CTI Jelentés

Biometrikus azonosítás

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
Fortes fortuna adiuvat

NEMZETI KIBERBIZTONSÁGI INTÉZET

Tartalomjegyzék

Mi az a biometrikus azonosítás és miért fontos?

A biometrikus azonosítás olyan technológia, amely az ember egyedi fizikai vagy viselkedési jellemzői alapján azonosítja vagy hitelesíti a személyazonosságot. A legismertebb példák az ujjlenyomat-olvasás, arcfelismerés vagy íriszszkennelés, de ide tartozik például az is, hogy valaki hogyan gépel vagy hogyan sétál.

Az elmúlt évtizedben a biometrikus azonosítás a jelszavakat és PIN-kódokat kiegészítő vagy helyettesítő módszerré vált, köszönhetően annak, hogy kényelmes, gyors és elméletileg nehezebben hamisítható. Az okostelefonoktól kezdve a határátlépő rendszereken át a vállalati beléptetésig egyre több területen alkalmazzák.

Ugyanakkor a biometrikus rendszerek bevezetése komoly kiberbiztonsági és adatvédelmi kihívásokat is rejt magában. A felhasználók számára nem mindig nyilvánvaló, hogyan tárolják az adataikat, hogyan lehet azokat visszaélésre felhasználni, és milyen támadási módszerek léteznek.

Ez a tudatosító anyag célja, hogy megismertesse a biometrikus azonosítás működését, előnyeit, kockázatait, és gyakorlati tanácsokat adjon a biztonságos használathoz.

A biometrikus azonosítás története

A biometrikus azonosítás alapgondolata nem a digitális korszak szüleménye: az emberek már évezredekkel ezelőtt is használták az egyedi testi jellemzőket – például az ujjlenyomatokat – azonosításra és hitelesítésre. A mai formájában ismert biometrikus technológia azonban csak a 19. századtól kezdett intézményesülni, és a 20. század végétől vált tömegessé a polgári alkalmazásban. A története során a biometrikus azonosítás rendészeti eszközből vált globális digitális infrastruktúrává.

A legkorábbi dokumentált felhasználásra i. e. 5000 körül került sor Babilóniában, ahol az agyagtáblákon rögzített szerződéseket ujjlenyomatokkal hitelesítették. Hasonló gyakorlatot követett az i. sz. 650 körüli Kína is, ahol aláírásként szolgált az ujjlenyomat hivatalos dokumentumokon. Ezek még nem rendszerszintű azonosítások voltak, hanem bizalmi aktusok, amelyek egyediségük miatt kaptak szerepet.

A modern biometrikus azonosítás születésének egyik mérföldköve az 1883-as év, amikor a francia Alphonse Bertillon bemutatta saját fejlesztésű módszerét, a bertillonage rendszert. Ez az eljárás az emberi test mérhető tulajdonságait – például kartávolságot, lábhosszt, fülmagasságot – használta személyek azonosítására, különösen a bűnüldözésben. Bár később bebizonyosodott, hogy a módszer hibalehetősége magas, ez volt az első szisztematikusan alkalmazott biometrikus rendszer, és hosszú éveken át használták Európában és az Egyesült Államokban is.

Ezzel párhuzamosan jelentek meg az első ujjlenyomat-alapú azonosítási rendszerek, amelyek mára a biometria legismertebb alkalmazásai közé tartoznak. 1888-ban a brit Francis Galton tudományos alapon kezdte kutatni az ujjlenyomatokat, és kimutatta, hogy azok egyediek és életre szólóan állandóak. Ezt követően 1892-ben az argentin Juan Vucetich vezette be először a gyakorlatban az ujjlenyomat-azonosítást egy bűnügyi eset során, amely a világ első hivatalos ujjnyom-azonosításos letartóztatásához vezetett.

