja a rendőrség annak 18 éves koráig szülő engedélye alapján. (Gyermekek elrablásának megelőzése érdekében)	493	1	5	3,10	1,461
12. Támogatom, hogy születéskor minden ember DNS mintáját rögzítsék (a bűncselekmények pontosabb felderíthetősége érdekében).	494	1	5	3,00	1,493

Forrás: A táblázat a szerző saját készítése a kérdőív kérdései és azok alpontjai alapján.

Az óvatosság jegyében a hetes kérdésre adható válaszok viszonylag kis variációja miatt (egytől négyig lehetett választani) a kapcsolat mérésére a Kendall-féle tau-b mutatót használtam, mely közepes, szignifikáns kapcsolatot mért a két

változó között (tau-b = 0,395; p<0,001). Ez a pozitív kapcsolat megjelenik abban is, hogy a hetes kérdésre („Tetszenek a biometrikus rendszerek, szívesen használom őket") adott válaszok egyes lehetőségeihez kapcsolódó átlagok pozitív tendenciát mutatnak – lásd 1. számú ábra.

1. számú ábra

A biometrikus azonosítási módszerekkel kapcsolatos elfogadást mérő index átlagos értékei a „Tetszenek a biometrikus rendszerek, szívesen használom őket" kérdésre adott válasz függvényében

Forrás: Az ábra a szerző saját készítése.

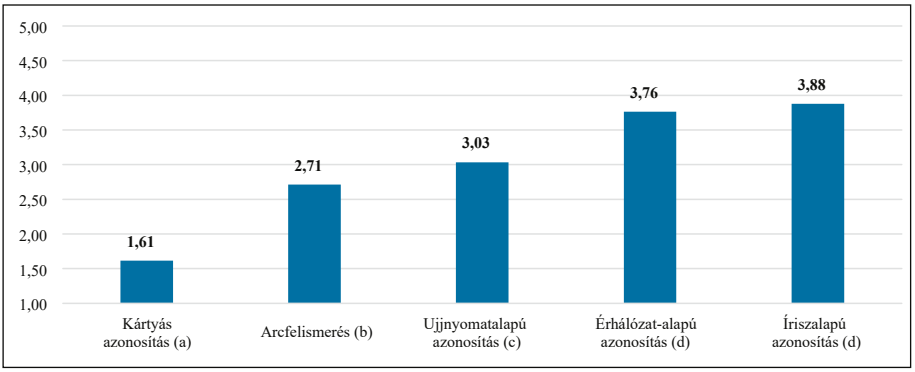
Az index és a 7. kérdésre adott válasz közötti bizonyított pozitív kapcsolat megerősíti feltételezésemet, azaz kijelenthető, hogy a biometrikus azonosítási módszerek elterjedésének legfőbb gátja a széles körű társadalmi elfogadás hiánya. Ennek okai átfogóbb vizsgálatot igényelnek, viszont elkezdtem azt vizsgálni, hogy vajon vannak-e olyan területek, ahol a biometrikus azonosítási megoldások alkalmazása a lakosság széles körű támogatottságát élvezi?

A kérdőív 11. kérdésblokkjában arra kértem a válaszolókat, hogy a felsorolt azonosítási megoldásokat biztonság szempontjából rangsorolják egytől ötig. A legkevésbé biztonságosat jelentette az egyes, míg a legbiztonságosabbat az ötös érték. Öt azonosítási rendszerre kérdeztem rá, melyek a következők voltak: kártyás azonosítás, ujjnyomatalapú azonosítás, arcfelismerés, íriszalapú azonosítás és érhálózat-alapú azonosítás. A rangsorszámok átalakulását összehasonlítottam ismételt méréses varianciaanalízis segítségével, melynek eredménye szignifikáns lett [Greenhouse-Geisser F (3,046; 1389,122) = 230,355; p<0,001], a hatás nagyságát mérő parciális éta-négyzet mutató pedig igen

magasnak mondható (h2 = 0,336). Az öt kategória átlagos rangszámai között a posthoc tesztek (Bonferroni-korrekció) egyetlen páros kivételével szignifikáns eltérést mutattak ki. Ezek alapján felállítható sorrend: a megkérdezettek legkevésbé biztonságosnak a kártyás azonosítást találták (1,61), ezt követte az arcfelismerés (2,71), majd az ujjlenyomat-alapú azonosítás (3,03) következett, végül holtversenyben legbiztonságosabbnak az érhálózat- (3,76) és az íriszalapú azonosítást (3,88) ítélték, lásd 2. számú ábra.

2. számú ábra

Az azonosítási megoldások átlagos rangszámai a biztonság szempontjából. [Zárójelben a posthoc tesztek eredményei alapján keletkezett szignifikáns eltéréseket jelölő kódok, ahol az eltérőek szignifikáns eltérést (például a ≠ b), a megegyezők (d = d) annak hiányát jelentik.]

