ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉSTERVEZET

UJHEGYI PÉTER

A biometrikus azonosítás elterjedésének elemző vizsgálata

Témavezetők: Dr. Szűcs Endre

Prof. Dr. Kovács Tibor (†)

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024.03.07.

TARTALOMJEGYZÉK

Bevezetés

Az informatikában dolgozom 1997 óta. Több mint 20 éve, még pályám kezdetén szervizvezetőként, később üzemeltetési, majd műszaki vezetőként dolgoztam. Nagyon sok informatikához kapcsolódó területen szereztem tapasztalatot, de ezek közül mindig is a biztonságtechnika foglalkoztatott a leginkább. Amikor 2013-ban kapcsolatba kerültem egy tenyérérhálózat alapú biometrikus azonosítási megoldással foglakozó kutató-fejlesztő céggel, azonnal éreztem, hogy megtaláltam azt, ami engem igazán érdekel. Azonosítási és beléptető megoldásokat terveztünk és telepítettünk itthon, majd később a környező országokban, illetve ennek kiszolgálására partnerhálózatot építettünk. Így kerültem kapcsolatba az Óbudai Egyetemmel és Kovács Tibor professzorral is, aki a Biztonságtechnikai Intézeti Tanszék vezetője és a biometria szakértője volt. Ő indította el korábban a biometria elterjedésnek vizsgálatát a tanszéken, engem is az Ő lelkesedése és motiválása hajtott ezen az úton, amit azóta is járok. A hazai kutatások áttekintését is az Ő munkáival kezd(t)em.

Értekezésemben a biometrikus alapú azonosítási rendszerek elterjedésével foglalkozom. A terjedelmi korlátok miatt leginkább a hazai vonatkozásaiban folytatom a kutatást, de több esetben kitekintek nemzetközi területre (pl. jogi részeknél), ahol a megértéshez, vagy a téma jobb alátámasztásához ez szükséges. Az elterjedés vizsgálata azért fontos, mert az azonosítást végző eszközök használata egyre természetesebbé válik (kamera rendszerek, fizetési megoldások, mobiltelefonok), a technológia fejlődésével egyre több rejtett azonosítási megoldásra van lehetőség, ami önmagában hatalmas kockázat, de a mai digitalizációs világunkban a kibertámadások száma is egyre növekszik, ami szintén magas kockázatot jelent a személyes adataink tekintetében. Kutatásom során megvizsgálom a biometrikus azonosítás definíciójának fejlődését és annak aktualitását, részletesen vizsgálom a biometrikus azonosítás jogi szabályozási fejlődését és összefüggéseit és különösen a mesterséges intelligenciával összefüggő szabályozásokat. Vizsgálatom során kitérek arra, hogy a biometrikus azonosítási megoldások elterjedése milyen akadályokba, problémákba ütközik, illetve, hogy az azonosítási megoldások a felhasználási területet szempontjának kivételével, milyen kockázatokat jelentenek. A témával összefüggő, néhány éven belüli kutatások, szakkönyvek és doktori értekezések a releváns fogalmakat definiálták, illetve a szakirodalom (Kovács jegyzet) világosan megfogalmazta ezeket, ezért a témámhoz szorosan nem kapcsolódó fogalommeghatározásoktól értekezésemben eltekintek.

Tudományos probléma megfogalmazása

A biometrikus azonosítás technikai megoldásaival szemben számtalan elvárás, ellenérzés és félelem alakult ki, melyek hatással vannak a megítélésére és a megoldások elterjedésére. Ezeknek a biztonság területét érintő innovatív megoldásoknak a problémaköreinek a feltárása és összefoglaló, elemző kutatása még kezdeti stádiumban van a tudományterületen. Ahhoz, hogy egy jó és hasznos technikai megoldást széles körben és biztonságosan, jogszerűen és célhoz kötöttség szempontból megfelelően tudjunk használni, szükséges vizsgálni a problémákat és tényezőket, annak érdekében, hogy ezekre megfelelő megoldásokat találjunk.

A biometrikus adatokon alapuló azonosító megoldásokkal szemben kialakult általános ellenérzések közé tartozik egyes megoldások egészségkárosító hatásától való félelem, a távoli és rejtett megfigyelésre, adatgyűjtésre, elemzésre alkalmas eszközök felhasználása és az ezekkel való visszaélés lehetősége, az új azonosítási technológiákból származó elemzett, következtetett adatokra épülő azonosítási lehetőségek és az adatokat gyűjtő és tároló szervezetek és a személyes adatok nem megfelelő kezelésének veszélyei. Hatással van a biometria elfogadására és alkalmazására az oktatás (kifejezetten a biztonságtechnikai oktatás), az aktuális élethelyzetünkre vonatkozó személyes jólétünk és biztonságunk helyzete, az egészségi helyzetünk, a rendvédelemmel és határvédelemmel foglalkozó szervezetek felhasználási területei hazai és nemzetközi szinten, a migrációs helyzet alakulása és hatásai, valamint a jogi és adatkezelésre, adatvédelemre vonatkozó szabályozás hazai és nemzetközi állapota.

Célkitűzések

Az értekezés elkészítésekor a következő célokat tűztem ki:

1. Feltárni a biometrikus azonosítási megoldások és a jogi szabályzás legfontosabb összefüggéseit hazai, európai, illetve az Egyesül Államok vonatkozásában. Elősegíteni és megkönnyíteni a nemzetközi szabályozások megértését, átvételét, bevezetését.
2. Folytatni az elmúlt 15 évben az Óbudai Egyetem Biztonságtudományi Doktori Iskolában végzett, a biometria elterjedésével összefüggő kutatásokat. Azonosítani új kutatási lehetőségeket és irányokat.

3. Összegezni a kutatás során az elterjedéssel kapcsolatosan azonosított problémákat és azok lehetséges megoldásait.
4. Feltárni a biometrikus azonosítási eljárások, a jogi szabályozás, az adatkezelés és adatvédelem információi közötti legújabb összefüggéseket.
5. Elemezni a biometrikus azonosítási megoldások kockázatait és ezzel elősegíteni a veszélyeinek a köztudatba építését és a tudatosabb felhasználást.

A téma kutatásának hipotézisei

Az alábbi hipotéziseket fogalmaztam meg:

Hipotézis 1 (H1): Feltételezem, hogy a biometrikus azonosítási módszerek széleskörű elterjedésének legfőbb gátja a társadalmi elfogadás hiánya.

Hipotézis 2 (H2): Feltételezem, hogy a biometrikus azonosítás jogszabályi környezete összefüggést mutat a mesterséges intelligencia fejlődésével és szabályozásával.

Hipotézis 3 (H3): Feltételezem, hogy vannak olyan biometrikus azonosítási megoldást használó területek, ahol a biometrikus azonosítási megoldások alkalmazását a lakosság széles körűen támogatja.

Hipotézis 4 (H4): Feltételezem, hogy az Óbudai Egyetemen végzett kutatás óta 2014-ről 2022-re a biometrikus adatok nyilvántartásba vételével kapcsolatos vélemény megváltozott és javulást mutat.

Hipotézis 5 (H5): Feltételezem, hogy a biometrikus azonosítás definíciója nem követi a technika fejlődését és ezért pontosítható az, a mai kornak megfelelő újabb azonosítási eljárásokkal.

Kutatási módszerek

A biometria, a biometrikus azonosítás és a megoldások elterjedése témakörök több területet is érintenek, így például jogtudományi, az informatikai biztonság, adatbiztonság, egészségügy és a rendvédelem területét is.

Az értekezés elkészítése során alkalmazott kutatási módszerek megválasztásánál törekedtem arra, hogy azok kielégítsék a holisztikus, teljességre törekvő látásmód követelményeit, de ugyanakkor az értekezés terjedelmi korlátait is figyelembe kellett venni, ami különösen nehéz a kutatott téma tekintetében, annak szerteágazó jellege miatt.

A tudományos kutatásoknál fontos az objektivitás elvének megőrzése és ennek érdekében feltétlen szükséges a tudományos problémák azonosítása, alapos megismerésük és a fejlődési lehetőségeiknek alapos vizsgálata [1].

Kutatómunkám során a témának nem csak az elméleti összefüggéseit dolgoztam fel, hanem annak gyakorlati megvalósításával kapcsolatos tapasztalatokra is építettem, így lehetőségem adódott kiemelten hasznosítani a szakmai pályámon a gyakorlati megvalósítással kapcsolatos munkatapasztalataimat. Így az értekezésben amellett, hogy feltárom és elemzem az elméleti aspektusokat, sok esetben a saját vélemények és értékelések során jelentős mértékben építek a gyakorlati tapasztalatokra. Ezek többek között kiterjednek biometrikus azonosító megoldások kiépítése és üzemeltetése területre, valamint a banki, pénzintézet informatikai rendszerek tervezésére és kiépítésére területre, melyek információs technológiai (Information Technology, továbbiakban: IT) biztonság és adatkezelés szempontból tartoznak a témához.

Az elméleti módszerekről és összefüggésekről többszáz magyar és külföldi szakirodalmat, tudományos művet és jogszabályt dolgoztam fel a munkám során, melyből 129 anyagot fel is használtam az értekezés megírásához. Ennek során alkalmaztam az analízis és szintézis módszereit, a tématerületeket alkotóelemeire bontottam és külön is mélységében tanulmányoztam, így lehetővé vált a részek megismerése. Az elemzések során a különálló részeket és területeket újra rendeztem és a hipotézisek szerinti felépítést figyelembe véve, számomra logikus egységbe foglaltam. Ennek során megvizsgáltam az összefüggéseket és megállapítottam, hogy a biometria elterjedése elsősorban nem azonosítástechnológiai kérdés, hanem a biometrikus adatok feldolgozásának IT módszertani kérdése és az ezekhez kapcsolódó adatkezelési és adatbiztonsági kockázatok függvénye. Kutatómunkámban fontos szerep jut az indukciónak, dedukciónak és az analógiának, ahogy kutatásom során részeire bontottam a problémákat, ezeket elemeztem és következtetéseket vontam le, mind mélyebben, ahogy az ismerttől haladtam az ismeretlen felé. A végrehajtott feladatokhoz kapcsolódó következtetések levonása után javaslatokat fogalmaztam meg [2].

Tanulmányoztam a témával kapcsolatos írott és elektronikus szakirodalmat, szabványokat, esettanulmányokat, jogszabályokat és törvényeket. Ezek feldolgozása, rendszerezése során alapvető módszerként az adaptációt használtam, ahogy az összefüggő információkat kiszűrtem és cél érdekében újra rendezve beépítettem az értekezésbe. A tématerületen rendelkezésre álló, általam fontosnak vélt szabványokra, a magyar és főként a külföldi nyomtatott és elektronikus internetes szakfolyóiratokra, a tervező, gyártó, telepítő, üzemeltető és őrző-védő cégek, valamint az illetékes hatóságok által közzétett esettanulmányokra, felmérésekre és a szakmaitudományos konferenciák anyagaira támaszkodtam. A biometria területén folytatott kutatásaim, a kapcsolódó jogi szabályozással összefüggő vizsgálataim és az adatfeldolgozással kapcsolatos általános biztonságtudományi összefüggések feltárása után elmondható, hogy a hazai kutatások relevánsnak tekinthetők nemzetközi viszonylatban.

Tapasztalati eredményekhez jutottam az ötszázas mintán elvégzett kérdőíves kutatásom során is, mely egy empirikus kvantitatív kutatási módszer.

Az értekezés terjedelmi korlátja és a feldolgozandó téma széles spektruma miatt nem volt célom a biometrikus azonosítási módszerek típusainak a részletes és elemző bemutatása, mert ezt már több tanulmány, kutatás és szakkönyv megtette. A kapcsolódó fejezetnél csak a leginkább a tárgyhoz tartozó és az általam szakmailag jelentősnek vélt, mértékadó hivatkozásokat mutatom be összefoglalóan és inkább az egyes technológiák gyengeségeire és erősségeire koncentráltam, melyek összefüggenek az elterjedéssel és a felhasználási lehetőségekkel.

A kutatásomat 2024. február 28-án zártam.

A doktori értekezés felépítése röviden összefoglalva

Az értekezés a kutatási téma célkitűzései, a hipotézisek és a feldolgozás logikája szerint került kidolgozásra.

Az azonosítás módszerei (1-es) fejezet: ebben a fejezetben bemutatom az egyén és a biztonság kapcsolatát, valamint a biometria tudományterület kapcsolatát a biztonsággal. A fejezetben összegzem – a korábbi mértékadó tankönyvek és kutatások alapján – a biometrikus azonosítás mérőszámait, valamint összegzem és rendszerezem az azonosító eljárásokat. Megvizsgálom a biometria fogalmának fejlődését, a biometrikus azonosítás hivatalos definíciójának fejlődését és az általam feltárt probléma alapján kiegészítve a korábbi általános definíciót, megalkotom a biometrikus azonosítás definíciójára a mai kor

eljárásait is magába foglaló legmegfelelőbb új meghatározást. A jelenlegi szakirodalmi definíció – az elmúlt évtizedre jellemző jogi szabályozottsági lemaradás okán – még nem kezelte a pszichológia és az érzelmi jellegű tulajdonságokat, és azoknak az azonosítási eljárásokban való használatát. Választ adok a H5-ös hipotézisre. Összegzem a biometrikus azonosítási megoldások és a felhasználásuk összefüggéseit az elterjedés szempontjából.

A biometrikus adatok védelmének és a mesterséges intelligencia fejlődésének összefüggései és a jogszabályi háttér (2-as) fejezet: ebben a fejezetben összegzem a személyes adatokkal, az adatbiztonsággal és a biometrikus azonosítási megoldásokkal kapcsolatos hazai és nemzetközi szabályozásokat, valamint elvégzem a biometrikus azonosítási rendszerek kockázatalapú értékelését. Vizsgálom az összefüggéseket a mesterséges intelligencia és a szabályozásának fejlődésével. Javaslatot tesztek a biometria elterjedésének gátló tényezőinek kezelésére. Választ adok a disszertáció H2-es hipotézisére.

Kérdőíves kutatás (3-es) fejezet: ebben a fejezetben bemutatom a kérdőíves kutatásom eredményeit, az összefüggéseit a korábbi kutatásokkal, és elvégzem ezen korábbi és jelenlegi kutatások eredményeinek kiértékelését, melyekből következtetéseket vonok le. Választ adok a H1, H3 és a H4 hipotézisekre. További kutatási lehetőségeket vázolok.

A biometria elterjedésének elemző kutatása több szakterületen erős támpontot adhat az azonosítási megoldások megfelelő kiválasztásához, az alkalmazás feltételeinek megértéséhez és szakmai átlátásához, illetve a bevezetésük kidolgozásához.

1. AZ AZONOSÍTÁS FAJTÁI

Ebben a fejezetben áttekintem az egyén és a biztonság kapcsolatát, valamint a biometria tudományterület kapcsolatát a biztonsággal. Összegzem korábbi mértékadó tankönyvek és kutatások alapján a biometrikus azonosítás mérőszámait, valamint összegzem és rendszerezem az azonosító eljárásokat. Vizsgálom a korábbi definíciók fejlődését, majd kiegészítem a biometrikus azonosítás és hitelesítés definícióját, hogy a modern biometrikus azonosítási technikák legújabb eljárásait is magába foglalja, ezáltal véleményem szerint még pontosabban fejezi ki a fogalmat. A biometriai azonosítás elterjedése témában végzett kutatásaim tapasztalatai alapján a korábbi meghatározás – az elmúlt évtizedre jellemző jogi szabályozottsági lemaradás miatt – még nem kezelte a pszichológia és az érzelmi jellegű tulajdonságokat és azoknak az azonosítási eljárásokban való használatát, ezért indokoltnak érzem a definíció kiegészítését.

1.1. Az egyén és a biztonság kapcsolata

A XXI. században extrém módon felgyorsult életvitelünk mellett valamilyen szinten mindenkiben felmerül a biztonság kérdése, de egyéntől és élethelyzettől függően mindenki mást ért rajta a mindennapi életben. Azonban, ha abból indulunk ki, hogy a döntéseink alapjai többnyire önmagunkkal függenek össze, tehát az egyénnel, akkor a legalapvetőbb szükségletek is közösségi normákon, vagy egyéni, emberi szükségleteken alapulnak. Az egyén döntései a szükségletek kielégítésére irányul, amelyben a biztonság is fontos tényező, tehát a döntéseket a szükségletek, és ebbe beleértve a biztonság iránti vágy befolyásolják. Ez pedig, véleményem szerint a biometria elterjedésével összefüggésben van.

Az emberi szükségletek összefüggéseinek szakértője, és a motivációelmélet kidolgozója, Abraham Maslow [3] amerikai pszichológus szerint az emberi szükségleteket hierarchikusan lehet rangsorolni (1. ábra). Ebben a hierarchiában a biztonság fogalma már nagyon hamar, az alapszinten megjelenik, azaz erre épül fel az összes többi emberi szükségletünk igénye. Amint az alsóbb szinten egy szükséglet teljesül, utána jelenhet meg a felette lévő szinten egy újabb.

1. ábra: Maslow szükséglet piramis[1] [4]

„*A biztonságtudomány célja a rendszerek biztonsági funkció központú elemzése, a rendszerbiztonság tervezése, részletes kidolgozása. Ezekből fakadóan a biztonságtudomány az egészségmegőrzés egyik eszköze és az objektív valóság létező állapotának egyik aspektusa is egyben. A biztonság iránti igény, akár a biztonsággal kapcsolatos problémák az emberi gondolkodással egyidős. A megismerés a kisebbtől a nagyobb felé, vagyis a kevésbé ismerttől a bonyolultabb megismerése felé halad, amelyben több kutató szakaszokat azonosít (ártatlanság, felfedezés, rendszer biztonság, biztonságtudomány).*” [5, p. 32.]

A létbiztonság és a közbiztonság szorosan összefonódik minden ember életében [6, p. 112.]. Ha a hétköznapi életünk mindennapjaiban az alapok rendezettek, megoldott a lakhatás és az élelmezés kérdése és ennek negatív irányú jelentős mérvű változása nem várható, akkor a létbiztonság kérdése rendben van. Ha a környezetünk is stabil, nem történik bűncselekmény vagy a közbiztonságot érintő incidens, akkor annyira és addig érzi magát az ember az idealizált állapot szerint biztonságban, amennyire a körülötte lévő környezet képes megelőzni és felismerni a fenyegetéseket, illetve javítani az esetlegesen bekövetkezett események káros hatásait. „*A biztonság egyrészt a veszély és fenyegetések hiányát, másrészt a veszély és a fenyegetések elhárításának képességét jelenti* [7]. *Ugyanakkor a biztonság nem egy elérhető állapot, mindig relatív, hiszen a fenyegetések*

[1] Az ábrát a szerző készítette.

sosem küszöbölhetők ki teljesen. A biztonság sokkal inkább tekinthető egy döntően percepcionális kérdésnek, vagyis azt, hogy az egyén és közösség mit gondol a biztonságról, az objektív biztonság (biztonsági helyzet) és a szubjektív biztonság (biztonságérzet, percepció) együttesen határozza meg, s korántsem biztos, hogy ez a két megközelítés mindig egybeesik." [8, p. 348.]. A biztonság tehát alapszükséglet, ami a legalapvetőbb motivációkra hat, ezért annak megléte, vagy hiánya jelentős befolyásoló tényező minden egyén számára.

1.2. A biometria és a biztonság kapcsolata

A biometriai elven működő azonosítási megoldások alkalmasak a biztonság növelésére, ezért fontos érteni a biometria és a biztonság kapcsolatát, mert így, az egyén és a biztonság kapcsolatának gondolatát folytatva vizsgálható és alátámasztható a biometria elterjedésével való összefüggésük.

„*A bűnözési statisztikák és társadalmi változások személyes érintettsége egyértelművé tette a társadalom minden rétege számára, hogy a klasszikus bűnüldözési technikák, erők, eszközök már nem elégségesek a kielégítő magán- és közbiztonság megteremtéséhez.* [9]*"* Innovációra tehát mind az állami védelmi szervek, mind a civil társadalom biztonságteremtő tevékenységében szükség van. Ebben az új és modern megoldások, köztük a biometrikus azonosítási eljárások jelenthetik az egyik hatékony megoldást. A biometrikus azonosítási eljárások technikai megfelelőségének felismerése mind a katonai, rendőri szakterületen, mind a civilszférában megtörtént. Jelenleg azonban több jogszabályi, etikai, társadalompolitikai kérdés tekintetében nincs egyetértés az érintett felek között, melyet az értekezés jogi feldolgozásánál részletesen be is mutatok. Legalapvetőbb probléma azonban, hogy a szakterületi kommunikáció hiányos, nem megfelelő, sok esetben hozzá nem értők nyilatkoznak a biometriáról úgy, hogy nem a biometriával és annak elfogadásával ténylegesen összefüggő veszélyekre vagy problémákra összepontosítanak [9].

Az azonosítási folyamat két jól elhatárolható részből áll. Az első rész a regisztráció, amely a rendszer használatára jogosult személy valamilyen jellemzőjének mintavételezéséből (maszk), majd a kiolvasott adathalmaz feldolgozásából, digitalizálásából és az adatok tárolásából áll. A második rész az azonosítás, amely ugyancsak mintavételezésből, majd digitalizálásból, ezután az adatok összehasonlításából áll. Ezt követően, ha a minta megegyezik az adatbázisban tárolt mintával, akkor

jogosultnak, ha nincs egyezés a tárolt és az éppen kiolvasott mintában, akkor jogosulatlannak nyilvánítja a rendszer az adott egyént mondjuk a belépésre, vagy valamilyen cselekvés elkezdésére a védendő létesítményben, hálózatban vagy valamilyen zártkörű rendszerben.

A különféle azonosítási módszerek közül három féle létezik. A tudásalapú, a birtoklásalapú és a biometriai jellemzőkre épülő módszerek. *„Mindegyik módszernek megvan a maga erőssége és gyengesége, ezért a kellő biztonsági szint eléréséhez együttesen, egyidőben és egyszerre javasolt legalább két eltérő elven alapuló módszert egymástól függetlenül ötvözni.”* [10]

1.3. A biometrikus azonosításhoz kapcsolódó fogalmak és mutatók

A biometrikus azonosítás korunk egyik legpontosabb személyazonosítási módszere, a biológiai jellemzők mérésével valósul meg. A felhasználó egy vagy több tulajdonságát, paraméterét veszi alapul. A témához kapcsolódó fogalmak a technika és a jogszabályok változásával folyamatosan fejlődnek.

1.3.1. A biometria fogalma

A kétezres évek elején Varga Domonkos és Oláh András (**2004**) akadémikusok megfogalmazásában: *„A **biometria** az emberek egyedi, változtathatatlan jellemzőinek számszerű leírásának tudománya. Jelen esetben a biometriát úgy lehet meghatározni, mint olyan mérhető testi, vagy viselkedésbeli jellemvonások összességét, amelyek mérése alkalmas arra, hogy egy adott személy azonosságát ellenőrizni lehessen (biometriák: ujjlenyomat, arc, kézgeometria, hang, aláírás, gépelési dinamika, DNS, írisz és retina).* [2, p. 40].”

A **biometria szó hivatalos meghatározása** a Nemzetközi Szabványügyi Szervezet (International Organization for Standardization, továbbiakban: ISO) által van meghatározva **2019**-ben, amely az alábbiak szerint szól: [11, p. 77]

„A biometria azon az elven alapul, hogy az egyének egyedi fiziológiai és / vagy viselkedési jellemzői, amelyeket az automatikus azonosítási rendszerek elemzésre használnak, lehetővé teszik azonosításukat és azonosításuk ellenőrzését.” Az ISO/IEC 19784-1:2019 szabvány meghatározza a biometrikus fogalmakat és a biometrikus információkat tartalmazó adattárolási formátumot.

Az ISO a világ legnagyobb szabványosítási szervezete, és számos szabványt dolgozott ki a biometria területén, amelyeknek a célja az azonosításra és az azonosítás ellenőrzésére szolgáló biometrikus rendszerek hatékonyságának és megbízhatóságának javítása. Ezért az ISO jogosult a biometria fogalmának meghatározására és szabályozására.

A Rendészettudományi Szaklexikon **2019**-ben a biometriát négyféle meghatározással definiálja. Az *„élőlények, azok testrészei, valamint életfolyamataik kvantitatív vizsgálata, illetve statisztikai összehasonlítása, tudományos feldolgozása során keletkező adat, illetve „az ember egy vagy több egyedi fizikai vagy viselkedési jellemzőjének mérésén alapuló azonosítása", valamint „mérhető testi, illetve viselkedésbeli jellemvonások, amelyek mérése alkalmas arra, hogy egy személy azonosságát ellenőrizni lehessen", továbbá „az ember valamely olyan jellemzőjének, adottságának a felhasználása az azonosítás során, amely személyenként egyedi, ugyanakkor elektronikus úton is jól feldolgozható, és a biometrikus azonosítás során ezekkel az emberi jellemzőkkel történik a személy azonosítása"* [12, p. 66.].

Az Országgyűlés Hivatala weboldalán [13] **2020**-ban a Képviselői Információs Szolgálat megfogalmazása szerint *„A **biometria** az emberek egyedi, tudományosan igazolt, fiziológiai, vagy viselkedésalapú jellegzetességeit felhasználó, mérhető, az egyéni azonosítást lehetővé tevő módszer* [14, pp. 118-126.], *ami az emberek egyedi, legnagyobb részben megmásíthatatlan és hamisíthatatlan tulajdonságait vizsgálja."* Jól láthatóan minden megfogalmazás az idő haladásától függetlenül a fizikai és viselkedésbeli jellemzők mérhetőségét és feldolgozását veszi alapul, de egyéb jellemzők feldolgozása még nem jelenik meg a definíciókban, pedig a technika már elérte azt a szintet, hogy más típusú jellemzők mérése is beépül a biometrikus azonosítási módszerekbe.

1.3.2. Biometrikus adat fogalma

Az Európai Adatvédelmi Testület által kiadott 95/46/EK irányelv 29. cikke alapján létrejött adatvédelmi munkacsoport 4/2007. számú személyes adatokról szóló véleményében (WP136) megfogalmazottak szerint **2012**-ben a **biometrikus adat** a következő módon van meghatározva: *„biológiai jellegzetességekként, viselkedési vonatkozásokként, pszichológiai sajátosságokként, életvitelként vagy olyan ismétlődő tevékenységekként, amelyek során e jellegzetességek és/vagy tevékenységek egyaránt egyedülállóak az érintett egyén vonatkozásában, továbbá mérhetőek, még ha a*

gyakorlatban a technikai mérésükhöz alkalmazott mintákat bizonyos fokú valószínűség jellemzi is” [15].

A Rendészettudományi Szaklexikon alapján **2019**-ben a biometrikus adat *„olyan adat, amely az ember mérhető testi adatait képezi le.”* [12].

1.3.3. Biometrikus azonosítás fogalma

A biometrikus azonosítás hivatalos definíciója a Nemzetközi Elektrotechnikai Bizottság (International Electrotechnical Commission, továbbiakban: IEC) által van meghatározva, amely az alábbiak szerint szól:

„Az azonosítás biometrikus módszere az egyén azonosítása olyan egyedi fizikai, biológiai vagy viselkedési jellemzőkön alapuló technológiával, mint például az ujjlenyomat, a tenyérnyomat, az arc, a retina, az írisz vagy az ujjvénás minta.”

Ez a definíció hangsúlyozza, hogy a biometrikus azonosítás olyan egyedi biológiai jellemzőkön alapul, amelyek egyénenként eltérnek. Az ilyen jellemzők digitális rögzítése és elemzése lehetővé teszi az egyének pontos és megbízható azonosítását. A biometrikus azonosítás széles körben használatos a biztonsági, jogi és üzleti alkalmazásokban, ahol a pontos és megbízható azonosítás kulcsfontosságú. Az IEC által kiadott IEC 60050-845 szabvány, amely a „biometria” témakört definiálja, utoljára **2011**-ben lett frissítve.

Rendészettudományi Szaklexikon alapján **2019**-ben a **biometrikus azonosítás** *„az ember valódi, tőle elválaszthatatlan azonosságán alapuló, fizikai és viselkedésbeli karaktervonásait, hitelesítő céllal mérő, elemző és azonosító számítógépes, információtechnológiai eljárás”*, illetve *„a személyazonosítás egyik fajtája, amely során az ember egyénenként eltérő, mérhető biológiai jegyein, élettani vagy viselkedési jellemzőin, a biometrián alapul az azonosítási eljárás”* [12]

Jól látható, hogy nincs egységesen elterjed definíció és a biometrikus azonosítás esetében a meghatározás a fizikai és viselkedési jellemzőkre korlátozódik.

1.3.4. A biometrikus azonosítás jellemzői

A biometrikus jellemzőknek két nagy csoportját különíthetjük el, a biológiai, valamint a viselkedési jellemzőket [16].

Biológiai (fizikai) jellemzők alapú azonosítási módszerek:

- bőrmintázat alapján – ujjnyomat, ujjlenyomat, ujjkép, tenyérnyomat,
- arc – arcfelismerés, termogramm,

- szem – írisz, retina,
- érhálózat – tenyérvéna, ujjvéna,
- illat, testszag, verejtékpórus elemzés,
- DNS,
- geometria – fülforma, kézgeometria, tartás, sziluett,
- szívritmus.

Viselkedési jellemzők alapú azonosítási módszerek:

- beszédhang,
- aláírás, íráskép-dinamika,
- gépelés, íráselemzés,
- mozgás-, járás-, sziluettelemzés,
- pszichológiai alapú elemzés.

„A folyamat egyfajta végeredményének tekinthetjük az eszköz rendeltetés szerinti működését, miszerint az adatbázisban szereplő mintát és az aktuálisan beolvasott mintát egyezőnek, a mintát jelenleg birtokló egyént jogosultnak nyilvánítja a rendszer, vagy pedig az adatbázisban szereplő minták egyikével sem azonos az aktuálisan beolvasott minta, így a minta tulajdonosát jogtalannak ítéli az eszköz. Ezen eredményen belül azt az eshetőséget figyelembe véve, hogy maga az eszköz követ el valamilyen hibát az azonosítás során, két fő mutatót alkalmaznak az eszközök minősítésére. Megkülönböztetünk úgynevezett téves elfogadási arányt (False Acceptance Rate, továbbiakban FAR), valamint téves elutasítási arányt (False Rejection Rate, továbbiakban FRR).” [17, p. 3]

- A FAR aránya: annak a valószínűsége, hogy a biometrikus rendszer tévesen azonosít valakit, vagy nem utasít el egy csalót. A hibásan elfogadott érvénytelen bevitelek százalékos arányát méri. Nevezik hamis pozitív aránynak is.
- Az FRR aránya: annak a valószínűsége, hogy a rendszer hibás elutasítást végez. Hibás elutasítás akkor történik, ha valójában jogosult, de a folyamat hibásan jogosulatlannak nyilvánítja, tehát az egyént a rendszer valamilyen hiba folytán nem rendeli hozzá a saját, meglévő biometrikus sablonjához. Nevezik hamis negatív aránynak is.

„A FAR-t és az FRR együttesen egy diagramon ábrázolva két görbét kapunk, amik egy ponton metszik egymást. Ezt a pontot nevezzük egyenlő hiba aránynak (Equal Error Rate, továbbiakban EER). Ebben a pontban a FAR és FRR ugyan azt az értéket veszi fel, tehát a hiba azonos." [17, p. 3]

Az FAR és FRR értékei együttesen vizsgálva (egymás függvényében) formálják az Olvasó Működési Karakterisztikát – azaz Receiver Operating Characteristics (a továbbiakban ROC) vonalát, amely jól jellemzi egy adott biometrikus eszköz működését a környezeti körülmények tekintetében [18].

A rendszert adatokkal kell feltölteni az adatfelvétel (enrollment) és template előállítás során, az ellenőrzés (veryfication), vagy azonosítás (identification) során az abban a pillanatban mért adatokat kell összehasonlítani az adatfelvétel során rögzített adatokhoz [19]. Jelentős előnye, hogy a különféle módszerek magát a személyt azonosítják és lehetőség van az élő személy, élő minta felismerésére is. Hátránya lehet a módszernek, hogy speciális szakértelmet és technikai eszközöket igényel, bár az utóbbi években a nagyfokú terjedése miatt az eszközök is könnyebben és olcsóbban elérhetők. A fogyatékkal élők esetén egyes módszerek nem, vagy csak megkötésekkel használhatók. Az azonosítás során alapul vett biometrikus jellemzők az idő múlásával változnak, vagy betegség, fizikai sérülések hatására alkalmatlanná válhatnak az azonosítás elvégzésére. Az azonosítás során felmerülhetnek higiéniai szempontok, melyek hátráltathatják a művelet elvégzését. Az adatrögzítéskor ugyanazon személytől felvett minta és az azonosítások során leolvasott minta soha nem tud teljesen megegyezni, így a biometrikus rendszerek egyik sarkalatos pontja a téves elfogadás és téves elutasítás aránya, ami befolyásolja a megbízhatóságot. Ezért minél több referenciapontot tartalmaz egy minta, annál jobban nőhet az ellenőrzési idő, de annál jobban paraméterezhető is, mit fogadjon el egy rendszer sikeres azonosításként ugyanattól a személytől, annak ellenére, hogy a két adott mintája valamilyen mértékben eltér egymástól.

A biometrikus azonosítóeszköz jellemezhető aszerint, hogy mennyire áll ellen az egyes minta-klónozó támadásokkal szemben, ez az Anti-Cloning Operations Methods (továbbiakban: ACOM) szám, és létezik index érték az eszközök célorientáltságának mérésére is, ez a feladatorientált alkalmazás (Mission Oriented Application, továbbiakban: MOA).

A biometrikus azonosítási rendszerek jellemzői:

- Pontosság: biometrikus rendszerek használatakor nehéz 100%-ban hibamentes eredményeket elérni. Ez lehet az adat megszerzésekor (mintavételezés) jellemző környezeti viszonyok eltérései miatt (pl. világítás, hőmérséklet stb.) és a használt berendezések (pl. kamerák, szkennelő eszközök stb.) különbségei miatt is. A leggyakrabban használt, szokásos teljesítményértékelési mérőszámok a hibás elfogadási arány és a hibás elutasítási arány, amelyek paraméterezéssel hozzáigazíthatók a használt rendszerhez.
- Kinyerhetőség: a tényező nagyban függ a felhasználási területtől, a környezettől és úgy általában sok külső és független befolyásolótól (pl. szenzorkoszolódás, időjárási viszonyok, fényhatás, felhasználó stb.) A Sikertelen Rögzítés (Failure to Acquire, továbbiakban: FTA) megmutatja az azonosító minta kinyerésének sikertelenségi arányát.
- Egyetemesség: adott felhasználói csoportra, népességre nézve vizsgáljuk, hogy a használt biometrikus technológiával milyen arányban fordul elő a sikeres vagy sikertelen sablonkinyerés. Ennek mérésére a mérőszám a Sikertelen Regisztráció (Failure to Enroll, továbbiakban: FTE). A felhasználószám függvényében a cél a leginkább optimális egyedi azonosítási megoldás kiválasztása, melynél a legkevesebb a kizáró tényező.

A biometrikus azonosítás összehasonlítási szempontjai [20]:

- Egyediség: minden mintának szükséges, hogy legyen egyedi azonosításra alkalmas mintázata, ami megkülönböztethető más mintákétól.
- Állandóság: a biometrikus minta egy bizonyos időszakon belül kellő mértékben változatlanul legyen kinyerhető.
- Egyetemesség: a vizsgált népességben a biometrikus minta minden alany esetében kinyerhető legyen.
- Mérhetőség: a gyakorlatban alkalmazható technikai módszerekkel jól mérhető az azonításra alkalmas egyedi azonosító jegyek sajátosságait kódoló egyedi jellemző.
- Összehasonlíthatóság: a rendszerben meglévő sablon könnyen összehasonlítható legyen a kinyert mintából származó adatokkal.
- Invazívitás: az emberi test bevonása ne legyen túlzott mértékű az azonosítás folyamatába.

- Teljesítmény: együttes mérőszám a pontosság, a sebesség és a biztonság vonatkozásában.
- Elfogadottság: a társadalom részéről ne legyen elutasított az alkalmazott eljárás.
- Kijátszás: ne legyen lehetőség az adott módszert megkerülni.

1.4. A biometrikus azonosítás és hitelesítés új meghatározása

A mai kor technológiai fejlődése 2023-ban már kikényszeríti, hogy sokkal pontosabban, kifinomultabban, és reagálva az elmúlt időszak biometrikus azonosítási megoldások körében lezajlott fejlődés trendjeire, azokkal kiegészítve, részletesebben határozzuk meg a biometrikus adat fogalmát, és így a biometrikus azonosítás és hitelesítés definícióját is.

A biometrikus kategorizálás, viselkedésdetektálás, érzelemfelismerés, biometrikus adatfeldolgozás és -elemzés, illetve a biometrikus profilalkotás során minden esetben a biometrikus adat tulajdonosára visszautaló adatok gyűjtésére és használatára van szükség. Tehát minden olyan adatgyűjtő technológiát, vagy elemző és értékelő műveletet ide kell értenünk, amely az ember fizikai, fiziológiai vagy viselkedési, érzelmi, vagy ezek elemzett, következtetett vonatkozásaival foglalkozik. A feldolgozás során az adott emberi egyedre jellemző feltételeket mér vagy következtet, beleértve a genetikai, fizikai, fiziológiai, viselkedési, pszichológiai vagy érzelmi jellegű tulajdonságokat és az ezekből kapott elemzett vagy következtetett adatokat is.