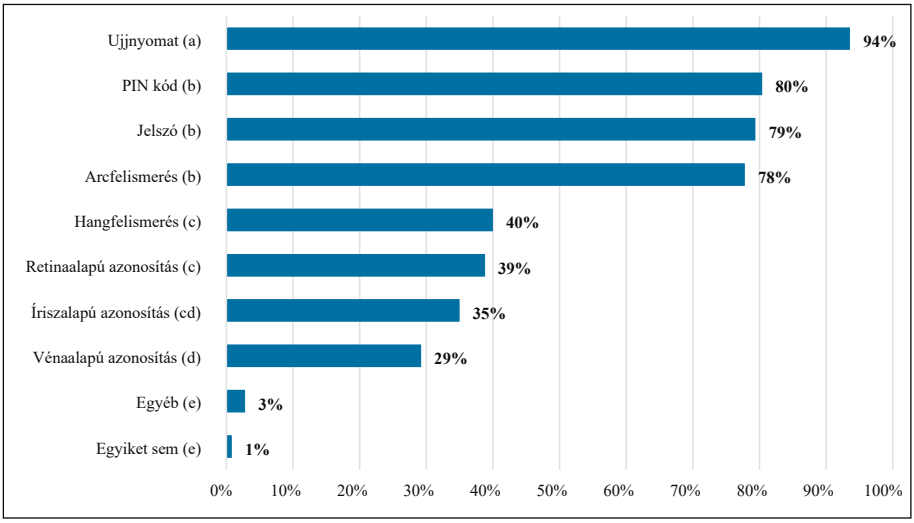


Forrás: Az ábra a szerző saját készítése.

A kérdőívem második kérdése pedig arra vonatkozott, hogy az általam felsorolt azonosítás és biometrikus azonosítási megoldásokról hallott már a megkérdezett, illetve melyiküket ismeri/használta már. Összesen nyolcat soroltam föl (PIN kód, jelszó, ujjnyomat, íriszalapú azonosítás, retinaalapú azonosítás, hangfelismerés, arcfelismerés, vénaalapú azonosítás), valamint az egyéb kategória létezett még mint választási lehetőség. A válaszadók szignifikánsan eltérő arányban ismerték a felsorolt lehetőségeket [Cochran's Q(9) = 2073,903; p<0,001], azok között pedig szignifikáns eltérés mutatható ki a Bonferroni korrekcióval elvégzett posthoc tesztek alapján. A legismertebb az ujjnyomat (94%), ezt követi a PIN kód (80%), jelszó (79%) és arcfelismerés (78%). Harmadik helyen szignifikáns eltérés nélkül következik a hangfelismerés (40%), a retinaalapú azonosítás (39%) és az íriszalapú azonosítás (35%). A legkevésbé ismert pedig a vénaalapú azonosítás (29%), lásd 3. számú ábra.

3. számú ábra

A „Ha hallott már biometrikus megoldásokról, melyik személyazonosítási módokat ismeri/használta már?” kérdésre adott válaszok jelölési aránya. [Zárójelben a posthoc tesztek eredményei alapján keletkezett szignifikáns eltéréseket jelölő kódok, ahol az eltérőek szignifikáns eltérést (például a ≠ b), a megegyezők/tartalmazók (c = c, cd = d) annak hiányát jelentik.]



Forrás: Az ábra a szerző saját készítése.

Az eredmények alapján látható, hogy mind a biztonság, mind pedig az ismertség/használat szempontjából léteznek olyan rendszerek, amelyek szignifikánsan a többiek fölé magasodnak, tehát vannak olyan területek, ahol a biometrikus azonosítási megoldások alkalmazása a lakosság széles körű támogatottságát élvezi. Az írisz- és az érhálózat-alapút tartják a legbiztonságosabbnak, ez kimutatható volt az indirekt kapcsolatból, de az, hogy mennyire támogatják a megkérdezettek az egyik vagy a másik azonosítást, azt további kutatásokkal, direkt kapcsolatot kutató kérdésekkel lehetne vizsgálni.

A kérdőívem három olyan területet tartalmazott, mely egyezett a 2014-es kutatás egyes területeivel, és azt vizsgálta, hogy a 2014-es, Földesi Krisztina általi kutatás óta a biometrikus adatok nyilvántartásba vételével kapcsolatos vélemény megváltozott-e. Nem teljesen azonos kérdésekkel, de azokat alapul véve össze tudtam hasonlítani a 2014-es állapotokat a 2022-es állapotokkal.

Elsőként a biometrikus rendszerekkel kapcsolatos pozitív attitűd összehasonlítását végeztem el független mintás T-próbával (7-es kérdés: „Tetszenek a biometrikus rendszerek, szívesen használom őket” alapján). Mivel a 2022-es felmérés erre a területre vonatkozó kérdése egy négyfokozatú, míg a 2014-es

kérdőív kérdése egy ötfokozatú skálán mérte a megkérdezettek válaszait, ezért a 2014-es kérdőív adatait transzformáltam egy 1-től 4-ig tartó ötfokozatú skálára. Ezután már összehasonlíthatók voltak a két felmérés átlagai (2014 Földesi: M = 3,28; SD = 0,750; 2022 Ujhegyi: M = 3,04; SD = 0,893). Szignifikáns különbség mutatható ki közöttük [Levene F (1;556) = 1,522; p = 0,218; t(556) = 1,944; p(1-oldalú) = 0,026], azaz a mintaátlagokból származó eltérés nem mintavételi hibának is betudható. Így kijelenthető, hogy a biometrikus rendszerekkel kapcsolatos vélemény nyolc év alatt szignifikánsan romlott, mert ahogy látható, a biometria tetszésindexe csökkent 3,28-ről, 3,04-re, ami szignifikáns romlás (M = átlag, SD szórás). Ennek okai szintén újabb vizsgálatokat igényelnek, de bizonyára az elmúlt időszak kiemelt történései (Pegazus botrány, kínai megfigyelő rendszerek hírei) az 1984-es orwelli vizionálás érzetét keltik, melyek nem segítik elő a technika terjedését.