1.4.1. A biometrikus azonosítás új meghatározása

Kutatásaim során nem találtam a biometrikus azonosítás meghatározására olyan új megfogalmazást, amely definíciószerűen kezeli az új jellemzőkre épülő megoldásokat. A fentieket figyelembe véve és levonva a következtetéseket, az eredmények alapján szerintem így pontosítható a biometrikus azonosítás modern meghatározása:

A **biometrikus azonosítás** (identifikáció, 1:n) a biológiai adat tulajdonosára visszautaló **fizikai, biológiai, viselkedési, pszichológiai vagy érzelmi állapot elemzett-következtetett jellemzőire épülő valószínűsítő eljáráson alapuló összehasonlító módszer**, **mely során** az egyén, **a** biometrikus **rendszer általi méréskor** (az azonosítási igény pillanatában) **megszerzett biometrikus adatainak** az adatbázisban **korábban**

eltárolt <u>többi</u> más **biometrikus sablonnal való összehasonlítása történik**, annak érdekében, **hogy kikeressük az egyént** (azaz, az egy a többhöz megfeleltetés folyamata).

Az azonosítás tehát egy tágabb módon értelmezhető módszer. Arra a kérdésre keressük a választ, hogy a sokaság közül ki ez az egy adott személy, azaz egyet keresünk ki a sok közül. Ez a folyamat a mai korra érvényes értelmezésem szerint kifejezetten kiterjed viselkedései, pszichológiai, vagy érzelmi állapotot kielemző, vagy kikövetkeztető folyamatokra, és a jelenlegi hivatalos megfogalmazások nem tartalmaznak ilyen széles körű biometriai azonosítási eljárásokat. Feltevésem szerint ezek az új módszerek, az ezekkel kapcsolatos kockázatok, ezeknek a kockázatoknak a kezelési lehetőségei lassan mennek végig azon a folyamaton, hogy egy új megoldás kialakulása után, a tapasztalatok alapján új meghatározások, definíciók és szabályzatok készüljenek. A döntéselőkészítő szakmai szervezetek munkája kiemelt jelentőségű, értekezésem jogi részt feldolgozó területénél ki is fogok térni arra, hogy például az AI kapcsán készülő szabályozások előkészületi anyagaiban (már EU-s szinten) megjelennek a pszichológiai és érzelmi állapotot elemezni képes rendszerek szabályozási javaslatai, mert ezekből az információkból is képesek a rendszerek biometrikus alapú azonosítást végezni. Következtetésem, hogy az értekezésem H5 hipotézise alátámasztható. Megvizsgáltam a biometrikus azonosítás definíciójának jelenlegi tartalmát és az nem kezeli a pszichológia, vagy érzelmi állapotokra épülő elemzett, következtetett adatokon alapuló biometrikus azonosítási módszereket, így azok nem követik a jelenlegi új megoldásokat, tehát ezeknek a beépítése egy új definícióba szakmailag szükséges és elvégezhető.

1.4.2. A biometrikus hitelesítés új meghatározása

A biometrikus hitelesítés definíciója a biztonságtechnikában és azon belül leginkább az informatikában elterjedt fogalom, és nem egy adott szervezet vagy testület határozta meg hivatalosan a fogalmat. Ennek eredményeképpen nincs egyetlen, mindenki által elfogadott hivatalos meghatározása a fogalomnak, sok szakkönyv gyakran használja a biometrikus azonosítás és biometrikus hitelesítés szavakat, de nem tesz lényegi különbséget köztük. A két definíció közötti fő különbség az, hogy az azonosítás során a rendszer csak a személy azonosságát állapítja meg, míg a hitelesítés során a rendszer azt is megerősíti, hogy a személy jogosult-e hozzáférni egy adott rendszerhez vagy szolgáltatáshoz. Azonban az informatikai biztonság területen számos standard és ajánlás létezik. Az ISO 19794-2:2011 szabvány 1.3.2 pontja szerint [21] a biometrikus hitelesítés

egy olyan eljárás, amely egy személy azon egyedi fizikai vagy viselkedési jellemzői alapján azonosítja és hitelesíti, amelyeket az emberi test vagy a személy által végzett tevékenységek generálnak. Az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézetének (NIST) pedig részletesen leírják a hitelesítési folyamatokat és az azokhoz kapcsolódó követelményeket. A fentieket figyelembe véve és levonva a következtetéseket, az eredmények alapján szerintem így pontosítható a biometrikus hitelesítés modern meghatározása, amely jobban hangsúlyozza a különbséget a biometrikus azonosítástól:

A biometrikus hitelesítés (authentikáció, 1:1), az a **valószínűsítő eljáráson alapuló ellenőrző protokoll**, ahol **az egyén biometrikus rendszer általi ellenőrzése** tipikusan az egyén (ellenőrzéskor megszerzett) **biometrikus adatainak az egyénről korábban letárolt biometrikus sablonjával való összehasonlítása történik** (azaz egy az egyhez megfeleltetési folyamat), **az egyén** másról vagy magáról állított **személyazonosságának ellenőrzésére**, **és** annak **megerősítésére**, hogy **a felhasználó jogosult-e hozzáférni** egy adott **rendszerhez** vagy **szolgáltatáshoz**.

A hitelesítés egy „egy az egyhez” összehasonlítás, mely megfelel egy adott, élő személy sablonjának, aki azt állítja, hogy azonossággal rendelkezik egy összekapcsolt sablonadatbázisban tárolt személyi sablonnal, mely azonossággal az is ellenőrizhető, hogy állítása igaz-e. Arra a kérdésre keressük a választ, hogy akit hitelesítünk az tényleg maga a deklarált személy-e.

A valószínűsítő eljárások során *„a szenzoroktól származó információt elő-feldolgozzák, ami azt jelenti, hogy a zavaró, vagy felesleges adatokat eltávolítják. Ez megfelel a lényeg kiemelésének, a kontúrok meghatározásának, majd körbevágásának. Az osztályba sorolás vagy klasszifikáció az adatfeldolgozás egyszerűsítését szolgálja. A kiértékelés és a feldolgozás további gyorsítása érdekében megállapítják az információt tömören, de még helyesen leíró jellemzőket. A jellemzőkből készített adatmaszk felhasználása kettős is lehet: egyrészről az elsőnek tekintett azonosításnál beillesztik a jövőbeli felhasználást biztosító adatbázisba, másrészről pedig (amennyiben rendelkezésre áll) összehasonlítják a meglévő, korábban eltárolt sablonokkal. Az extrahált forma és a tárolt sablonok között mindig van eltérés, ezért valószínűségszámítási módszerekkel – így különösen a Bayes-analízisből származtatott becslésekkel – állapítják meg az egymásra legjobban hasonlító mintapárt. A rendszerek jellemzően az idegműködést utánzó neurális-hálókra, vagy a vélelmeket holisztikusan kezelő, számos tekintetben az emberi döntés logikáját követő Bayes-hálókra visszavezetett*

módszerekre épülnek." [22] Belátható, hogy az 1: n alapú azonosítás során, mikor egy nagy adatbázisból kell kikeresni sok minta közül a megfelelőt, ott nagyon sokat számít a biometrikus azonosítási megoldások központi problematikája, a nagy háttérkapacitás és performancia igény, továbbá, hogy az azonosítási események során ugyanazon személy is mindig változó mintát ad le, hiszen a test változása, a körülmények változása folyamatosan befolyásolja a mintaadást. Éppen ezért az egyéni azonosítójegyeket és ezek adatait rugalmasan, illetve gyorsan kell kezelni. Értelemszerűen az egyéni azonosítójegyek száma és vizsgálatuk módja függ az azonosítási folyamat fajtájától és struktúrájától is. Így amennyiben 1: n azonosítási folyamatot vizsgálunk, akkor több egyéni azonosítójegyet kell megkeresni és összehasonlítani, mint amikor 1:1 hitelesítést hajtunk végre. A multimodális azonosítással elérhető, hogy több mintavételi lépést kelljen elvégezni, így egy lépés által bírt hibaterhelés fajlagos súlya csökkenthető.

1.5. A biometrikus azonosítási megoldások

Ebben a pontban nem célom az azonosítási megoldások részletes, mindenre kiterjedő bemutatása, mert az már meghaladná értekezésem megcélzott terjedelmét és ezek széles körben és gyakran feldolgozott tartalmak. A biometria elterjedésével kapcsolatban számomra a kutatás szempontjából az a leginkább a tárgyhoz kapcsolódó, hogy a megoldásoknak milyen előnyei és hátrányai vannak a felhasználási terület függvényében, és ezeknek mi az összefüggése az elterjedéssel.

Felhasználási jellegét tekintve a biometrikus azonosítását végző megoldások a következő főbb csoportokba sorolhatók [19, pp. 15-16.].

Kereskedelmi szolgáltatások:

- Hozzáférés kezelés számítógépek, eszközök, berendezések eléréséhez
- Hozzáférés kezelés adatok eléréséhez
- Online, vagy offline szolgáltatások elérése
- Beléptetési megoldások, munkaidő nyilvántartás
- Pénzfelvétel automatából, pénzügyi szolgáltatások elérése

Hatósági (állami) alkalmazások:

- Személyazonosság igazolása
- Határátlépés, útlevelek
- Szociális támogatások folyósítása
- Fegyverhasználat

Katonai programok

Társadalmi és egyészségügyi ügyek intézése

Adathozzáférések

Bűnügyi, bírósági felhasználás

Halottak azonosítása

Bűnözők felderítése, azonosítása

Kapcsolatok felderítése

Eltűnt személyek felkutatása

1.5.1. Ujjnyom, ujjnyomat, ujjlenyomat alapú azonosítás

Az ujjnyom az ember által megérintett tárgyakon ottmaradó, általában rossz minőségű lenyomat. Az ujjlenyomat általában a rendőrségi nyilvántartásokban használt, az ujjról készült jó minőségű kép, mely az ujjvégi ujjperc, a köröm egyik szélétől másik széléig tartó lenyomata. Az ujjnyomat a síkfelületre helyezett ujj ott maradó, kétdimenziós, jó minőségű lenyomata [23]. Az ujj vagy akár a tenyér felületén lévő bőr barázdáltságát az úgynevezett fodorszálak és fodorvonalak alkotják. Ezek rögzítése gyors és hatásos azonosítási eljárás, mely a bűnüldözés korai szakaszának szinte egyeduralkodó megoldása volt. Bár az egyik legrégebbi biometrikus azonosítási módszerként tartjuk számon, mind a mai napig a leginkább elfogadott és elterjedt módszer. A folyamat során nagyságrendileg 15-50 külső jellemzőt mérünk, de a legtöbb felhasználási esetben nem érintésmentes technológia, ezért a detektort bizonyos helyzetekben tisztítani szükséges. A minta könnyen másolható, mert akár akaratlanul is ott marad az arra alkalmas felületen (például üvegfelületen), így a minta tulajdonosának tudta és jóváhagyása nélkül is lehetséges a minta begyűjtése. Az emberiség 3-5 százalékának esetében nem alkalmazható, mert nem rendelkeznek elektronikus mintavételre alkalmas ujjnyomattal. Általános esetben 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. Beléptetési megoldásokban széles körben alkalmazzák a kicsi és olcsó szenzorok alkalmazhatósága miatt, ezért költséghatékony megoldás. Az Európai Unió kötelező előírásai alapján 2014. október 11-től a schengeni térség valamennyi külső határán, – így Magyarország esetében az ukrán, román, szerb és horvát határszakaszon, valamint a nemzetközi repülőtereken – a határforgalom-ellenőrzés korábbi gyakorlata a

vízumkötelezett utasok vonatkozásában ujjnyomat alapú személyazonosítással egészült ki [24]. Széles körben elterjed a mobiltelefonok, táblagépek és notebookok esetében, ahol az eszközbe való belépés, vagy a fizetési szolgáltatások igénybevételénél használható. A csecsemő 7 hónapos korától már kialakul a minta, és az évek során nem változik [25]. Az egyészségügyi területen történő felhasználást hátráltathatja az orvosi gumikesztyű használata.

1.5.2. Arc alapú azonosítás

Az egyik legismertebb technológia, és a mindennapi életünkben sokszor előforduló megoldás. Beléptető rendszerek, biztonsági ellenőrzések (pl. repülőtér), határátlépés során használt megoldás. A telefonok, tabletek, notebookok zárolásának feloldására sok esetben használt biometrikus azonosítási módszer, mely közkedvelt megoldás lett, és közel mindenkihez eljutott már. Ma már szinte a legtöbb kamerás rendszer ajánl valamilyen arc alapján történő azonosítási megoldást. A technológia felhasználása gyakori, emiatt elfogadottsága magasnak számít, külső paraméterek alapján történik az azonosítás, a mérés során nem igényel fizikai kapcsolatot, de a kamera és a személy helyzete és még számos külső tényező (pl. megvilágítás) jelentősen befolyásolja a sikerességet. Könnyen használható, közepesen költséghatékony módszer, az eszközök telepítése szakértelmet kíván [26].

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, ami visszaélésre adhat lehetőséget. Ez ellenérzést válthat ki és sértheti a személyiségi jogokat. Bármilyen, megfelelő minőségű mozgóképből kivett, vagy internetről letöltött megfelelő felbontású kép alapján is működhet az azonosítás. Mesterséges intelligenciával támogatott megoldások esetén még a kamerába nézni sem szükséges, meglepően kevés paraméter alapján is lehet sikeres az azonosítás [27].

A technológia az arc jellegzetes pontjait, azok távolságát, arányát méri. Anyajegyek és más jellegzetes azonosítók keresése (pl. forradások, tetoválások) segítik a folyamatot, a ráncok és bőrpórus vizsgálat alapján akár az illető korának meghatározása is lehetséges. Idetartozik a fülforma alapján történő személymeghatározás, illetve az új megoldások

között léteznek olyan technológiák, melyek kiegészítő jelleggel, profilból képesek a fejforma és a fül formája alapján azonosítást végezni.

A technológia pontossága alacsony, sérülékenysége igen magas, [28] könnyen elérhető, hogy jó minőségű, nagy felbontású képek alapján COVID-maszkok használatával fizetési vagy azonosítási szolgáltatások sérülékenységét kihasználják [29]. A rendszerek legtöbb esetben nem tartalmaznak élőminta felismerést segítő hardver-szoftver megoldásokat.

1.5.3. Íriszalapú azonosítás

A szem szivárványhártyájának mintázatát dolgozza fel a rendszer többféle módszer alapján. Az íriszkép a magzati lét nyolcadik hónapjától a halál pillanatáig változatlan [30, p. 315.], széles körben alkalmazható és két eltérő személy mintája egyezőségének 10^{70} az esélye [23].

Belső biometrikus jellemzőt mér, nagyon pontos technológia, érintésmentes az azonosítás folyamata és a szem nincs kitéve annyi sérülésnek, mint mondjuk egy ujjlenyomat azonosítás esetén az ujjaink [26, p. 149.]. 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 szempontjából. Nagyjából 400 jellemzőt vesz figyelembe az azonosítás során, az egyik legpontosabb technika, de különféle szembetegségekre és a fényviszonyokra érzékenyek ezek a megoldások. Az egyik legnagyobb felhasználási területe az Arab Emírségekben található, ahol határellenőrzési és biztonsági célokra használják [30, p. 335.].

1.5.4. Retinaalapú azonosítás

A szem hátsó falán futó érhálózat mérésével a retinahártya erekben gazdag és teljesen egyedi véredény szerkezete alapján azonosít az eszköz, mely során infrafény alapú megvilágítást használ a technológia. Nagy pontosságú megoldás [31, p. 52.], 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, valamint a látómező egy pontjára való

fókuszálási igénye megköveteli az alany együttműködését, amely kevésbé előnyös a tömeges gyors azonosítási igénynél, ugyanakkor nagy pontossága miatt előnyt élvez például a hadiiparban, az online szolgáltatások elérése területen, vagy a kiemelt fontosságú objektumoknál [32, pp. 35-36.].

1.5.5. Érhálózat, tenyérerezet-alapú azonosítás

Ujj- vagy tenyérérhálózat azonosítás során belső adatokat mérünk. A szenzor 740 és 1000 nm közötti tartományba eső infravörös fény által megvilágított, széndioxiddal dúsult vér áramlását érzékeli a vénás erekben, tehát csak élő minta mérésére alkalmas. A mintavételezés során mért referenciapontok milliós nagyságrendűek, nagy pontosságú és gyors megoldás. A legújabb technológiák nem igényelnek különösebb együttműködést a felhasználóval, 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, de a fényviszonyokra érzékeny a megoldás. A népesség legszélesebb körében alkalmazható lehet, kevés a fizikai kizáró ok, mert érhálózatot több testrészen is lehet azonosítani, ujjakon, kézfejen, tenyéren, alkaron is. 12 éves kor alatt a gyermekek növekedésével járó változások miatt évenkénti mintafelvétel, ismételt regisztráció javasolt. Pandémiás időszakban, az egyészségügyi területen történő felhasználás esetén az orvosi gumikesztyű használata több területen kizáró ok lehet. Nincs a módszernek ismert egészségügyi elutasítottsága, mert a kezünket alkalmazzuk általában az azonosításhoz, nem kell megérinteni mások után az eszközt. Egypetéjű ikrek esetén is működik, szélsőséges időjárási viszonyokban is jól használható. Rejtett vagy távoli azonosításra nem, vagy nehezen használható. A hamis minta előállítása rendkívül nehézkes, mert az erek mintázata emberi szemmel nem látható teljes egészében [33].

1.5.6. Kézgeometria-alapú azonosítás

A technológia 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 felismerés pontossága magas [34, pp. 172-190.]. 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, kevésbe gyakorlott felhasználóknál is jól alkalmazható.

Külső paramétert mér, A módszer az ujjak hosszát, szélességét, a területet, az ízületeknél lévő szögeket, valamint ezek arányait vizsgálja, nagyságrendileg 30 körüli mérési pontot rögzítve [35, pp. 91-107.]. Ennek következtében az azonosítást megnehezíti, vagy akár lehetetlenné is teszik a kéz deformációs megbetegedései, elváltozásai, a bandázs, a kesztyű vagy nagyobb gyűrű viselése [36]. Hízás, ízületi betegség hatására megváltozott kézgeometria okozhat azonosítási problémát, erre érzékeny a technológia. Egészségügyi területen, vagy a pandémiás védekezés miatt sok esetben szükséges lehet gumikesztyű használata, ez viszont hátráltathatja a kézgeometria alapú azonosítást. Alkalmazzák a megoldást az Egyesült Államokban atomerőművekben, de a Tel Avivi repülőtéren is, mert nem tolakodó eljárás és gyors azonosítást tesz lehetővé, az idő változásával a kéz alakja is változik, ezért a jobb pontosság érdekében javasolt már biometrikus megoldásokkal együtt (multibiometric configuration) használni [32, pp. 186-190.].

1.5.7. Hangalapú azonosítás

A hang a leginkább hozzáférhető biometrikus jellemző, nincs szükség bonyolult rögzítő eszközre vagy átviteli rendszerre a mai erősen digitalizált világunkban. Hangazonosítás során először a hang frekvenciáját azonosítják, majd a későbbi fázisban a hang egyéb tulajdonságait: a hangszínt, a hanglejtést és a ritmust. Jelentős különbség van három módszer között, az egyik a hangalapú hitelesítés, mint tipikusan a telefonon keresztüli hozzáférés kezelés hangellenőrzéssel, a másik az ún. „speaker detection”, mint a telefonközpontokban a feketelista észlelés, vagy lehallgatás. Harmadik eset a „forensic speaker recognition” mely esetén a beszédet, magát a hangot és a kibocsátójának egyedi jellemzőit ismeri fel a rendszer. Ez utóbbi megoldást használják bíróságokon a hang bizonyítékként való felhasználásra, vagy rendőrségi nyomozásokban [35, p. 151.]. 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 egyéb tényezőtől. Rendkívül egyedi minden minta [37]. Az azonosítási folyamat során nem szükséges az egyén beleegyezése a mintavételhez vagy az azonosításhoz. Belső ismérvű 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 [35, pp. 151-170.]. Ideális körülmények között nagy pontosságú a technológia, de az általános felhasználási területekben nincs élőmintaazonosítás, és az ideális körülmények

is ritkák, így inkább másodlagos megoldásként jelent nagy potenciált. A virtuális és különféle AI-alapú technikák elterjedésével korábbi hangok és videók rögzítésével és feldolgozásával könnyen készíthető hamisított videó- és hanganyag, vagy a saját hangunkon beszélő avatár, mint az Apple iOS17-ben a Personal Voice [34, pp. 172-190.].

1.5.8. Fülformaalapú azonosítás

Az emberi fül jellegzetességeinek megfigyelésén, geometriai mérésén alapuló azonosítási technológia. Az érdekessége, hogy míg az arc leírására rengeteg szavunk létezik, addig a fül alakját nehéz pontosan megfogalmazni, egyedi jellemzőit lehetetlen egyszerű szavakkal leírni, az átlagembernek nincs hozzá megfelelő szókincse, ezért szakértői tudást igényel [38]. De ettől még a számítógépek nagy hatékonysággal tudják felismerni az egyedi jellegzetességeket. *„A fül változatos alakját minden esetben a fülkép alapján azonosítjuk, mely a térbeli fül alakzat kétdimenziós képe. A fülképhez távoli személyazonosítás esetében videofelvétel, vagy fénykép alapján juthatunk. Büntetésvégrehajtási területen történő alkalmazásnál nem csak fülkép, hanem fülnyomat alapján is van lehetőség az azonosításra, ilyenkor csak a kontúrokat használják."* [39, p. 23]

A testrész könnyen eltakarható, kalappal, sállal, hosszú hajjal meg lehet akadályozni a távoli, beleegyezés nélkül történő azonosítást. Kereskedelmi fogalomban nem jellemző a fülforma alapú azonosítás, kiegészítő megoldásként használják olyan helyzetekben, ahol oldalirányú profilkép áll rendelkezésre [35, pp. 176-181.]. A fül az öregedés során stabil, az arcvonásoktól eltérően kevés változás mutat az idő elteltével.

1.5.9. DNS-mintázat azonosítás

A genetikai információt a nukleotidok sorrendje hordozza. Az emberi DNS 3 milliárd bázispárjának elrendezése egyedi, a sorrend megállapításával lehet azonosítani az adott személyt. Az eljárás így rendkívül hosszadalmas lenne, mégy úgy is, hogy a nukleotid-térkép 99 százaléka mindenkinél egyforma és a személyek azonosítását a maradék 1 százalékon kell elvégezni. Ma a leggyakrabban használt DNS-ujjlenyomat vizsgáló eljárás a polimeráz láncreakció (polymerase chain reaction, PCR). Alkalmazásához csak kis mennyiségű DNS szükséges, és a vizsgálat egyetlen éjszaka elvégezhető. A DNS-molekula egyedi szakaszait mesterségesen elállított „primer" molekulával jelölik meg, és annyi másolatot készítenek belőlük, amennyi elegendő a

gélelektroforézises szétválasztáshoz [40]. Nagy azonosítási pontosságú megoldás, de lassú és drága technológia, nagy szakértelmet igényel, laboratóriumban végezhető a folyamat. A berendezés és a szükséges eszközök mérete általában nagy, ezért a felhasználási területek korlátozottak. A folyamathoz szükség van nagy számítási kapacitással rendelkező szervergépekre, feldolgozó számítógépekre.

A DNS-minta szinte bárhonnan begyűjthető. Háborúban elesett katonák azonosításában, vagy bűnügyi nyomozás esetén ez az előnye a megoldásnak, de ez egyben a hátránya is, hiszen más esetben az alany beleegyezése nélkül is megszerezhető, és az azonosítás is elvégezhető.

A kezdetekhez képest már jelentősen csökkent az azonosítási idő és az azonosítás költsége is, de ez még mindig nem teszi versenyképessé a módszert az általánosabb felhasználhatóság szempontjából a többi, elterjedtebb és egyszerűbb biometrikus azonosítási megoldásokkal szemben [41].

1.5.10. Aláírás

Az aláírás alapú biometrikus hitelesítés egy olyan viselkedés alapú biometrikus technika, amely a személy viselkedését vizsgálja a kézírás sajátosságai és dinamikája alapján majd végzi el az azonosítást. Az aláírás felismerés az aláírás geometriai és statikus elemzését jelenti a vizuális jellemzők esetén, a biometrikus aláírás során pedig a dinamikus jellemzőket elemzik. Ilyen dinamikus rendszer lehet egy tablet eszköz, amely digitális aláírása használható és ilyen dinamikus jellemző lehet a tollnyomás erőssége, a tollvonás sebessége, az írás gyorsulása vagy lassulása, az írásszög, a betűk formája, az aláírás vonalainak iránya, vastagsága, illetve egyéb dinamikai jellemzők. Lehetőség van a statikus és dinamikus jellemzők együttes vizsgálatával elvégezni az aláírás hitelesítést [42]. Fontos megemlíteni, hogy önmagában nem egyetlen egy sajátosság, vagy jellemző, csakis az írássajátosságok komplex halmaza alkalmas adott grafikai produktum személyhez köthetőségének megállapítására. Az esetekben nem egyszerűen egy aláírásról elkészített grafikai kép elektronikus feldolgozása történik, hanem egy magasabb szinten történő, mérési folyamatokkal egybekötött, biometrikus azonosítókat is mérő digitalizációs technika alkalmazásáról van szó, mely során a kézírást feldolgozó szoftver vita esetén a szakértői vizsgálatát is lehetővé kell tegye. A digitalizált aláírás egyre elterjedtebb a hitelesített okiratok felhasználási területen, mert összetett megoldás, de a digitális megoldások terjedésével könnyű a felhasználhatósága, jól integrálható pénzügyi

szolgáltatási, a közszféra, vagy például közjegyzői felhasználási területen. További felhasználási területei széleskörűek, például jelenléti ív kitöltésekor, postai küldemény átvételénél, kérelem benyújtásánál, egy közüzemi szerződés megkötésénél, egy bankkártya használatánál vagy önkormányzati ügyintézés során alkalmazzák [43]. Jól ismert és elfogadott módszer, a dokumentumok hitelesítésére régóta használt eljárás. Költséghatékony, más biometrikus megoldásokhoz képest egyszerűbb hardvert és eszközöket igényel (pl. tablet) és a megoldással csökkenthető a papíralapú dokumentumok előállítása [43, p. 95.]. Hátránya az aláírások változása, a körülmények, a hangulat, az egészségi állapot is könnyen befolyásolja, ami hibás azonosításhoz vezet. Az aláírás-alapú biometrikus azonosítás ellenőrzése kihívást jelenthet, különösen, ha az eredeti aláírást hitelesítés nélkül rögzítették, magas a hamisíthatósága. Az aláírás-alapú biometrikus azonosításhoz szükség van egy referenciamintára, ami a felhasználó eredeti aláírását jelenti. Az ilyen mintavételezési folyamat és az azonosító algoritmusokhoz szükséges képzés idő- és erőforrásigényes lehet.

1.5.11. Gépírás- és egérmozgás-elemzés

A gépelési karakterisztika vagy a felhasználó finommotoros dinamikájának és egérmozgásának sajátosságai olyan viselkedési faktor, ami folyamatosan azonosítja a felhasználót, ezekben tipikus minták fedezhetők fel, amelyek metaadatokként rögzíthetők. Ha a felhasználói munkafolyamat rögzítésre kerül, pontos képet lehet alkotni a viselkedésről, ezekből pedig profilok építhetők, a felhasználókat kategorizálni lehet a gépírás [43, p. 47.], vagy egérmozgási minták alapján. Visszaélések során ezekben a mintákban eltérés következik be, melyek kiválthatnak riasztásokat. A hagyományos azonosítási eljárásokban egy adott időpillanatban történik az ellenőrzés, a viselkedési faktor bevezetésével viszont valós időben a teljes folyamat során lehetőség van a kontrollra. A rendszer betanítása, finomhangolása időigényes, csak nagyon magas biztonsági követelmények esetén térül meg [44].

1.5.12. Mozgás-, járás- és testalkatelemzés

A mozgás-, járás- és testalkatelemzés-alapú biometrikus azonosítás a gyenge biometrikus azonosítási kategóriába tartozik, leginkább már azonosított személyek újrafelismerését teszi lehetővé. Olyan technológia, amely az egyén mozgásmintáit, járást és testalkatát használja az azonosításra és azonosságuk ellenőrzésére. Ennek az

azonosítási módszernek számos előnye van. Először is, az egyén mozgásmintái és járása egyedi jellemzőket hordoz, ami lehetővé teszi az azonosítást [32, pp. 182-185.]. Az egyén testalkata, például testmagassága, testaránya vagy testtartása is egyedi lehet, így további biometrikus jellemzőket ad a rendszerhez. Egy másik előny az, hogy a mozgás-, járás- és testalkatelemzés-alapú biometrikus azonosítás könnyen használható, mivel nem igényel bonyolult vagy hosszadalmas képzési folyamatot és lehetőséget ad valós időben történő, vagy felévétel alapján utólag történő elemzésre. Az algoritmusok kiértékelik és összehasonlítják az egyén jelenlegi mozgását és testalkatát a már korábban rögzített mintázatokkal, ami gyors és hatékony azonosítást eredményez. Ezenkívül a mozgás-, járás- és testalkatelemzés-alapú biometrikus azonosítás kevésbé érzékeny a változó környezeti tényezőkre, mint például a fényviszonyok vagy a zaj. Mivel az egyén sajátos mozgásmintái és testalkata alapján történik az azonosítás, a rendszer stabilitása és megbízhatósága javul, ugyanakkor nagyban befolyásolja a ruházat, a lábbeli fajtája, a kamerához viszonyított irány és sebesség, a járófelület típusa, ezeket figyelembe kell venni az azonosítás során. Jól alkalmazható cselekvésfelismerési megoldásokban, például határátlépésnél a zavart, gyanús viselkedés kiszűrésére. Azonban a módszernek vannak bizonyos hátrányai is. Először is, az egyén mozgására és változó testalkatára (elhízás) való folyamatos figyelem nagyobb hardverigényt és számítási erőforrásokat igényelhet, illetve sokszor ellenőrzött környezetben használható ki a megoldás előnye. Alkalmazható rejtett azonosításra, az alany beleegyezése nélküli megoldásra, rejtett profilozásra, anomália detektálásra. Többszenzoros LIDAR vagy mélységszenzoros megoldásokkal nagyobb, dinamikus helyszínek megfigyelésére is lehetőség van [45].

1.5.13. A fejezet összefoglalása, következtetések

Ebben a fejezetben bemutattam az összefüggést az egyén és a biztonság kapcsolatában és rámutattam, hogy amennyiben nő az igény a biztonság iránt, akkor csökkenhet az ellenállás a biztonságot megteremtő módszerekkel szemben, mert minél inkább csökken az egyén biztonságérzete, annál jobban nő az igénye a biztonság iránt (kevésbé elutasító a biztonság növelését célzó megoldásokkal szemben). Ez nagyobb elfogadást okoz a megoldások tekintetében, még akár lemondás árán is a személyes jogok területén. A biztonságérzet csökkenése következtében növekvő elfogadás vagy a felhasználók kényelmi igényeinek kiszolgálását célzó növekedések miatt a biometrikus azonosítási megoldás felhasználásának növekedése egyben növekedő kockázatot jelent a

felhasználónál. Ezért fontos ezeknek a kockázatoknak az értése és kezelése. Összegeztem a biometrikus azonosítással kapcsolatos fogalmakat és mutatókat, a biometrikus adat fogalmát és változását az idő múlásával, mert az ezekben történő fejlődés és változás támasztja alá a biometrikus azonosítás fogalmának fejlődési szükségszerűségét. Összegeztem az azonosító eljárásokat a felhasználási szempontokat figyelembe véve az elterjedéssel összefüggő tényezőkkel egyetemben. Megalkottam a biometrikus azonosítás és a hitelesítés modern, a mai kor technológiai újdonságait is figyelembe vevő definícióját, azaz a pszichológiai és érzelmi jellemzőkre alapuló elemző és következtető eljárásokat is magába foglaló legmegfelelőbb meghatározást. A jelenleg érvényben lévő definíció, véleményem szerint összhangban az elmúlt évtizedre jellemző lemaradással, még nem kezeli a pszichológia és az érzelmi jellegű tulajdonságokat és azoknak az azonosítási eljárásokban való használatát. Ezzel alátámasztottam a H5 hipotézisemet, mert az új definíció megalkotása szükségszerű és elvégezhető volt.

Ebben a fejezetben elemeztem a biometrikus azonosító megoldásokat az elterjedés szempontjából és feldolgoztam az AI-val összefüggő kutatásokat és fejlesztéseket is. Rámutattam arra, hogy az AI-val összefüggő fejlesztések kockázatai mennyire erősen összefüggenek a biometriával és annak elterjedésével. Erre kiváló kiragadott példa az AI-val kiegészített arcfelismerőrendszer, mely tanulók óra alatti reakcióit figyeli, de ugyanakkor súlyos behatolás a gyermekek magánéletébe.

Disszertációm következő fejezetében a biometrikus azonosítás és az AI-technológiák jogszabályi környezetével foglalkozom, mert ennek megértése szükséges az elterjedés vizsgálata szempontjából, illetve a tématerületre kiemelten jellemző, hogy a szabványok megléte, a jogi szabályozottság állapota nagymértékben hatást gyakorol a felhasználási területekre, és ezzel az elterjedésre.

A jelenlegi mesterséges intelligencia alapú rendszerek képesek arra, hogy hangminták alapján bárki hangját és fényképek, videók alapján bárki vizuális megjelenését (pl. képet, videót) meghamisítsák az online térben, ezáltal, amit vizuális érzékszerveinkkel hallunk és látunk, azokban egyre kevésbé hihetünk. Könnyen a hackertámadások áldozatává válhat a hiteles tájékoztatás és eljöhet az az idő, amikor az online jelenlét valódiságának igazolására élőminta-felismerésen alapuló komplex, multimodális biometrikus rendszerekre lehet szükség. Ez viszont kifejezetten megköveteli a megfelelő szabályozottságot.

2. A BIOMETRIKUS ADATOK VÉDELMÉNEK ÉS A MESTERSÉGES INTELLIGENCIA FEJLŐDÉSÉNEK ÖSSZEFÜGGÉSEI ÉS A JOGSZABÁLYI HÁTTÉR

Ebben a fejezetben összegzem a személyes adatokkal, az adatbiztonsággal és a biometrikus azonosítási megoldásokkal kapcsolatos hazai és nemzetközi szabályozásokat, valamint elvégzem a biometrikus azonosítási rendszerek felhasználási területfüggetlen kockázatalapú értékelését. Igazolom az értekezés H2-es hipotézisét.

A biometrikus adatok gyűjtéséről és kezeléséről – meglátásom szerint – nincs egységes összhang az érintett felek között, a jogvédő szervezetek, a jogalkotók és a szakmaiszervezetek eltérő álláspontot képviselnek. Egyetértek Werner állításával, a „*jogi szabályozás csak lassan követi le a technikai fejlődés adta sérülékenységi hézagok okozta jogi hiányosságokat*” [46, p. 11.]. Az elemzésen, következtetésen alapuló, mesterséges intelligenciát használó rendszerek kapcsán pedig kezdeti fázisban jár a szabályozás, nincs megfelelő összhang országok és nemzetek szabályozási és a gyakorlati alkalmazása között. Olyan nézetkülönbség és ellentét feszül egymásnak, mint például, hogy melyik a fontosabb, a biometrikus rendszerekkel megteremthető jobb közbiztonság és az ezzel együtt járó módon az azonosítási megoldások szélesebb körű elterjedése, esetleg a felhasználók beleegyezését nem igénylő rendszerek használata, avagy a személyi szabadságjogok és a személyes adatok védelme? Arra pedig egyáltalán nincsenek átfogó és biztos alapokat adó kutatások és általánosítható megoldások, mi történik, ha biometrikus adataink illetéktelen kezekbe kerülnek, hiszen azokat nem tudjuk minden esetben olyan könnyen lecserélni, mint egy PIN-kódot vagy jelszót.

Az Európai Parlament Állampolgári Jogi és Alkotmányügyi Tematikus Főosztálya rendelt meg egy tanulmányt [47] a JURI (Európai Parlament jogi ügyi bizottsága) és a PETI (Európai Parlament petíciókkal foglalkozó) bizottsága felkérésére, mely etikai és jogi szempontból elemzi a biometrikus technikák alkalmazását. A biometrikus technikák számos konkrét etikai kérdést vetnek fel, mivel az egyén nem tudja könnyen megváltoztatni a biometrikus jellemzőket, és mivel ezek a technikák hajlamosak behatolni az emberi testbe és végső soron az emberi énbe, így nagy kockázatot jelentenek, ami jelentősen megnöveli az elutasítását is a megoldásoknak. A további kérdések általánosabban kapcsolódnak a nagyszabású megfigyeléshez, az algoritmikus

döntéshozatalhoz vagy a profilalkotáshoz. A tanulmány a biometrikus technikák különböző típusait elemzi, és következtetéseket von le az uniós jogszabályokra vonatkozóan.

Biometrikus technikák jelentik azokat a technológiákat melyek fizikai, fiziológiai vagy viselkedési adatok speciális technikai feldolgozására jöttek létre, figyelembe véve az emberi test egyéb aspektusait, így a mozgást is beleértve, mindezt az egyének azonosítása, hitelesítése vagy kategorizálása érdekében. A legújabb technológiák már képesek az egyének átmeneti vagy állandó állapotának észlelésére, vagy akár komplex módon a jövőbeli állapot vagy viselkedés vagy szándék előrejelzésére. A hagyományos azonosítási megoldások mellett, mint az ujjlenyomat, mint az arc vagy az érhálózat, megjelentek az új típusú érzékeléseken alapuló megoldások, mint a szívverés és az agyhullámok, valamint az agyi interfacek, melyek mérik a neuroaktivitást, és ezeket a jeleket olvasható bemenetté alakítják. Ezek a megoldások egyrészt hasznosak a betegségek észlelésére, de ugyanakkor lehetőséget adnak a gondolatok és szándékok előrejelzésére, vagy akár az agy működésének befolyásolására, ami etikailag megkérdőjelezhető. A 2021. április 21-én kiadott AI-ról szóló szabályozás (Artificial Intelligence Act, továbbiakban: AIA) különböző területei foglalkoznak ezekkel a kérdésekkel.