A 2022-es felmérés tartalmazott egy kérdést arra vonatkozólag, hogy a megkérdezett tart-e a biometrikus azonosítást végző rendszerek egészségkárosító hatásától. Viszont a 2014-es megkérdezéssel ellentétben nem egy ötfokozatú skálán, hanem egy igen/nem állítással mértem.

Az első gondolatom az volt, hogy amennyiben a 2014-es felmérés csak az „egyáltalán nem jellemző (1)" kategóriájával (67,80%) azonosítjuk a 2022-es felmérés „nem" válaszát (91,95%), akkor megfelelő választ kapok, és ekkor szignifikáns növekedés mutatható ki ($z = 5,696$; $p<0,001$) az elfogadottság tekintetében. Ebben az esetben kevesebben tartanak a biometrikus azonosítási rendszerek egészségkárosító hatásától, mint 2014-ben. Aztán belegondolva a válaszokba, logikusabbnak gondolom a „nagyon félek az egészségkárosító hatásól" és a „kicsit félek az egészségkárosító hatástól" típusú válaszokat egy oldalra sorolni, és így egyesítve az „egyáltalán nem jellemző (1)" és a „kis mértékben jellemző (2)" kategóriákat (89,83%), akkor már nem szignifikáns a csökkenés ($z = 0,559$; $p = 0,072$), tehát az egészségkárosító hatást hasonló mértékben veszélyesnek értékelték, mint 2014-ben.

A 2022-es kérdőív hatodik kérdéscsoportja azt vizsgálta, hogy milyen érzelmi és gondolati attitűdök fűződnek a beléptető rendszerekhez. Itt összesen kilenc tényező volt felsorolva, melyek közül akár többet is megjelölhetett a megkérdezett. Ugyanezeket a kategóriákat tartalmazta a 2014-es felmérés is, kettő kivételével. Összehasonlítva a két kérdőívre adott válaszok esetében az igenek arányát, szignifikáns eltérés mutatható ki mind a hét tényező esetében.

A jelölések a következő érzelmi és gondolati attitűdök esetén növekedtek 2014-ről 2022-re:

- Nem zavar, hozzászoktam.
- Tetszik, érdekel a működésük.

- Biztonságos.
- Modern, gyors, egyszerű.
- Fontos a kényelem és a mögöttes szolgáltatás.

A következő tényezők pedig kisebb arányban kaptak jelölést 2022-ben 2014-hez viszonyítva:
- Furcsa, érdekes érzés a használatuk.
- Zavaró és kellemetlen.

Mindkét felsorolásban ugyanolyan jellegű állítások szerepelnek, azaz a pozitív állítások esetében szignifikáns növekedés, a negatív állítások esetében pedig szignifikáns csökkenés mutatható ki, tehát megállapítható, hogy a beléptetőrendszerekhez kapcsolódó érzelmi és gondolati attitűdök pozitív irányba változtak az elmúlt nyolc év alatt, lásd 4. számú táblázat és 4. számú ábra.

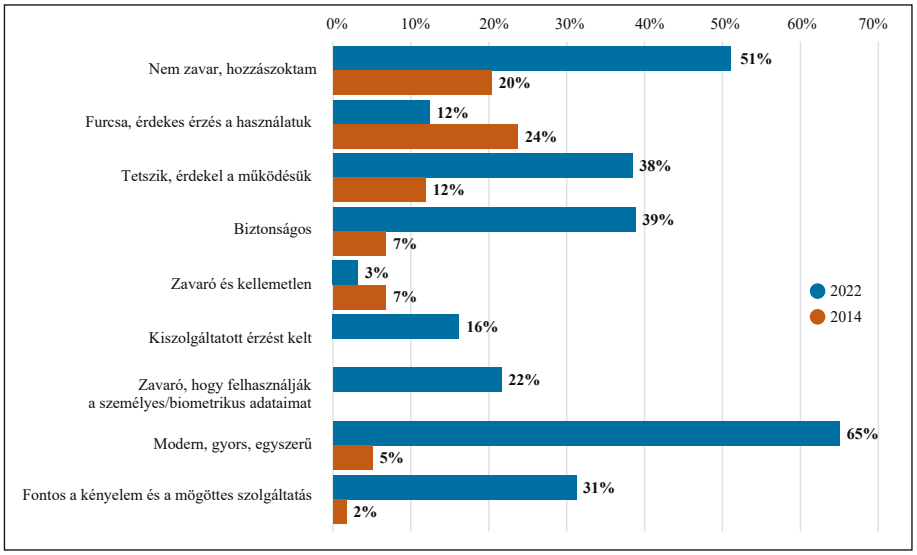
4. számú táblázat
A beléptetőrendszerekhez kapcsolódó érzelmi és gondolati attitűdök alakulása 2014-ről 2022-re, valamint az összehasonlító tesztstatisztikák