A biometrikus azonosítással kapcsolatban felvetődő fő etikai probléma, hogy a begyűjtött biometrikus adatból készült sablon eltárolása után a személy bármikor és bárhol azonosítható, miután a digitalizált egyedi jellemző nem változtatható meg, hiszen az az adott személy testének részéből képzett adat. Ezek összegyűjtése ellentétben áll az ember autonómiájával és néhány biometrikus adat esetén akár a méltóságával. Ezek közterületen történő gyűjtése, vagy tömeges megfigyelésre való alkalmazása messze túlmutat a világ demokratikusabb felének etikai normáin. Az ilyen rendszerekhez kapcsolt elemző és kategorizáló képességek még további etikai és morális kérdéseket vetnek fel, mert az eredményeik alkalmasak nem megfelelő következtetések levonására, megbélyegzésre vagy megkülönböztetésre. Ezek új szabályozási lehetőségeket jelentenek a „neuro-jogok” területén, beleértve a szellemi joghoz, a magánélethez és a mentális teljességhez (mental integrity) való jogot.

Az AIA-ra vonatkozó, közelmúltban kialakított javaslatok bár jó irányba haladnak, de még mindig nem foglalkoznak megfelelően az etikai aggályokkal és az ebből származó kockázatok kezelésével. A biometria tudományterületnek és a kapcsolódó szabályozásnak meg kell alkotnia a közeli jövőben a biometrikus alapú adatok új

meghatározását, mely az általános adatvédelmi rendeletben (General Data Protection Regulation, továbbiakban: GDPR) megfogalmazottaktól eltérően, a biometrikus adatok fogalmától jól érzékelhetően megkülönböztetve kezeli a biometrikus kategorizáló rendszer és az érzelemfelismerő rendszer fogalmakat. Az azonosítási folyamatok szempontjából fontos pontosabban meghatározni a távoli azonosítás és a valós idejű azonosítás fogalmait, és be kell vezetni a biometrikus következtetések meghatározást, hogy ezek kockázatai megfelelően kezelhetők legyenek. Szabályozni szükséges a biometrikus alapú AI támogatású döntési rendszerek használatát és a kategorizáló rendszereket [47].

Mai viszonylatokban a „biometrikus technikák" kifejezés egyértelműen magába foglalja például a billentyűleütések vagy az egér mozgásdinamikájának elemzését, a gesztusok dinamikáját vagy a járás- és mozgásjellemzőket. A kifejezés mai szabályozástechnikai értelemben viszont nem értelmezhető úgy, mint ami magába foglalja az emberi akarat által irányított viselkedést, mint a vásárlási magatartást, böngészési szokásokat. Addig, míg az ilyen viselkedéseket elemezni képes rendszereket fejlesztenek és ebből következtetéseket vonnak le, melyek kiterjedhetnek genetikai, fizikai, fiziológiai vagy érzelmi, pszichológiai természetű jellemzőkre, addig indokolt ezeknek a pontosabb szabályozása az alanyok védelme érdekében. Növekvő tendencia ezeknek a gyenge (weak), vagy puha (soft) biometrikus adatoknak a felhasználása a multimodális rendszerekben. Ezen a területen a legújabb irányzatok közé tartoznak azok a továbbfejlesztett érzékelők, melyek lehetővé teszik új típusú jelek feldolgozását. EEG-n és EKG-n keresztül szívverés ás agyhullám adatok feldolgozását, vagy a BCI interfacek jeleit, melyek a neuroaktivitást, agyi aktivitást fordítják le feldolgozható formátumra. Ezek alkalmasak a szándékok és gondolatok észlelésére, értékelésére, előrevetítésére.

2.1. A biometrikus azonosítás és a személyes adatok kezelésének jogi háttere

A biometriával összefüggésben a személyes adatok kezelésének, az AI szabályozásának fő pontjait és mérföldköveit tekintem át az alábbiakban, törvényeken, szabályzatokon, szakértői csoportok javaslatain keresztül Magyarországon és az Európia Unióban. A 2. számú mellékletben szereplő 12. táblázat jó áttekinthetősége és önálló értelmezhetősége érdekében, minden lényegi információt tartalmazóan sorolom fel a fontos mérföldköveket és a jelentőségüket a biometria elterjedése szempontjából, de az

értekezésben, a táblázatos forma megkötöttségei nélkül, a disszertáció szempontjából lényeges információkkal is kiegészítem azokat, így a kiegészítő információk értelmezhetősége miatt a szöveg és a táblázat között ismétlések vannak.

Az 1992. évi LXIII. törvény az első törvény Magyarországon, amely az adatvédelemmel foglalkozik.

1994-ben az Informatikai Tárcaközi Bizottság 8. számú ajánlása került kiadásra, mely az informatikai biztonsági követelményeket egy módszertani kézikönyvben foglalja össze.

Az 1995/46/EK az első Európai Uniós jogszabály, amely az adatvédelemmel foglalkozik, azonban nem szabályozza konkrétan a biometria alkalmazását.

Az Informatikai Tárcaközi Bizottság 1996-os 12. számú ajánlása az informatikai rendszerek biztonsági követelményeiről szól.

Az Egyesült Királyságban működő Biometric Working Group (biometrikus munkacsoport) által összeállított legjobb gyakorlatok jegyzéke.

A jegyzék tartalmazza a következő témaköröket:

- Tesztelési stratégia és terv kidolgozása
- Teszteszközök és -technikák kiválasztása és alkalmazása
- Adatgyűjtés és -feldolgozás
- Teszteredmények kiértékelése és jelentéskészítés
- Adatvédelem és biztonság

2002/17/EK rendelet az Európai Parlament és a Tanács 2002/EC irányelve, amely az elektronikus hírközlő hálózatok és szolgáltatások közös szabályairól szól. Az irányelv célja az volt, hogy biztosítsa az uniós tagállamok közötti együttműködést a személyazonosság igazolására szolgáló hivatalos dokumentumok elismerése terén. Az irányelv előírta, hogy az uniós tagállamoknak kötelezően kell elfogadniuk az egymás által kiállított személyazonossági igazolványokat és útlevélkártyákat. Tartalmazza az egyes állampolgári igazolványokhoz kapcsolódó biometrikus adatok kezelésének feltételeit.

A 2003. évi C. elektronikus hírközlésről szóló törvény szerint az elektronikus hírközlési szolgáltatóknak biztosítaniuk kell a felhasználók adatainak védelmét, beleértve a biometrikus adatokat is.

2252/2004/EK tanácsi rendelet előírta a tagállamoknak az EU-ban, hogy a közös műszaki és biztonsági követelmények elfogadását követően az érintett okmányokba biometrikus azonosító adatokat kell illeszteni.

Az Európai Unió (EU) Bizottságának 2006/VI/28 határozata, amely meghatározta a digitális ujjlenyomatokkal kapcsolatos követelményeket a második generációs útlevelekhez (biometrikus útlevél). A határozat 2006 júniusában született. Az új követelmények azt jelentették, hogy az EU országoknak a biometrikus útlevelek kiállításakor digitalizált ujjlenyomatokat kellett tartalmazniuk, amelyek segítik azonosítani az útlevél tulajdonosát és megakadályozzák a hamisítást. A határozatot az EU országoknak 2006 szeptemberéig kellett bevezetniük. A digitalizált ujjnyomatok követelménye a biztonsági okokból szükséges lépés volt az útlevelek személyazonosságot igazoló szerepének megerősítése érdekében. Az ilyen biometrikus adatokat az útlevélben biztonságosan kell tárolni, és csak a hatóságok számára kell hozzáférhetővé tenni. A határozat a *„Biometrikus azonosító adatokkal rendelkező úti okmányokra vonatkozó közös elemekről szóló, 2004. december 13-i 2252/2004/EK európai parlamenti és tanácsi határozat végrehajtására irányuló bizottsági határozat”* címen található a dokumentumban, a 22. oldaltól kezdve.

2007-ben az ISO 24709 szabvány az úgynevezett „biometrikus teljesítménymérő eszközök” (BPP) tesztelési eljárásait írja le. Ez az eljárás lehetővé teszi a biometrikus rendszerek teljesítményének mérését és összehasonlítását, hogy megbizonyosodjunk arról, hogy megfelelően működnek-e a különböző körülmények között.

A 2009. évi XLVII. törvény Magyarországon a személyes adatok védelmével és a közérdekű adatok nyilvánosságával kapcsolatos szabályokat tartalmazza. A törvénynek nincs kifejezetten biometriával kapcsolatos része, azaz nem említi kifejezett módon a biometriai adatokat vagy az azonosítás technológiáját. Azonban a törvény általános rendelkezései érintik a személyes adatok kezelését és védelmét, amelyek között lehetnek biometrikus adatok is. A törvény előírja, hogy a személyes adatok kezelése során a jogos érdekekkel összeegyeztethető módon kell eljárni, és tiszteletben kell tartani az adatok alanyainak jogait, beleértve a tájékoztatáshoz, hozzáféréshez, javításhoz és törléshez való jogot.

A 2010. évi CXXVI Adatvédelmi Törvény tette lehetővé a biometrikus aláírások használatát a fővárosi és megyei kormányhivatalok ügyfélszolgálatain, a járási (fővárosi kerületi) hivatalok kormányablakaiban, illetve a települési ügysegédeknél az elektronikus dokumentumok ügyfél általi hitelesítésére, megfelelő biometrikus adatok felhasználásával, biometrikus verifikáció céljából. A magyar 2010. évi CXXVI. törvény (a továbbiakban: Adatvédelmi törvény) a személyes adatok védelméről és a magánélet védelméhez való jogról szól. Az Adatvédelmi törvény kiemelt figyelmet fordít a

biometria és az ezzel kapcsolatos személyes adatok védelmére is. Az Adatvédelmi törvény szerint a biometrikus adatok (például az ujjlenyomat, arcfelismerő adatok) kezelése csak akkor engedélyezett, ha az adatkezelés a személyes adatok kezelésének céljaihoz és az adatkezelési elvekhez alkalmazkodik. Az adatkezelésnek a jogos érdekeknek megfelelőnek, arányosnak és átláthatónak kell lennie. Az Adatvédelmi törvény a biometrikus adatok kezelésének feltételei között előírja, hogy az érintetteknek tájékoztatást kell kapniuk az adatkezelésről, az adatkezelés céljairól, az adatkezelőről és az adatkezelési elvekről. Emellett az adatkezelőnek biztosítania kell az adatok biztonságát, és megfelelő intézkedéseket kell hoznia a jogosulatlan hozzáférés, az adatvesztés vagy az adatok megváltoztatása ellen. Az Adatvédelmi törvény további előírásokat is tartalmaz a biometrikus adatok kezelésével kapcsolatban. Például az érintettnek jogában áll kérni az adatai törlését vagy korlátozását, valamint jogában áll tiltakozni az adatkezeléssel szemben. Az adatkezelőnek az érintettek jogait és az adatvédelmi előírásokat tiszteletben kell tartania, és a jogsértések esetén az adatvédelmi hatósághoz kell fordulni. Az Adatvédelmi törvény szigorú előírásokat tartalmaz a biometrikus adatok kezelésével kapcsolatban, hogy biztosítsa az érintettek jogait és az adatok védelmét. Az adatkezelőknek meg kell felelniük ezeknek az előírásoknak, hogy megfelelően kezeljék a biometrikus adatokat.

A magyar 2011. évi XCII. törvény (a továbbiakban: Információs önrendelkezési jogról és az információszabadságról szóló törvény) az adatvédelmi törvénnyel együtt szabályozza a személyes adatok védelmére vonatkozó kérdéseket Magyarországon. Az Információs önrendelkezési jogról és az információszabadságról szóló törvény kifejezetten foglalkozik a biometria és az ezzel kapcsolatos személyes adatok védelmével. Az ilyen adatokat csak akkor lehet kezelni, ha az adatkezeléshez az érintett előzetesen hozzájárult, vagy ha az adatkezelés a jogszabályban meghatározott célból történik, és az ahhoz szükséges. Az Információs önrendelkezési jogról és az információszabadságról szóló törvény az érintettek jogait és az adatkezelők kötelezettségeit is részletesen meghatározza a biometrikus adatok kezelésével kapcsolatban. Az érintetteknek joguk van tájékoztatást kapni az adatkezelés céljáról, az adatkezelőről és az adatok továbbításáról. Az adatkezelőnek biztosítania kell az adatok biztonságát és megfelelő intézkedéseket kell tennie az adatok védelme érdekében. Az Információs önrendelkezési jogról és az információszabadságról szóló törvény előírja továbbá, hogy az adatkezelőnek az adatkezelés előtt tájékoztatnia kell az érintetteket az adatkezelés módjáról, valamint az adatok felhasználásának jogszabályban meghatározott

céljáról. Az adatkezelőnek emellett biztosítania kell az érintettek számára a biometrikus adatok törlésének, helyesbítésének és az adatkezeléssel szembeni tiltakozás jogát. Összefoglalva, az Információs önrendelkezési jogról és az információszabadságról szóló törvény az érintettek jogait és az adatkezelők kötelezettségeit is meghatározza a biometrikus adatok kezelése kapcsán, hogy biztosítsa az adatok védelmét és az érintettek jogainak védelmét Magyarországon.

Az Európai Adatvédelmi Testület (European Data Protection Board, továbbiakban: EDPB) 29-es munkacsoportja 2012-ben kiadott egy munkaanyagot az „Opinion 3/2012 on Developments in Biometric Technologies" címmel, amelynek célja a biometrikus technológiák adatvédelmi kihívásainak és a személyes adatok védelmének vizsgálata volt. A munkaanyag részletesen bemutatja a biometrikus technológiák működését, azokat a folyamatokat, amelyeken keresztül az adatokat gyűjtik, tárolják és felhasználják, valamint az ezen folyamatok során felmerülő adatvédelmi kockázatokat. A munkaanyagban említik, hogy a biometrikus technológiák gyakran magukkal hordoznak súlyos adatvédelmi kockázatokat, mivel az ilyen rendszerek által felhasznált személyes adatok az egyén szervezetének legérzékenyebb adatai közé tartoznak. A dokumentum az adatvédelmi kockázatokat felismerve számos ajánlást tesz a biometrikus technológiák fejlesztése és alkalmazása során az adatvédelem biztosítása érdekében. Ezek közé tartozik a személyes adatok minimális gyűjtése és tárolása, a személyes adatok anonimizálása és az anonim adatok használata, a magas szintű adatbiztonsági intézkedések alkalmazása, valamint az érintettek tájékoztatása és hozzájárulásának beszerzése. Az EDPB 29-es munkacsoportja azt is javasolta, hogy a biometrikus technológiákkal foglalkozó szervezetek szorosan együttműködjenek az adatvédelmi hatóságokkal, és a technológiák fejlesztése során alkalmazzák az adatvédelmi alapelveket és a jogi előírásokat, hogy biztosítsák a személyes adatok védelmét és az egyének jogait.

Az EDPD 29-es munkacsoportja 2012. április 27-én kiadott ajánlásában az „Automatikus biometrikus azonosító rendszerek alkalmazása a határellenőrzésben és határőrizetben" címmel részletesen foglalkozik a biometrikus azonosítás alkalmazásának adatvédelmi szempontjaival. Az ajánlás különös figyelmet szentel a személyes adatok védelmének, valamint a biometrikus adatok kezelési és tárolási biztonságának. Az ajánlás célja, hogy segítséget nyújtson az olyan rendszerek létrehozásában, amelyek teljes mértékben betartják az adatvédelmi jogszabályokat és az alapvető jogokat.

A magyar Polgári Törvénykönyv (továbbiakban: PTK) 2013. évi V. tv. 2:59.§-a az adatvédelemre vonatkozó rendelkezéseket tartalmazza. A törvény az adatok kezelése

során a személyes adatok védelmének alapelvére hivatkozik, amelynek értelmében minden adatkezelőnek gondoskodnia kell arról, hogy az adatok kezelése során az érintettek jogait tiszteletben tartsák, és az adatokat biztonságosan kezeljék. A biometrikus technológiákkal kapcsolatban a törvény azt mondja, hogy az ilyen technológiákkal kapcsolatos személyes adatok kezelése csak a személyes adatok védelmének elveivel összhangban történhet.

Ez azt jelenti, hogy az adatkezelőnek biztosítania kell a személyes adatok biztonságát, és az érintetteknek joguk van az adatkezeléssel kapcsolatos tájékoztatáshoz, az adatok helyesbítéséhez, törléséhez, valamint tiltakozáshoz. A törvény azt is meghatározza, hogy az adatkezelőnek kötelessége az érintettek személyes adatainak védelme és a jogainak tiszteletben tartása érdekében megfelelő technikai és szervezési intézkedéseket alkalmaznia, amelyek az adatok biztonságát garantálják. Az adatvédelmi szabályok megsértése esetén az érintettek jogosultak az adatkezelővel szemben jogi lépéseket tenni, és az adatkezelőnek az érintettekkel szembeni kártérítési kötelezettsége is lehet. Összességében a PTK 2013. évi V. tv. 2:59.§-a a személyes adatok védelmére vonatkozó általános elveket határozza meg, és különösen kiemeli az adatkezelés biztonságának fontosságát. A biometrikus technológiákkal kapcsolatban a törvény megköveteli, hogy az adatkezelés során az adatvédelmi alapelveknek megfelelően történjen, és biztosítja az érintettek jogait az adatkezeléssel kapcsolatban. Ez a törvény teremtette meg a jogalapot a közigazgatás és a kritikusnak minősíthető infrastruktúrák, a létfontosságú rendszerelemek egyenszilárdságú védelmének kialakításához és fenntartásához.

2004. évi I. törvényt módosító 2014. évi XXVII., sporttörvény, mely szabályozza a nem bűnügyi célú biometrikus személyazonosítási módszereket (képmásból, ujjnyomatból, íriszképből vagy érhálózatból képzett nem visszafejthető, alfanumerikus kód) és azok használatának módját. A stadionok és a sportrendezvények biztonságának céljából e törvény okán vált lehetővé a biometrikus személyazonosítások alkalmazása az állami szektoron kívül, nem polgári jogi feltételek alapján.

Az Európai Unió általános adatvédelmi rendelete, azaz a GDPR 2016. április 27-én lépett hatályba, de alkalmazása csak 2018. május 25-étől kötelező. A rendelet magyarországi hatályba lépése megegyezik az európai hatálybalépéssel, vagyis 2018. május 25-től alkalmazandó Magyarországon. A GDPR értelmében biometrikus adatnak tekintendő minden olyan sajátos technikai eljárásokkal nyert személyes adat, ami egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozik, és amely

lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását. A biometrikus adatok kezelésekor a GDPR alapelvei közül néhány fontosabb a következők:

- Adatvédelem elve: a biometrikus adatokat csak azok a szervezetek kezelhetik, amelyek számára ez szükséges az adott feladat elvégzéséhez.
- Adattárolás korlátozása: a biometrikus adatokat csak azokban az adatbázisokban lehet tárolni, amelyeknek célhoz kötötten szükségük van rájuk.
- Adattörlési elv: amint a biometrikus adatokra nincs szükség, azokat el kell távolítani a rendszerből.
- Adatbiztonság elve: a biometrikus adatokat megfelelő biztonsági intézkedésekkel kell védeni a jogosulatlan hozzáférés és a jogosulatlan felhasználás ellen.

A GDPR korlátozza az automatizált egyéni döntéshozatali rendszerek használatát és a profilalkotást.

A személyes adatoknak, ideértve a biometrikus adatokat is, bűnmegelőzési célú kezelése, azaz bűncselekmények kivizsgálása, felderítése vagy üldözése során történő kezelése nem tartozik a GDPR hatálya alá, ekkor a Bűnüldözési Irányelv (LED, Law Enforcement Directive) [48] az irányadó. A LED már szigorúan korlátozza a biometrikus és egyéb érzékeny adatok feldolgozását ezekben a különleges esetekben.

Az Európai Bizottság javaslata a biometrikus adatok használatáról az EU határain az Európai Parlament és Tanács 2018/0104 (COD) rendeletének a része. Ez a rendelet az úti okmányok biztonsági jellemzőiről és az ezekben szereplő biometrikus azonosító adatok feldolgozásáról szól, és az EU határellenőrzési rendszerének részét képezi. A rendelet szerint az úti okmányokban tárolt biometrikus adatokat kizárólag az utazó azonosítására és az utazó okmányainak ellenőrzésére lehet felhasználni, és csak azok a hatóságok férhetnek hozzá, amelyek jogosultak az utazási okmányok ellenőrzésére.

A COM (2018) 237 final jelentés és az EU AI-stratégia közötti kapcsolat az, hogy mindkét dokumentum célja az Európai Unió szabályozói keretének javítása az innovatív technológiák, különösen az AI és a gépi tanulás (ML) terén. Az EU AI-stratégia célja az, hogy elősegítse az AI fejlődését az EU-ban, miközben megőrzi az uniós értékeket, az emberi jogokat és az adatvédelmet. Az EU AI-stratégia továbbá magában foglalja az AI-re vonatkozó uniós jogszabályok felülvizsgálatát és a szabályozási keret kialakítását, amely biztosítja az etikus és biztonságos AI alkalmazást. A COM (2018) 237 final jelentés az AI-ra vonatkozó szabályozási környezet kialakításának fontosságára hívja fel a figyelmet, illetve javaslatokat tesz az adatvédelem, a biztonság, az etikai és a társadalmi

kérdésekkel kapcsolatos aggályok kezelésére. A két dokumentum összekapcsolódik, mivel mindkettő az innovatív technológiák szabályozásának javítását célozza az EU-ban.

A magyar 2019. évi CXXXIV. törvény a biometrikus adatok kezelésére vonatkozó szabályokat határozza meg, és összhangban van az Európai Unió által elfogadott általános adatvédelmi rendelettel (GDPR). A törvény szabályozza a biometrikus adatok kezelésének feltételeit és az adatvédelmi kötelezettségeket, beleértve a biometrikus adatok védelmét, a felhasználók tájékoztatását és az érintettek jogait. Ezen törvény hatályba lépése előtt a biometrikus adatok kezelése kizárólag jogszabály alapján, vagy az érintett önkéntes hozzájárulása alapján volt lehetséges. A 2019. évi CXXXIV. törvény jelentős változásokat hozott a korábbi biometriát kezelő törvényekhez képest, például az előírt adatvédelmi kötelezettségek szigorításával, valamint az érintettek jogainak kiterjesztésével. Az 2019. évi CXXXIV. törvény egyik fontos szigorítása a biometrikus adatok kezelésének szabályozása, amely a korábbi törvényhez képest további jogosultságokat és kötelezettségeket ír elő a szervezeteknek. A törvény szerint a biometrikus adatok kezelésének az érintettek előzetes, kifejezett és tájékozott hozzájárulásán alapuló adatkezelési céljai között kell szerepelnie. Ez azt jelenti, hogy az érintetteknek tisztában kell lenniük azzal, hogy milyen adatokat kezelnek róluk, miért és kiknek szolgáltatják ezeket az adatokat. Az új törvény szigorítja az adatvédelmi szabályokat is. Az adatoknak biztonságban kell lenniük, és csak olyan szervezeteknek adhatók át, amelyeknek szüksége van rájuk a biometrikus azonosítási folyamatok végrehajtásához. A törvény kiterjeszti az érintettek jogait is, így többek között lehetővé teszi számukra az adatkezelés elleni tiltakozást, az adatok hozzáférhetőségét és azok javítását, illetve a biometrikus azonosító adatok törlését. Az új törvény továbbá előírja, hogy az adatokat csak a legfontosabb célokra szabad használni, és nem szabad az érintettek személyes adatait más célra használni. Az érintetteknek joguk van tudni, hogy milyen célokra használják az adataikat, és az adatkezelőnek tájékoztatnia kell őket erről. A törvénynek van néhány olyan rendészeti és bűnügyi vonatkozása is, amelyek a biometrikus adatok kezelésével kapcsolatosak. Az egyik ilyen vonatkozás a bűnügyi nyilvántartásokra vonatkozik. A törvény kimondja, hogy a bűnügyi nyilvántartásokban csak azok a biometrikus adatok kezelhetők, amelyek szükségesek a bűncselekmények megelőzéséhez, felderítéséhez és az elkövetők azonosításához. Ez magában foglalhatja az ujjlenyomatokat, a tenyérnyomatokat, a fotókat, a DNS-mintákat és más biometrikus adatokat. Az ilyen adatokat azonban csak a jogos érdek, valamint a személyes adatok védelmére és az emberi méltóság tiszteletben tartására vonatkozó alapelvek betartása

mellett lehet kezelni. A törvénynek van még egy rendészeti vonatkozása is, amely a biometrikus azonosítással kapcsolatos. A törvény kimondja, hogy a biometrikus azonosítás csak az érintett személy beleegyezése esetén végezhető el. Azonban bizonyos esetekben, például a hatóságok által végrehajtott bűnügyi nyomozások során, az érintett személy beleegyezése nélkül is elvégezhető a biometrikus azonosítás. Ilyenkor azonban szigorú szabályoknak kell megfelelni, amelyeket a törvény részletesen meghatároz.

A 2019/1157/EU rendelet az Európai Unió polgárai és családtagjaik számára kiállított uniós szintű biztonsági elemekkel rendelkező igazolványok és tartózkodási engedélyek biztonsága témában. A rendelet célja, hogy biztosítsa az uniós szintű biztonsági elemekkel ellátott személyazonossági igazolványok és tartózkodási engedélyek kiállítását. A rendelet tartalmazza az egyes igazolványokhoz kapcsolódó biometrikus adatok kezelésének feltételeit is. A rendelet célja továbbá, hogy javítsa az állampolgárok és a családtagjaik személyazonosságának igazolására szolgáló dokumentumok biztonságát, illetve segítse az adatvédelmet és az adatbiztonságot az ilyen dokumentumok kezelése során. A 2002/17/EK irányelvet frissítette és kiegészítette az uniós szintű biztonsági elemekkel ellátott személyazonossági igazolványok és tartózkodási engedélyek kiállítására vonatkozóan.

Az Európai Bizottság 2019. április 24-én javaslatot tett a biometrikus adatok használatával kapcsolatos uniós határellenőrzési rendszer bevezetésére. A javaslat része volt az általános uniós határellenőrzési rendszer (EU Entry/Exit System, EES) és az utasazonosítási rendszer (Interoperability Regulation) felülvizsgálatának, amelyek célja az EU külső határainak hatékonyabb védelme. A javaslat értelmében az EU külső határain történő utazás során a harmadik országbeli állampolgárok és uniós állampolgárok útlevelében szereplő arcképfelvételt a határon felvett ujjlenyomatokkal együtt az útlevelük adataival együtt rögzítenék, és ezeket a rendszer összehasonlítaná az illető személy korábbi utazási adataival. Az új rendszer célja a határellenőrzés hatékonyságának és biztonságának javítása, az illegális migráció és a terrorizmus elleni harc erősítése. Az Európai Parlament és a Tanács 2019 novemberében elfogadta a javaslatot, azonban az adatvédelmi aggályok miatt a javaslat több kritikát is kapott az adatvédelmi aktivisták és egyes uniós tagállamok részéről, akik szerint a rendszer túlzottan invazív lehet az utazók magánélete szempontjából.

A 2020-ban kiadott Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése, COM (2020) 65 final, szakpolitikai alternatívákat határoz meg arra vonatkozóan, hogyan érhető el a mesterséges intelligencia elterjedésének

előmozdítására és az ilyen technológiák bizonyos felhasználásához kapcsolódó kockázatok kezelésére irányuló kettős célkitűzés. Az európai adatstratégia kidolgozása és megjelenésének ideje.

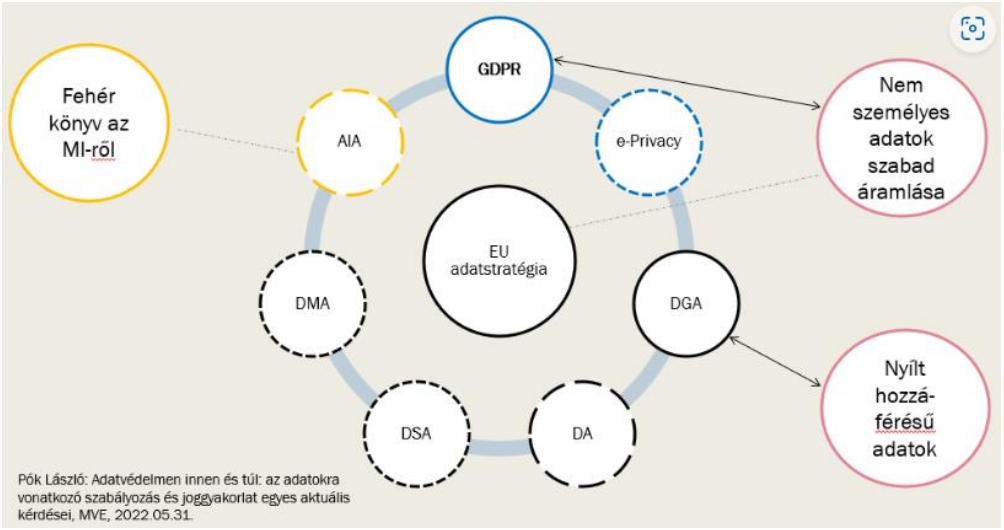
Magyarországon 2020. július 22-én a Magyar Közlönyben jelent meg az adatvédelmi hatóságok és az információs önrendelkezési jogot érintő egyes kérdések rendezéséről szóló 2020. évi LVIII. törvény. Ezen törvény hatálya kiterjed az adatvédelmi hatóságok működésére és hatáskörére, valamint az információs önrendelkezési jogot érintő kérdésekre, így az adatvédelmi eljárásokra és a bírságokra is. A törvény lehetővé teszi a biometrikus adatok kezelését a koronavírus-járvány kapcsán, például az arcfelismerés használatát a járványügyi intézkedések végrehajtásához.

2021. április 21-én megjelent a COM (2021) 206 final, 2021/0106 (COD) a mesterséges intelligenciára vonatkozó harmonizált szabályok (az MI-ről szóló jogszabály) megállapításairól. A javaslat célja a bizalmi ökoszisztéma kialakítására vonatkozó (Fehér könyv szerinti) második célkitűzés megvalósítása azáltal, hogy javaslatot tesz a megbízható mesterséges intelligenciára vonatkozó jogi keretre. A javaslat az uniós értékeken és az alapvető jogokon alapul, és arra irányul, hogy bizalmat ébresszen az egyénekben és más felhasználókban a mesterséges intelligencián alapuló megoldások alkalmazása iránt.

Az EU-ban 2021. május 20-án jelent meg az Európai Parlament és Tanács 2016/679 rendeletének (általános adatvédelmi rendelet, GDPR) kiegészítése a személyes adatok védelmével kapcsolatban, a bűncselekmények megelőzése, nyomozása, felderítése és üldözése céljából történő adatkezelésről szóló 2016/680 európai parlamenti és tanácsi rendelet.

Megjelent az európai adatkormányzásról szóló (2022/868 sz., Data Governance Act, továbbiakban DGA) rendelet, mely az uniós európai adatstratégia jogalkotási folyamatából indult ki. *„A DGA személyes adatokra és nem személyes adatokra is vonatkozik.* ***Adatnak*** *minősülnek az aktusok, tények vagy információk bármilyen digitális megjelenítése, vagy az említett aktusok, tények és információk összeállításai, többek között hang-kép- vagy audiovizuális felvétel formájában is. Ezen belül* ***személyes adat*** *a GDPR szerinti személyes adat, míg* ***nem személyes adat*** *minden a személyes adatoktól eltérő adat. (A DGA a nem személyes adatok vonatkozásában több olyan rendelkezést is tartalmaz, amely a GDPR alapján ismerősnek tűnhet, pl. az adattovábbításokkal kapcsolatban.). A DGA célja, hogy keretet teremtsen a közszférabéli szervezetek birtokában lévő olyan adatok további felhasználására, amelyek valamilyen szempontból*

védett kategóriába esnek, pl. kereskedelmi adatokra vonatkozó titoktartás, statisztikai adatvédelem, harmadik felek szellemitulajdon-jogainak védelme vagy személyes adatok védelme." [49] A rendeletet **2023. szeptember 24-től** kell alkalmazni.



2. ábra: Európai Unió adatvédelmi stratégia [49]

Megjelent a 2023. évi XLIII. törvény az egyének védelméről a személyes adatok gépi feldolgozása során. Minden fél felelőssége, hogy garantálja az adatkezelők és adott esetben az adatfeldolgozók által a személyes adatokhoz való illetéktelen hozzáférés, azok jogellenes megsemmisítése, elvesztése, felhasználása, módosítása vagy nyilvánosságra hozatala elleni védekezéshez szükséges intézkedések megtételét. Továbbá, kötelesek haladéktalanul értesíteni a 15. cikk szerinti felügyeleti hatóságokat adatvédelmi incidensek esetén, amennyiben azok komolyan sértik az érintettek jogait és alapvető szabadságait. Csak megfelelő biztosítékok mellett kezelhetők bizonyos kategóriákba tartozó adatok, mint például genetikai, büntetőügyi, biometrikus adatok, és azok, amelyek az egyén faji, etnikai, politikai, vallási, egészségügyi státuszára vagy szexuális életére utalnak. Ezeknek a biztosítékoknak meg kell védeniük az érintetteket az érzékeny adatok kezeléséből fakadó kockázatokkal, különösen a diszkrimináció veszélyével szemben.

2.2. Összefüggések a mesterséges intelligencia fejlődésével

Az alábbi alfejezetben kifejezetten az elmúlt pár év jogi és szabályzói fejlődését vizsgálom, és kutatom azokat a megerősítő tényeket, melyek alátámasztják azt a feltevésem, hogy az Európai Unió jogalkotói és szakmai szervezetei a különféle, 2022 végétől piacra lépett nagy nyelvi modellek, mesterséges intelligencia megoldások

hatására kiemelten kezdenek foglalkozni a személyes adatok kezelésével, és a szabályozottsági lemaradást a technika fejlődése mögött megpróbálják behozni, mely hatással lehet a biometrikus azonosítási megoldások szabályozására és elterjedésére is.

Az EU adatstratégiája, beleértve a GDPR szabályozást, a személyes adatok áramlására vonatkozó rendeleteket, a nyílt hozzáférésű adatokra vonatkozó irányelveket, az AI-stratégiát, nagymértékben összefügg a biometrikus adatok kezelésével, és így közvetetetten annak elterjedésével.

A GDPR szabályozás még nem tesz jelentős különbséget személyes adat és különleges adat (biometrikus adat) között, de később ezt a 2016/679 EU Parlament és a Tanács rendelete már alkalmazza [50].

- „személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;
- „adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;
- „biometrikus adat”: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;

Az MI technológiáktól széles körű gazdasági és társadalmi előnyöket várnak el különböző szektorokban, ideértve a környezetvédelmet és az egészségügyet, a közszférát, pénzügyi területet, mobilitást, belügyi területet és mezőgazdaságot is. Különösen hasznosak lehetnek az előrejelzés jellegű megoldásokban, a folyamatok és az erőforrások optimalizálásában, valamint a szolgáltatások személyre szabásában. Azonban az MI rendszerek következtében az alapvető jogokra gyakorolt hatások, amelyek az EU Alapjogi Chartája által védettek, valamint azok a biztonsági kockázatok, amikor az MI

technológiákat termékek és szolgáltatások részeként alkalmazzák, aggodalmakat vetnek fel. Különösen az AI rendszerek veszélyeztethetik az alapvető jogokat, mint például a diszkriminációmentesség joga, a szólásszabadság, az emberi méltóság, személyes adatvédelem és magánélet jogai. Tekintettel ezeknek a technológiáknak a gyors fejlődésére, az utóbbi években az MI szabályozása központi kérdéssé vált az Európai Unióban. A döntéshozók azt ígérték, hogy kidolgoznak egy „emberközpontú" megközelítést az MI-hez, hogy biztosítsák, hogy az európaiak használhassák az új technológiákat az EU értékei és elvei szerint kifejlesztve és működve. A 2020-as Mesterséges Intelligencia fehér könyvében (COM (2020) 65 final, Fehér könyv a mesterséges intelligenciáról) az Európai Bizottság elkötelezte magát az MI elterjedésének előmozdítása mellett és az ehhez a technológiához kapcsolódó bizonyos felhasználási kockázatok kezelése mellett. Az anyagban szoros összefüggés található az MI elterjedése, a személyes adatok védelme, a biometrikus adatok és azok védelme és ezáltal a biometrikus azonosítási megoldások elterjedése között. Habár az Európai Bizottság kezdetben lágy jogi megközelítést alkalmazott a 2019-es Etikai Iránymutatásaival és a Bizalomra méltó MI-re vonatkozó ajánlásaival, azóta áttért egy jogalkotási megközelítésre, és az MI rendszerek fejlesztésére, piacra dobására és használatára vonatkozó harmonizált szabályok elfogadását szorgalmazza.