	2022			2014			Teszt	
	n	Igen (fő)	Igen (%)	n	Igen (fő)	Igen (%)	z	szig
Furcsa, érdekes érzés a használatuk	500	62	12,4%	59	14	23,7%	-2,401	0,004
Nem zavar, hozzászoktam	500	255	51,0%	59	12	20,3%	4,459	<0,001
Tetszik, érdekel a működésük	500	192	38,4%	59	7	11,9%	4,026	<0,001
Biztonságos	500	194	38,8%	59	4	6,8%	4,864	<0,001
Zavaró és kellemetlen	500	16	3,2%	59	4	6,8%	-1,400	0,040
Kiszolgáltatott érzést kelt	500	81	16,2%				NA	NA
Zavaró, hogy felhasználják a személyes/biometrikus adataimat	500	108	21,6%				NA	NA
Modern, gyors, egyszerű	500	325	65,0%	59	3	5,1%	8,839	<0,001
Fontos a kényelem és a mögöttes szolgáltatás	500	156	31,2%	59	1	1,7%	4,769	<0,001

Forrás: A táblázat a szerző saját készítése.

4. számú ábra

A beléptetőrendszerekhez kapcsolódó érzelmi és gondolati attitűdök alakulása 2014-ről 2022-re



Forrás: Az ábra a szerző saját készítése.

A négy demográfiai változó (nem, korcsoport, lakhely jellege, legmagasabb iskolai végzettség) viszonylatában megvizsgáltam azt, hogy az egyes biometrikus azonosítási megoldásokat a megkérdezettek hogyan rangsorolták a biztonság szempontjából. A nők és a férfiak egyetlen azonosítási megoldást sem értékelték eltérő módon, azaz szignifikáns különbség nem mutatható ki a négy azonosítási megoldás nemek szerinti megítélése esetén, lásd 5. számú táblázat.

5. számú táblázat

A biometrikus azonosítási megoldások megítélése a nők és a férfiak szerint, továbbá az összehasonlító statisztikáik

	Nem	n	Átlag	Szórás	Levene (F/Szig)	T-próba* (t/szig)
Ujjnyomatalapú azonosítás	Nő	129	3,06	1,123	0,838	0,006
	Férfi	351	3,06	1,096	0,361	0,995
Arcfelismerés	Nő	121	2,80	0,928	5,262	-1,113
	Férfi	348	2,69	1,025	0,022	0,267
Íriszalapú azonosítás	Nő	126	3,79	1,040	0,278	0,899
	Férfi	347	3,88	1,066	0,598	0,369
Érhálózat-alapú azonosítás	Nő	123	3,67	1,441	4,209	0,981
	Férfi	345	3,81	1,308	0,041	0,328

Forrás: A táblázat a szerző saját készítése.

Biometrikus azonosítási megoldások megítélését kutató kérdések, valamint a korcsoport, a lakhely és legmagasabb iskolai végzettség ordinális skálákon kerültek mérésre, ezért a közöttük levő kapcsolat erősséget a Kendall-féle tau-b mutatóval mértem. Szignifikáns összefüggést három esetben lehetett kimutatni. Valaki minél idősebb generációhoz tartozik, annál kevésbé érzi biztonságosnak az érhálózat-alapú azonosítást (Kendall's tau-b = -0,097; p = 0,015). Amennyiben a megkérdezett minél magasabb rangú településen lakik, annál kevésbé találta biztonságosnak az arcfelismerés rendszerét (Kendall's tau-b = -0,099; p = 0,012).

Végül az alacsonyabb iskolai végzettséggel rendelkezők azok, akik inkább biztonságosnak ítélték az érhálózat-alapú azonosítást a magasabb végzettségűekhez képest (Kendall's tau-b = -0,081; p = 0,034). Bár három esetben sikerült szignifikáns összefüggést találni a demográfiai változók és a biometrikus azonosítási megoldások megítélése között, azonban ezek mind gyenge kapcsolatok, és többségében nem mutatható ki szignifikáns összefüggés a vizsgált változók között, lásd 6. számú táblázat.

6. számú táblázat

A biometrikus azonosítási megoldások megítélésének, továbbá a megkérdezett korcsoportjának, lakhelyének és legmagasabb iskolai végzettségének összefüggése. (Zárójelben a szignifikancia értékek szerepelnek, ha az érték kisebb mint 5%, akkor szignifikáns, ezeket szürkével jelöltem.)

	Ujjnyomatalapú azonosítás	Arcfelismerés	Íriszalapú azonosítás	Érhálózat-alapú azonosítás
Mely generációba tartozik?	0,012	0,029	0,031	-0,097
	(0,768)	(0,461)	(0,443)	(0,015)
Hol lakik?	-0,016	-0,099	0,057	0,023
	(0,689)	(0,012)	(0,146)	(0,557)
Legmagasabb iskolai végzettség	-0,006	0,035	0,027	**-0,081**
	(0,87)	(0,360)	(0,486)	(0,034)

Forrás: A táblázat a szerző saját készítése.

Jól látható, hogy ha növekszik az iskolai végzettség, akkor csökken az érhálózat-alapú azonosítás elfogadottsága (sötétszürkével és félkövér betűtípussal kiemelve a jobb áttekinthetőség kedvéért).

5. kérdés: Adatvédelmi, személyes adatainak adatkezelési szempontjából aggályosnak tartja-e a biometrikus azonosítási rendszereket, tart-e attól, hogy a biometrikus adatai illetéktelen kezekbe kerülnek?

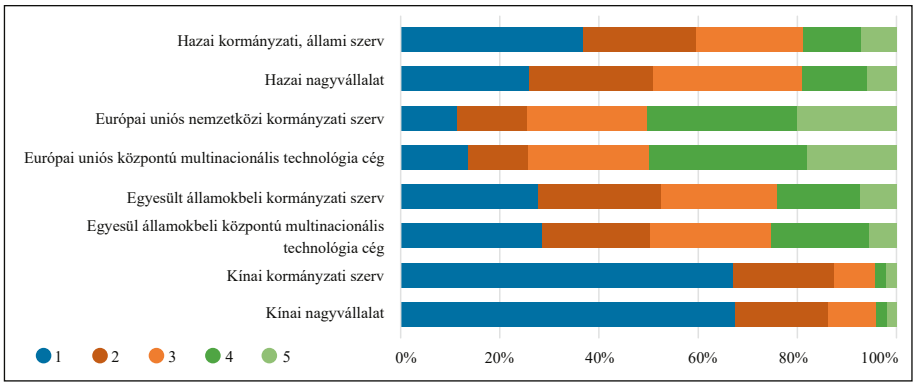
A válaszadók 71%-a tart attól, hogy a biometrikus adatai illetéktelen kezekbe kerül. Aki a 4-es kérdésnél azt válaszolta, hogy támogatja a biometrikus adatok rögzítését, közülük 38% bízik abban, hogy biometrikus adatuk nem kerül illetéktelen kezekbe, még a többieknél ez az arány mindössze 8%.

9. kérdés: Egy széles körben használt biometrikus azonosítási megoldás esetén hol érzi adatait a leginkább biztonságban?

A kérdésre adott válaszokból megállapítható, hogy a válaszadók legjobban az Európai uniós központi adatkezelőkben bíznak, legkevésbé pedig a kínai adatkezelőkben. A kérdőív külön kezelte a nagyvállalatokat és a kormányzati szerveket, de ezek között releváns különbség nem mutatkozott.

5. számú ábra

Hol érezzük az adatainkat leginkább biztonságban

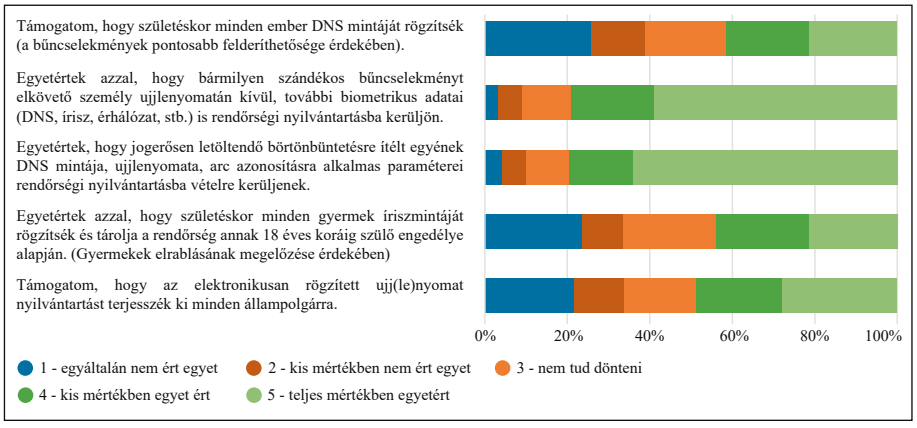


Forrás: Az ábra a szerző saját készítése.

12. kérdés: Milyen mértékben ért egyet a következő állításokkal?

6. számú ábra

Biometrikus adatok rögzítésével kapcsolatos válaszok



Forrás: Az ábra a szerző saját készítése.

A feltett kérdéseket kiértékelve megállapítható, hogy a válaszadók egy része támogatja a DNS-minták születéskori rögzítését és ugyanennyien ellenzik.

A következő kérdések arra vonatkoztak, hogy kiterjesszék-e minden állampolgárra a biometrikus adat rögzítését. Itt a mérleg abba az irányba mutatott, hogy inkább igen.

Sokkal határozottabb a helyzet azonban, amikor egy bűncselekmény elkövetőjéről van szó. Ebben az esetben ugyanis jól láthatóan a válaszadók egyetértenek azzal, hogy a személyről több biometrikus adat is tárolásra kerüljön.

14. kérdés: Az Ön megítélése szerint a biometrikus azonosítási megoldások vissza fognak szorulni?

A válaszolók 98%-a azt mondta, hogy a biometrikus azonosítási megoldások nem fognak visszaszorulni.