Az EU-n kívülre, nemzetközi szintre kitekintve, az Egyesült Államok kezdetben enyhébb álláspontot foglalt el az MI-vel kapcsolatban, az utóbbi időben egyre hangosabbak lettek a szabályozásra vonatkozó felhívások [51]. Kína Kiberterületi Adminisztrációja is konzultált egy MI szabályozási javaslatról [52], míg az Egyesült Királyság egy innovációbarát szabályozási elvek rendszerén dolgozik [53]. Nemzetközi szinten az Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) 2019-ben elfogadott egy (nem kötelező érvényű) ajánlást az MI terén [54], az UNESCO 2021-ben Ajánlásokat fogadott el az MI etikájáról [55], és a Európa Tanács jelenleg egy nemzetközi egyezményen dolgozik az MI területén [56]. Ezenfelül az újonnan létrehozott EU-USA technológiai partnerség keretében (a Kereskedelmi és Technológiai Tanács), az EU és az USA igyekszik kialakítani egy közös megértést az olyan elvekről, amelyek pontosan meghatározzák a megbízható és felelős MI-t. Az EU törvényhozói 2023 májusában közös állásfoglalást adtak ki, amelyben felszólították Biden elnököt és az Európai Bizottság elnökét, Ursula von der Leyen-t, hogy hívjanak össze egy csúcstalálkozót annak érdekében, hogy megoldást találjanak a fejlett MI rendszerek, például a ChatGPT fejlesztésének ellenőrzésére.

A mesterséges intelligencia alapú rendszerek és szolgáltatások gyorsan fejlődnek. Meg fogják változtatni életünket azáltal, hogy javítják az egészségügyi ellátást (pontosabbá teszi a diagnosztikát, lehetővé teszik a betegségek hatékonyabb megelőzését), növelik gazdálkodásunk hatékonyságát, hozzájárulnak az éghajlatváltozás mérsékléséhez és az ahhoz való alkalmazkodáshoz, a megelőző karbantartások révén javítják a termelési rendszerek hatékonyságát, növelik az európai polgárok biztonságát, és számos egyéb módon is hatással lesznek ránk, amelyről ma még csak álmodunk. Ugyanakkor a mesterséges intelligencia rendszerek számos olyan potenciális kockázattal is járnak, mint az átláthatatlan döntéshozatal, a nemi és más alapon történő megkülönböztetés, a magánéletünkbe való betolakodás, vagy a bűncselekmények céljából történő felhasználás.

A mesterséges intelligencia alkalmazása során adatokat kombinálnak algoritmusokkal és számítási teljesítménnyel. Ezért a mesterséges intelligencia modern világunkban megfigyelhető előretörésének fő mozgatórugói a számítástechnika fejlődése és az adatok egyre nagyobb mértékű, gyors rendelkezésre állása lesz.

A mesterséges intelligenciára vonatkozó jövőbeli európai szabályozási keret kulcsfontosságú elemei egyedülálló „bizalmi ökoszisztémát” hoznak létre. E célból biztosítani kell az uniós szabályoknak – köztük az alapvető jogok védelmére és a fogyasztóvédelemre vonatkozó szabályoknak – való megfelelést, mindenekelőtt az EU-ban üzemeltetett, nagy kockázatot jelentő MI-rendszerek esetében (ide nem értve a bűncselekmények megelőzése és feltárása céljából alkalmazott megoldásokat, mert ezekre más szabályok vonatkoznak). A bizalmi ökoszisztéma kiépítése önmagában is EU-s politikai célkitűzés, amelynek bizalmat kell ébresztenie a polgárokban a mesterséges intelligenciával kapcsolatos alkalmazások iránt, valamint jogbiztonságot kell nyújtania a vállalatok és az állami szervezetek számára a mesterséges intelligenciát használó innovációhoz. A Bizottság határozottan támogatja „Az emberközpontú mesterséges intelligencia iránti bizalom növelése” című közleményben (COM (2019) 168) körvonalazott emberközpontú megközelítést, valamint figyelembe fogja venni a magas szintű MI-szakértői csoport által kidolgozott etikai iránymutatások kísérleti szakaszában szerzett információkat is.

Az EU-szintű vita élén, az Európai Parlament arra kérte az Európai Bizottságot, hogy értékelje az MI hatásait, és dolgozzon ki egy EU keretrendszert az MI területén, széleskörű 2017-es ajánlásaiban [57], amelyek a robotika polgári jogi szabályairól szóltak. Azóta, 2020-ban és 2021-ben, a Parlament számos nem jogalkotási állásfoglalást

fogadott el, amelyek az EU intézkedéseit sürgették, valamint két jogalkotási állásfoglalást, amelyek az MI területén az EU jogalkotás elfogadását kérték. Az első jogalkotási állásfoglalás [58] arra kérte a Bizottságot, hogy hozzon létre egy jogi keretet az etikai elvek tekintetében az MI, a robotika és a kapcsolódó technológiák fejlesztése, bevezetése és használata számára az Unióban. A második jogalkotási állásfoglalás a polgári felelősség igényeinek jogi keretének harmonizációját és szigorú felelősségi rendszer bevezetését szorgalmazta a magas kockázatú MI rendszerek üzemeltetői számára [59]. Ezenkívül a Parlament elfogadott egy sor ajánlást, amelyek az EU közös megközelítésére szólítottak fel az MI területén az iparjogvédelem, büntetőjog, oktatás, kultúra, audiovizuális területeken, valamint a polgári és katonai AI használat tekintetében.

Az Európai Tanács korábban többször is felszólította Bizottságot a közös MI-szabályok elfogadására, beleértve azt is 2017-ben és 2019-ben. Az utóbbi időben, 2020-ban a Tanács arra kérte a Bizottságot, hogy terjesszen elő konkrét javaslatokat, amelyek figyelembe veszik a meglévő jogszabályokat, és kövessék a kockázatalapú, arányos és szükség esetén szabályozó megközelítést [60]. Ezenkívül a Tanács felkérte az EU-t és a tagállamokat, hogy fontolják meg hatékony intézkedéseket a digitális technológiák, beleértve az MI-t, potenciális hatásainak azonosítása, előrejelzése és reagálása érdekében a fundamentális jogokra.

A 2020 februárjában elfogadott Mesterséges Intelligencia Fehér Könyvet követően a Bizottság kiterjedt nyilvános konzultációt indított [61], és közzétett egy hatásvizsgálatot az MI szabályozásáról [62], egy támogató tanulmányt [63] és egy tervezetet [64], amelyekre különböző érdekelt felek visszajelzése érkezett. A hatásvizsgálatában a Bizottság számos problémát azonosít az MI rendszerek fejlesztése és használata során, azok sajátos jellemzői miatt. A 2021 áprilisában bemutatott AI szabályozás tervezet egy horizontális EU jogalkotási eszközként lett kialakítva, és alkalmazható minden olyan MI rendszerre, amelyet az Unió piacára készítenek vagy használnak. Általános célja az, hogy biztosítsa a belső piac megfelelő működését olyan feltételek létrehozásával, amelyek lehetővé teszik a megbízható MI rendszerek fejlesztését és használatát az Unióban. A tervezet egy harmonizált jogi keretrendszert állít fel az AI termékek és szolgáltatások fejlesztéséhez, azoknak az Unió piacára való bevezetéséhez és használatához. Emellett az AI-állás tervezete számos konkrét célt tűz ki: (i) biztosítani, hogy az EU piacán lévő MI rendszerek biztonságosak legyenek, és tiszteletben tartsák az érvényben lévő EU jogszabályokat, (ii) jogbiztonságot teremteni az AI-be való befektetés és innováció

elősegítése érdekében, (iii) fokozni az EU jogszabályok alapján érvényesülő alapvető jogok és az AI rendszerekre vonatkozó biztonsági követelmények hatékony végrehajtását, valamint (iv) elősegíteni a törvényes, biztonságos és megbízható AI alkalmazások egységes piacának kialakítását, és megakadályozni a piaci fragmentációt.

Az új AI keretrendszer, az Európai Unió Működéséről Szóló Szerződés (Treaty on the Functioning of the European Union, továbbiakban: TFEU) 114. és 16. cikkén alapulva, technológiafüggetlen meghatározást rögzítene az AI rendszerekre és egy kockázatalapú megközelítést alkalmazna, amely eltérő követelményeket és kötelezettségeket határozna meg az AI rendszerek fejlesztése, azok piacra dobása és felhasználása terén az EU-ban. Gyakorlatban a javaslat meghatározza a piacra kerülés előtti AI rendszerek tervezésére és fejlesztésére vonatkozó kötelező általános követelményeket, és harmonizálja az utólagos ellenőrzések módját. A tervezett AI szabályozás kiegészítené a meglévő és a várható, horizontális és szektorális EU biztonsági szabályozásokat. A Bizottság azt javasolja, hogy kövessék az új jogalkotási keret (New Legislative Framework, továbbiakban: NLF [65]) logikáját, azaz az EU megközelítését, amely biztosítja, hogy a termékek széles skálája megfeleljen az alkalmazandó jogszabályoknak, amikor azokat az EU piacra helyezik ki, az egyezőségi értékelések és a CE-jelölés használatával. Az új szabályok elsősorban az EU-n belül működő AI rendszerek szolgáltatóira, vagy harmadik országokban működő AI rendszerekre alkalmazandók, amelyeket az EU piacra helyeznek ki vagy használnak az EU területén. Annak érdekében, hogy elkerüljék a szabályozás kijátszását, az új szabályok alkalmazódnak azokra a szolgáltatókra és felhasználókra is, akik harmadik országokban helyezkednek el, ahol az általuk létrehozott rendszerek kimenetét az EU-ban használják. Azonban a tervezett rendelet nem alkalmazható kizárólag katonai célokra fejlesztett vagy használt AI rendszerekre, harmadik országok közintézményeire, nemzetközi szervezetekre vagy hatóságokra, amelyek AI rendszereket alkalmaznak a jogi együttműködés és az igazságügyi együttműködés keretében kötött nemzetközi egyezmények alapján.

A Mesterséges Intelligencia definíciója

Az tudományos közösség által elfogadott mesterséges intelligenciának egyetlen meghatározása nincs [66], és az 'MI' kifejezést gyakran használják egyfajta általános kifejezésként különböző számítógépes alkalmazásokra, amelyek különböző technikákon

alapulnak, és olyan képességeket mutatnak, amelyeket általában és jelenleg az emberi intelligenciával társítanak.

A Fehér könyv [67] előzménye, a COM (2018) 237 final: *„A mesterséges intelligencia intelligens viselkedésre utaló rendszereket takar, amelyek konkrét célok eléréséhez elemzik a környezetüket és – bizonyos mértékű autonómiával – intézkedéseket hajtanak végre. A mesterséges intelligencián alapuló rendszerek lehetnek kizárólag szoftver-alapú rendszerek, amelyek a virtuális világban működnek (pl. hangasszisztensek, képelemző szoftverek, keresőprogramok, hang- és arcfelismerő rendszerek), illetve a mesterséges intelligencia beépíthető hardvereszközökbe is (pl. fejlett robotok, autonóm járművek, drónok és a tárgyak internetéhez kapcsolódó alkalmazások).”* [68, p. 1]

Az MI terén tevékenykedő Felső Szintű Szakértői Csoport javasolt egy alapvető MI-definíciót, amelyet egyre inkább alkalmaznak a tudományos irodalomban. A COM(2018) 237 final, 8. o.: *„A mesterséges intelligencián (Artificial Intelligence – AI) alapuló rendszerek olyan, emberek által megtervezett szoftverrendszerek (és lehetőség szerint hardverrendszerek), amelyek összetett céljukra tekintettel a fizikai vagy a digitális dimenzióban úgy működnek, hogy a környezetüket adatszerzés révén észlelik, értelmezik a gyűjtött strukturált és nem strukturált adatokat, ismereteik alapján érvelnek, vagy ezekből az adatokból származó információkat dolgoznak fel, valamint eldöntik, hogy az adott cél eléréséhez melyek a leghatékonyabb intézkedések. Az MI-rendszerek használhatnak szimbolikus szabályokat, vagy numerikus modellt is betanulhatnak, és a magatartásukat is megváltoztathatják annak elemzése révén, hogy a korábbi intézkedések hogyan hatottak a környezetre.”* [68, p. 8]

A Bizottság azonban úgy találta, hogy az 'MI rendszer' fogalmát tisztábban kellene meghatározni, tekintettel arra, hogy az új AI keretrendszer alatt a jogi felelősségek meghatározása szempontjából kritikus, mi is számít 'MI rendszernek'. A Bizottság ezért javasolja, hogy létre kell hozni egy 'MI rendszer' jogi meghatározását az EU jogában, amely nagyrészt az OECD által már használt definícióra épül.

A tervezet 3. cikk (1) bekezdése kimondja, hogy az 'mesterséges intelligencia rendszer' azt jelenti: *„…olyan szoftver, amely [az 2. mellékletben felsorolt* [69]*] módszerekkel és megközelítésekkel készült, és adott emberi meghatározott célokra olyan kimeneteket generálhat, mint tartalom, előrejelzések, javaslatok vagy az általa interaktáló környezeteket befolyásoló döntések”*. A javaslat 1. melléklete felsorolja azokat a módszereket és megközelítéseket, amelyeket ma használnak az MI rendszerek fejlesztéséhez. Ennek megfelelően az 'MI rendszer' fogalma szoftveralapú technológiákat

foglal magában, mint például a 'gépi tanulás', 'logikai és tudásalapú' rendszereket és 'statisztikai' megközelítéseket. Ez a széleskörű meghatározás magában foglalja az olyan MI rendszereket, amelyek önállóan vagy termék részeként használhatók. Ezenkívül a tervezett jogszabály jövőbiztosnak szándékozik lenni, és lefedni a jelenlegi és a jövőbeni MI technológiai fejleményeket. Ebből a célból a Bizottság kiegészítené az 1. melléklettel az új megközelítéseket és technikákat, amelyeket az MI rendszerek fejlesztéséhez alkalmaznak, ahogyan azok előkerülnek - a delegált jogi aktusok elfogadásával (4. cikk). Ezenkívül a 3. cikk hosszú definíciós listát tartalmaz, ideértve az 'MI rendszer' szolgáltatóját és felhasználóját (mind a köz- és magánszervezetekre vonatkozóan), valamint az 'importőrt' és a 'forgalmazót', az 'érzelemfelismerést' és a 'biometrikus kategorizálást'.

„A biometrikus adatok távoli azonosítás céljára való gyűjtése és felhasználása – például arcfelismerő rendszerek nyilvános helyeken való alkalmazása révén – egyedi kockázatokat hordoz az alapvető jogokra nézve. Például az emberek méltóságára nézve. Ehhez kapcsolódik, hogy az arcfelismerési technológia használatát érintően az alapvető jogok megsértésére vonatkozó aggályok elsősorban a magánélet tiszteletben tartásához és a személyes adatok védelméhez való joggal kapcsolatosak." [68, pp. 9-13]

Ez hatással lehet a megkülönböztetésmentességre és a különleges csoportok – például a gyermekek, az idősek és a fogyatékossággal élő személyek – jogaira is. Továbbá a technológia használata nem veszélyeztetheti a véleménynyilvánítási, az egyesülési és a gyülekezési szabadságot sem. A távoli biometrikus azonosításra szolgáló MI-rendszerek használatának alapvető jogokat érintő következményei a használat céljától, körülményeitől és hatókörétől függően jelentősen eltérőek lehetnek.

Az uniós adatvédelmi szabályok alapesetben tiltják a biometrikus adatoknak a természetes személyek egyedi azonosítása céljából történő kezelését, és ez alól csak bizonyos feltételek mellett engednek kivételt. (Az általános adatvédelmi rendelet 9. cikke, a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv 10. cikke, illetve még az uniós intézményekre és szervekre alkalmazandó (EU) 2018/1725 rendelet 10. cikke alapján.)

Az általános adatvédelmi rendelet szerint ilyen adatkezelésre konkrétan csak korlátozott számú okból kerülhet sor, elsősorban alapvető közérdekből. Ezt a fajta adatkezelést uniós vagy nemzeti jog alapján lehet csak végezni, az arányosság követelményének és az adatvédelemhez való jog lényegének tiszteletben tartásával, megfelelő biztosítékok mellett. A bűnüldözésben érvényesítendő adatvédelemről szóló

irányelv értelmében ilyen adatkezelés csak szigorú szükségesség esetén, alapesetben uniós vagy nemzeti jog szerinti engedéllyel és megfelelő biztosítékok mellett végezhető. Mivel a biometrikus adatoknak valamely természetes személy egyedi azonosítása céljából történő bármely kezelése szabályozott esetet jelent az uniós jogban meghatározottak alapján, ezért az Európai Unió Alapjogi Chartájának hatálya alá tartozik. Következésképpen a jelenlegi uniós adatvédelmi szabályoknak és az Alapjogi Chartának megfelelően a mesterséges intelligencia csak akkor használható fel távoli biometrikus azonosítás céljára, ha az ilyen felhasználás kellően indokolt, arányos és megfelelő biztosítékok mellett történik. A távoli biometrikus azonosítást meg kell különböztetni a biometrikus azonosítástól, mert az MI alkalmazások kifejezetten alkalmasak távoli biometrikus azonosításre és más intruzív megfigyelési célokra történő felhasználásra és ezért mindig „nagy kockázatúnak" kell minősíteni, vagyis ilyen esetekben mindig alkalmazandók a kötelező követelmények [67, p. 22].

„A mesterséges intelligencia fejlesztőire és alkalmazóira már ma is alkalmazandók az alapvető jogokra (pl. adatvédelem, magánélet védelme, megkülönböztetésmentesség), a fogyasztóvédelemre, valamint a termékbiztonságra és termékfelelősségre vonatkozó uniós jogszabályok. A fogyasztók ugyanilyen szintű biztonságot és jogokat várnak el, függetlenül attól, hogy egy termék vagy egy rendszer a mesterséges intelligenciára támaszkodik-e vagy sem. A mesterséges intelligencia bizonyos sajátosságai (pl. átláthatatlanság) azonban megnehezíthetik e jogszabályok alkalmazását és végrehajtását. Ezért meg kell vizsgálni, hogy a jelenlegi jogszabályok képesek-e kezelni a mesterséges intelligencia kockázatait, és a végrehajtásuk hatékonyan kikényszeríthető-e, vagy a jogszabályok kiigazítása, esetleg új szabályozás kialakítása szükséges.

A mesterséges intelligencia által fokozottan lehetővé válik az emberek mindennapi szokásainak figyelemmel kísérése és elemzése. Fennáll például annak a kockázata, hogy a mesterséges intelligenciát az uniós adatvédelmi és egyéb szabályokat sértő módon, állami hatóságok vagy más szervek tömeges megfigyelésre, a munkáltatók pedig munkavállalóik viselkedésének megfigyelésére használhatják. Nagy adatmennyiségek elemzésével és az adatok közötti összefüggések azonosításával a mesterséges intelligencia személyek adatainak visszakeresésére és anonim jellegének megszüntetésére is felhasználható lehet, ami új személyesadat-védelmi kockázatokat teremt olyan adatkészletek esetében is, amelyek önmagukban véve nem tartalmaznak személyes adatokat." [70]

Véleményem szerint itt kapcsolódik össze a mesterséges intelligencia felhasználása és a biometrikus azonosítás elterjedésének kérdése, mert az AI használatával és az adatelemzésekkel nagymértékben nő a kockázat, hogy megfelelő szabályozás nélkül az anonim adatokból az algoritmusokkal biometrikus azonosítás történik. Ez alapján alátámasztható a hipotézisen (H2), a biometria elterjedésének tényezői jelentősen összefüggenek az adatvédelmi, adatkezelési és a mesterséges intelligencia szabályozásokkal, melyek véleményem szerint abba az irányba mutatnak, hogy ahogyan az informatikai biztonságot is kockázat alapon kell megítélni, úgy a mesterséges intelligencia keretrendszerét és a biometrikus megoldások szabályozását is kockázati alapon, a felhasználási terület függvényében kell kialakítani. Az viszont kimondható, hogy a 2021 előtti időszakra jellemző, adatvédelemre vonatkozó jogi, szabályzói hiányosságokat az EU hatékonyan elkezdte ledolgozni. Az Európai Bizottság 2021 áprilisában előterjesztett egy javaslatot az Európai Unió AI szabályozási keretrendszeréről. Az AI-tervezet az első olyan kísérlet, amely egy átfogó szabályozást hozna létre a területen. A javasolt jogi keret az AI rendszerek konkrét felhasználására és az ezzel járó kockázatokra összpontosít. A Bizottság azt javasolja, hogy az EU jogszabályokban technológiától függetlenül definiálja az AI rendszereket, és osztályozást állítson fel különböző követelményekkel és kötelezettségekkel egy 'kockázatalapú megközelítésen' alapulva. Néhány AI rendszer, amely "elfogadhatatlan" kockázatokat mutatna, tilos lenne. Számos "magas kockázatú" AI rendszer engedélyezett lenne, de bizonyos követelmények és kötelezettségek mellett, hogy hozzáférést szerezzen az EU piacához. Azok az AI rendszerek, amelyek csak "korlátozott kockázatot" jelentenek, nagyon könnyű átláthatósági kötelezettségeknek lennének kitéve. A Tanács 2021 decemberében elfogadta az EU tagállamok általános álláspontját, majd a Parlament 2023 júniusában szavazott róla. Az EU jogalkotók most tárgyalásokat kezdenek az új jogszabály véglegesítéséhez, jelentős módosításokkal a Bizottság javaslatához, beleértve az AI rendszerek definíciójának felülvizsgálatát, a tiltott AI rendszerek listájának kibővítését, valamint kötelezettségeket az általános célú AI és generatív AI modellekre.

Az EU szabályozási folyamata rámutatott arra, hogy a mesterséges intelligencia meghatározása mellett fontos a "kockázat", a "magas kockázat", az "alacsony kockázat", a "távoli biometrikus azonosítás" és a "kár" fogalmának meghatározása is. A szakértői csoportok és a konzultációban résztvevő piaci szereplők többsége kifejezetten támogatta a kockázatalapú megközelítést. A válaszadók úgy vélték, hogy a kockázatalapú keretrendszer alkalmazása jobb megoldást nyújt, mint az általános szabályozás, amely

minden MI-rendszert érint. A kockázatokat és fenyegetéseket ágazati és eseti alapú megközelítéssel kell kezelni. A kockázatok kiszámításánál figyelembe kell venni a jogokra és a biztonságra gyakorolt hatást.

Véleményem szerint ez kifejezetten igaz általánosságban a biometrikus rendszerekkel kapcsolatos kockázatokra is.

A nagy kockázatú MI rendszerek és a távoli biometrikus azonosítás kockázatai a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításai közül (2021/0106 (COD)): A távoli biometrikus azonosító rendszer e rendeletben használt fogalmát funkcionális értelemben kell meghatározni, olyan AI-rendszerként, amelynek célja természetes személyek távolról történő azonosítása a személy biometrikus adatainak egy referencia-adatbázisban szereplő biometrikus adatokkal való összevetése révén, anélkül, hogy előzetesen tudomása lenne arról, hogy a célszemély jelen lesz-e és azonosítható-e, függetlenül az alkalmazott konkrét technológiától, folyamatoktól vagy a biometrikus adatok típusától. Figyelembe véve eltérő jellemzőiket és használati módjaikat, valamint a különböző kockázatokat, különbséget kell tenni a „valós idejű" és a „nem valós idejű" távoli biometrikus azonosító rendszerek között. A „valós idejű" rendszerek esetében a biometrikus adatok rögzítése, összehasonlítása és azonosítása azonnal, majdnem azonnal vagy mindenesetre jelentős késleltetés nélkül történik. E tekintetben nem engedhető meg, hogy a szóban forgó AI-rendszerek „valós idejű" használatára vonatkozó kisebb késleltetésekre legyen lehetőség, és ezáltal az e rendeletben foglalt szabályokat bárki megkerülje. A „valós idejű" rendszerek olyan „élő" vagy megközelítőleg „élő" anyagot, például videofelvételt használnak, amelyet kamera vagy hasonló funkciójú más eszköz generál. A „nem valós idejű" rendszerek esetében ezzel szemben a biometrikus adatokat már rögzítették, és az összevetésre és az azonosításra csak jelentős késleltetéssel kerül sor. Olyan anyagokról van szó, mint például a zártláncú televíziós kamerák vagy magánkészülékek által előállított képek vagy videofelvételek, amelyek a rendszer érintett természetes személyek tekintetében történő használata előtt keletkeztek.

Az AI-rendszereknek természetes személyek „valós idejű" távoli biometrikus azonosítására, a nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő használata különösen betolakodik az érintett személyek jogaiba és szabadságába, mivel hatással lehet a lakosság nagy részének magánéletére, az állandó megfigyelés érzetét keltheti, és közvetve visszatarthat a gyülekezési jog szabadsága és más alapvető jogok gyakorlásától. Ezenkívül a hatás azonnali jellege és az ilyen „valós időben"

működő rendszerek használatával kapcsolatos további ellenőrzések vagy korrekciók korlátozott lehetőségei fokozott kockázatot jelentenek a bűnüldözési tevékenységek által érintett személyek jogaira és szabadságaira nézve. E rendszerek bűnüldözési célú használatát ezért meg kell tiltani, kivéve három, kimerítő jelleggel felsorolt és szűken meghatározott helyzetet (áldozatok felkutatása, terrortámadás veszélye, illetve speciális esetekben bűncselekmények felderítése), amelyekben a használat feltétlenül szükséges egy olyan jelentős közérdek érvényesítéséhez, amelynek fontossága meghaladja a kockázatokat [71].

A mesterséges intelligencia alapú rendszerek, melyeket elemzésekre, következtetésekre és másodlagos, harmadlagos folyamatok során azonosítási feladatokra lehet alkalmazni, vagy a bűnüldözésben megelőzés céllal használni, különösen sok társadalmi vitát és megosztottságot fog okozni véleményem szerint. Nagyon érzékenyen kell ezt a területet kezelni, és minél előbb az összes érintett bevonásával széles körben társadalmi és szakmai fórumokon keresztül egyeztetéseket folytatni a szabályozásról, mert a nem jól kezelt és alulszabályozott folyamatok, a megoldások visszaéléssel kapcsolatos lehetőségei miatt hatványozottan negatívan hathatnak a biometria elterjedésére.

2.2.1. A kockázatértékelés keretrendszere

Olyan világot élünk, ahol fokozódnak a nemzetközi konfliktusok, egyre több fronton nyílnak fegyveres összetűzések, az országok és a régiók fokozzák a hadi kiadásokra fordított kereteket, akkor a lakosság biztonságérzete csökken. Ilyen helyzetben természetes lehet a biztonságnövelő megoldások növekvő elfogadottsága (biztonság utáni vágy, mint alapszükséglet), éppen ezért ezek kockázataival is érdemes tisztában lenni. A kockázatok értékelésére szabványok, keretrendszerek állnak rendelkezésre, melyek részletes bemutatására nem térek ki, mert nem az értekezés témája. Munkám során az International Standard, IEC/FDIS 31010:2009 szabványt vettem alapul [72].

A kockázat becslés a kockázat azonosításból, a kockázatelemzésből és a kockázat értékelésből áll. A kockázatokat általában szervezeti szinten, osztályok szintjén, projecteknél, vagy egyedi tevékenységeknél értékelhetők. Különböző eszközök és technikák alkalmazhatók a különböző kontextusokban.

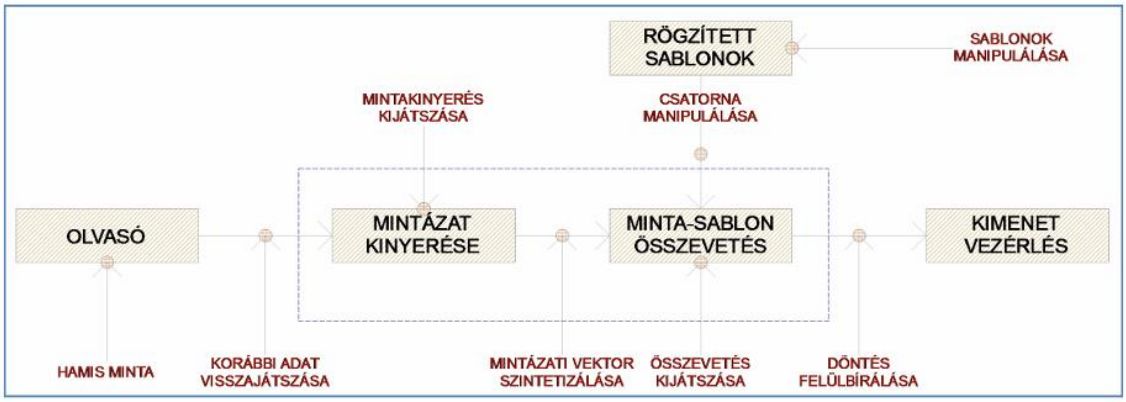
A kockázatazonosítás magába foglalja a kockázat okainak és forrásainak felkutatását és leírását. Ennek módszerei az evidencia alapú módszer, ahol check-listák és történelmi adatok alapján történik az áttekintés, a rendszeres csoportmódszer, ahol egy szakértőkből álló csapat rendszeres folyamatot követ a kockázatok azonosításához egy strukturált kérdéssorozat alkalmazásával és az induktív következtetési technikák módszer, például a Hazard and Operability módszer (továbbiakban: HAZOP).

A kockázatelemzés tartalmazza a kockázati események következményeinek és valószínűségeinek a meghatározását és kombinálását annak megállapítására, hogy milyen szintű a kockázat. A kockázatok elemzésére alkalmazott módszerek lehetnek minőségi, fél-kvantitatív vagy kvantitatív jellegűek. A részletesség mértéke a konkrét alkalmazástól, a rendelkezésre álló megbízható adatoktól és még szervezeti, vagy a felhasználási területi tényezőktől is függ. A minőségi értékelés a következményt, a valószínűséget és a kockázat szintjét olyan jelentőségi szintekkel határozza meg, mint "magas", "közepes" és "alacsony", összevonhatja a következményeket és a valószínűséget, és a kapott kockázatszintet minőségi kritériumokkal összeveti. Kutatásom során én is ezt a módszert használtam, így a kockázatértékelés magában foglalja a becsült kockázati szintek összehasonlítását a meghatározott kockázati kritériumokkal, annak érdekében, hogy meghatározzuk a kockázat mértékének és típusának jelentőségét.

Valamennyi szemponthoz három értékelési kimenet (válasz) rendelhető	
Kockázat szempontból nem elfogadható	magas
Kockázat szempontból nem optimális	közepes
Kockázat szempontból optimális	alacsony

A szempontrendszer alapjai

Az általam kidolgozott szempontrendszer azt mutatja be, hogy a különböző felhasználási területeken alkalmazott biometrikus azonosítási megoldások különböző szempontok alapján milyen eltérő kockázatot képviselnek. A biometrikus azonosítási rendszerek sérülékenységi lehetőségeit figyelembe véve a kockázatok vizsgálata szempontjából kizárom azokat a tényezőket, melyek az azonosítási rendszer informatikai komponenseivel (3. ábra) vannak összefüggésben, illetve a felhasználási területtel összefüggő szempontokat is, és csak az azonosításokat az azonosítási eljárás fajtája és a mintaadás szempontjából vizsgálom.



3. ábra: Egy általános biometrikus azonosítási rendszer sérülékenységi lehetőségei [73, pp. 223-228]

2.2.2. A biometrikus azonosítási megoldások és a kockázatok kapcsolata

A biometrikus azonosítási megoldások jellemzői alapján vizsgálható a felhasználók szempontjából a kockázat. Fontos kiemelni, hogy általában a kockázatelemzés nagyban függ a helyi specifikumoktól, mint a felhasználás környezete, a felhasználás célja és módja, a kiszolgáló informatikai környezet paramétereitől és még számos tényezőtől is. Az általam meghatározott 14 paraméterrel - megítélésem szerint - elvégezhető egy független, általános vizsgálat a biometrikus azonosítási megoldások kockázataival kapcsolatban. Meglátásom szerint ezek a kockázatok összefüggésben vannak az azonosítási megoldások elterjedésével.

Egyetemesség (universality)

A vizsgált környezetben a biometrikus minta minden alany esetében kinyerhető legyen. Az egyetemesség mérésére alkalmazható mérőszám a Failure to Enroll (továbbiakban FTE), amely megmutatja az adott környezetre vonatkoztatva, hogy milyen arányban fordulnak elő azon személyek, akik mintái az adott biometrikus azonosítási technikával nem ismerhetőek fel, így már a sablon kinyerése is akadályba ütközik. Az általános cél az, hogy a felhasználási terület ismeretében minél szélesebb körben, minden felhasználóra alkalmazható legyen az azonosítási technika, de kockázat szempontjából minél több személy esetén alkalmazható, annál nagyobb kockázatot jelent [32, pp. 29-30.].

Az azonosításhoz használt minták az emberi test geometriai vagy viselkedési jellemzőiből, vagy ezekből származtatott, következtetett adatokból származnak, de a népességet tekintve ez nem minden esetben áll rendelkezésre. Az arcfelismerésnél, az

érhálózat alapú megoldásoknál, a DNS azonosításnál, a hang alapú megoldásoknál és a szokáselemzésen alapuló megoldásoknál egyetemesség szempontjából kevesebb kizáró tényező áll rendelkezésre a többi megoldáshoz képest. Aláírás esetén az írástudatlanság, kézgeometria, retina, írisz és ujjnyomat esetén testi, biológiai eredetű hiányosságok és fogyatékosságok miatt vannak kizáró tényezők, pl. a népesség 1-3 százalékának nem áll rendelkezésre és nem megfelelő az ujjnyomata [74].

Egyediség (uniqueness)

A biometrikus minta egyedisége biztosítja az egyének megkülönböztetését. Minden mintának szükséges, hogy legyen egyedi azonosításra alkalmas mintázata, amely alapján megkülönböztethető más mintáktól. A minták hasonlósága magas FAR és FRR értékeke eredményez, amely kihat az azonosítás biztonságára és egyben a kockázataira [74, pp. 6-7.]. A leginkább egyedi mintázatok az írisz, az ujjnyomat, az arc, az érhálózat, egyediség szempontjából a kisebb kockázatot jelentik [75] [76] [77]. Kevés kutatás áll még rendelkezésre, véleményem szerint a kevésbé egyedi minták alapján történő azonosítási megoldások nagyobb kockázatot képviselnek [78].

Elfogadottság (acceptability)

Az azonosítási megoldásokkal kapcsolatban számos félelem és ellenézés alakulhat ki egyéni és társadalmi szinten is. Az elfogadottság azt jelenti, hogy a rendszert használó egyén mennyire együttműködő az azonosítási folyamat során, vagy az ellenérzései miatt befolyásoló tényező lép fel a mintaadás elvégzése során. Fontos szempont, hogy az azonosítás során az egyén bevonódása a folyamatba ne legyen túlzott mértékű. A retina azonosítással kapcsolatban ismertek a félelmek, sokan vélik ártalmasnak a szem megvilágítását (vagy legalább tartanak egészségkárosító hatásától), és a szenzor szemhez túl közeli pozicionálása sem közkedvelt. Az ujjnyomat- és DNS alapú azonosítási technológiák alkalmazása szorosan kapcsolódik a bűnüldözési és kriminalisztikai tevékenységekhez, amelyek jelentős mértékben befolyásolják a módszer percepcióját és elfogadottságát a társadalomban [32, pp. 29-30.] [74, pp. 6-7.].

Kijátszhatóság (circumvention)

A biometrikus azonosítási megoldások kapcsán a kijátszhatóság (spoofing vagy impersonation attack) egy olyan biztonsági kihívást jelent, amelyben egy támadó szándékosan próbálja megtéveszteni a biometrikus rendszert, hogy az tévesen hitelesítse

őt egy másik, jogos felhasználóként. Ez általában úgy történik, hogy a támadó utánozza vagy reprodukálja a jogos felhasználó biometrikus adatait – például ujjlenyomatot, arcképet, íriszképet vagy hangmintát –, és ezeket az adatokat használja fel az azonosító rendszer megtévesztésére. A kijátszhatóság mértékét gyakran a rendszer által a hamisítási kísérletekkel szemben tanúsított ellenálló képessége határozza meg. A magas szintű biztonságú biometrikus rendszerek fejlett detektálási mechanizmusokkal rendelkeznek a hamisítási kísérletek felismerésére, így csökkentve a sikeres támadások valószínűségét [31] [79] [80] [81] [82].

Elérhetőség (availability)

Az ismert technológiák segítségével hatékonyan megszerezhető az az információ, amely a biometrikus minták egyediségét kódolja, ami kulcsfontosságú szerepet játszik abban, hogy mennyire egyszerű a mintából az azonosításhoz szükséges képet előállítani. Fontos megjegyezni, hogy nem minden biometrikus jellemző áll rendelkezésre egyszerűen. Könnyen kinyerhető adatok esetén az illetéktelenek számára is könnyebb lesz hozzáférniük és felhasználniuk őket, így nagyobb a kockázat, míg nehezen kinyerhető adatoknál az illetéktelenek számára is nehezebb lesz hozzáférniük és felhasználniuk őket. Arcfelismerés esetén a minta elérhetősége jobb, egy fénykép vagy video alapján is könnyen elvégezhető, míg mondjuk retina azonosítás esetén a fej pontos pozicionálása és a szem megvilágítása szükséges [74].

Élőminta felismerés (live pattern recognition)

A biometrikus azonosítások kapcsán az "élőminta felismerés" paramétere egy biztonsági mechanizmus, amely annak értékelésére szolgál, hogy a biometrikus rendszerbe bemutatott minta valós, élő személytől származik-e, és nem egy hamisított vagy mesterségesen létrehozott reprodukciót használnak-e az azonosítási kísérlet során. Ez a paraméter segít megelőzni a csalási kísérleteket, mint például a biometrikus spoofingot vagy maszkhasználatot, ahol az azonosító rendszer megtévesztésére törekvő személyek hamis vagy manipulált biometrikus mintákat használnak a jogosulatlan hozzáférés megkísérlésére. A retina alapú azonosításnál az élőminta felismerés magában foglalhatja a retinán belüli véráramlás vizsgálatát vagy más élettani reakciók észlelését, az írisz alapú azonosítás esetében a pupilla reflex vizsgálatát, az írisz mintázatának spontán változásainak észlelését, vagy a szemhéj villódzásának és mozgásának analízisét. A hangalapú biometrikus azonosítás során az élőminta felismerés azt a képességet jelenti,

hogy a rendszer képes megkülönböztetni a valódi, élő emberi hangot a felvételektől vagy szintetizált hangoktól. Ez magában foglalhatja a háttérzaj elemzését, a beszéd mintázatának, a hangszín változásainak, vagy akár a légzés és egyéb jellegzetes hangjellemzők figyelembe vételét, amelyek nehezen reprodukálhatók vagy szimulálhatók Az élőminta felismerés technológiák különböző módszereket alkalmazhatnak még, mint például a mozgás analízisét, a bőrhőmérséklet vizsgálatát, a pulzus érzékelését, vár áramlását, pislogást vagy más élettani és viselkedési jellemzők detektálását, hogy biztosítsák a minta élő eredetét [83, pp. 569-571.]. Amennyiben az azonosítás megvalósítható élőminta felismerés nélkül és könnyen elérhető a technológia, akkor magas a kockázat.