15. kérdés: Ön az elmúlt 10 évben kapott-e tájékoztatás, oktatást a biometrikus azonosításokról, azok előnyéről és veszélyeiről, illetve a témához szorosan kapcsolódó adatkezelési szabályozásokról? (Kérem az egyéb mezőben itt jelölje, ha tanulmányai összefüggésben állnak a biometriával, biztonságtechnikával.)

A válaszadók 67%-a – a válaszok szerint – nem kapott tájékoztatást, oktatást a biometrikus azonosításokról, azok előnyéről és veszélyeiről, illetve a témához szorosan kapcsolódó adatkezelési szabályozásokról az elmúlt tíz évben.

Összefoglalás, konklúzió

Az összeállított kérdőívet 500-an töltötték ki, a korábbi kutatásoknál nagyobb létszámmal és szélesebb körben történt a felmérés (nem csak egyetemi és rendőri állomány között). A biometrikus megoldások ismertsége nőtt az elmúlt időkben, ami nem meglepő az okos eszközök és a kényelmi megoldások terjedése mellett. A biometrikus rendszerek elfogadottsága az elmúlt nyolc évben szignifikánsan romlott. Kijelenthető, hogy a biometrikus azonosítási módszerek elterjedésének legfőbb gátja a széles körű társadalmi elfogadás hiánya, viszont emellett vannak olyan területek, ahol a biometrikus azonosítási megoldások alkalmazása a lakosság támogatottságát élvezi. Az írisz- és az érhálózat-alapú megoldást tartják a legbiztonságosabbnak, de például minél idősebb generációhoz tartozik a válaszoló, annál kevésbé érzi biztonságosnak az érhálózat alapú azonosítást. Emellett, ahogy növekszik az iskolai végzettség, úgy csökken az érhálózat-alapú azonosítás elfogadottsága. A megkérdezettek az egészségkárosító hatást hasonló mértékben veszélyesnek értékelték, mint 2014-ben, ami meglepő, mert az egészségügyi kockázatot alátámasztó hírek, kutatások nem jelentek meg.

A korábbi és a friss kutatás alapján megállapítható, hogy a biometrikus azonosítás egyik specifikus területén, a beléptetőrendszerekhez kapcsolódó érzelmi és gondolati attitűdök pozitív irányba változtak az elmúlt nyolc év alatt. Az elmúlt évek alatt a felhasználók jobban hozzászoktak ezekhez a rendszerekhez, kevésbé érzik furcsának ezeket, többen ítélik biztonságosnak a megoldásokat, mint korábban, és többen érdeklődnek a működés iránt. Fontos lett a kényelem és a modern, gyors megoldások használata. Az attitűdök vizsgálati kérdései közé 2022-ben bekerült egy új kérdés a későbbi kutatási célok érdekében, hogy vajon mennyire változik a jövőben a biometrikus adatok illetéktelen felhasználásának félelme a felhasználóknál?

Szintén ezzel a kérdéskörrel függ össze, hogy a válaszadók 71%-a tart attól, hogy a biometrikus adatai illetéktelen kezekbe kerülnek. Ez egy nagyon magas érték, és azt gondolom a megoldások elterjedésének és támogatásának legfőbb gátja jelenleg. A bizalmatlanság megjelenhet mind az adatkezelőkkel kapcsolatban, azaz, hogy a technológiát használó kormányzati szervek vajon mikor és mire használják fel a személyes adatainkat, mind pedig az adatkezelés technikai módszereivel kapcsolatban, azaz elég biztonságos-e az adatkezelés a különféle rossz szándékú támadásokkal szemben. A kérdésre adott válaszokból megállapítható, hogy a válaszadók legjobban az európai uniós központi adatkezelőkben bíznak, legkevésbé pedig a kínai adatkezelőkben. A válaszok – véleményem szerint – jól mutatják, hogy ahol törekednek arra, hogy a törvényi keretek megfelelőek legyenek és támogatják a személyes adatok védelmét, ott a felhasználók is jobban bizalmat szavaznak a megoldásoknak. Ezt indirekt módon támasztja alá (de további kutatásokat igényel), hogy az iskolai végzettség növekedésével csökken a biometrikus megoldások támogatottsága, hiszen a képzett felhasználó jobban tisztában van a kockázatokkal. Ezeket a kockázatokat a biometrikus megoldások felhasználásának erősebb szabályozásával és az adatkezelési, adatvédelmi megoldások biometriára kialakított szabványosításával lehetne csökkenteni.

Melléklet – A 2022-es kutatási kérdőív

Neme:

férfi / nő

Kor alapján mely generációba tartozik:

Z generáció (1995-2009) / Y generáció (1980-1994) / X generáció (1965-1979) / Baby-boom (1946-1964) / Veteránok (1945 előtt)

Hol lakik:

Főváros / Megyeszékhely / Város / Község / Falu

Legmagasabb iskolai végzettség:
Általános iskola / Érettségi / Szakmunkásképző / BSc (régi főiskolai végzettség) / MSc (régi egyetemi végzettség) / PhD / Jelenleg a felsőoktatásban tanulok / Posztgraduális képzésben veszek részt / Egyéb: ……

1. Ha hallott már biometrikus azonosításról, mi a jellemzőbb a megoldások ismerete kapcsán Önre?
   Egyáltalán nem ismerem a megoldásokat / Felületes ismereteim vannak / Követem az eseményeket és általánosan tájékozott vagyok / Utána olvasok, ismereteim naprakészek
2. Ha hallott már biometrikus megoldásokról, melyik személyazonosítási módokat ismeri / használta már?
   PIN kód / Jelszó / Ujjnyomat / Retina alapú azonosítás / Írisz alapú azonosítás / Hangfelismerés / Arcfelismerés / Érhálózat (véna) alapú azonosítás / Egyiket sem / Egyéb, éspedig: ...……
3. Inkább ellenezné vagy inkább támogatná a biometrikus adatainak rögzítését és szélesebb körű felhasználását a mindennapi élet megkönnyítése érdekében?
   Inkább ellenzem / Inkább támogatom
4. Inkább ellenezné, vagy inkább támogatná a biometrikus adatok rögzítését és szélesebb körű felhasználását mondjuk a gyermekek biztonsága, vagy általánosságban a mindennapok létbiztonságának növelése érdekében?
   Inkább ellenzem / Inkább támogatom
5. Adatvédelmi, személyes adatainak adatkezelési szempontjából aggályosnak tartja-e a biometrikus azonosítási rendszereket, tart-e attól, hogy a biometrikus adatai illetéktelen kezekbe kerülnek?
   Igen / Nem
6. Érzelmi és gondolati attitűdök a beléptető rendszerekkel kapcsolatban. Kérem jelölje meg azokat, amelyeket Önmagára igaznak érez. (Több mezőt is megjelölhet)
   Furcsa, érdekes érzés a használatuk / Nem zavar, hozzászoktam / Tetszik, érdekel a működésük / Biztonságos / Zavaró és kellemetlen / Kiszolgáltatott érzést kelt / Zavaró, hogy felhasználják a személyes, biometrikus adataimat / Modern, gyors, egyszerű / Fontos a kényelem és a mögöttes szolgáltatás
7. Tetszenek a biometrikus rendszerek, szívesen használom.
   Egyáltalán nem jellemző / Kis mértékben jellemző / Többnyire jellemző / Teljes mértékben jellemző
8. Tart-e attól általánosságban, hogy a biometrikus azonosítást végző rendszerekben használt biometrikus mintáját ellopják vagy a kezelő cég nem kezeli megfelelő gondossággal, a jogszabályoknak megfelelően?
   Egyáltalán nem jellemző / Kis mértékben jellemző / Többnyire jellemző / Teljes mértékben jellemző

9. Egy széles körben használt biometrikus alapú azonosítási megoldás esetén hol érzi az adatait a leginkább biztonságban? Jelölje 1-es értékkel a legkevésbé biztonságos, 5-ös értékkel az Ön szerint legbiztonságosabb helyet.
   Európai Uniós központú multinacionális technológia cég / Egyesül Államokbeli központú multinacionális technológia cég / Hazai nagyvállalat / Európai Uniós nemzetközi kormányzati szerv / Egyesült Államokbeli kormányzati szerv / Hazai kormányzati, állami szerv / Kínai kormányzati szerv / Kínai nagyvállalat
10. Tart-e Ön a biometrikus azonosítást végző rendszerek egészségkárosító hatásától? (pl. retina, írisz, érhálózat azonosítás)
    Igen / Nem
11. Rangsorolja 1-től 5-ig az alábbi azonosítási megoldásokat a biztonság szempontjából. Jelölje 1-es értékkel a legkevésbé biztonságos, 5-ös értékkel az Ön szerint legbiztonságosabb megoldást.
    Kártyás azonosítás / Ujjnyomatalapú azonosítás/ Arcfelismerés / Íriszalapú azonosítás / Érhálózat-alapú azonosítás
12. Milyen mértékben ért egyet a következő állításokkal? 1 = egyáltalán nem ért egyet, 2 = kis mértékben nem ért egyet, 3 = nem tud dönteni, 4 = kis mértékben egyet ért, 5 = teljes mértékben egyet ért.

	1	2	3	4	5
Támogatom, hogy az elektronikusan rögzített ujj(le)nyomat nyilvántartást terjesszék ki minden állampolgárra.					
Egyetértek azzal, hogy születéskor minden gyermek íriszmintáját rögzítsék és tárolja a rendőrség annak 18 éves koráig szülő engedélye alapján (gyermekek elrablásának megelőzése érdekében).					
Egyetértek, hogy jogerősen letöltendő börtönbüntetésre ítélt egyének DNS mintája. ujjlenyomata, arc azonosítására alkalmas paraméterei rendőrségi níilvántartásba vételre kerüljenek.					
Egyetértek azzal, hogy bármilyen szándékos bűncselekményt elkövető személy ujjlenyomatán kívül további biometrikus adatai (DNS, írisz, érhálózat, stb.) is rendőrségi nyilvántartásba kerüljön.					
Támogatom, hogy születéskor minden ember DNS mintáját rögzítsék (a bűncselekmények pontosabb felderíthetősége érdekében).					