Érintésnélküli technológia (contactless)

A biometrikus azonosítási technikák érintésmentes megoldása olyan módszer, amely lehetővé teszi egyén azonosítását vagy hitelesítését fizikai érintkezés nélkül, azaz a felhasználónak nem szükséges közvetlenül érintkeznie egy olvasó eszközzel vagy szenzorral. Kényelem és az azonosítás sebessége szempontjából előnyös lehet a megoldás. Az eszközök fizikai érintése szempontjából több dimenzióban vizsgálható a kockázat, mert a készülékek érintése nélkül csökken a keresztfertőzés kockázata, ami különösen fontos a COVID utáni időszakban is, az ilyen megoldások higiénikusabbá teszik a használatot. Mivel nincs szükség fizikai érintkezésre, csökkenhet az eszköz fizikai sérülése vagy manipuláció lehetősége és így annak a kockázata is. Az érintésmentes technológiák esetében a támadók kísérletet tehetnek arra, hogy hamis biometrikus mintákkal (például fotók, videók vagy hangfelvételek használata) megtévesszék a rendszert. Az érintésmentes rendszerek nem minden esetben képesek olyan könnyen ellenőrizni a minta "élő" voltát, mint az érintésalapú rendszerek. Az érintésmentes technológiák érzékenyebbek lehetnek a környezeti tényezőkre, mint a fényviszonyok vagy háttérzaj. A támadók kihasználhatják ezeket a sebezhetőségeket, például manipulálva a környezeti feltételeket annak érdekében, hogy javítsák a hamis biometrikus adatok felismerésének esélyét.

Alany beleegyezésével megszerezhető minta (sample obtainable with consent)

A megszerezhető minták gyűjtése és felhasználása az érintett személy előzetes, tájékoztatáson alapuló, önkéntes és konkrét beleegyezésével történik. Ez a folyamat magában foglalja az alany tájékoztatását a biometrikus adatok gyűjtésének céljáról,

módszereiről, a tárolás időtartamáról, valamint az adatokhoz való hozzáférésről és azok védelméről. Az alany beleegyezése azt jelenti, hogy aktív és egyértelmű hozzájárulást ad az adatainak gyűjtéséhez és felhasználásához, amely hozzájárulás bármikor visszavonható. Az azonosítás folyamata minél inkább megvalósítható beleegyezés nélkül, annál nagyobb kockázatot jelent.

Jelenlét alapú azonosítás (presence / non presence based)

Jelenlét alapú (Presence-Based) azonosítások olyan biometrikus azonosítási módszerek, amelyek az érintett személy fizikai jelenlétét igénylik a biometrikus adatok gyűjtéséhez és az azonosításhoz. Ezek a módszerek gyakran magasabb szintű biztonságot és kevésbé manipulálhatóságot biztosítanak, mivel a biometrikus mintavétel közvetlen interakciót igényel az azonosító rendszerrel. A jelenlét nélküli (Non-Presence-Based) azonosítási módszerek pedig azok, amelyek nem igénylik az érintett személy fizikai jelenlétét a biometrikus adatok gyűjtése és azonosítása során. Ezen módszerek esetében az azonosítás történhet távoli vagy előre rögzített biometrikus adatok (például videók, fényképek) alapján. Ez a megközelítés rugalmasabb és kényelmesebb lehet a felhasználók számára, de bizonyos esetekben növelheti a csalás és az adatmanipuláció kockázatát.

Alkalmasság távoli, rejtett azonosításra (remote, covert identification)

Távoli, rejtett azonosítás lehetővé teszi az egyének azonosítását vagy ellenőrzését távolról, vagy anélkül, hogy tudomást szereznének az azonosítási folyamatról. A rejtett azonosítás (Covert Identification) során az egyéneket anélkül lehet azonosítani, hogy ők maguk tudnának az azonosítási folyamat létezéséről. Ez a módszer gyakran biztonsági, megfigyelési, vagy bűnüldözési célokból kerül alkalmazásra, ahol fontos, hogy az azonosítás észrevétlen maradjon az érintett személy számára. A felhasználók szempontjából a távoli, rejtett azonosításra alkalmas megoldások jelentik a nagyobb kockázatot.

Minta változatlansága/állandósága az időben (permanence)

A paraméter azt jelenti, hogy a biometrikus adatok kinyerése mennyire marad konzisztens az idő múlásával, azaz a biometrikus minták milyen mértékben képesek fenntartani azonosítási pontosságukat hosszú időn keresztül, figyelembe véve az egyén fizikai és biológiai változásait, mint például az öregedés, sérülések, vagy egyészségügyi, életmódbeli változások hatásait. A szempont ott fontos a hosszú távú biometrikus

alkalmazások felhasználásának tervezésekor, ahol az egyének éveken vagy évtizedeken keresztül kerülnek azonosításra ugyanazon biometrikus adatok alapján. A letárolt minta rendszeres aktualizálásával javítható a minta állandósága egy adott rendszerben, ha erre a felhasználási terület lehetőséget biztosít. Amennyiben erre nincs lehetőség, a minta állandóságával egyenes arányban nő a kockázat [32, pp. 29-30.] [74, pp. 6-7.].

Külső vagy belső biometrikus jellemző (external or internal biometric)

A külső biometrikus azonosítás a test külső jellemzőire támaszkodik, míg a belső biometrikus azonosítás a test belső tulajdonságait használja fel. A külső jegyek könnyebben mérhetők és megfigyelhetők, de az idővel könnyebben változhatnak. Belső biometrikus jegyek általában stabilabbak és egyediek, nehezebben változtathatók meg. A külső jegyek gyakran nyilvánosan hozzáférhetők, emiatt lehet magas az adatvédelmi kockázatuk, az egyének akár a tudtuk nélkül is azonosíthatók. A belső adatok kezelése és tárolása mégis magasabb szintű adatvédelmi kockázatot jelent, mivel ezek az adatok érzékeny biológiai és egészségügyi információkat is tartalmazhatnak. A kockázatok mértékének értékelésekor fontos figyelembe venni, hogy a belső jegyeken alapuló biometrikus azonosítás technikailag megbízhatóbb és nehezebben hamisítható, de az adatvédelmi és etikai kockázatok miatt általában nagyobb aggodalomra ad okot. A belső adatok kompromittálása esetén az egyének személyes autonómiája és biztonsága súlyosabban érintett lehet, mint a külső adatok esetében. Ezért, bár a belső jegyeken alapuló azonosítás biztonsági szempontból előnyösebbnek tűnhet, a vele járó adatvédelmi és etikai kockázatok miatt összességében nagyobb kockázat és nagyobb körültekintést igényel.

Használható biometrikus kategorizálásra (used for biometric categorization)

Ahogy azt a 2.3.3 pontban kifejtettem a kategorizálás csak a puha vagy gyenge biometrikus adatoknál alkalmazható és használata olyan adatoknál lehetséges, amelyek önmagukban nem alkalmasak az egyértelmű azonosításra, de alkalmasak kategóriába sorolása, mint például életkor vagy az etnikai származás. Amennyiben az azonosítási megoldás alkalmas kategorizálásra, akkor az nagyobb kockázatot jelent [47].

Használható biometrikus alapú érzelemfelismerésre és következtetésre (used for biometric based emotion recognition and inference)

A biometrikus azonosítás során a rendszer az adott emberi egyedre jellemző feltételeket méri vagy következtet az adatokból, beleértve a genetikai, fizikai, fiziológiai, viselkedési, pszichológiai vagy érzelmi jellegű tulajdonságokat és az ezekből kapott elemzett vagy következtetett adatokat is. Ezekből az adatokból többek között vallási, politika, vagy akár szexualitással összefüggő információ származtathatók, melyek érzékeny adatoknak tekinthetők és az ilyen rendszerek használata nagyobb kockázatot jelenthet [47].

A fenti kockázati paraméterekhez tartozó meghatározás az 1. táblázatban látható.

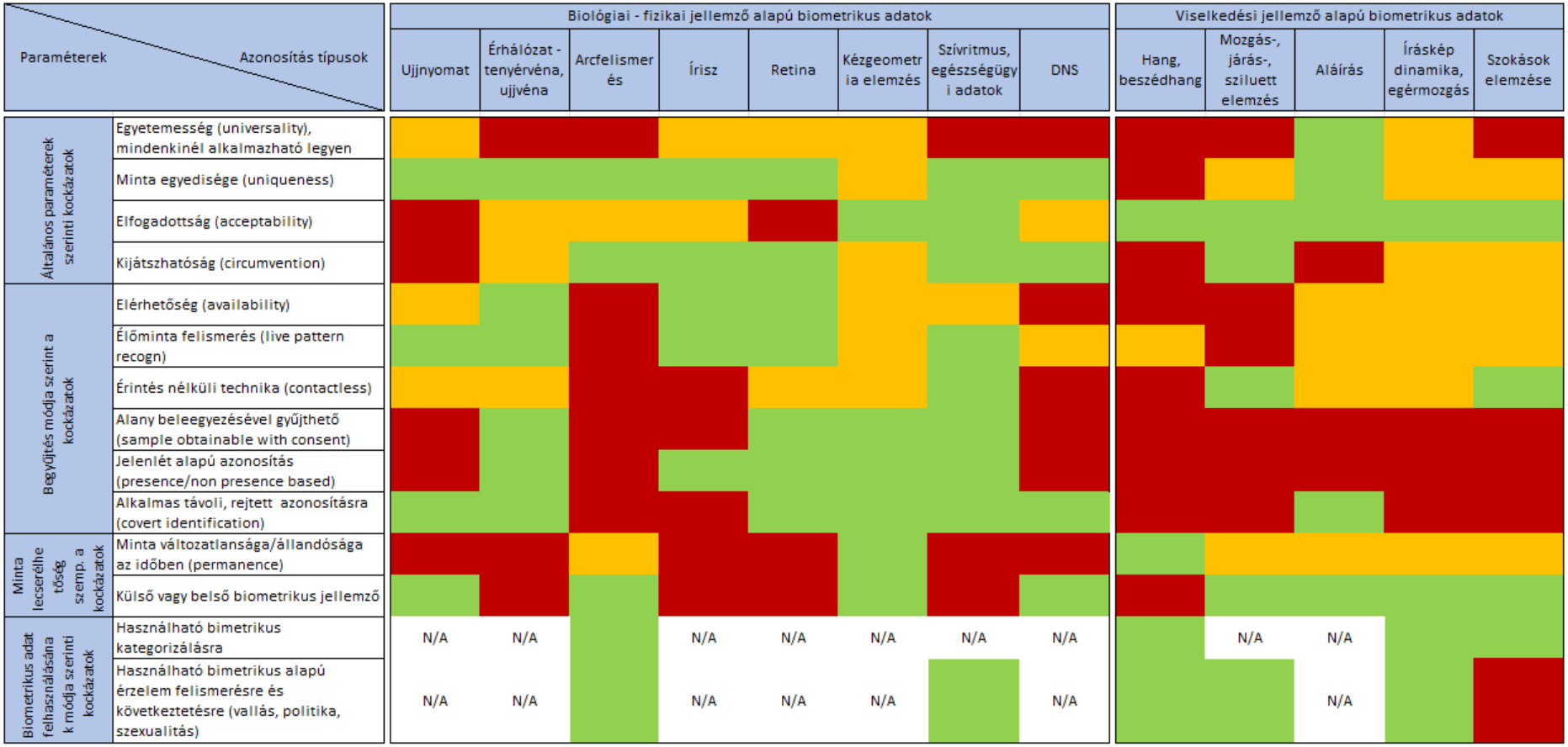
Paraméterek	Kockázati szint	Meghatározás
Elfogadottság	Magas	Vannak ismert elutasítottsággal kapcsolatos tényezők, vagy a megoldás invazívabb jellegű
	Közepes	Kevésbé elutasított vagy invazívabb a mintaadás folyamata
	Alacsony	Nem elutasított, nem különösebben invazív vagy nem áll rendelkezésre információ a mintaadás folyamatával kapcsolatban
Kijátszhatóság	Magas	Mintaadás szempontjából sok, ismert, vagy könnyű kijátszási módszer létezik
	Közepes	Mintaadás szempontjából kevés kijátszási módszer áll rendelkezésre, vagy csak nehezen megvalósítható
	Alacsony	Nem áll rendelkezésre módszer vagy nem ismert
Elérhetőség	Magas	Ismert technológiák segítségével hatékonyan és könnyen szerezhető meg az információ
	Közepes	Kevesek által elérhető bonyolult módszerekkel, de könnyen szerezhető meg az információ
	Alacsony	Kevesek által elérhető bonyolult módszerekkel és nehezen szerezhető meg az információ
Élőminta felismerés	Magas	Könnyen elérhető technológiával megvalósítható az azonosítás élőminta felismerés nélkül
	Közepes	Kevesek számára elérhető technológiával valósítható meg az azonosítás élőminta felismerés nélkül
	Alacsony	Nem valósítható meg az azonosítás élőminta felismerés nélkül, vagy nincs információ róla
Érintésmentes	Magas	Könnyen elérhető technológiával megvalósítható az azonosítás érintésmentesen
	Közepes	Kevesek számára elérhető technológiával valósítható meg az azonosítás érintésmentesen
	Alacsony	Nem valósítható meg az azonosítás érintésmentesen
Beleegyezés	Magas	A minta begyűjthető az egyén tudta nélkül
	Közepes	Nem értelmezhető ennél a szempontnál
	Alacsony	A minta kifejezetten az egyén aktív közreműködésével gyűjthető be
Jelenlét	Magas	Az azonosításhoz nem szükséges a személy fizikai jelenléte
	Közepes	Nem értelmezhető ennél a szempontnál
	Alacsony	Az azonosításhoz szükséges a személy fizikai jelenléte
Távoli, rejtett	Magas	Az azonosítás elvégezhető távolról az egyén tudta nélkül
	Közepes	Nem értelmezhető ennél a szempontnál
	Alacsony	Az azonosítás nem végezhető el távolról az egyén tudta nélkül
Állandóság	Magas	A minta az idő múlásával nem, vagy csak nagyon kis mértékben, hosszú idő alatt változik. Nincs jelentős ismert külső behatás
	Közepes	A minta az idő múlásával változik, vagy van a mintára hatást gyakorló tényező
	Alacsony	A minta könnyen változik az idő múlásával, vagy több külső tényező könnyen hatást gyakorol
Külső/belső	Magas	Belső biometrikus adatok alapján történő azonosítás magasabb kockázatot jelentenek
	Közepes	Nem értelmezhető ennél a szempontnál
	Alacsony	Külső biometrikus adatok alapján történő azonosítás alacsonyabb kockázatot jelentenek
Kategorizálás	Magas	Az azonosítási megoldás használható kategorizálásra
	Közepes	Nem értelmezhető ennél a szempontnál
	Alacsony	Az azonosítási megoldás nem használható kategorizálásra, vagy nem ismert ilyen megoldás
Következtetés	Magas	Az azonosítási megoldás következtetésre kategorizálásra
	Közepes	Nem értelmezhető ennél a szempontnál
	Alacsony	Az azonosítási megoldás nem használható következtetésre, vagy nem ismert ilyen megoldás

1. táblázat: Biometrikus azonosítási megoldások 14 szempontjának kockázati paraméterének meghatározása.[2]

[2] A táblázat a szerző saját szerkesztése.

A biometrikus rendszerek fejlődésével, az eszközök tesztelési eredményei kiértékelésével és a gyakorlati tapasztalatok bővülésével szükségesnek tartom ezen szempontok pontosítását és kiegészítését, illetve figyelembevételét a biometrikus azonosítási eljárások felhasználási módjának. Álláspontom szerint nem lehet örökérvényű kockázatelemzést elvégezni csak akkor, ha módszer és eszköz-specifikus alkalmazhatósági szempontrendszert állítunk fel [84, pp. 80-81.].

A 2. számú táblázatban a biometrikus azonosítási technikák 14 szempont [78, pp. 3958-3968.] [85] alapján elvégzett minőségi értékelés jellegű kockázatelemzése látható.



2. táblázat: Biometrikus azonosítási megoldások kockázatelemzése[3] [86, pp. 10-15.] [87, pp. 22-29.]

[3] A táblázat a szerző saját szerkesztése.

Az elemzési módszertan véleményem szerint megfelelő a kockázatok egyszerű rangsorolására, mert ezt a fajta elemzés széles körben használható egyszerű módszertanként annak meghatározására, hogy az adott kockázat elfogadható-e vagy sem, olyan esetekben, amikor nem áll rendelkezésre minden információ [88].

A szempontrendszer alapján a legkevésbé kockázatos megoldás a kézgeometria, azután a retina és az érhálózat alapú biometrikus azonosítási megoldás. A leginkább kockázatos megoldás a hang alapú, az arcfelismerés és a szokások elemzésén alapuló megoldások. Annak érdekében, hogy a kockázatokat megfelelő módon kezelni lehessen az AI szabályozásnak a biometrikus azonosítással mutatott összefüggései miatt, az Európai Parlament AI-ra kialakított javaslatát véleményem szerint alkalmazni lehet a biometriai azonosítási megoldásokra, de már a felhasználási terület figyelembevételével. A felhasználási lehetőségek kockázat alapú szempontjainak figyelembe vételével a következő csoportosítás végezhető el [89].

Elfogadhatatlan kockázat – Tiltott biometrikus megoldások

Biometrikus azonosítási rendszerek, melyek alkalmazása összefügghet az emberek biztonságával, megélhetésével és jogaival és egyértelmű fenyegetésnek tekinthető ezekre.

- Káros manipulatív technikákkal összefüggésben alkalmazható megoldások (reklámozásban, marketingben, politikában, vagy terápiás megoldásokban biometrikus és elemzett adatok segítségével az egyénre visszavezetetett azonosítás által);
- Kihasználják a specifikus sebezhető csoportokat (fizikai vagy mentális fogyatékosság);
- Olyan biometrikus rendszerek, amelyeket közhatalmak vagy azok nevében társadalmi pontozási célokra használhatók;
- 'Valós idejű' távoli biometrikus azonosítási rendszerek nyilvánosan hozzáférhető helyeken a rendfenntartási célokra, kivéve néhány korlátozott és szabályozott esetet.

Magas kockázat – Szabályozott magas kockázatú biometrikus rendszerek

Amelyek káros hatást gyakorolnak az emberek biztonságára vagy alapvető jogaira. Megkülönböztethető két kategória a magas kockázatú biometrikus rendszerek között.

Rendszerek, amelyek biztonsági komponenseként működnek egy termék részeként, vagy az EU egészségügyi és biztonsági harmonizációs jogszabályai alá tartoznak (pl. játékok, légi közlekedés, autók, orvostechnikai eszközök, lift). Rendszerek, amelyeket nyolc konkrét területen alkalmaznak

- Biometrikus azonosítás és kategorizáció;
- Kritikus infrastruktúra kezelése és üzemeltetése;
- Oktatás és szakmai képzéssel kapcsolatos rendszerek;
- Foglalkoztatás, munkaerőmenedzsment és az önfoglalkoztatáshoz való hozzáférés;
- Az alapvető magán- és közszolgáltatásokhoz és előnyökhöz való hozzáférés;
- Rendfenntartás;
- Migráció, menedékjog és határellenőrzési menedzsment;
- Igazságszolgáltatás és demokratikus folyamatok adminisztrációja.

Minden ilyen magas kockázatú biometriai azonosítási rendszernek meg kellene felelnie egy szabályrendszernek, amely magában kell foglalja az alábbi követelményeket:

Előzetes megfelelőségi értékelési követelmény: A magas kockázatú biometriai rendszerek szolgáltatóinak regisztrálniuk kellene rendszereiket az Európai Unió szerte irányított adatbázisban, (amit például az AI szabályozás mintájára az Európai Bizottság kezelhet), mielőtt piacra dobhatnák vagy szolgáltatásba helyezhetnék. A már meglévő termékbiztonsági jogszabályok által szabályozott bármilyen biometrikus vagy AI alapú termék és szolgáltatás azokba a már meglévő harmadik fél által történő megfelelőségi keretekbe tartozik, amelyek már érvényesek (például az orvostechnikai eszközök esetén). Azoknak a magas kockázatú rendszerek szolgáltatóinak, amelyeket jelenleg nem szabályoz az EU jogszabálya, saját megfelelőségi értékelést (önértékelést) kell készíteniük, amely bizonyítja, hogy megfelelnek az új követelményeknek. A biometrikus azonosításra használt magas kockázatú AI rendszereknek kell megfelelniük egy ’bejelentett szervezet’ által végzett megfelelőségi értékelésnek.

Egyéb követelmények: Az ilyen magas kockázatú rendszereknek számos követelménynek kell megfelelniük, különösen a kockázatkezelés, tesztelés, műszaki robusztusság, adatképzés és adatirányítás, átláthatóság, emberi felügyelet és kiberbiztonság területén. Ebben az összefüggésben a magas kockázatú rendszerek szolgáltatóinak, importőreinek, forgalmazóinak és felhasználóinak többféle kötelezettségnek kellene eleget tenniük. Az EU-n kívüli szolgáltatóknak szükséges lehet

egy azonosított képviselőre az EU-ban, hogy (többek között) biztosítsák a megfelelőségi értékelést, létrehozzák a piaci monitorozási rendszert és szükség esetén korrekciós intézkedéseket tegyenek.

Arcfelismerés: Az MI technológiai fejlődése hajtja az olyan biometrikus technológiák, mint az arcfelismerési technológiák (FRT-k) felhasználását, amelyeket magánszemélyek vagy közhatalmak alkalmaznak ellenőrzésre, azonosításra és kategorizálásra. Az AI rendszerek alkalmazása, beleértve az arcfelismerési technológiákat is, a magán- vagy közhatalmak által történő verifikációs, azonosítási és kategorizálási célokra. A tervezett AI-szabályozás, a már alkalmazott jogszabályokon túl (pl. adatvédelem és diszkriminációmentesség), új szabályokat javasol az FRT-k számára, és ezeket megkülönbözteti a 'magas kockázatú' vagy 'alacsony kockázatú' használati jellemzőik szerint. A valós idejű arcfelismerési rendszerek használata nyilvánosan hozzáférhető helyeken a rendfenntartási célokra tilos lenne, hacsak a tagállamok nem engedélyezik őket fontos közrendvédelmi okokból, és megfelelő bírósági vagy közigazgatási engedélyeket adnak ki. Számos más FRT, amelyet nem rendfenntartási célokra használnak (pl. határellenőrzés, piacterek, tömegközlekedés és akár iskolák), engedélyezhető lenne, egy megfelelőségi értékelés és az EU piacra kerülése előtt az biztonsági követelmények teljesítése esetén.

Korlátozott kockázat: Átláthatósági kötelezettségek

A 'korlátozott kockázatot' prezentáló rendszerek, például az emberekkel interakcióba lépő rendszerek (például chatbotok), érzelemfelismerő rendszerek, biometrikus kategorizáló rendszerek, valamint az olyan AI rendszerek, amelyek kép-, hang- vagy videótartalmat generálnak vagy manipulálnak (például deepfake-ek), csak korlátozott átláthatósági kötelezettségek alá esnének.

Alacsony vagy minimális kockázat: Nincsenek kötelezettségek

Minden más, csak alacsony vagy minimális kockázatot prezentáló biometrikus azonosítást végző rendszer fejleszthető és használható lenne az EU-ban, anélkül, hogy megfelelne bármilyen további (az eddigieken túlmutató) jogi kötelezettségnek. Azonban a javaslat célja, hogy irányelvek létrehozásával ösztönzve legyenek a nem magas kockázatú rendszerek szolgáltatói, hogy önkéntesen alkalmazzák a magas kockázatú rendszerek kötelező követelményeit.

Ugyanakkor a polgári jogi szervezetek az arcfelismerésnek és egyéb biometrikus adatoknak az indokolatlan vagy önkényes célú használatának betiltását követelik nyilvános vagy nyilvánosan hozzáférhető helyeken, valamint korlátozásokat szorgalmaznak az MI rendszerek használata tekintetében, beleértve a határellenőrzést és az előre jelző rendőrségi tevékenységeket. Az AccessNow[4] úgy véli, hogy a tiltott MI gyakorlatokra vonatkozó rendelkezések túl homályosak, és szélesebb körű tilalmat javasol az MI alkalmazására az emberek fiziológiai, viselkedési vagy biometrikus adatok alapján történő kategorizálására, az érzelmek felismerésére, valamint az ilyen technológiák veszélyes használatára a rendőrségi munka, migráció, menedékjog és határkezelés kontextusában. Továbbá, erősebb hatásvizsgálati és átláthatósági követelményeket követelnek. Az Európai Vállalkozások Szövetsége hangsúlyozza [90], hogy általános bizonytalanság van az MI értékláncában (fejlesztők, szolgáltatók és az MI rendszerek felhasználói) részt vevő különböző szereplők szerepeivel és felelősségeivel kapcsolatban. Ez különösen kihívást jelent azoknak a vállalatoknak, amelyek általános célú alkalmazásprogramozási interfészeket vagy nyílt forráskódú MI modelleket biztosítanak, amelyek nem kifejezetten nagy kockázatú MI rendszerekre szántak, de harmadik felek által olyan módon használják őket, amelyet nagy kockázatúnak lehet tekinteni. Azt is szorgalmazzák, hogy a 'nagy kockázatú' meghatározását a mérhető kár és a potenciális hatás alapján kellene újra definiálni. Az AlgorithmWatch javasolja [91], hogy a konkrét szabályok alkalmazhatósága nem függhet a technológia típusától, hanem annak egyénekre és a társadalomra gyakorolt hatásától kellene függenie. Új szabályokat követelnek, amelyek az MI rendszerek hatása alapján vannak meghatározva, és ajánlják, hogy minden üzemeltető végezzen hatásvizsgálatot, amely esetenként értékeli a rendszer kockázati szintjeit.

Összefoglalt következtetésem, hogy – a GDPR szabályzaton túlmenően – a mesterséges intelligencia szabályozásával, annak a személyes adatok adatkezelési szabályozásával párhuzamosan, megfelelő szabványokat kell kidolgozni a különféle forrásból származtatott biometrikus adatok tárolására és felhasználására, amely magába foglalja a kategorizálásból és a következtetésekből előállított elemzett és feldolgozott adatokat is. A szabványok kifejezetten biometriára vonatkozó kidolgozásával, meglévő szabványok átdolgozásával és frissítésével megteremthető lenne egy olyan, kifejezetten biometrikus azonosítási megoldásokra vonatkozó, egyszerűsített auditálható folyamat,

[4] https://www.accessnow.org/

mely által garantálható a biometrikus adatok védelme, ezáltal csökkenthető a kockázat, de mindenképpen a kockázatokkal arányos intézkedéseket lehet kidolgozni és ami még fontosabb, a felhasználókat a kockázatokkal arányosan tájékoztatni szükséges, amely hozzájárulna a biometria elterjedéséhez.

2.3. Az elterjedést gátló tényezőinek lehetséges kezelési módszerei

Alapul véve a biometrikus azonosítási rendszerek kockázat alapú megközelítését, összefoglalom az elterjedés gátló tényezői kapcsán feltárt problémák lehetséges kezelési módszereit.

A biometrikus rendszerek sebezhetősége nagyban összefügg az elterjedésüket gátló tényezőkkel, hiszen, ha kockázatot lát a felhasználó a biometrikus adatainak kezelésével, felhasználásával kapcsolatban, akkor kevésbé fogja használni az adott technológiát.

2.3.1. Szabványok felülvizsgálata és jogszabályi harmonizáció, auditálhatóság

A tudás és birtoklás alapú hitelesítési mechanizmusok fő biztonsági szempontú gyengesége az a tény, hogy a tudás, valamint egy tárgy birtoklása nem különbözteti meg a személyt egyedileg. A modern biometrikus technológiák fokozottabb biztonsági szintet nyújtanak egy új dimenzió bevezetésével a hitelesítési folyamatokban, ez a dimenzió pedig az úgynevezett tulajdonság szerinti bizonyítás. A biometrikus azonosítási technológia mögött működő informatikai és biztonsági architektúra tervezése és telepítése azonban kritikus fontosságú az egész rendszer biztonságával kapcsolatban, számos kockázatot rejt. Ezeknek az általános IT rendszereknek a szabályokon alapuló kiépítésére és üzemeltetésére nemzetközi biztonsági szabványok állnak rendelkezésre, mint az ISO/IEC 17799:2005 [92] vagy a COBIT [93]. Ezek a szabványok általános irányelveket tartalmaznak a biztonságos architektúra helyes kialakítására és működtetésére a rendszer minden elemével kapcsolatban, valamint a kockázatok felmérésével kapcsolatban is. Ezekből az ismert kockázatokból a gyakori kockázatokra vonatkozó tudásbázis áll össze, mely biztosítja a hatékony védekezést is [94].

Biometrikus specifikus szabványok tekintetében az ANSI X9.84 Biometrikus Információmanagement és Biztonság szabvány áll rendelkezésre, és ennek a szabványnak az összevetése szükséges az európai ajánlásokkal [95].

Az Európai Unióban a szabványügyi tevékenységet az Európai Szabványügyi Szervezet (European Committee for Standardization, továbbiakban: CEN), az Európai Elektrotechnikai Szabványosítási Szervezet (European Committee for Electrotechnical Standardization, továbbiakban: CENELEC) és az Európai Telekommunikációs Szabványügyi Intézet (European Telecommunications Standards Institute, továbbiakban: ETSI) végzi. Ezek a szervezetek felelősek az európai szabványok kidolgozásáért és harmonizálásáért.

Biometria témában az európai szabványosítási szervezetek több szabványt és ajánlást is kidolgoztak.

- CEN/TS 15480: Biometrikus technológiák - Adatvédelem és adatbiztonság követelményei.
- CEN/TS 16234-1: Biometrikus azonosítás - Azonosítási profilok és tesztelés - Rész 1: Keretrendszer.
- CEN/TS 16234-2: Biometrikus azonosítás - Azonosítási profilok és tesztelés - Rész 2: Finger Minutiae alapú technológia.
- CEN/TS 16234-3: Biometrikus azonosítás - Azonosítási profilok és tesztelés - Rész 3: Arcfelismerés alapú technológia.

Ezek a szabványok és ajánlások részletezik a biometriai technológiák alkalmazását, az adatvédelem és adatbiztonság követelményeit, valamint az azonosítási profilokat és tesztelési módszereket. Az európai szabványosítási szervezetek folyamatosan dolgoznak a szabványok fejlesztésén és frissítésén annak érdekében, hogy az adatvédelem és a biztonság szempontjait figyelembe vegyék a biometria területén.

A CEN/TS 15480 egy technikai specifikáció (Technical Specification, továbbiakban: TS) az európai szabványosítási rendszerben, amely a „Biometrikus technológiák - Adatvédelem és adatbiztonság követelményei” témakörben ad iránymutatást. Bár a technikai specifikáció nem egy teljes értékű európai szabvány, mégis fontos iránymutatást és követelményeket tartalmaz a biometrikus technológiák alkalmazására vonatkozóan. A CEN/TS 15480 célja, hogy meghatározza az adatvédelem és adatbiztonság általános követelményeit a biometrikus technológiák alkalmazásában. Ez magában foglalja a biometrikus adatok kezelésével és tárolásával kapcsolatos előírásokat, valamint az adatbiztonsági intézkedésekkel és az adatvédelmi elvekkel kapcsolatos ajánlásokat. A specifikáció kitér a biometrikus adatok kezelésének jogi és etikai kérdéseire, valamint az érintettek tájékoztatásának és hozzájárulásának

fontosságára. Továbbá, részletesen tárgyalja a biometrikus adatok tárolására és továbbítására vonatkozó biztonsági intézkedéseket, például az adatvédelmi elvek betartását, a titkosítást, az adatintegritást és az adathozzáférési szabályokat.

A CEN/TS 15480 szabvány célja, hogy biztosítsa a biometrikus technológiák alkalmazásával járó adatvédelmi és adatbiztonsági kockázatok minimalizálását, és iránymutatást nyújtson a megfelelő gyakorlatokhoz és intézkedésekhez. Az irányelv segíti a biometrikus rendszerek tervezőit, üzemeltetőit és felhasználóit az adatvédelem és adatbiztonság megfelelő szintjének elérésében.

Fontos megjegyezni, hogy a CEN/TS 15480 egy technikai specifikáció, és nem jogilag kötelező erejű dokumentum. Azonban sok esetben ajánlott és hasznos iránymutatást nyújt a biometrikus technológiák alkalmazásában érdekelt felek számára az adatvédelem és adatbiztonság terén.

Ezeknek a szabványoknak a felülvizsgálata és az AI kapcsán kialakított új jogszabállyal történő harmonizációja szükséges a biometrikus azonosítási rendszerekkel szembeni bizalom erősítéséhez, valamint, hogy az ilyen adatokat tároló és ilyen rendszereket használó szolgáltatók (akár állami szervek is) független módon auditálhatók legyenek.

2.3.2. A biometrikus azonosítási rendszerek sebezhetőségei és kezelési lehetőségei

Mintahamisítás, utánzás (spoofing, mimicry, artefacts) – A minőségileg gyenge biometrikus rendszerimplementációk kifejezetten védtelenek az ilyen jellegű támadásokkal szemben. Kereskedelmi forgalomban kapható szilikon vagy zselatin alapú mesterséges ujj megtéveszthetti az ujjlenyomat érzékelőket. A felületeken otthagyott ujjnyomat a bűnüldözésben is használt grafitporos módszerrel könnyen megszerezhető, digitalizálható, grafikai szoftveres technológiákkal a minta tisztítható és a kontrasztok javíthatóak, majd 3D nyomatási, vagy marási módszerekkel a helyettesítő minta előállítható. Képek, maszkok alkalmazhatók az arcfelismerő berendezések átverésére, hangfelvételek és beszédszintetizáló megoldások alkalmazhatók a hangfelismerő rendszerek támadására, megtévesztésére. Ezek elkerülésére élőminta felismerés funkció szükséges, mely során több tulajdonság, mint pl. relatív dielektromos állandó, vezetőképesség, szívverés, hőmérséklet, vérnyomás paraméterek kombinációjának egyidejű mérését végzik az azonosított személy valós jelenlétének megerősítésre. A

leghatékonyabb védelem a multimodális rendszerek alkalmazása, mely élőminta felismerés mellett, de több, az azonosított egyénre jellemző biometrikus adatot mér.

Szerver oldali kockázatok, hamis sablonok – A komolyabb biometrikus azonosító rendszerek mögött általában hagyományos IT szerver környezeti architektúrák működnek. Itt kerülnek tárolásra az élő mintából átalakított sablonok (1:n), hálózati és adatbázis műveletek futnak az azonosítás során. Az ilyen alapszintű rendszerek védelme szerencsére a biometriától függetlenül is kiemelt kérdés több évtizede, nemzetvédelmi, pénzintézeti, katonai és egyéb szektorok folyamatosan frissítik ajánlásaikat a sérülékenységi kockázatok csökkentésére. A támadás akkor tud sikeresen megtörténni, ha a csalónak sikerül az eredeti sablont kicserélni, vagy valaki más neve alatt beilleszteni hamis sablont. Ez ellen egyszer írható, vagy írásvédett tárolási megoldásokkal lehet védekezni, illetve gyengébb, de még mindig elfogadható megoldásként a sablonok megfelelően magas szintű titkosításával, illetve megfelelő ellenőrző kontrollok bevezetésével is. Ezek technológia megfelelőségét a nemzetközi szabványok biztosítják, a valós bevezetési megfelelőségét pedig az auditok [96].

Kommunikációs kapcsolatok – a működtető környezet különböző komponensei között futó adatkommunikáció rögzíthető és újra visszajátszható. Az elektronikus megszemélyesítés jelensége jól kezelhető a komponensek integritásának növelésével (hardveres biztonsági modul), vagy a biometrikus sablon átvitelének a csökkentésével, vagy biztonságos kezelésével. Erre jó megoldás az olyan vezérlések alkalmazása, ahol a tárolt jel és a kommunikáció során használt jel között szabályozott kapcsolat áll fenn.

Keretrendszer – különböző biztonsági szintek kiszolgálása különböző sablonokkal. Más azonosító használata a kényelmi alkalmazásokhoz, és a nagy biztonságot igénylő esetekben. A kritikusságtól függően egyedi kódolási algoritmusok használata, illetve a kódolási algoritmusok hash függvényekkel való kombinációja. A sablonok és hozzátartozó jogosultságok azonnali visszavonásának lehetőségét biztosítani kell.

Komponens szabotálás – biztosítani kell, hogy a rendszer elemei olyan egyedi azonosítókkal legyenek ellátva, hogy azok tervezett (karbantartás) vagy illegális tevékenységből eredő (csalás) folyamat során ne legyenek cserélhetők a rendszer által nem ellenőrzött és kontrollált elemekre.

Regisztrálás, adminisztráció és rendszerhasználat – a regisztrációs fázisban nagy a rendszerek kitettsége, hogy manipulálás történik a nyers biometrikus adatokkal, vagy a sablonokkal. A gyenge rendszeradminisztráció lehetőséget biztosít a csalóknak a rendszerkonfiguráció megváltoztatására, ami eredményezheti azt is, hogy a FAR értéke

változik, ezáltal kevésbé utasít el nem megfelelő mintákat. Minden biometrikus azonosítási rendszer alapvetése, hogy a regisztrációkor felvett minta és a mindennapi azonosítások során adott minta között vannak eltérések, hiszen az ember is változik, a környezet is változik, kétszer nem lehet teljesen megegyező mintát adni. A rendszereknek mégis döntést kell hozni, hogy az adott illető jogosult-e vagy nem. A regisztrációkor felvett adatból nyert sablon, és ugyanazon személy által az azonosítás pillanatában adott minta egyezőségének eldöntése az érzékeny pontja a rendszereknek. Könnyen belátható, hogy ebbe az állapotba való illetéktelen belenyúlás komoly veszélyt rejt, ezért a regisztrációs folyamatot, az adminisztrációs feladatokat és a rendszer használatát jelentő folyamatokat minél inkább felügyelt környezetben és módon javasolt kezelni. Ezeket a folyamatokat és eljárásokat szabályozni szükséges, melyeket nemzetközi szabványok alapján és a bevett jó gyakorlatok elvén kell a rendszerhez igazítani, de mindenképpen irányított és felügyelt körülmények között szükséges a regisztrációt elvégezni.

Tápellátás kiesés és zaj – tűréshatáron kívüli feszültségingadozás, vagy az érzékelők elárasztása „zajadatokkal" a rendszer meghibásodásához vezethet. Villogó fény az optikai érzékelőkbe, szennyeződés rászórása a szenzorokra, magas hőmérséklet vagy páratartalom, folyadék felvitele az arra érzékeny megoldások érzékelőire, nem várt és szükségtelen hatásokat okoznak. A kontrollált rendszerkörnyezet és a fokozott biztonsági ellenőrzések csökkentik ezeket a hatásokat.

Teljesítmény és időtényezők elemzése – a rendszert alkotó feldolgozó egységek (pl. processzorok) energiafogyasztásának rögzítése és elemzése révén kinyerhető a chipen futó szoftverkód, vagy akár a futtatott parancs. Teljesítményelemzési és differenciálteljesítmény-elemzési technikákkal a kriptográfia algoritmusok is feltörhetők (pl. DES), ha elég sok adat áll rendelkezésre egy statisztikai elemző szoftvernek, mondjuk a regisztráció vagy az azonosítási folyamatok adatsorairól. Ezek kivédésére alacsony fogyasztású mikrokontrollerek és kifejezetten erre a célra beépített zajgenerátorok, vagy a valós áramfelvételt elfedő fogyasztók beépítése javasolt [97] [98].

Megmaradó minták (residual characteristic) – az optikai elven működő ujjnyomat érzékelő felületén maradó ujjlenyomat alkalmas bizonyos esetekben az újbóli azonosításra. Egy vékony zacskó, gumikesztyű és melegvíz segítségével az előző azonosítás megismételhető az érzékelőre való nyomással, vagy grafitporral és ragasztószalaggal az üveglapon maradó nyomot rögzítve ismételten felhasználható. A szalag finom elmozdításával még a kicsit az előzőtől eltérő adatbevitel is megvalósul és

megtéveszthető a rendszer. [31]. A nem optikai típusú azonosítás ellenáll ennek a csalásnak, illetve interaktív hitelesítés folyamat kialakítása szükséges.

Kitettség a brute-force támadásokkal szemben – a támadó sorozatosan nagy mennyiségű azonosítási próbát hajt végre. Biometrikus azonosítási módszereknél ez nem annyira elterjedt, mivel nehezebb a próbaadatok beillesztése a rendszerbe, de a lehetőséget ki kell zárni. Megoldás ugyanaz, mint a jelszavak esetében, adott próbálkozási szám után a rendszer elkezdni a próbálkozások lehetőségét lassítani, majd végén a felhasználói fiókot, a hozzáférést zárolni kell.

Ellopott biometrikus adat – az egyik legnagyobb félelem a biometrikus azonosításokkal kapcsolatban, hogy mi történik, ha ellopják az egyén egyedi biometrikus azonosítás során használt adatait. Megújíthatóság és megmásíthatóság szempontjainak bevezetése szükséges az azonosítási rendszerekkel kapcsolatban. Mivel a biometrikus adatok forrása nem változtatható meg, a személyazonossági kapcsolat létrehozását célzó biometrikus rendszereket úgy kell megtervezni, hogy a felvételi folyamat és a biometrikus adatok feldolgozása lehetővé tegye, hogy több és egymástól független biometrikus sablon legyen kinyerhető ugyanabból a forrásból, hogy a sablonokat adatsértés vagy technológiai fejlődés esetén ki lehessen cserélni. A biometrikus rendszereket úgy kell megtervezni, hogy lehetőség legyen a személyazonossági kapcsolat visszavonására, annak megújítása, vagy tartós törlése céljából, például, ha visszavonják a hozzájárulást. A Turbine technológia például olyan módon védi a biometrikus sablont, hogy az ujjlenyomat-információkat titkosítási transzformációval vissza nem fejthető kóddá alakítja, amely lehetővé teszi a bitenkénti összehasonlítás útján való megfeleltetést. Az átalakított biometrikus adatokat a biometrikus mintákra és az eredeti sablonokra visszavezethetetlennek tartják. Ezenkívül a felhasználók bizalmának erősítése érdekében ez a kulcs visszavonható is lesz, azaz új, független kulcs generálható a biometrikus személyazonosságok újbóli létrehozásához [15].

2.3.3. A fizikai biztonság rizikófaktorba tartozó problémák és gátló tényezők

Befogadás – előfordulhat, hogy egyes biometrikus adatokat nehéz, vagy lehetetlen bizonyos személyektől megbízhatóan levenni, ezért multimodális biometrikus adatokra és/vagy megfelelő technikai, eljárási intézkedésekre van szükség a kizáró tényezők csökkentése érdekében.

Megbízhatóság – a biometrikus deduplikáció lehet a legjobb megoldás az egyediség megállapítására nagy populációban, azonban nem minden biometrikus módszer biztosít azonos szintű pontosságot.

Adatvédelem – a biometrikus adatok használata kockázatot jelent a magánélet és az adatvédelem tekintetben, amelyeket jogi és műszaki, működési kontrollokkal kell mérsékelni.

Fenntarthatóság – a biometrikus adatok levételének és biztonságos tárolásának költségei magasak, és a technológiák eltéréséből adódóan a mintákat frissíteni szükséges.

A mintaadás, az azonosítás nehézségeinek 5 kategóriája

- Akik fizikailag nem képesek biometrikus mintát adni, sérülések miatt, fogyatékkal élők stb.
- Olyan személyek, akinél nehéz megbízható, jó minőségű mintát venni, vagy nehézkes a hitelesítés, mint a kétkezi munkások, idősek, gyerekek, albinizmussal élők.
- Azok az emberek, akik megtagadják a biometrikus adataiknak a megadását, vallási, vagy kulturális okok miatt, vagy a fizikai érintés elutasítása miatt. Egészségügyi kockázatok miatti félelem,
- Környezeti és eljárási problémák miatti nehézségek
- Nehézkes körülmények, mint az adott technológiának éppen nem megfelelő időjárás, túl erős napfény, páratartalom, szél, por. A minta rögzítését végző alacsony képzettsége, vagy kapacitáshiány, alacsony morál, időhiány.

Egyéni jogok védelme – leplezett adatgyűjtés, adattárolás és adatfeldolgozás lehetősége, valamint a rendkívül különleges információkat tartalmazó anyagok gyűjtése, ami az egyén legféltettebb szférájába törhet be. A leplezett technikák lehetővé teszik az személyeknek tudtukon kívüli azonosítását, ami a magánéletet érintő súlyos fenyegetést eredményez, és csökkenti a személyes adatok feletti ellenőrzést. Ez súlyos következményekkel jár az egyének azon képességére, amelynek értelmében önkéntes hozzájárulást adhatnak vagy egyszerűen csak tájékozódhatnak a feldolgozásról.

Ezenkívül egyes rendszerek titokban az érzelmi állapothoz vagy testi jellemzőkhöz kapcsolódó adatokat gyűjthetnek, és egészségügyi adatokat fedhetnek fel, ami aránytalan adatfeldolgozást, illetve a 95/46/EK irányelv 8. cikkének értelmében vett különleges adatok feldolgozását eredményezi

Személyazonossággal való csalás, azonosítás vagy hitelesítés esetében – az ettől való félelem csökkenthető, ha az adatfelvétel során biztonsági szempontból biztosítottak a körülmények, az adatfelvételt hitelesített személy végzi jól meghatározott cél érdekében, a biometrikus adatfelvételt végző eszköz megbízható eszköz kell legyen, melyet csalással nem lehet megtéveszteni, és olyan adatot kell rögzítsen, melyet távolról, az egyén tudta nélkül nem lehet megszerezni. Lehetőség szerint biztosítani kell, hogy a biometrikus adat megfelelően titkosított sablonban kerüljön eltárolásra, a tároló környezet informatikai biztonsága szabályozott és ellenőrzött legyen. A biometrikus adat lehetőség szerint ne adatbázisban, ne központi módon legyen tárolva. Az adattárolás és feldolgozás jogszerű legyen, és érvényesüljön a szabályzatokban meghatározott összes elv.

A leolvasások eredménye soha nem egyezik meg teljesen, így érzékeny pontja ezeknek a rendszereknek a hibatűrés mértéke, hiszen ez ronthatja az azonosítás megbízhatóságát mind a téves elfogadás, mind a téves elutasítás szempontjából.

A számítógép nem biztos, hogy le tudja ellenőrizni a leolvasó hardver hitelességét, így az is támadások célpontja lehet.

Jogi, adatvédelmi kérdéseket vethet fel, ha a leolvasás akár távolról, az adott személy beleegyezése nélkül is megtörténhet (például arc-azonosítás).

Bizonyos módszerektől való idegenkedés, például az ujjlenyomat azonosítás összekötése a bűnüldözéssel, melyet oktatással lehet kezelni.

2.4. Összefoglalás és a H2 hipotézis megválaszolása

A biometrikus azonosítás és a személyes adatok kezelésének jogi hátterének fejlődését feldolgoztam hazai és nemzetközi szinten. A feldolgozás során az elmúlt pár év hatásait figyelembe véve feldolgoztam az összefüggéseket az MI fejlődésével és közben áttekintettem az MI definíciójának fejlődését és azonosítottam azokat a főbb pontokat, melyek a jogszabályalkotás legújabb kulcspontjai, mint a távoli biometrikus azonosítási megoldások kockázatai, a következtetésen és kategorizáláson alapuló megoldások kockázatai. Ezekből kiindulva kialakítottam egy szempontrendszert, mellyel elvégezhető a biometrikus azonosítási megoldások felhasználási terület független kockázat értékelése. A fejezet végén összefoglaltam az azonosítási megoldások és a kockázatok kapcsolatát és az azonosítási megoldások elterjedésének gátló tényezőit és ezek kezelésére adható válaszokat.

A fejezetben kiemeltem a jogszabályok harmonizációjával és a szabványok frissítésével kapcsolatos javaslatokat, illetve a biometrikus adatok tárolását, feldolgozását végző rendszerek auditálhatóságának fontosságát, mert meglátásom szerint leginkább nem a biometrikus rendszerekkel kapcsolatos a felhasználói bizalmatlanság, hanem az azok környezetét, háttérinfrastruktúráját jelentő informatikai környezet sebezhetőségét tartják magasnak, illetve magas az adatkezelőkbe vetett bizalmatlanság is. Ezeket pedig a jogszabályok, a szabványok és az ilyen adatokat tároló rendszerek törvényileg kötelező auditálhatósága fogja javítani.

A jogalkotás mindig le lesz maradva a technológia mögött, de tapasztalatom alapján az EU elkezdte beépíteni az újabb azonosítási módszereket és az AI-val összefüggő szakmai pontokat a szabályozásokba, különösen az adatkezeléssel kapcsolatos szabályzói folyamatokat, mert a mesterséges intelligencia hirtelen megjelenése és elterjedése a piacon kényszerítő hatással bírt a jogalkotókra.

A legújabb jogszabályokat átvizsgálva meg tudom válaszolni a kutatásom elején felállított hipotézisemet.

Hipotézis 2 (H2): Feltételezem, hogy a biometrikus azonosítás jogszabályi környezete összefüggést mutat a mesterséges intelligencia fejlődésével és szabályozásával.

A vizsgálatom alapján megállapítom, hogy az AI-szabályozás többszörösen összefügg a biometrikus azonosítással és annak szabályozásával kapcsolatban a jogalkotók törekednek az összhang kialakítására. Ezen stratégiák és szabályzatok célja a teljes folyamatláncon végigfutó szabályozás, együttműködés és információcsere kialakítása a gyártók, jogalkotók és szakmai döntéshozók, kormányzati és hatósági szervek között. A magas szintű döntéselőkészítő dokumentumok és tanulmányok kiemelt témája az oktatás erősítésének fontossága, mely jelentősen hozzájárul a biometrikus megoldások elterjedéséhez, hiszen, ha érti a felhasználó a kockázatokat és nem fél a nem megfelelő adatkezeléstől, mert biztosítva látja jogait és biometrikus adatainak megfelelő védelmét és felhasználását, akkor kevésbé ellenzi a technológiát ebből a szempontból. Amennyiben a szabályzások megfelelően kényszerítik a szereplőket a biztonságos infrastruktúrák kialakítására, auditálható és jogkövető módon történik az adatok kezelése és a felhasználók bizalma megnő a megoldásokkal szemben, valamint kialakulnak a biometrikus azonosítási rendszerekre vonatkozó megfelelő szabványok, akkor várhatóan a biometrikus azonosítási megoldások is szélesebb körben terjednek el.

A szabványok kialakítása a megfelelő szakmai szervezetek hatásköre. Amíg a nemzetközi szabályozást és ajánlást alapul véve az országok, a tagországok saját jogalkotása nem kényszeríti ki, hogy a biometrikus adatokat tároló rendszerek védelme megfelelő szabályokon és szabványokon alapuljon, addig is az adatkezelés kockázatainak kiértékelésével és a kockázatok egyéni kezelésével érdemes biztonságos megoldásokat kidolgozni. Ennek elősegítése érdekében dolgoztam ki a biometrikus azonosítási megoldások kockázatértékelését, mely a felhasználói jogok és az adatvédelem szoros kapcsolatából kiindulva a biometrikus azonosítási rendszerek által feldolgozott és felhasznált különféle típusú biometrikus adatok kockázatai alapján állít fel rangsort.

3. KÉRDŐÍVES KUTATÁS

Ebben a fejezetben bemutatom a kérdőíves kutatásom eredményeit, az összefüggéseit a korábbi kutatásokkal, és elvégzem ezen korábbi és jelenlegi kutatások eredményeinek kiértékelését, melyekből következtetéseket vonok le. Választ adok a H1, H3, H4 hipotézisekre.

3.1. A biometrikus azonosítás elfogadásával és elterjedésével összefüggő korábbi kutatások

A biometrikus azonosítások elterjedése számos tényezőtől függ, a technológia újszerűségétől és egyszerűségétől, a felhasználási területtől, a biztonsági kihívásoktól, a nemzetközi és hazai jogi szabályozástól és 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. *„A biometrikus rendszerek felhasználói elfogadottsága nem minden esetben pozitív, hiszen a kommunikáció hiánya, félreinformálás, tévhitek vagy a negatív attitűd eredményezhetik a biometrikus azonosítás rossz vagy hamis megítélését. A viselkedés alakítását az attitűd megismerésén és formálásán keresztül lehet elérni. Az attitűd vizsgálatánál az affektív, konatív és kognitív összetevőket, valamint az attitűd funkcióját együttesen kell megállapítani. A biometrikus azonosítók elfogadását nem egyénenként, hanem csoporton belül lehet a leghatékonyabban vizsgálni. Mivel a csoport közös magatartását nagyban befolyásolja a véleményvezérek magatartása, ezért elengedhetetlen annak részletes vizsgálata.”* [99]

A biometrikus azonosítási megoldások ismertségének, elfogadásának és elterjedésének hazai vizsgálata nem tekint vissza több tízéves múltra, de abban a kedvező helyzetben vagyunk, hogy a területen már történt kutatás [100], így ezekből kiindulva és az adatainak egy részével van lehetőség az összehasonlításra, mely egy új kutatással elvégezhető. A korábbi kutatások a biometrikus azonosítási eljárások alkalmazási gyakorlatának fejlesztési irányainak meghatározásának érdekében vizsgálta, hogy milyen változások történtek a társadalmi elfogadottság tekintetében, illetve milyen averziók kapcsolhatók az eljárásokhoz. *„Az attitűdbeli változások, társadalmi, kognitív folyamatok ugyanis elsődleges hatással vannak az innovatív technikák gyakorlatban történő*

alkalmazásának és az ezzel összefüggő jogi háttér befolyásolásában." [101] A 2002-es vizsgálat még a jogelőd Budapesti Műszaki Főiskola, Bánki Donát Gépészmérnöki Kar, Gépszerkezettani és Biztonságtechnikai Intézete, Biztonságtechnikai Laboratóriumában, a 2014-es vizsgálat az Óbudai Egyetem Biztonságtudományi Doktori Iskola keretein belül került megvalósításra.

3.2. Kutatás módszertan, a mérés környezete

A 2022-es kutatásom kérdőíve (1. számú melléklet) a korábbi kutatások kérdéseit felhasználva, illetve azokat kiegészítve a biometria elterjedését, az elterjedés gátló tényezőit és a felhasználók érzelmi és gondolati attitűdjét vizsgálja. A kérdőív anonim és önkéntes alapon került kitöltésre általános és véletlenszerű válaszadók által, melyekben szerepeltek egyetemi hallgatók, munkahely, lakóhely, érdeklődési kör, hobbival kapcsolatos szociál média csoportok válaszadói.

A vizsgálat során a mintanagyságra való tekintettel a központi határeloszlás tétele alapján feltételeztem a számított statisztikák normalitását, így a paraméteres próbák ezen alkalmazási feltételét adottnak vettem [102]. A Likert-skálán mért változókat alkalmasnak ítéltem a parametrikus próbákra, valamint lineáris modellekben való szerepeltetésre [103]. Amennyiben kevés ismérvváltozattal rendelkezett egy változó, úgy a Kendall-féle tau-b mutató segítségével mértem annak más változókkal való kapcsolatának szorosságát. Több változó átlagának egymással való összehasonlítását a Greenhouse-Geisser korrekcióval ellátott ismételt méréses varianciaanalízissel hajtottam végre. Az egyes változók posthoc páronkénti összehasonítása során a Bonferroni-korrekcióval ellátott teszteredményeket közöltem. Több minőségi ismérv gyakoriságainak összehasonlításakor a Cochrane Q tesztet alkalmaztam. Két csoport átlagának összehasonlítását a független mintás t-próba megfelelő változatával hajtottam végre, melyben a választás alapja a szóráshomogenitás Levene-féle tesztjének eredménye volt. Két sokasági arány összehasonlítását a független mintás aránytesztelés z-próbájával végeztem el. A saját készítésű index megbízhatóságának mérésére a Cronbach-alfa mutatót használtam fel. Valamennyi számítás az IBM SPSS Statistics 25. verziójával, valamint saját – MS Excelben elvégzett – számításokkal történtek. A statisztikai próbák során azok szignifikancia szintjét egységesen 5%-ban határoztam meg.

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 (33,0%), 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 vesznek részt: 2,6%), vagy pedig alacsony (szakmunkásképző: 1,4%; általános iskola: 1,4%) iskolai végzettséggel rendelkezik. Lásd 3. táblázat.

	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%

3. táblázat: A minta megoszlása a demográfiai változók mentén[5]

3.3. Saját kutatás bemutatása

1. kérdés: Ha hallott már a biometrikus azonosításról, mi a jellemzőbb a megoldások ismerete kapcsán Önre?

Erre a kérdésre a következő arányban válaszoltak:

[5] A táblázat a szerző saját szerkesztése.

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

A válaszokból megállapítható, hogy a válaszadók alapvetően tudják, hogy mi az a biometrikus azonosítás. Megközelítőleg fele-fele arányban oszlanak meg abból a szempontból, hogy csak felületes ismereteik vannak (230 fő), vagy tájékozottak (205 fő) a témában. Van egy kiemelkedő 12% is, aki utána olvas a témának (60 fő), érdeklődik utána, vagy ismeretei naprakészek.

A korábbi, az Óbudai Egyetemen végzett kutatásokra alapozva azt feltételeztem, hogy a biometrikus azonosítási módszerek elterjedésének legfőbb gátja a széleskörű társadalmi elfogadás hiánya. A kérdőíves kérdések ennek vizsgálatára irányultak, melyet a kérdőív egyik kérdése és egy általam létrehozott index közötti kapcsolat vizsgálatával végeztem el [102] [103].

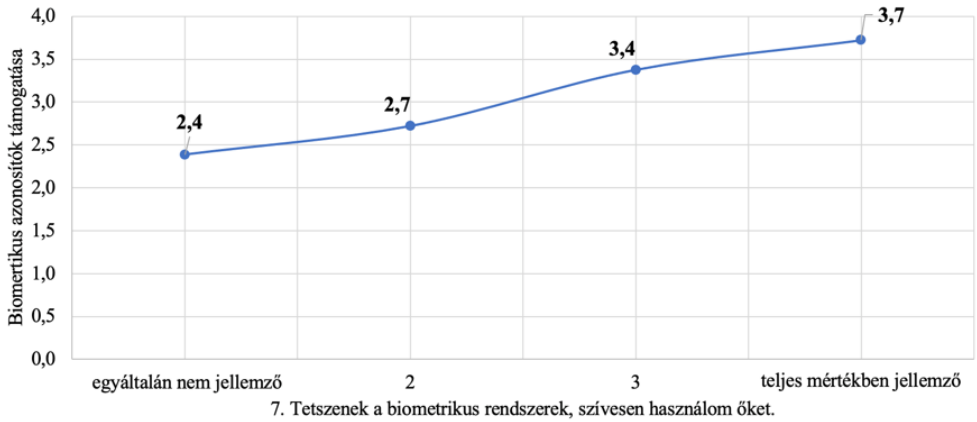
H1 hipotézis vizsgálata: Feltételezem, hogy a biometrikus azonosítási módszerek széleskörű elterjedésének legfőbb gátja a széleskörű társadalmi elfogadás hiánya.

Az első hipotézisem vizsgálatát a kérdőív egyik kérdése és egy általam létrehozott index közötti kapcsolat vizsgálatával végeztem el. 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 (4. táblázat alapján); megbízhatóságát teljes mértékben igazolja a Chronbach-alfa mutató magas értéke (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 4. táblázat. Megjegyzendő, hogy a 3., 4., 10. kérdések lehetséges válaszai az „igen” és a „nem” lehetett, ezért azokat átkódoltam rendre négyre és kettőre.

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

4. táblázat: A biometrikus azonosítási módszerekkel kapcsolatos elfogadást mérő index komponensei.[6]

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 4. ábra.



4. ábra: A biometrikus azonosítási módszerekkel kapcsolatos elfogadást mérő index átlagos értékei a „Tetszenek a biometrikus rendszerek, szívesen használom őket.” kérdésre adott válasz függvényében.[7]

[6] A táblázat a szerző saját szerkesztése.
[7] Az ábrát a szerző készítette.

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

H3 hipotézis vizsgálata: Feltételezem, hogy vannak olyan biometrikus azonosítási megoldást használó területek, ahol a biometrikus azonosítási megoldások alkalmazása a lakosság széleskörű támogatottságát élvezi.

A kérdőív 11. kérdésében arra kértem a válaszolókat, hogy a felsorolt azonosítási megoldásokat biztonság szempontjából rangsorolják egytől ötig. A legkevésbé biztonságos jelentette az egyes, míg a legbiztonságosabbat az ötös érték. Öt azonosítási rendszerre kérdeztem rá, melyek a következők voltak: kártyás azonosítás, ujjnyomat alapú azonosítás, arcfelismerés, írisz alapú 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. Lásd a 5. táblázatban.

Azonosítási megoldás	Átlag	St. hiba	CI95 alsó	CI95 felső
Kártyás azonosítás	1,615	0,059	1,499	1,731
Ujjnyomat alapú azonosítás	3,033	0,051	2,932	3,133
Arcfelismerés	2,711	0,046	2,62	2,802
Írisz alapú azonosítás	3,877	0,049	3,782	3,973
Érhálózat alapú azonosítás	3,764	0,063	3,64	3,887

5. táblázat: Az azonosító megoldások leíró statisztikái[8]

[8] A táblázat a szerző saját szerkesztése.

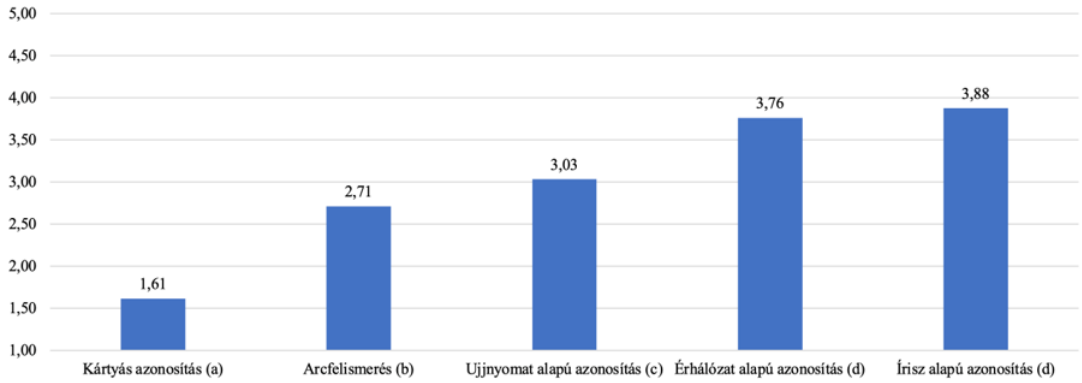
Valamint:

(I) Azonosítási megoldás	(J) Azonosítási megoldás	Átlagok eltérése(I-J)	St. Hiba	Szig
Kártyás azonosítás	Ujjnyomat alapú azonosítás	-1,418	0,071	<0,001
	Arcfelismerés	-1,096	0,083	<0,001
	Írisz alapú azonosítás	-2,263	0,094	<0,001
	Érhálózat alapú azonosítás	-2,149	0,106	<0,001
Ujjnyomat alapú azonosítás	Kártyás azonosítás	1,418	0,071	<0,001
	Arcfelismerés	0,322	0,072	<0,001
	Írisz alapú azonosítás	-0,845	0,083	<0,001
	Érhálózat alapú azonosítás	-0,731	0,102	<0,001
Arcfelismerés	Kártyás azonosítás	1,096	0,083	<0,001
	Ujjnyomat alapú azonosítás	-0,322	0,072	<0,001
	Írisz alapú azonosítás	-1,166	0,075	<0,001
	Érhálózat alapú azonosítás	-1,053	0,087	<0,001
Írisz alapú azonosítás	Kártyás azonosítás	2,263	0,094	<0,001
	Ujjnyomat alapú azonosítás	0,845	0,083	<0,001
	Arcfelismerés	1,166	0,075	<0,001
	Érhálózat alapú azonosítás	0,114	0,072	1
Érhálózat alapú azonosítás	Kártyás azonosítás	2,149	0,106	<0,001
	Ujjnyomat alapú azonosítás	0,731	0,102	<0,001
	Arcfelismerés	1,053	0,087	<0,001
	Írisz alapú azonosítás	-0,114	0,072	1

6. táblázat: Az azonosítási megoldások Bonferroni-korrekción alapuló posthoc teszt-eredményei[9]

Ezek alapján felállítható sorrend: legkevésbé biztonságosnak a kártyás azonosítást találták a megkérdezettek (1,61), ezt követte az arcfelismerés (2,71), majd az ujjnyomat alapú azonosítás (3,03) következett végül nagyjából hasonló mértékben legbiztonságosabbnak az érhálózat (3,76) és az írisz alapú azonosítást (3,88) ítélték. Lásd 5. ábra.

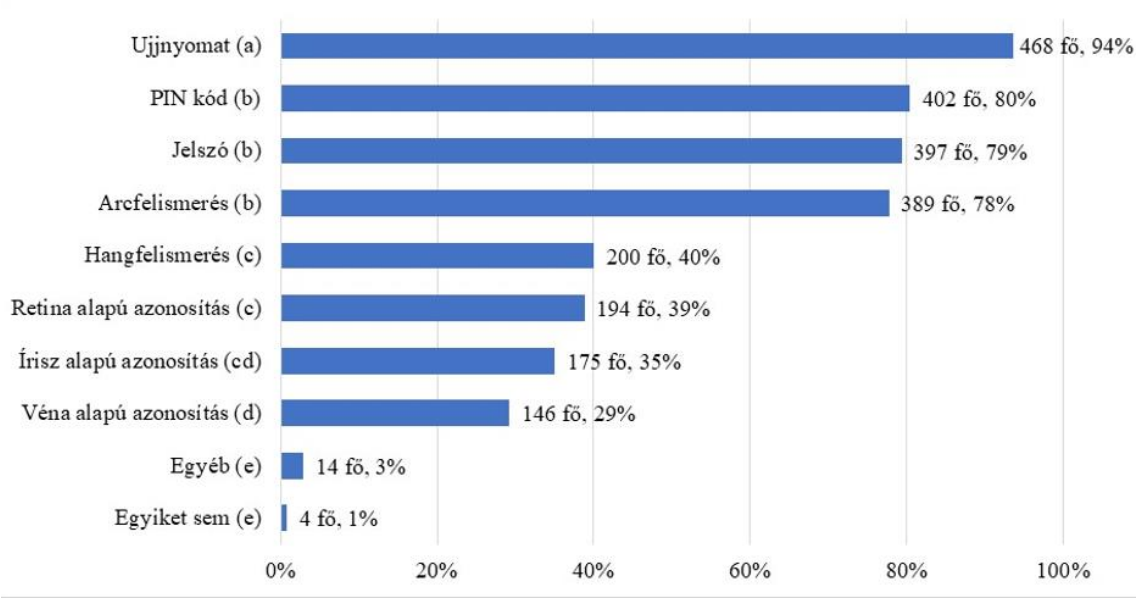
[9] A táblázat a szerző saját szerkesztése.



5. 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 (pl. a≠b), a megegyezők (d=d) annak hiányát jelentik.)[10]

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, írisz alapú azonosítás, retina alapú azonosítás, hangfelismerés, arcfelismerés, véna alapú 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 retina alapú azonosítás (39%) és az írisz alapú azonosítás (35%). A legkevésbé ismert pedig a véna alapú azonosítás (29%). Lásd 6. ábra.

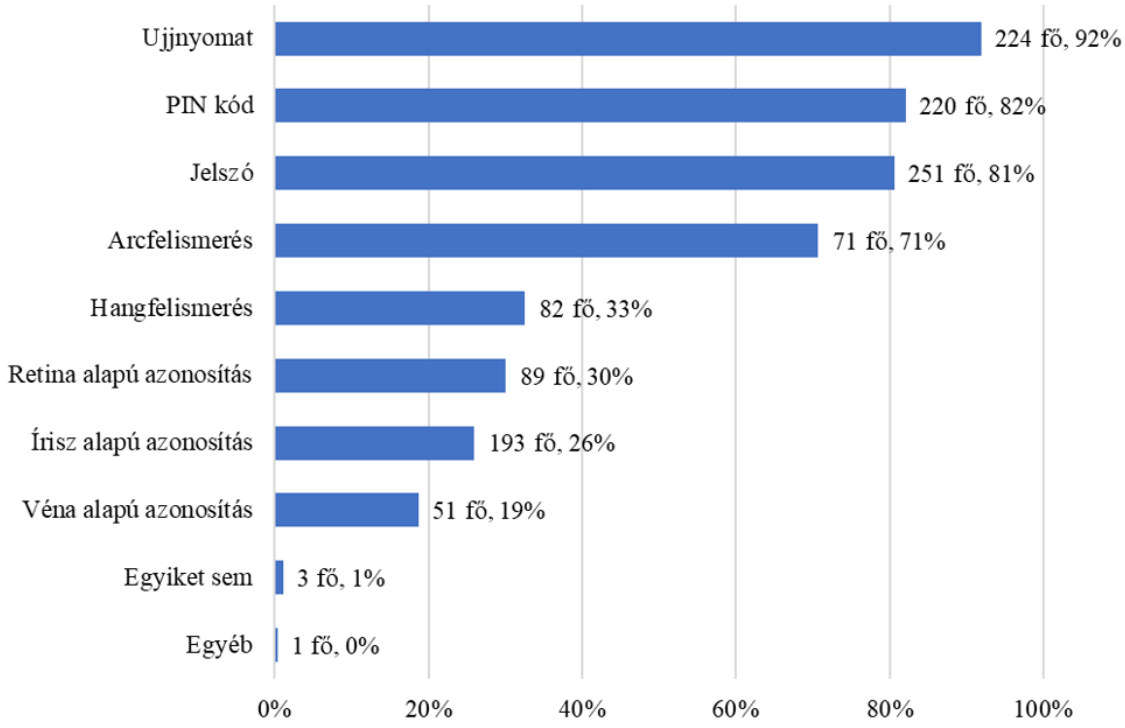
[10] Az ábrát a szerző készítette.



6. ábra: A „Ha hallott már biometrikus megoldásokról, melyik személyazonosítási módokat ismeri/használta már?” kérdésre adott válaszok jelölési aránya a teljes mintán. (Zárójelben a posthoc tesztek eredményei alapján keletkezett szignifikáns eltéréseket jelölő kódok, ahol az eltérőek szignifikáns eltérést (pl. a≠b), a megegyezők/tartalmazók (c=c, cd=d) annak hiányát jelentik.)[11]

A 7. ábrán látható, hogy a „hallott már biometrikus megoldásokról, melyik személyazonosítási módokat ismeri/használta már?” kérdésre adott válaszok jelölési aránya azok között a válaszadók között, aki a felületesen ismeri a biometrikus megoldások választ választották.

[11] Az ábrát a szerző készítette.



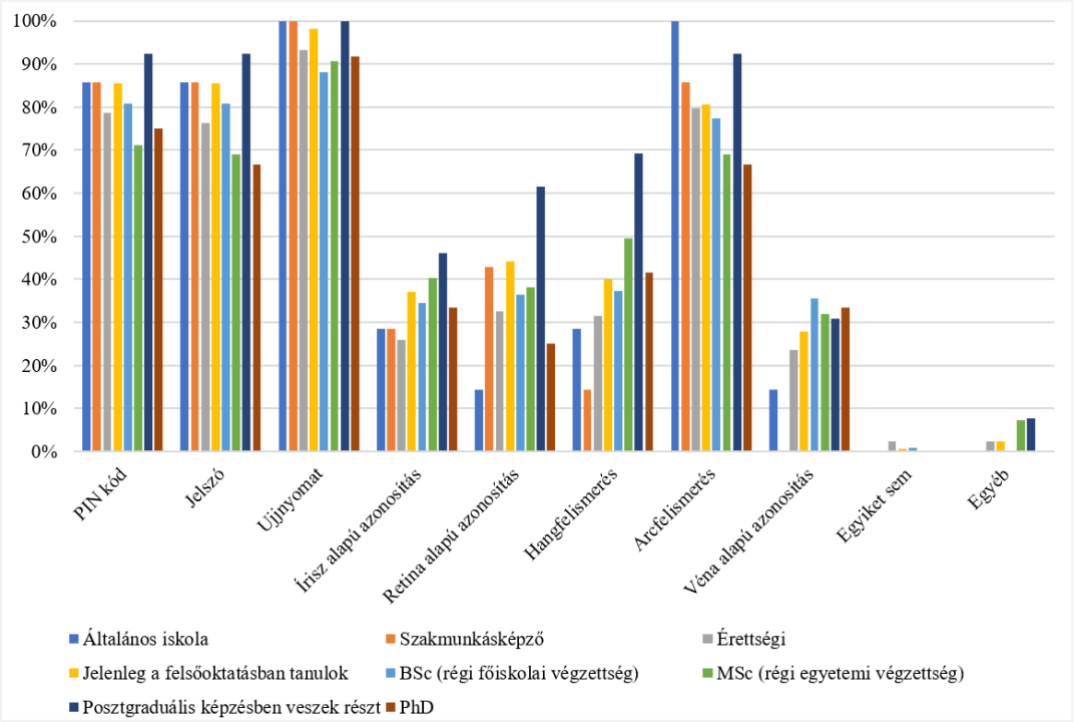
7. ábra: A „hallott már biometrikus megoldásokról, melyik személyazonosítási módokat ismeri/használta már?” kérdésre adott válaszok jelölési aránya a felületes ismeretekkel rendelkező között. [12]

Iskolai végzettség szerinti eredmények

Legmagasabb iskolai végzettség --->	Általános iskola	Szakmunkásképző	Érettségi	Jelenleg a felsőoktatásban tanulok	BSc (régi főiskolai végzettség)	MSc (régi egyetemi végzettség)	Posztgraduális képzésben veszek részt	PhD	Összesen
PIN kód	86%	86%	79%	85%	81%	71%	92%	75%	80%
Jelszó	86%	86%	76%	85%	81%	69%	92%	67%	79%
Ujjnyomat	100%	100%	93%	98%	88%	91%	100%	92%	94%
Írisz alapú azonosítás	29%	29%	26%	37%	35%	40%	46%	33%	35%
Retina alapú azonosítás	14%	43%	33%	44%	36%	38%	62%	25%	39%
Hangfelismerés	29%	14%	31%	40%	37%	49%	69%	42%	40%
Arcfelismerés	100%	86%	80%	81%	77%	69%	92%	67%	78%
Véna alapú azonosítás	14%	0%	24%	28%	35%	32%	31%	33%	29%
Egyiket sem	0%	0%	2%	1%	1%	0%	0%	0%	1%
Egyéb	0%	0%	2%	2%	0%	7%	8%	0%	3%

7. táblázat: Iskolai végzettség szerint az azonosítási megoldások ismertségi aránya[13]

[12] Az ábrát a szerző készítette.
[13] A táblázatot a szerző készítette.