13. Kérem tegye sorrendbe, hogy az Ön megítélése szerint a biometrikus azonosítási megoldás térhódítása milyen sorrendet fog követni? 1 - leghamarabb, 5 - legkésőbb
    Bankszektor, pénzügyi tranzakciók: .....
    Népszavazási és választási rendszerek: .....
    Szolgáltató szektorok (pl. utazás): .....
    Kényelmi szolgáltatások (pl. beléptetés): .....
    Országok közötti megállapodások alapján személyazonosítás (pl. igazoltatás, határátlépés ellenőrzés szigorítása): .....

14. Az Ön megítélése szerint a biometrikus azonosítási megoldások vissza fognak szorulni?
    Igen / Nem
    Miért (opcionális)?: ……
15. Ön az elmúlt 10 évben kapott e tájékoztatás, oktatást a biometrikus azonosításokról, azok előnyéről és veszélyeiről, illetve a témához szorosan kapcsolódó adatkezelési szabályozásokról?
    Nem / Igen, éspedig: ……
    (kérem itt jelölje, ha tanulmányai összefüggésben állnak a biometriával, biztonságtechnikával)

Felhasznált irodalom

Balla J. (2017). A schengeni elvek szerinti határforgalom-ellenőrzés tartalmi elemei Magyarországon 2016-ban. *Magyar Rendészet*, *17*(3), 13–30.

Balla J. (2019). *A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ-, illetve közbiztonság alakulására*. Dialóg Campus Kiadó.

Besenyő, J. (2017). Low-cost attacks, unnoticeable plots? Overview on the economical character of current terrorism. *Strategic Impact, 62*(1), 83–100.

Fejes A. (2018). Beszéd alapján történő személyazonosítás új kihívásai a kriminalisztikában. *Magyar Rendészet*, *18*(2), 117–126.

Gulyás, L. & Kovács, A. (2021). Biometric Authentication System based on Hand Geometry and Palmprint Features. In Imai, F., Distante, C. & Battiato, B. (Eds.), *Proceedings of the International Conference on Image Processing and Vision Engineering* (pp. 58–65). https://doi.org/10.5220/0010408900580065

Kovács T. & Ujhegyi P. (2021). Csökkentett paraméterű biometrikus azonosítási lehetőségek a kritikus infrastruktúrák és a speciális objektumok védelménél. *Biztonságtudományi Szemle, 3*(1), 137–146.

Lumley, T., Diehr, P., Emerson, S. & Chen, L. (2002). The Importance of the Normality Assumption in Large Public Health Data Sets. *Annual review of public health, 23*(1), 151–169. https://doi.org/10.1146/annurev.publhealth.23.100901.140546

Norman, G. (2010). Likert scales, levels of measurement and the “laws” of statistics. *Advances in Health Sciences Education, 15*(5), 625–632. https://doi.org/10.1007/s10459-010-9222-y

Sharan, J., Gordon, T. J. & Florescu, E. (2021). *Tripping Points on the Roads to Outwit Terror.* Springer. https://doi.org/10.1007/978-3-030-72571-6_12

Tajti B. (2012). A biometrikus ujjnyomat azonosításának új lehetőségei. *Hadmérnök, 7*(1), 48–58.

A cikkben található online hivatkozások

URL1: *The world's scariest facial recognition company, explained*. https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement?fbclid=IwAR0c4rkztQXDWxguNFeCa-iGHMhPKC2VVPBEiWqVA_Sey78rcA5ZJLfM7LY

URL2: *Ongoing Face Recognition Vendor Test. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8331.pdf*

URL3: *Biometric data in documents. https://www.academia.edu/33526570/Biometric_data_in_documents_Biztonsagpolitika_2013*

URL4: *Összehasonlító kutatáselemzés a biometrikus személyazonosító-beléptető rendszerek, eljárások 2006. és 2014. évi társadalmi averzív reakcióinak vizsgálatára.* http://www.securinfo.hu/wp-content/uploads/2015/06/20150602_osszehasonlito_elemzes_a_biometrikus_szemely-azonosito_rendszerek.pdf

Alkalmazott jogszabályok

Európai Parlament és a Tanács (EU) 2017/2226 rendelete (2017. november 30.) a tagállamok külső határait átlépő harmadik országbeli állampolgárok belépésére és kilépésére, valamint beléptetésének megtagadására vonatkozó adatok rögzítésére szolgáló határregisztrációs rendszer (EES) létrehozásáról és az EES-hez való bűnüldözési célú hozzáférés feltételeinek meghatározásáról, valamint a Schengeni Megállapodás végrehajtásáról szóló egyezmény, a 767/2008/EK rendelet és az 1077/2011/EU rendelet módosításáról HL L 327, 2017.12.9.

Európai Parlament és a Tanács (EU) 2019/1896 rendelete (2019. november 13.) az Európai Határ- és Parti Őrségről, valamint az 1052/2013/EU és az (EU) 2016/1624 rendelet hatályon kívül helyezéséről.

Regulation Of the European Parliament And Of The Council, Brussel, 2016.5.4, Com (2016) 272

Regulation Of the European Parliament And Of The Council, Brussel, 2016.5.4, Com (2016) 272

A cikk APA szabály szerinti hivatkozása

Ujhegyi P. (2023). A biometria elterjedésének elemzése. *Belügyi Szemle*, *71*(8), 1463–1491. https://doi.org/10.38146/BSZ.2023.8.7