8. ábra: Iskolai végzettség szerint az azonosítási megoldások ismertségi aránya[14]

Általános iskola: Az általános iskolai végzettséggel rendelkező válaszadók 100%-os ujjlenyomat- és arcfelismerő módszerek ismeretéről/használatáról számoltak be, ami az összes kategória közül a legmagasabb. Az írisz alapú, a retina alapú, a hangfelismerés és a véna alapú azonosítás ismerete/használata viszonylag alacsonyabb.

Szakmunkásképző: Ebben a csoportban az ujjlenyomat-azonosítás 100%-a, a PIN-kód, a jelszó és az arcfelismerés pedig magas százalékban jelenik meg. Nevezetesen, 0%-nak van ismerete a vénaalapú azonosítás kapcsán.

Érettségi: A diplomások aránya a legtöbb kategóriában valamivel alacsonyabb az alapfokú végzettségűekhez képest, és továbbra is az ujjlenyomat-azonosítás a legismertebb/használt: 93 százalék.

Felsőoktatás (jelenlegi hallgatók): Ezek a válaszadók minden kategóriában magas százalékarányról számoltak be, 98%-os ujjlenyomat-azonosítással, ami arra utal, hogy a jelenlegi felsőoktatási hallgatók széles körben ismerik és használják a biometrikus megoldásokat.

[14] Az ábrát a szerző készítette.

BSc (régi főiskolai végzettség): Az alapdiplomával rendelkezők számára az ujjlenyomat-azonosítás ismerete/használata magas, 88%-os, de észrevehetően visszaesik az írisz alapú, a retina alapú és a hangfelismerés a jelenleg magasabb végzettségűekhez képest.

MSc (régi egyetemi diploma): Ez a csoport 91%-ban nagyfokú jártasságot mutat az ujjlenyomat-azonosításban, és jelentős mértékben ismeri/használja az egyéb módszereket, például az írisz alapú és a hangfelismerést. 7% az „Egyéb" kategóriában is, ami a második legmagasabb a posztgraduális válaszadók után.

Posztgraduális képzés: A posztgraduális képzésben részt vevő válaszadók az írisz alapú (46%), a retina alapú (62%) és a hangfelismerő (69%) módszerek ismeretéről/használatáról számoltak be. Az „Egyéb" módszerek esetében is magas, 8%-os arányuk van, ami arra utal, hogy ismerik vagy használtak kevésbé elterjedt azonosítási módszereket.

PhD: A doktori fokozattal rendelkező válaszadók eltérően ismerik a különböző módszereket: jelentős arányban 92% az ujjlenyomat-azonosítás, de alacsonyabb százalék az újabb vagy kevésbé elterjedt technológiák esetében, mint például a retina-alapú azonosítás és a vénás azonosítás.

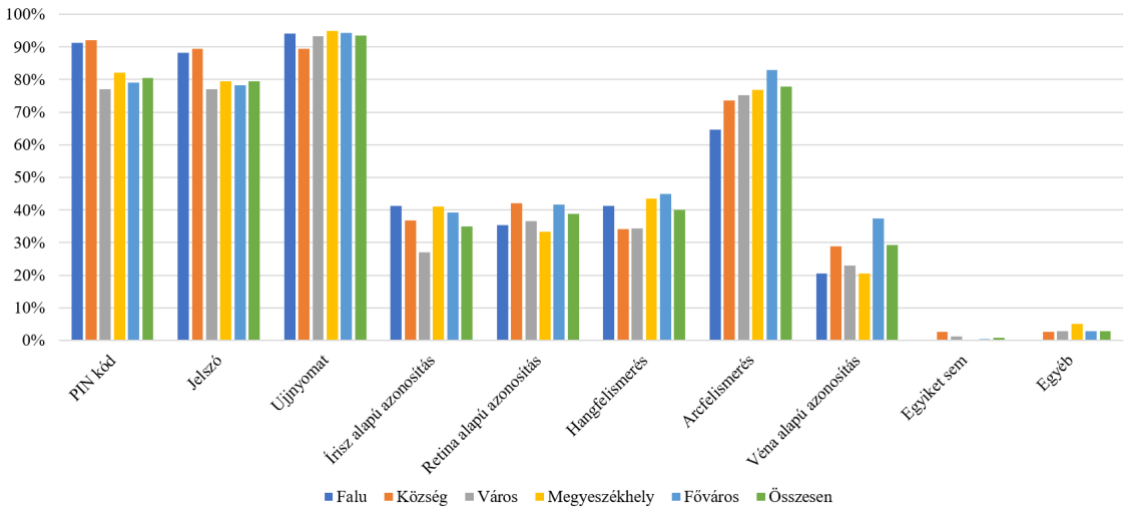
Összességében az ujjlenyomat- és arcfelismerés a legismertebb/használt azonosítási módszer minden oktatási szinten. Az a tendencia, hogy az iskolai végzettség emelkedésével a kifinomultabb biometrikus módszerek (például írisz alapú, retina alapú, hangfelismerés) ismertsége vagy alkalmazása is növekszik. Vannak azonban kivételek, mint például a retina alapú azonosítás magas szintű ismerete a szakképzésben részt vevők körében, és az arcfelismerés aránya a PhD-vel rendelkezők körében más kategóriákhoz képest. Az „Egyéb" kategóriát leginkább a posztgraduális képzésben részt vevők jelölik meg, ami arra utal, hogy ki vannak téve a felmérésben fel nem sorolt azonosítási módszereknek, vagy ismerhetnek ilyen módszereket.

Lakhely szerinti eredmények

A 8. táblázat az emberek különböző azonosítási módszerek ismertségéről vagy használatáról szóló felmérési adatokat tartalmaz, lakóhelyük szerint szegmentálva.

Lakhely jellege	Falu	Község	Város	M.székhely	Főváros	Összesen
PIN kód	91%	92%	77%	82%	79%	80%
Jelszó	88%	89%	77%	79%	78%	79%
Ujjnyomat	94%	89%	93%	95%	94%	94%
Írisz alapú azonosítás	41%	37%	27%	41%	39%	35%
Retina alapú azonosítás	35%	42%	37%	33%	42%	39%
Hangfelismerés	41%	34%	34%	44%	45%	40%
Arcfelismerés	65%	74%	75%	77%	83%	78%
Véna alapú azonosítás	21%	29%	23%	21%	37%	29%
Egyiket sem	0%	3%	1%	0%	0%	1%
Egyéb	0%	3%	3%	5%	3%	3%

8. táblázat: Lakhely szerinti megoszlás[15]



9. ábra: Lakhely szerinti megoszlás[16]

Falu: A falvak lakói arról számolnak be, hogy az alapvető biztonsági intézkedéseket, például a PIN-kódokat (91%) és a jelszavakat (88%) jól ismerik vagy használják. Az ujjlenyomat-azonosítás terén is kiemelkedően magas az ismerete (94%). A fejlettebb biometrikus technológiák, például az írisz és a retina alapú azonosítás, valamint a hangfelismerés azonban kevésbé ismertek ennek a csoportnak. Az arcfelismerést a többség (65%) ismeri, míg a legkevésbé a vénaalapú azonosítást (21%).

[15] A táblázatot a szerző készítette.
[16] Az ábrát a szerző készítette.

Község: Az adatok nagyon hasonlóak a falvakéhoz, az arcfelismerés (74%) és a vénás azonosítás (29%) ismeretében vagy használatában valamivel magasabb. Ez arra utal, hogy a biometrikus módszerek könnyebben hozzáférhetőek vagy ismertebbek a községekben, mint a falvakban.

Város: A városlakók alacsonyabb százalékban ismerik vagy használják a PIN-kódokat és jelszavakat, mint a falubeliek/községekben élők. Az ujjlenyomat-azonosítás ismerete azonban magas (93%). Az olyan fejlett biometrikus adatok, mint az írisz és a retina alapú azonosítások, kevésbé ismertek, hasonlóan a kisebb közösségekhez. Az arcfelismerés meglehetősen gyakori (75%), de a vénaalapú azonosítást kevesebben (23%) ismerik.

Megyeszékhely: Ez a csoport rendelkezik a legtöbb bejelentett ujjlenyomat-azonosító használattal vagy ismeretekkel (95%). Más biometrikus módszerekkel, mint például az írisz alapú, a retina alapú és a hangfelismeréssel kapcsolatos ismeretük közepes szintű hasonlóan a többi lakóhelytípushoz képest. A megyeszékhely lakói jelentős mértékben ismerik az arcfelismerést (77%).

Főváros: A fővárosiak az ujjlenyomat (94%) és az arcfelismerő (83%) azonosítási módszerek magas szintű ismeretéről vagy használatáról számoltak be, ami a biometrikus technológiákhoz való jobb hozzáférést vagy azok nagyobb mértékű alkalmazását jelezheti. Arról is beszámolnak, hogy a kisebb területekhez képest jobban ismerik a vénaalapú azonosítást (37%).

Általánosságban elmondható, hogy egy tendencia azt mutatja, hogy a fejlettebb biometrikus technológiák általában kevésbé ismertek az emberek számára, függetlenül attól, hogy hol élnek, és az arc- és ujjlenyomat-felismerés a leggyakoribb az összes lakástípusban. Ez annak tudható be, hogy e technológiák széles körben elterjedtek a mobileszközökön és más elérhető platformokon. Az adatok arra is utalnak, hogy a sűrűbben lakott vagy városi területeken (városok, megyeszékhelyek, fővárosok) lakók jobban ismerik az azonosítási módszerek szélesebb körét, ami a technológiához való jobb hozzáférést tükrözheti ezeken a területeken.

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 azonosítási módok, amelyek szinte minden válaszadó számára ismertek (pl: ujjnyomat (CI95: 91,45%; 95,75%), PIN kód (CI95: 76,91%; 83,89%), jelszó (CI95: 76,91%; 83,89%) és arcfelismerés (CI95: 74,14%; 81,46%)), de vannak olyanok is, amit csak kevesen ismernek (pl.: véna alapú azonosítás

(CI95: 25,20%; 33,20%), írisz alapú azonosítás (CI95: 30,80%; 39,20%), retina alapú azonosítás (CI95: 34,51%; 43,09%), és hangfelismerés (CI95: 35,69%; 44,31%)). Kimondható, hogy vannak olyan területek, ahol a biometrikus azonosítási megoldások alkalmazása a lakosság széleskörű támogatottságát élvezi. Az írisz és az érhálózatot tartják a legbiztonságosabbnak, ez kimutatható volt az indirekt kapcsolatból, de hogy mennyire támogatják a megkérdezettek az egyik, vagy a másik azonosítást, azt további kutatásokkal, direkt kapcsolatot kutató kérdésekkel lenne lehetséges vizsgálni.

H4 hipotézis vizsgálata: Feltételezem, hogy az Óbudai Egyetemen végzett kutatás óta 2014-ről 2022-re a biometrikus adatok nyilvántartásba vételével kapcsolatos vélemény megváltozott és javulást mutat.

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.

A minták összetételében mutatkozó különbségek felismerése döntő fontosságú e vizsgálatok eredményeinek értelmezésekor. A rendőrök hivatásukból adódóan egyedi perspektívával rendelkeznek a rendészeti, biztonsági és adatvédelmi kérdésekben, ami jelentősen befolyásolhatja a biometrikus adatok nyilvántartásával kapcsolatos véleményüket. Ez a szakmai nézőpont olyan elfogultságot eredményezhet, amely nem tükrözi a szélesebb közvéleményt. Ezenkívül a biometrikus technológiának való napi kitettségük a bűnüldözési kontextuson belül arra késztetheti őket, hogy tájékozottabb és potenciálisan kedvezőbb véleményük legyen az ilyen technológia hasznosságáról és megbízhatóságáról. Ezért, ha összehasonlítjuk válaszaikat a nagyközönség és az egyetemi lakosság válaszaival – akiknek nem biztos, hogy azonos szintű a kitettsége, vagy a szakmai érdeklődése a biometrikus adatok iránt, – olyan eredményeket kaphatunk, amelyek nem hasonlíthatók össze közvetlenül a mögöttes tapasztalati és perspektívabéli különbségek miatt.

Kutatásomban az összehasonlítás korlátainak felvázolásakor fontos, hogy átláthatóak legyünk azon tényezők tekintetében, amelyek megkérdőjelezik a két adatsor közvetlen összehasonlíthatóságát. Az eredeti tanulmány, amelyet a rendőri állomány egy meghatározott csoportjával végeztek, a biometrikus adatokkal kapcsolatos speciális ismeretekkel és attitűdökkel rendelkező demográfiai csoportot képviseli. Másrészt, a

jelenlegi kutatás egy szélesebb demográfiai csoportot ölel fel, amely magában foglalhat olyan egyéneket, akik sokféle tapasztalattal és a biometrikus technológiában jártassággal rendelkeznek. Az idő múlásával a technológiával és a magánélettel kapcsolatos társadalmi attitűdök fejlődtek, és ezek a változások valószínűleg az eltérő válaszokban is megmutatkoznak. Ezen túlmenően a két tanulmány közötti módszertani eltérések, beleértve a kérdőívek felépítésének lehetséges különbségeit és a felmérések közötti nyolc év közötti különbséget, azt jelentik, hogy minden közvetlen összehasonlítást átgondoltan kell megközelíteni. Bár a közvetlen statisztikai összehasonlítás e korlátok miatt nem biztos, hogy megbízható, a tanulmányok még mindig értékes betekintést nyújtanak a biometrikus adatok nyilvántartásával kapcsolatos közvélemény időbeli változásaiba.

Elsőként a biometrikus rendszerekkel kapcsolatos pozitív attitűd összehasonlítását végeztem el független mintás T-próbával (7-es kérdés: Tetszenek a biometrikus rendszerek, szívesen használom őket kérdés alapján). Mivel a 2022-es felmérés erre a területre vonatkozó kérdése egy négy fokozatú, míg a 2014-es kérdőív kérdése egy 5-fokozatú skálán mérte a megkérdezettek válaszait, ezért a 2014-es kérdőív adatait transzformáltam egy 1-től 4-ig tartó ötfokozatú skálára. Ezután már összehasonlíthatóak 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 8 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 megfigyeléssel, adatokkal történő visszaéléssel kapcsolatos kiemelt történései (Pegazus botrány, Kínai megfigyelő rendszerek hírei) az 1984-es orwelli vizionálás érzetét keltik a népesség körében, 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 öt fokozatú 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. De aztán belegondolva a válaszokba, logikusabbnak gondoltam 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 kérdése 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, (51%, 255 fő)
- Tetszik, érdekel a működésük, (38,4%, 192 fő)
- Biztonságos, (38,8%, 194 fő)
- Modern, gyors, egyszerű, (65%, 325 fő)
- Fontos a kényelem és a mögöttes szolgáltatás, (31,2%, 156 fő)

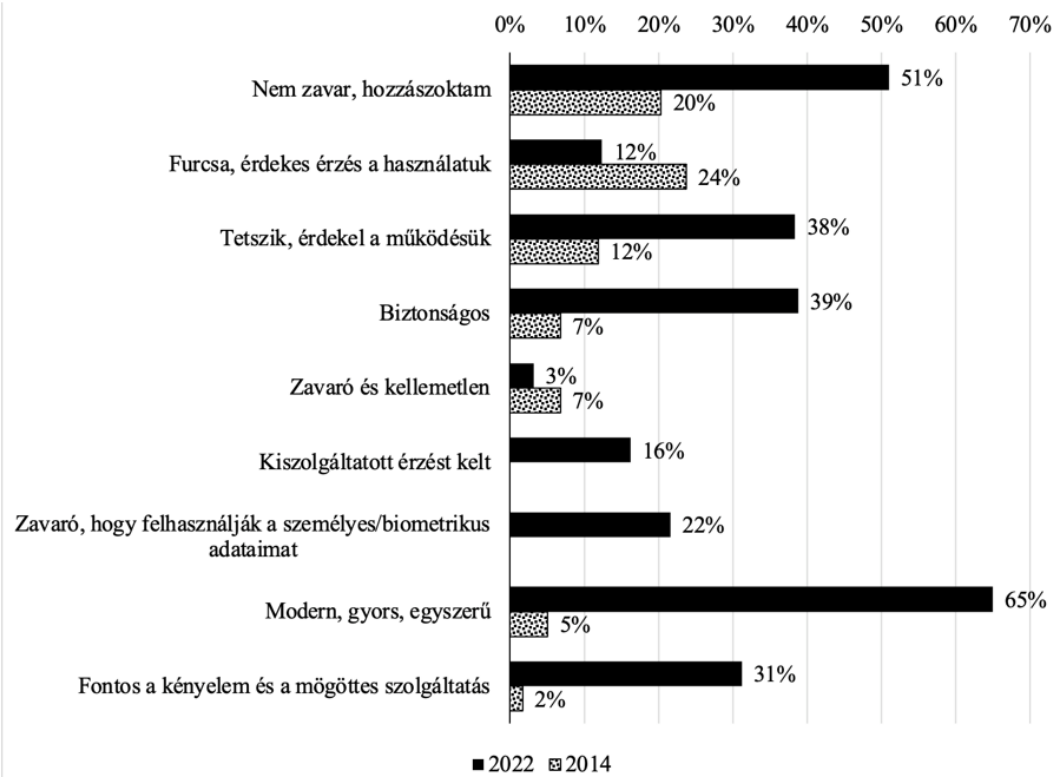
A következő tényezők pedig kisebb arányban kaptak jelölést 2022-ben 2014-hez viszonyítva:

- Furcsa, érdekes érzés a használatuk, (12,4%, 62 fő)
- Zavaró és kellemetlen, (3,2%, 16 fő)

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 beléptető rendszerekhez kapcsolódó érzelmi és gondolati attitűdök pozitív irányba változtak az elmúlt nyolc év alatt. Lásd 9. táblázat és 10. ábra.

	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

9. táblázat: A beléptető rendszerekhez kapcsolódó érzelmi és gondolati attitűdök alakulása 2014-ről 2022-re, valamint az összehasonlító tesztstatisztikák[17]



10. ábra: A beléptető rendszerekhez kapcsolódó érzelmi és gondolati attitűdök alakulása 2014-ről 2022-re. [100]

A négy demográfiai változó (nem, korcsoport, lakhely jellege, legmagasabb iskolai végzettség) viszonylatában megvizsgáltam azt, hogy az egyes biometrikus azonosítási megoldásokat hogyan rangsorolták a megkérdezettek biztonság szempontjából. A nők és a férfiak egyetlen azonosítási megoldást sem értékeltek eltérő módon (2022-es kérdőívben), azaz szignifikáns különbség nem mutatható ki a négy azonosítási megoldás nemek szerinti megítélése esetén. Lásd 10. táblázat.

[17] A táblázat a szerző saját szerkesztése.

	Nem	n	Átlag	Szórás	Levene (F/Szig)	T-próba* (t/szig)
Ujjnyomat alapú 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
Írisz alapú 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

10. táblázat: A biometrikus azonosítási megoldások megítélése a nők és a férfiak szerint, továbbá az összehasonlító statisztikáik.[18]

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 mutat jelentős összefüggést a demográfiai változók és a biometrikus azonosítás megoldások megítélése között, azonban ezek mind gyenge kapcsolatok, és többségében nem mutatható ki szignifikáns összefüggés a vizsgált változók között. Lásd 11. táblázat.

	Ujjnyomat alapú azonosítás	Arc-felismerés	Írisz alapú 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**
	(0,870)	(0,360)	(0,486)	(0,034)

11. 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[19]

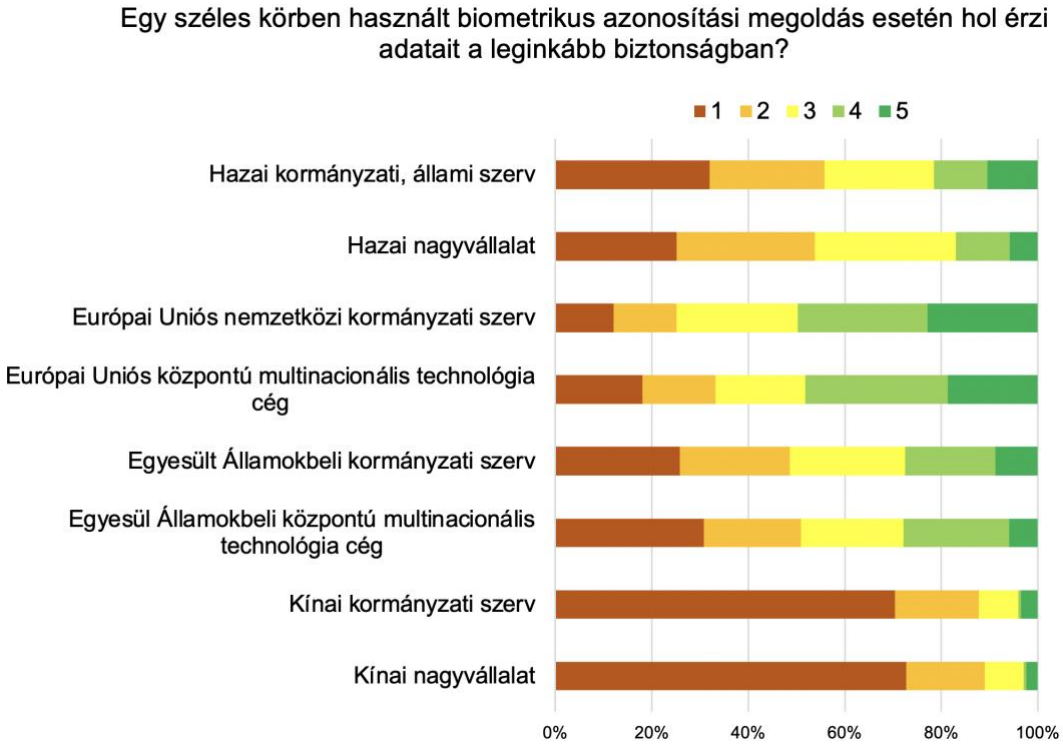
[18] A táblázat a szerző saját szerkesztése.
[19] A táblázat a szerző saját szerkesztése.

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?

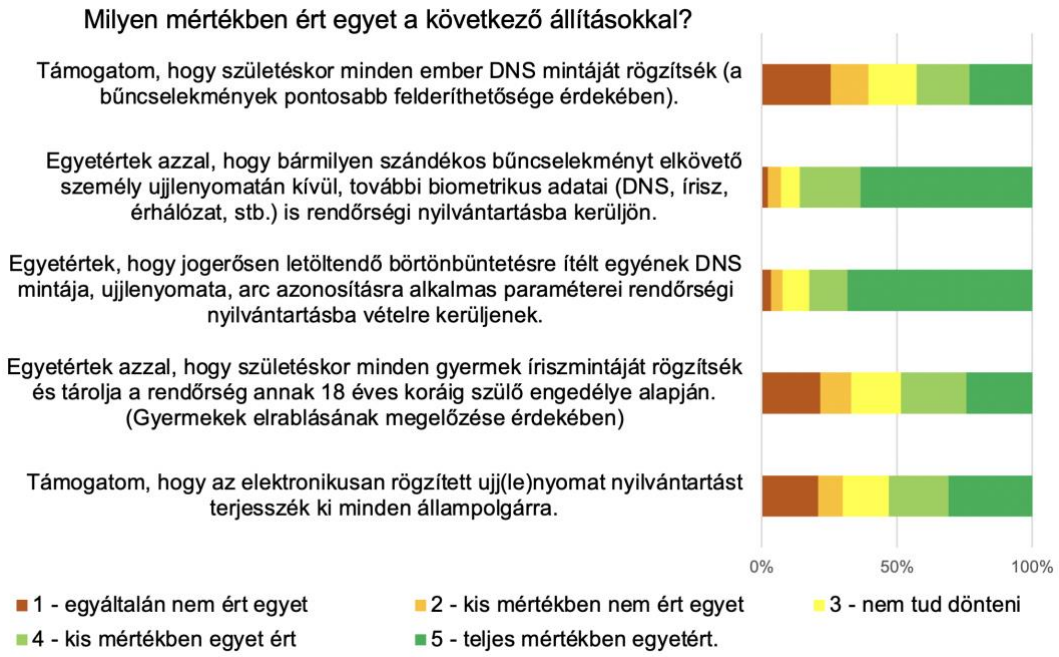


11. ábra: Hol érezzük az adatainkat leginkább biztonságban.[20]

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.

[20] Az ábrát a szerző készítette.

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



12. ábra: Biometrikus adatok rögzítésével kapcsolatos válaszok.[21]

A feltett kérdéseket kiértékelve megállapítható, hogy a válaszadók egy része támogatja a DNS minták születéskori rögzítését és ugyanennyi rész ellenzi.

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

Sokkal határozottabb a helyzet azonban, amikor egy bűncselekmény elkövetőjéről van szó. Ebben az esetben ugyanis a válaszadók jól láthatóan 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 tájékoztatást, 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)

[21] Az ábrát a szerző készítette.

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 10 évben.

3.4. Saját kérdőíves kutatás összefoglalása, következtetések

Az összeállított kérdőívet 500-an töltötték ki, a korábbi kutatásoknál nagyobb létszámon és szélesebb körben történt a felmérés (nem csak egyetemi és rendőri állományon). A biometrikus megoldások ismertsége nőtt az elmúlt időkben, ami nem meglepő az okos eszközök és a biometriával összefüggő azonosítási és hitelesítési megoldások terjedése mellett. A biometrikus rendszerek elfogadottsága az elmúlt 8 évben szignifikánsan romlott. Hipotézisem megválaszolásaként kijelenthető, hogy a biometrikus azonosítási módszerek széleskörű elterjedésének legfőbb gátja a széleskörű társadalmi elfogadás hiánya, viszont emellett vannak olyan területek, ahol a biometrikus azonosítási megoldások ismertsége és alkalmazása a lakosság széleskörű 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 beléptető rendszerekhez kapcsolódó érzelmi és gondolati attitűdök pozitív irányba változtak az elmúlt nyolc év alatt. Következtetésem, hogy az elmúlt évek alatt a felhasználók jobban hozzászoktak ezekhez a rendszerekhez, kevésbé érzik furcsának azokat, 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?

A válaszadók 71%-a tart attól, hogy a biometrikus adatai illetéktelen kezekbe kerül. Ez egy nagyon magas érték és következtetésem, hogy 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 törvényi és szabályzati keretek megfelelőek legyenek, és támogatják a személyes adatok védelmét, ott a felhasználók is jobban szavaznak bizalmat 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.

4. ÖSSZEGZETT KÖVETKEZTETÉSEK

Új tudományos eredmények

Értekezésemben a hazai biometrikus azonosítás elterjedésének elemző vizsgálatát végeztem el. Az értekezést alátámasztó kutatásokból megállapítottam, hogy a biztonság, a biometria és a mesterséges intelligencia a jövőben jobban össze fog olvadni, így az adatvédelem és a jogi környezet fejlődése a téma elengedhetetlen része marad.

Az eredményeim az alábbiak.

H1: Igazoltam, hogy a biometrikus azonosítási módszerek széleskörű elterjedésének legfőbb gátja még ma is a társadalmi elfogadás hiánya.

H2: Igazoltam, hogy a biometrikus azonosítás jogszabályi környezete összefüggést mutat a mesterséges intelligencia fejlődésével és szabályozásával.

H3: Igazoltam, hogy vannak olyan biometrikus azonosítási megoldást használó területek, ahol a biometrikus azonosítási megoldások alkalmazását a lakosság széles körűen támogatja.

H4: Megcáfoltam, hogy az Óbudai Egyetemen végzett kutatás óta 2014-ről 2022-re a biometrikus adatok nyilvántartásba vételével kapcsolatos vélemény megváltozott és javulást mutat.

H5: Igazoltam, hogy a biometrikus azonosítás meghatározása nem követi a technika fejlődését és ezért pontosítható az, a mai kornak megfelelő újabb azonosítási eljárásokkal.

Ajánlások

A témával kapcsolatban további kutatásra javaslom az alábbi pontokat.

Kvalitatív (fókuszcsoportos) kérdőíves kutatással feltárni a biometrikus rendszerek felhasználóinak attitűdjét, és annak befolyásolására alkalmas eszközöket, és vizsgálni a felhasználói elfogadottság széles körben történő fokozásának lehetőségeit. Az attitűd vizsgálatot érdemes lenne nagyobb létszámú csoportokon vizsgálni a biometriával kapcsolatosan, amikor a véleményvezérek kevésbé érvényesülnek.

A mintakinyerés szabványosításával és erre alapuló megoldásokkal, multimodális rendszerek egymásra épülésével és egymás adatainak alátámasztásával miként lehetne pontosítani az azonosítási folyamatokat, hogy a mintakinyerési és összevetési

algoritmusok több forrásból származó, de kevesebb fajlagos információval is pontos eredményt adjanak.

Hazai és nemzetközi biometriával összefüggő kutatások hatásainak elemzése a biometria elterjedésével kapcsolatban.

Biometria fejlődésének történelme, mely szorosan összekapcsolódik az elterjedéssel.

Összehasonlító kutatás végzése többféle biometrikus azonosítási megoldásra tömeges beléptetés esetén, annak érdekében, hogy a megoldások sebessége, felhasználhatósága összehasonlító kutatással alátámasztható legyen.

FELHASZNÁLT IRODALOM

[1] BEREK Lajos - BEREK László - RAJNAI Zoltán: Tudományos kutatás folyamata és módszerei; 2018, ÓE-BGK 3073, ISBN 978-963-449-071-5.

[2] *BONCZ Imre: Kutatásmódszertani alapismeretek; Pécsi Tudományegyetem Egészségtudományi Kar, 2015.*

[3] ROÓZ József - HEIDRICH Balázs: Vállalati gazdaságtan és menedzsment alapjai; Budapest, 2013.

[4] *MASLOW, A.: Motivation and Personality, 1954.*

[5] LASZ György: A biztonságtechnika alapjainak megjelenése az objektumvédelem gyakorlatában; Hadmérnök, 2011, 3. sz., p. 32.

[6] *GÁL István László: Nemzetbiztonsági szakági jogi alapismeretek; NKE, 2020.*

[7] *Nemzeti Közszolgálati Egyetem online lexikon, Ludovika kiadó, https://lexikon.uni-nke.hu/szocikk/biztonsag-2/, letöltés dátuma: 2023.12.11.*

[8] *TÉGLÁSI András: A szociális jogok alkotmányos védelme – különös tekintettel a szociális biztonság alapjogi védelmére; Dialóg Campus kiadó, 2019.*

[9] FÖLDESI Krisztina: Korporális gátak a biometrikus eljárások rendvédelmi alkalmazásában; 2015. http://www.pecshor.hu/periodika/XVI/foldesi.pdf, letöltés időpontja: 2019.11.10.

[10] KISS Tibor - SZEGŐ Tamás: A személyazonosítás múltja, jelene és jövője; E-közigazgatás, 2017, 10. évf., 2. sz., pp. 54-65. https://kozszov.org.hu/dokumentumok/UMK_2017/2/06_A_szemelyazonositas_multja.pdf, letöltés ideje: 2021.06.07.

[11] *NIELES, M. - DEMPSEY, K. - PILLITTERI, V.: An introduction to information security. National Institute of Standards and Technology, Gaithersburg, MD, 2017, https://doi.org/10.6028/NIST.SP.800-12r1.*

[12] *BODA József: Rendészettudományi Szaklexikon, Dialóg Campus, 2019.*

[13] *Országgyűlés Hivatala, Képviselői Információs Szolgálat, https://www.parlament.hu/documents/10181/4464848/Infojegyzet_2020_27_biometrikus_azonositas.pdf/46c081f0-1f32-891d-1473-52d97952a958?t=1588237454148, letöltés dátuma: 2024.01.21.*

[14] *HAZAI Lászlóné: Módszerek, technikák a biometrikus arcfelismerésben, -azonosításban, Belügyi Szemle, 2019, 67. évf. 1. sz..*

[15] 95/46/EK irányelv 29. cikke alapján létrejött adatvédelmi munkacsoport: 4/2007. számú személyes adatokról szóló véleménye (WP136), 2007.

[16] *NÉMETH Attila - TÓTH Gergely: Az arcfelismerő rendszerek alkalmazása, Belügyi Szemle, 2019, 67(1),6, pp. 127–136. https://doi.org/10.38146/BSZ.2019.1.10.*

[17] KOVÁCS Tibor - MILÁK István - OTTI Csaba: A biztonságtudomány biometriai aspektusai; http://www.pecshor.hu/periodika/XIII/kovacsti.pdf, letöltés időpontja: 2019.11.10.

[18] LUIS-GARCÍA R. - LÓPEZ C. A. - AGHZOUT O. A. - ALZOLA J. R.: Biometric identification systems; Signal Processing, 2003, vol. 83 (12), pp. 2539-2557.

[19] *CZÚNI László: Biometria a számítógépes személyazonosításban - vizuális módszerek, Pannon Egyetem, 2015.*

[20] SRIVASTAVA, H.: A Comparison Based Study on Biometrics for Human Recognition; IOSR Journal of Computer Engineering, Vols. e-ISSN: 2278-0661, p-ISSN: 2278-8727, 2013, Volume 15, Issue 1, pp. 22-29.

[21] *International Elektrotechnical Commission, https://webstore.iec.ch/publication/10792, letöltés dátuma: 2023.12.12.*

[22] DOMOKOS Andrea - ORBÁN József: Az identifikáció múltja és jövője; Tanulmány; Miskolci jogi szemle, 2017, 12. évf., 1. sz., pp. 5-18.

https://www.mjsz.uni-miskolc.hu/files/egyeb/mjsz/201701/3_domokosorban.pdf, letöltés ideje: 2023.02.11.

[23] TAJTI Balázs: A biometrikus ujjnyomat azonosításának új lehetőségei; Hadmérnök, 2021, VII. Évf. 1. sz., pp. 48-58.

[24] *Tájékoztató a VIS ujjnyomat alapú ellenőrzési rendszerének bevezetéséről, Police.hu, https://www.police.hu/hu/hirek-es-informaciok/hatarinfo/vizuminformacios-rendszer, letöltés dátuma: 2024.01.20.*

[25] *MAIO, D. - MALTONI, D. - CAPPELLI, R. - WAYMAN, JL. - JAIN, A: Proceedings of international conference on pattern recognition (ICPR), 2002, pp 744–747.*

[26] *ZAHID, R.: Biometric Systems, design and applications, 2011, ISBN 978-953-307-542-6, pp. 55-108.*

[27] HEILWEIL, R.: The World's scariest facia recognition company, 2020, https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement?fbclid=IwAR0c4rkztQXDWxguNFeCa-iGHMhPKC2VVPBEiWqVA_Sey78rcA5ZJLfM7LY.

[28] NGAN, M. - GROTHER, P. - HANAOKA, K.: Ongoing Face Recognition Vendor Test (FRVT) Part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms; National Institute of Standards and Technology Interagency, 2020.

[29] SHARAN, Y. - GORDON, T. J. - FLORESCU, E.: Tripping Points on the Roads to Outwit Terror; Advanced Sciences and Technologies for Security Applications, Springier, 2021.

[30] *BOULGOURIS, N.V. - PLATANIOTIS, K.N. - TZANAKOU, E. M.: BIOMTRICS, Thory, Methods, and Applications, IEEE Press Series on Computational Intelligence, 2010, ISBN 978-0470-24782-2 , p. 315.*

[31] ŐSZI Arnold: A biometrikus azonosítási rendszerek helye és szerepe az e-kereskedelemben; PhD értekezés, Óbudai Egyetem, 2019.

[32] *JAIN, A.K. - ROSS, A.A. - NANDAKUMAR, K.: Introduction to Biometric, Springier, 2011, ISBN 978-0-387-77325-4, pp. 35-36.*

[33] *BioSec Technológia, https://www.biosecgroup.com/hu/technologia, letöltés dátuma: 2024.01.20.*

[34] *GYARMATI Ervin - KREISZ Gábor: Az informatikai biztonság helyzete Magyarországon, Taksony, 2006, pp. 172-190.*

[35] *JAIN, A.K. - FLYNN, P. - ROSS, A.A: Handbook of Biometrics, Springer kiadó, 2008, ISBN-13: 978-0-387-71040-2. pp. 91-107.*

[36] GULYÁS Laura - KOVÁCS András: Biometric Authentication System based on Hand Geometry and Palmprint Features; International Conference on Image Processing and Vision Engineering, 2021, Vol. 1. pp. 58-65. ISBN: 978-989-758-511-1.

[37] FEJES Attila: Beszéd alapján történő személyazonosítás új kihívásai a kriminalisztikában; Magyar Rendészet, 2018/2. pp. 117-126.

[38] *ANTI Csaba: A személyleírás, Semmelweis Kiadó, 2017.*

[39] Budapesti Műszaki és Gazdaságtudományi Egyetem, Távoli személyazonosítási technikák irodalomkutatás kötet, 2005.

[40] *https://www.kfki.hu/~cheminfo/hun/hir/cikk/dns.html, letöltés dátuma: 2024.02.02.*

[41] ŐSZI Arnold: Az e-kereskedelem elvárásai a biometriával szemben; MEB 2014, 12th International Conferenceon Management, Enterprise and Benchmarking, Budapest, Hungary, 2014. Május 30-31, HU ISSN 2061-9499.

[42] *SALAMIN Ágota: Biometrikus aláírás technológiájának vizsgálata adatvédelmi, illetve információbiztonsági szempontból, Szakcikk adatbázis, 2020/2.*

[43] *VIGH András: A kézírásvizsgálat mint a személyazonosítás eszköze, Dialóg Campus, 2020.*

[44] *Egérmozgás azonosítása, https://sentinel.graboxy.com/, letöltés időpontja: 2023.09.29.*

[45] GÁLAI Bence - BENEDEK Csaba: Járás alapú személyazonosítás és cselekvésfelismerés LiDAR szenzorokkal; MTA, In: Képfeldolgozók és Alakfelismerők Társaságának Konferenciája, Szovata, Románia. http://real.mtak.hu/63650/1/Galai_Benedek_Kepaf.pdf.

[46] *WERNER Gábor Ákos: A multimodális biometrikus azonosító rendszerek kockázat alapú vizsgálata Fuzzy logika és neurális hálózatok segítségével; PhD értekezés, Óbudai Egyetem, 2019.*.

[47] WENDEHORST, C. – DULLER, Y.: Európeam Parliament Study: Biometric Recognition and Behavioural Detection; 2021 augusztus, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf, letöltés ideje: 2023.04.11.

[48] Európai Parlament és a Tanács, 2016/680 irányelve, https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L0680, letöltés ideje: 2023.04.11.

[49] PÓK László: Jönnek az adatszövetkezetek?, 2022. https://gdpr.blog.hu/2022/06/27/jonnek_az_adatszovetkezetek#more17867113, letöltés ideje: 2022.12.01.

[50] *Az Európai Parlament és a Tanács 2016/679 rendelete, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.HUN&toc=OJ:L:2016:119:FULL119%3AFULL#d1e1459-1-1 letöltés dátuma: 2024.02.01.*

[51] *https://www.brookings.edu/articles/the-us-government-should-regulate-ai/, letöltés dátuma: 2024.02.01.*

[52] *https://copyrightblog.kluweriplaw.com/2023/05/22/generative-ai-services-in-china-public-consultation-on-the-regulation-for-generative-artificial-intelligence-services/, letöltés dátuma: 2024.02.01.*

[53] *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1176103/a-pro-innovation-approach-to-ai-regulation-amended-web-ready.pdf, letöltés dátuma: 2024.02.01.*

[54] *https://www.oecd.org/digital/artificial-intelligence/, letöltés dátuma: 2024.02.01.*

[55] *https://www.unesco.org/en/artificial-intelligence/recommendation-ethics, letöltés dátuma: 2024.02.01.*

[56] *https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f, letöltés dátuma: 2024.02.01.*

[57] *https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html, letöltés dátuma 2024.02.01.*

[58] *https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/2012(INL), letöltés dátuma: 2024.02.01.*

[59] *https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html, letöltés dátuma: 2024.02.01.*

[60] *https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf, letöltés dátuma: 2024.02.01.*

[61] *https://wayback.archive-it.org/12090/20210304034028/https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence, letöltés dátuma: 2024.02.01.*

[62] *https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence, letöltés dátuma: 2024.02.01.*

[63] *https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1/language-en, letöltés dátuma: 2024.02.01.*

[64] *https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206, letöltés dátuma: 2024.02.01.*

[65] *https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en, letöltés dátuma: 2024.02.01.*

[66] *https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf, letöltés dátuma. 2024.02.01.*

[67] *Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése, COM(2020) 65 final, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0065, letöltés ideje: 2023.04.11.*

[68] *COM(2018) 237 final, EU AI (MI) stratégia. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN, letöltés ideje: 2023.03.25.*

[69] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206, letöltés dátuma: 2024.02.01.*

[70] *EURÓPAI PARLAMENT ÉS A TANÁCS: COM(2018) 795 Coordinated plan on Artificial Intelligence. https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2018)795&lang=en letöltés ideje: 2023.07.16.*

[71] *COM(2021) 206 final, 2021/0106 (COD), A mesterséges intelligenciára vonatkozó harmonizált szabályok (az MI-ről szóló jogszabály) megállapításairól. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206, letöltés ideje: 2023.04.11.*

[72] *nternational standard, IEC/FDIS 31010:2009, 11. oldal 5. fejezet.*

[73] *RATHA, N. K.; CONNELL, J. H.; BOLLE, R. M.: "An Analysis of Minutiae Matching Strength," Proceedings of the 3rd International Conference on Audio-*

and Video Based Biometric Person Authentication (AVBPA '01), Vols. Halmstad, Sweden, June 2001, pp. 223-228.

[74] *ZHANG, D. - LU, G.: 3D Biometrics - Systems and Applications. Springer, Hong Kong, 2013, ISBN 978-1-4614-7399-2.*

[75] *https://www.idemia.com/press-release/idemia-cements-its-biometric-technologies-leadership-latest-nist-rankings-2023-09-07, letöltés dátuma: 2023.12.01.*

[76] *JIANG, R. - AL-MAADEED, S. - BOURIDANE, A. - CROOKES, P.D. - BEGHDAD, A. (eds): Biometric Security and Privacy. Signal Processing for Security Technologies. Springer, Cham. 2016. https://doi.org/10.1007/978-3-319-47301-7_2.*

[77] *KARIMI, Z.: A big survey on Biometric for Human Identification, Springer, 2022.*

[78] *SUNIL, S.H. - PRASHANTH, C.R. - RAJA, K.B.: Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends. International Journal of Advanced Networking and Applications. 2019. 10. 3958-3968. 10.35444/IJANA.2019.10048..*

[79] *WANG, Y. - DASS, S.C. - MAHOO, M.H.: Facial Expressions as a Vulnerability in Face Recognition, kiadó: IEEE Transactions on Biometrics, Behavior, and Identity Science, 2021, https://ieeexplore.ieee.org/document/9506444, letöltés dátuma: 2024.02.01.*

[80] *MARKOWITZ, J.: Voice Biometric, https://www.researchgate.net/publication/27293606_Voice_Biometrics, letöltés dátuma: 2024.02.01.*

[81] *RATHA, N.K. - CONNELL, J.H. - BOLLE, R.M.: Remote Fingerprinting on Internet-Wide Printers Based on Neural Network, kiadó: IEEE Security & Privacy, 2011, https://ieeexplore.ieee.org/document/9014144, letöltés dátuma: 2024.02.02.*

[82] *Európai Bizottság, Tabula Rasa project, Biometrikus rendszerek sérülékenységeinek kutatása, ec.europa.eu/commission/presscorner/detail/en/MEMO_13_924, letöltés dátuma: 2024.02.02.*

[83] *ŐSZI Arnold - KOVÁCS Tibor: Theory of the Biometric-based Technology in the field of e commerce, CINTI 12th IEEE International Symposium, Óbuda University, 2011. november 21-22, ISBN: 978-1-4577-0043-9. pp 569-571.*

[84] BALLA József: A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ-, illetve közbiztonság alakulására; Dialóg Campus Kiadó, Budapest, 2019.

[85] *AHMAD, Z. - AJMAL, M. - AHMAD, F. - CHAUDARY, M.H. - NASEER, M.: Comparative Analysis of Biometric Recognition Techniques. Bahria University Journal of Information and Communication Technologies, 2018, Vol11, Issue 1, ISSN – 1999-4974.*

[86] *TRIPATHI, P.: "A Comparative Study of Biometric Technologies with Reference to Human Interface", International Journal of Computer Applications, 2011, 14(5), pp. 10-15.*

[87] *SRIVASTVA, H.: "A Comparison Based Study on Biometrics for Human Recognition", International Journal of Computer Engineering, 2013, vol.15, pp. 22-29.*

[88] *ISO31010 - B.29 Consequence/Probability matrix elemzés.*

[89] *Európai Parlament, Artificial Intelligence Act, COM(2021)206 21.4.2021 2021/0106(COD) https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf, letöltés dátuma: 2024.02.20.*

[90] *https://enterprisealliance.eu/wp-content/uploads/2021/10/Joint-Letter-on-AI-Proposal.pdf, letöltés dátuma: 2024.02.28.*

[91] *https://algorithmwatch.org/en/wp-content/uploads/2021/08/EU-AI-Act-Consultation-Submission-by-AlgorithmWatch-August-2021.pdf, letöltés dátuma: 2024.02.28.*

[92] *ISO/IEC 17799:2005: Information technology — Security techniques — Code of practice for information security management, 2005. https://www.iso.org/standard/39612.html, letöltés ideje: 2022.12.01.*

[93] *COBIT: https://www.isaca.org/resources/cobit, letöltés ideje: 2022.12.01.*

[94] *KING, M. - DALTON, C. - OSMANOGLU, T.: Security Architecture. RSA press USA, 2001..*

[95] *American National Standards Institute: American National Standard for Financial Services. ANSI X9.84-2018. Biometric Information Management and Security for the Financial Services Industry. 2018. https://webstore.ansi.org/standards/ascx9/ansix9842018.*

[96] *IST-1999-20078 Business environment of biometrics involved in e-commerce: https://cordis.europa.eu/project/id/IST-1999-20078/results, letöltés ideje: 2022.12.01.*

[97] *GANDOLFI, K. - MOURTEL, C. - OLIVIER, F.: Electromagnetic Analysis: Concrete Results. Lecture Notes in Computer Science, Springer-Verlag, 2001, Vol. 2162. pp. 251-261.*

[98] *KOCHER, P. - JAFFE, J. - JUN, B. és társai: Introduction to differential power analysis. Journal of Cryptographic Engineering, 2011, vol. 1, pp. 5–27. https://doi.org/10.1007/s13389-011-0006-y.*

[99] OTTI Csaba - VALOCIKOVÁ Cyntia: Biztonsági rendszerek felhasználói attitűdje, értékelése és befolyásolásának lehetőségei; Hadmérnök, 2019, XIV. évf., 1. sz., pp. 32-41.

[100] FÖLDESI Krisztina - KOVÁCS Tibor: Összehasonlító kutatáselemzés a biometrikus személyazonosító-beléptető rendszerek, eljárások 2006. és 2014. évi társadalmi averzív reakcióinak vizsgálatára.

[101] *https://www.securinfo.hu/wp-content/uploads/2015/06/20150602_osszehasonlito_elemzes_a_biometrikus_szemelyazonosito_rendszerek.pdf, letöltés dátuma: 2023.12.01.*

[102] LUMLEY, T. - DIEHR, P. - EMERSON, S. - CHEN, L.: The importance of the normality assumption in large public health data sets. Annual review of public health, 2002, 23, pp. 151–169.

[103] NORMAN, G.: Likert scales, levels of measurement and the "laws" of statistics. Advances in health sciences education : theory and practice, 2010, 15(5), pp. 625–632. https://doi.org/10.1007/s10459-010-9222-y.

[104] *1992. évi LXIII. Törvény, adatvédelmi törvény a személyes adatok védelméről. https://njt.hu/jogszabaly/1992-63-00-00, letöltés ideje: 2023.02.11.*

[105] *Informatikai Tárcaközi Bizottság 8. számú ajánlása, informatikai biztonsági módszertani kézikönyv. https://dsd.sztaki.hu/mockups/itb/ajanlasok/a8/index.html, letöltés ideje: 2023.02.11.*

[106] *Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31995L0046&from=en.*

[107] *Informatikai Tárcaközi Bizottság 12. számú ajánlása az informatikai rendszerek biztonsági követelményeiről. https://dsd.sztaki.hu/mockups/itb/ajanlasok/a12/index.html, letöltés ideje: 2023.02.11.*

[108] *A biometrikus rendszerek teszteléséhez használható legjobb gyakorlatok jegyzékét, Good Practice Guide for Biometric Systems Testing.*

https://www.gov.uk/government/publications/biometric-testing-for-government/biometric-testing-for-government.

[109] *2002/17/EK rendelet az Európai Parlament és a Tanács 2002/EC irányelve, amely az elektronikus hírközlő hálózatok és szolgáltatások közös szabályairól szól.*

[110] *2003. évi C. törvény, elektronikus hírközlésről szóló törvény. https://net.jogtar.hu/jogszabaly?docid=a0300100.tv, letöltés ideje: 2023.02.16.*

[111] *2252/2004/EK tanácsi rendelet a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32004R2252&from=en.*

[112] *2006/VI/28-as bizottsági határozat. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=OJ:C:2006:247:TOC, letöltés ideje: 2023.02.16.*

[113] *ISO 24709 szabvány a biometrikus rendszerek megfelelőségének teszteléséről. https://www.iso.org/standard/44704.html, letöltés ideje: 2023.02.19.*

[114] *2009. évi XLVII törvény a bűnügyi nyilvántartási rendszerről. https://mkogy.jogtar.hu/jogszabaly?docid=a0900047.TV, letöltés ideje: 2023.02.19.*

[115] *2010. évi CXXVI törvény, Adatvédelmi Törvény. https://net.jogtar.hu/jogszabaly?docid=A1000126.TV, letöltés ideje: 2023.02.19.*

[116] *2011. évi CXII. Törvény, az információs önrendelkezési jogról és az információszabadságról szóló törvény. https://net.jogtar.hu/jogszabaly?docid=a1100112.tv, letöltés ideje: 2023.02.19.*

[117] *Opinion 3/2012 on Developments in Biometric Technologies. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf, letöltés ideje: 2023.03.20.*

[118] *Automatikus biometrikus azonosító rendszerek alkalmazása a határellenőrzésben és határőrizetben. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp190_en.pdf, letöltés ideje: 2023.03.20.*

[119] *Magyar PTK 2013. évi V.tv, 2:59§, törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. https://net.jogtar.hu/jogszabaly?docid=A1300050.TV, letöltés ideje: 2023.03.20.*

[120] *2004. évi I. törvényt módosító 2014. évi XXVII., sporttörvény. https://njt.hu/jogszabaly/2004-1-00-00, letöltés ideje: 2023.03.25.*

[121] *GDPR. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, letöltés ideje: 2023.03.25.*

[122] *2018/0104. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32019R1157, letöltés ideje: 2023.03.25.*

[123] *2019. évi CXXXIV. Törvény, a biometrikus azonosításról szóló törvény. https://magyarkozlony.hu/dokumentumok/c7e1e8606dd1361a72d77734515809ee71c76f6e/letoltes, letöltés ideje: 2023.04.11.*

[124] *2019/1157/EU rendelet. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R1157&from=EN, letöltés ideje: 2023.04.11.*

[125] *(EU) 2019/817 rendelet. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0817&from=EN. letöltés ideje: 2023.04.11.*

[126] *2020. évi LVIII. Törvény a veszélyhelyzet megszűnésével összefüggő átmeneti szabályokról és a járványügyi készültségről. https://magyarkozlony.hu/dokumentumok/b18d1fb3c742aa2bd183b15a32fe4425e603f2c2/letoltes, letöltés ideje: 2023.04.11.*

[127] *2016/680 rendelet (2016. április 27). https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32016L0680, letöltés ideje: 2023.04.11.*

[128] *2022/868 számú Data Governance Act (DGA) rendelet. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022R0868&from=EN, letöltés ideje: 2023.04.11.*

[129] *https://net.jogtar.hu/jogszabaly?docid=A2300043.TV&timeshift=21001231&searchUrl=/gyorskereso?keyword%3Dbiometrikus, letöltés dátuma: 2024.02.01.*

RÖVIDÍTÉSJEGYZÉK

AIA: Artificial Intelligence Act

BCI: Brain-Computer Interfaces, agy-számítógép interfészek

BRUTE-FORCE: A brute force-támadás olyan jelszófeltörő módszer, ami az összes lehetséges variáció végigpróbálásával dolgozik (ez ellen védenek többek között a CAPTCHA-k).

CODIS: Combined DNA Index System

DGA: Data Governance Act

DNS: az elnevezés a dezoxiribonukleinsav szóból származik. Elnevezése az angol nyelvű szakirodalomban DNA vagy teljes nevén deoxyribonucleic-acid.

FAR: Az angol „False Acceptance Rate" (téves elfogadás) kifejezés kezdőbetűiből származik. Megadja, hogy milyen arányban azonosítja a rendszer a nem jogosult felhasználót jogosultként.

FBI: Federal Bureau of Investigation (Szövetségi Nyomozó Iroda)

FRR: Az angol „False Rejection Rate" (téves elutasítás) kifejezés kezdőbetűiből származik. Megadja, hogy milyen arányban azonosítja a rendszer a jogosult felhasználót nem jogosultként.

EER: Az angol „Equal Error Rate" kifejezés kezdőbetűiből származik. Azt a pontot adja, ahol a FAR és az FRR értékei egymással egyenlők.

GDPR: General Data Protection Regulation

IEC: International Electrotechnical Commission

ISO: Nemzetközi Szabványügyi Szervezet

IT: Information Technology

MI: mesterséges intelligencia

NIST: National Institute of Standards and Technology

TCP/IP: Az internet protokoll, a TCP/IP betűszó angol rövidítésből keletkezett: Transmission Control Protocol / Internet Protocol (átviteli vezérlő protokoll/internet protokoll). A TCP/IP egy olyan protokollkészlet, amely arra lett kidolgozva, hogy hálózatba kapcsolt számítógépek egymás között megoszthassák erőforrásaikat.

ZERO-KNOWLEDGE: A zero-knowledge azonosítási módszer olyan kriptográfiai protokoll, amely lehetővé teszi egy fél (például egy felhasználó) számára, hogy bizonyítson egy állítást egy másik fél (például egy szerver) számára anélkül, hogy közvetlenül kiadná az érzékeny információt.

ÁBRAJEGYZÉK

TÁBLÁZATJEGYZÉK

A TÉZISPONTOKHOZ KAPCSOLÓDÓ TUDOMÁNYOS KÖZLEMÉNYEK

Tudományos és szakmai folyóirat megjelenések

Megjelenés dátuma	Megjelenés helye	Cikk címe	Idézés
2021.05.14	Honvédségi Szemle	A biometria kialakulásáról és alkalmazásáról	Ujhegyi, P. (2021). A biometria kialakulásáról és alkalmazásáról. Honvédségi Szemle – Hungarian Defence Review, 149(3), 135–149, https://doi.org/10.35926/HSZ.2021.3.11
2020.09.07	Biztonságtudományi Szemle	Adatkezelés mesterfokon – a biometrikus azonosítás és a jogszabályi háttér	Ujhegyi, P., Kun, T., Adatkezelés mesterfokon – a biometrikus azonosítás és a jogszabályi háttér, Biztonságtudományi Szemle, 2020. II. évf. 3. szám
2021.10.07	Safety and Security Sciences Review (Biztonságtudományi Szemle)	Reduced-parameter biometric identification capabilities to protect critical infrastructures and special objects	Ujhegyi, P. Kovács, T., Reduced-parameter biometric identification capabilities to protect critical infrastructures and special objects, Safety and Security Sciences Review, Vol 3, NO 1 (SI), 2021.
2022.08.05	Journal of Security and Sustainability Issues	Managing the New Wave of Migration With Biometric Identification	Ujhegyi, P. Kovács, T., Managing the New Wave of Migration With Biometric Identification, Journal of Security and Sustainability Issues, Volume 12, Issue 1 (2022), pp.39-49, https://doi.org/10.47459/jssi.2022.12.4
2023.08.15	Belügyi Szemle	A biometria elterjedésének elemzése	Ujhegyi P. (2023). A biometria elterjedésének elemzése. Belügyi Szemle , 71(8), 1463-1491. https://doi.org/10.38146/BSZ.2023.8.7
2023. november	Biztonságtudományi Szemle	A biometrikus adatok védelemének és az AI fejlődésének összefüggései	Ujhegyi, P., Őszi, A., A biometrikus adatok védelmének és a mesterséges intelligencia fejlődésének összefüggései, Biztonságtudományi Szemle, 2023
2023.10.25	1. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencia	A biometriát használó eszközök elterjedésének vizsgálata többféle aspektusból	Ujhegyi, P., Som, Z., A biometriát használó eszközök elterjedésének vizsgálata többféle aspektusból, Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencia, 2023.11.25, ISBN 978-963-449-344-0
2023.10.25	1. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencia 2023	Nemzetközi kutatások áttekintő elemzése az egyén információbiztonság tudatossági szintjének mérési módszereire	Berek László, Bak Gerda, Ujhegyi Péter, Som Zoltán, Répás József, Pető Richárd: Nemzetközi kutatások áttekintő elemzése az egyén információbiztonság tudatossági szintjének mérési módszereire, Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencia, 2023.11.25, ISBN 978-963-449-344-0
2023.11.10	Kandó konferencia 2023	Az egyén információbiztonsági tudatossági szintjének megállapítására elterjedt mérési módszerek összefoglaló elemzése nemzetközi kutatások alapján	Berek László, Bak Gerda, Ujhegyi Péter, Som Zoltán, Répás József, Pető Richárd: Az egyén információbiztonsági tudatossági szintjének megállapítására elterjedt mérési módszerek összefoglaló elemzése nemzetközi kutatások alapján, Biztonságtudományi Szemle különszám, 2024

KÖSZÖNETNYILVÁNÍTÁS

Ezúton köszönöm meg mindazoknak, akik önzetlenül segítettek az értekezésem megírásában. Elsősorban családomnak, fiamnak, akik elfogadták, hogy az időt tőlük vettem el a kutatással és az anyag elkészítésével. Külön köszönöm édesapámnak a sok lektorálási tanácsot és az alaposságra vonatkozó példamutatását, melyet kortól függetlenül mindennél többre értékelek. Köszönetet mondok Prof. Dr. Kovács Tibor egyetemi docens Úrnak, hogy inspirált a doktori tanulmányok és a kutatások elkezdésében, és annak megszeretésében pedig hatalmas lelkesedése és mindig a szükséges mértékű támogatása jelentett felbecsülhetetlen értéket számomra. Professzor Úr sajnos nem érhette meg dolgozatom befejezését. Köszönetet mondok Dr. Szűcs Endre Tanár Úrnak, aki vállalta a témavezető konzulens szerepét és hogy sikeresen befejezhettem vele a kutatásomat, hasznos ötleteivel végig támogatott engem és alapos odafigyeléssel ellenőrizte és segítette a munkámat.

Köszönöm az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának, Prof. Dr. Rajnai Zoltánnak, továbbá az Alkalmazott Informatikai és Alkalmazott Matematikai Doktori Iskolájának, valamint az Alkalmazott Biometria Intézetének, hogy megteremtették az inspiráló kutatáshoz és tudományos munkához a szükséges feltételeket és lehetőséget adtak a kutatásra, mely munka során megtaláltam a kutatómunka szépségét és élvezetét. Ez nagy örömet okozott a munkám során.

Rajtuk kívül az értekezésem megírásában igen sok támogatást kaptam számos PhD hallgatótól, ezúton köszönöm nekik is mindennapi értékes segítségüket.

Legvégül, de nem utolsó sorban köszönettel tartozom az Óbudai Egyetemen dolgozó valamennyi kedves munkatársamnak, kollégámnak, akik egy nagyon jó hangulatú környezetet kialakítva segítettek át a nehéz pillanatokon.

MELLÉKLET

1. számú melléklet: Kérdőív

Tisztelt Válaszoló!

Ujhegyi Péter vagyok, PhD hallgató az Óbudai Egyetemen. Kutatási területem a biztonságtechnikán belül a biometrikus azonosítási megoldások elterjedése. Az alábbi önkéntes és anonim kérdőív kitöltésben és a felhívás további megosztásában szeretném a segítségét kérni. A megválaszoláshoz szükséges idő maximum 4-6 percet vesz igénybe a megítélésem szerint.

Együttműködését nagyon köszönöm! A kérdőív online is elérhető a QR kód segítségével!

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 / Ujjnyomat alapú azonosítás/ Arcfelismerés / Írisz alapú 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 szülői engedély alapján (gyermekek elrablásának megelőzése érdekében).					
Egyetértek, hogy jogerősen letöltendő börtönbüntetésre ítélt egyének DNS mintája, ujjlenyomata, arc azonosításra alkalmas paraméterei rendőrségi nyilvántartásba 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)

A kérdőív az alábbi direktlinken érhető el: https://docs.google.com/forms/d/13SoFCY7TaqsaTYa82XQisK2H1oIGryKJ6AHPb1ilfmo/edit?ts=624ac9b5

2. számú melléklet: Táblázat

Kibocsátó szervezet, jogi forma	Megjelenés	Megnevezés, azonosító	Jelentősége a biometria elterjedése szempontjából
Magyar Országgyűlés	1992	1992. évi LXIII. Törvény, adatvédelmi törvény a személyes adatok védelméről [104]	Az első olyan törvény Magyarországon, amely az adatvédelemmel foglalkozik, azonban nem szabályozza konkrétan a biometria alkalmazását.
Magyar Miniszterelnöki Hivatal Informatikai Koordinációs Iroda	1994	Informatikai Tárcaközi Bizottság 8. számú ajánlása, informatikai biztonsági módszertani kézikönyv [105]	Az informatikai biztonságra vonatkozó, előremutató követelményeket ajánló módszertani kézikönyv
Európai Unió adatvédelmi irányelve	1995	1995/46/EK [106]	Az első európai uniós jogszabály, amely az adatvédelemmel foglalkozik, azonban nem szabályozza konkrétan a biometria alkalmazását.
Magyar Miniszterelnöki Hivatal Informatikai Koordinációs Iroda	1996	Informatikai Tárcaközi Bizottság 12. számú ajánlása az informatikai rendszerek biztonsági követelményeiről [107]	Informatikai biztonsági követelményeket tartalmazó ajánlás
Egyesült Királyság - Biometria Munkacsoport (Biometric Working Group)	2000	A biometrikus rendszerek teszteléséhez használható legjobb gyakorlatok jegyzékét, Good Practice Guide for Biometric Systems Testing [108]	Az Egyesült Királyságban működő biometrikus munkacsoport (Biometric Working Group) által összeállított legjobb gyakorlatok jegyzéke tartalmazza azokat a legjobb gyakorlatokat, amelyeket javasolt alkalmazni a biometrikus rendszerek tesztelése során, annak érdekében, hogy a rendszer megbízhatósága és hatékonysága optimalizálható legyen.
Európai Parlament és a Tanács irányelve	2002	2002/17/EK rendelet az Európai Parlament és a Tanács 2002/EC irányelve, amely az elektronikus hírközlő hálózatok és szolgáltatások közös szabályairól szól [109]	Az irányelv célja az volt, hogy biztosítsa az uniós tagállamok közötti együttműködést a személyazonosság igazolására szolgáló hivatalos dokumentumok elismerése terén.
Magyar Országgyűlés	2003	2003. évi C. törvény, elektronikus hírközlésről szóló törvény [110]	Az elektronikus hírközlési szolgáltatóknak biztosítaniuk kell a felhasználók adatainak védelmét, beleértve a biometrikus adatokat is.
Európai Parlament és a Tanács rendelete	2004. december 13	2252/2004/EK tanácsi rendelet [111]	Előírta a tagállamoknak, hogy a közös műszaki és biztonsági követelmények elfogadását követően az érintett okmányokba biometrikus azonosító adatokat kell illeszteni.
Európai Unió Bizottságának határozata	2006	2006/VI/28-as bizottsági határozat [112]	Az Európai Unió (EU) Bizottságának határozata, amely meghatározta a digitális ujjlenyomatokkal kapcsolatos követelményeket a második generációs útlevelekhez (biometrikus útlevél). A határozat 2006 júniusában született.
ISO	2007	ISO 24709 szabvány a biometrikus rendszerek megfelelőségének teszteléséről [113]	Az ISO 24709 szabvány az úgynevezett „biometrikus teljesítménymérő eszközök” (BPP) tesztelési eljárásait írja le. Ez az eljárás lehetővé teszi a biometrikus rendszerek teljesítményének mérését és összehasonlítását, hogy megbizonyosodjunk arról, hogy megfelelően működnek-e a különböző körülmények között.

Kibocsátó szervezet, jogi forma	Megjelenés	Megnevezés, azonosító	Jelentősége a biometria elterjedése szempontjából
Magyar Országgyűlés	2009	2009. évi XLVII törvény [114]	Törvény a bűnügyi nyilvántartási rendszerről, az EU tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek
Magyar Országgyűlés	2010	2010. évi CXXVI törvény, Adatvédelmi Törvény [115]	A törvény tette lehetővé a biometrikus aláírások használatát a fővárosi és megyei kormányhivatalok ügyfélszolgálatain. Adatvédelmi törvény a személyes adatok védelméről és a magánélet védelméhez való jogról szól. Az Adatvédelmi törvény kiemelt figyelmet fordít a biometria és az ezzel kapcsolatos személyes adatok védelmére is.
Magyar Országgyűlés	2011	2011. évi CXII. Törvény, az információs önrendelkezési jogról és az információszabadságról szóló törvény [116]	A magyar 2011. évi XCII. törvény az adatvédelmi törvénnyel együtt szabályozza a személyes adatok védelmére vonatkozó kérdéseket Magyarországon. Az Információs önrendelkezési jogról és az információszabadságról szóló törvény kifejezetten foglalkozik a biometria és az ezzel kapcsolatos személyes adatok védelmével.
Európai Adatvédelmi Bizottság, 29-es Munkacsoport	2012. március 22	Opinion 3/2012 on Developments in Biometric Technologies [117]	Az Európai Adatvédelmi Bizottság (EDPB) 29-es munkacsoportja 2012-ben kiadott egy munkaanyagot az „Opinion 3/2012 on Developments in Biometric Technologies” címmel, amelynek célja a biometrikus technológiák adatvédelmi kihívásainak és a személyes adatok védelmének vizsgálata volt. A munkaanyag részletesen bemutatja a biometrikus technológiák működését, azokat a folyamatokat, amelyeken keresztül az adatokat gyűjtik, tárolják és felhasználják, valamint az ezen folyamatok során felmerülő adatvédelmi kockázatokat.
Európai Adatvédelmi Bizottság, 29-es Munkacsoport	2012. április 27.	Automatikus biometrikus azonosító rendszerek alkalmazása a határellenőrzésben és határőrizetben. [118]	Az Európai Adatvédelmi Bizottság (EDPB) 29-es munkacsoportja 2012. április 27-én kiadott ajánlásában az „Automatikus biometrikus azonosító rendszerek alkalmazása a határellenőrzésben és határőrizetben” címmel részletesen foglalkozik a biometrikus azonosítás alkalmazásának adatvédelmi szempontjaival.
Magyar Polgári Törvénykönyv	2013. április 15.	Magyar PTK 2013. évi V.tv, 2:59§, törvény az állami és önkormányzati szervek elektronikus információbiztonságáról [119]	Magyar Polgári Törvénykönyv (PTK) 2013. évi V. tv. 2:59.§-a az adatvédelemre vonatkozó rendelkezéseket tartalmazza. A törvény az adatok kezelése során a személyes adatok védelmének alapelvére hivatkozik, amelynek értelmében minden adatkezelőnek gondoskodnia kell arról, hogy az adatok kezelése során az érintettek jogait tiszteletben tartsák és az adatokat biztonságosan kezeljék.

Kibocsátó szervezet, jogi forma	Megjelenés	Megnevezés, azonosító	Jelentősége a biometria elterjedése szempontjából
Magyar Polgári Törvénykönyv	2014.	2004. évi I. törvényt módosító 2014. évi XXVII., sporttörvény [120]	Szabályozza a nem bűnügyi célú biometrikus személyazonosítási módszereket (képmásból, ujjnyomatból, íriszképből vagy érhálózatból képzett nem visszafejthető, alfanumerikus kód) és azok használatának módját. A stadionok és a sportrendezvények biztonságának céljából e törvény okán vált lehetővé a biometrikus személyazonosítások alkalmazása az állami szektoron kívül, nem polgári jogi feltételek alapján.
Európai Parlament és a Tanács	2016. április 27.	GDPR [121]	Az Európai Unió általános adatvédelmi rendelete, azaz a GDPR 2016. április 27-én lépett hatályba, de alkalmazása csak 2018. május 25-étől kötelező. A rendelet magyarországi hatályba lépése megegyezik az európai hatálybalépéssel, vagyis 2018. május 25-től alkalmazandó Magyarországon. A GDPR értelmében biometrikus adatnak tekintendő minden olyan sajátos technikai eljárásokkal nyert személyes adat, ami egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozik, és amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását.
Európai Bizottság javaslata a biometrikus adatok használatáról az EU határain	2018.	2018/0104 [122]	Az Európai Bizottság javaslata a biometrikus adatok használatáról az EU határain az Európai Parlament és Tanács 2018/0104 (COD) rendeletének a része. Ez a rendelet az úti okmányok biztonsági jellemzőiről és az ezekben szereplő biometrikus azonosító adatok feldolgozásáról szól, és az EU határellenőrzési rendszerének részét képezi.
Európai Parlament és a Tanács	2018. április 25.	COM (2018) 237 final, EU AI-stratégia [68]	A COM (2018) 237 final jelentés és az EU AI-stratégia közötti kapcsolat az, hogy mindkét dokumentum célja az Európai Unió szabályozói keretének javítása az innovatív technológiák, különösen az AI és a gépi tanulás (ML) terén. Az EU AI-stratégia célja az, hogy elősegítse az AI fejlődését az EU-ban, miközben megőrzi az uniós értékeket, az emberi jogokat és az adatvédelmet.
Magyar Országgyűlés	2019.	2019. évi CXXXIV. Törvény, a biometrikus azonosításról szóló törvény [123]	A magyar 2019. évi CXXXIV. törvény a biometrikus adatok kezelésére vonatkozó szabályokat határozza meg, és összhangban van az Európai Unió által elfogadott általános adatvédelmi rendelettel (GDPR). A törvény szabályozza a biometrikus adatok kezelésének feltételeit és az adatvédelmi kötelezettségeket, beleértve a biometrikus adatok védelmét, a felhasználók tájékoztatását és az érintettek jogait. Ezen törvény hatályba lépése előtt a biometrikus adatok kezelése kizárólag jogszabály alapján vagy az érintett önkéntes hozzájárulása alapján volt lehetséges.

Kibocsátó szervezet, jogi forma	Megjelenés	Megnevezés, azonosító	Jelentősége a biometria elterjedése szempontjából
Európai Parlament és Tanács	2019.	2019/1157/EU rendelet [124]	Rendelet az Európai Unió polgárai és családtagjaik számára kiállított uniós szintű biztonsági elemekkel rendelkező igazolványok és tartózkodási engedélyek biztonsága témában. A rendelet célja, hogy biztosítsa az uniós szintű biztonsági elemekkel ellátott személyazonossági igazolványok és tartózkodási engedélyek kiállítását.
Európai Bizottság	2019. április 24.	(EU) 2019/817 rendelet [125]	Az Európai Bizottság 2019. április 24-én javaslatot tett a biometrikus adatok használatával kapcsolatos uniós határellenőrzési rendszer bevezetésére. A javaslat része volt az általános uniós határellenőrzési rendszer (EU Entry/Exit System, EES) és az utasazonosítási rendszer (Interoperability Regulation) felülvizsgálatának, amelyek célja az EU külső határainak hatékonyabb védelme.
Európai Bizottság	2020. február 19.	Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése, COM (2020) 65 final, 2020. [67]	A Fehér könyv szakpolitikai alternatívákat határoz meg arra vonatkozóan, hogyan érhető el a mesterséges intelligencia elterjedésének előmozdítására és az ilyen technológiák bizonyos felhasználásához kapcsolódó kockázatok kezelésére irányuló kettős célkitűzés.
Magyar Országgyűlés	2020. július 22.	2020. évi LVIII. törvény [126]	Magyarországon 2020. július 22-én a Magyar Közlönyben jelent meg az adatvédelmi hatóságok és az információs önrendelkezési jogot érintő egyes kérdések rendezéséről szóló 2020. évi LVIII. törvény. Ezen törvény hatálya kiterjed az adatvédelmi hatóságok működésére és hatáskörére, valamint az információs önrendelkezési jogot érintő kérdésekre, így az adatvédelmi eljárásokra és a bírságokra is.
Európai Parlament és Tanács	2021. április 21.	COM (2021) 206 final, 2021/0106 (COD), A mesterséges intelligenciára vonatkozó harmonizált szabályok (az MI-ről szóló jogszabály) megállapításairól [71]	A javaslat célja a bizalmi ökoszisztéma kialakítására vonatkozó (Fehér könyv szerinti) második célkitűzés megvalósítása azáltal, hogy javaslatot tesz a megbízható mesterséges intelligenciára vonatkozó jogi keretre. A javaslat az uniós értékeken és az alapvető jogokon alapul, és arra irányul, hogy bizalmat ébresszen az egyénekben és más felhasználókban a mesterséges intelligencián alapuló megoldások alkalmazása iránt.
Európai Parlament és Tanács	2021. május 20.	2016/680 rendelet [127]	Az EU-ban 2021. május 20-án jelent meg az Európai Parlament és Tanács 2016/679 rendeletének (általános adatvédelmi rendelet, GDPR) kiegészítése a személyes adatok védelmével kapcsolatban a bűncselekmények megelőzése, nyomozása, felderítése és üldözése céljából történő adatkezelésről szóló 2016/680 európai parlamenti és tanácsi rendelet.

Kibocsátó szervezet, jogi forma	Megjelenés	Megnevezés, azonosító	Jelentősége a biometria elterjedése szempontjából
Európai Parlament és Tanács	2022. május 30.	2022/868 számú Data Governance Act (DGA) rendelet [128]	Megjelent az európai adatkormányzásról szóló (2022/868 sz., Data Governance Act, DGA) rendelet, mely az uniós európai adatstratégia jogalkotási folyamatából indult ki.
Magyar Országgyűlés	2023 évi XLIII törvény	Törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezménynek a Strasbourgban, 2018. október 10. napján kelt módosító Jegyzőkönyve kihirdetéséről [129]	A személyes adatok védelmét a társadalomban betöltött szerepének fényében kell értelmezni, és azt a többi emberi joggal és alapvető szabadságjoggal, így különösen a véleménynyilvánítás szabadságával is össze kell egyeztetni. Köz vagy magánérdek közti különbségtétel.

12. táblázat: A biometria, a személyes adatok védelme és az AI szabályozásának fejlődése[22]

[22] A táblázat a szerző saját szerkesztése.