1901-ben a londoni Scotland Yard hivatalosan is bevezette az ujjnyomatalapú azonosítást, amely hamar elterjedt a brit gyarmati rendszer egészében, például Indiában és Dél-Afrikában is. 1905-től az FBI is elkezdte az ujjlenyomatok nyilvántartását az Egyesült Államokban, és 1924-ben már külön hivatal jött létre az ujjlenyomatok feldolgozására.

A 20. század második felében megjelentek az első gépesített és számítógépes biometrikus rendszerek, kezdetben katonai és titkosszolgálati célokra. Az 1970-es években a New Jersey Institute of Technology kutatói kifejlesztették az első automatikus ujjlenyomat-felismerő rendszert (AFIS), amelyet később az FBI is adaptált. Az első kereskedelmi célú arcfelismerő rendszerek az 1990-es évek elején jelentek meg, még alacsony pontossággal és nagy hibahatárral.

A 2000-es évek elején elindult a biometrikus útlevelek bevezetése, először az Egyesült Államokban a 2001. szeptember 11-i terrortámadások után. Az Európai Unió 2004-ben fogadta el az első olyan rendeletet, amely kötelezővé tette a biometrikus fénykép és ujjlenyomat integrálását az úti okmányokba (2252/2004/EK rendelet). A cél a határbiztonság megerősítése és az identitáscsalások visszaszorítása volt.

Közben 2009-ben elindult az indiai Aadhaar rendszer, amely világszinten is példátlan volumenű biometrikus adatgyűjtést valósított meg: több mint 1,3 milliárd ember arcképét, ujjlenyomatát és íriszmintáját rögzítették egyetlen adatbázisban. Ez a projekt komoly adatvédelmi és etikai vitákat váltott ki, különösen 2018-ban, amikor biztonsági kutatók feltárták, hogy az adatbázishoz jogosulatlanul is hozzá lehetett férni.

A biometrikus azonosítás a 2010-es évektől kezdve robbanásszerű fejlődésnek indult a mesterséges intelligencia és a mélytanulás térnyerésével. A deep learning alapú arcfelismerés jelentősen javította az azonosítás pontosságát, és ezzel párhuzamosan megjelentek a valós idejű, passzív biometrikus megfigyelőrendszerek, például városi térfigyelők vagy repülőtéri beléptető kapuk. Ugyanebben az időszakban indult a mobiltelefonok biometrikus azonosítása is: a Touch ID 2013-as, majd a Face ID 2017-es bevezetése új szintre emelte az azonosítás hétköznapi alkalmazását.

A jelenlegi trendek a decentralizált tárolás, a folyamatos autentikáció, valamint a biometrikus adatok kriptográfiai védelmének fejlesztése felé mutatnak. Ugyanakkor a technológia társadalmi hatásai – megfigyelés, diszkrimináció, visszaélés lehetősége – új szabályozási kihívásokat vetnek fel, amelyekre a következő években sürgős választ kell adni.

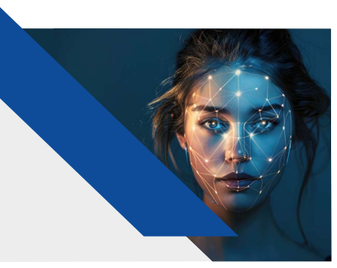
A biometrikus azonosítás története így nem csupán a technológia fejlődéséről szól, hanem egyben arról is, hogyan alakítja a digitális világ az emberi identitás védelmét, jogait és sebezhetőségeit.

A biometrikus azonosítás típusai

A biometrikus azonosítási módszerek két fő kategóriába sorolhatók: fizikai (statikus) és viselkedési (dinamikus) jellemzőkön alapuló rendszerekre. A fizikai biometria az emberi test stabil, genetikailag meghatározott sajátosságait használja fel, míg a viselkedési biometria az egyénre jellemző mozgási vagy cselekvési mintákat elemzi. Az elmúlt években egyre nagyobb teret nyernek az úgynevezett multimodális rendszerek is, amelyek többféle biometrikus azonosítót kombinálnak a megbízhatóság és biztonság növelése érdekében.

A fizikai biometria legelterjedtebb példája az ujjlenyomat-azonosítás, amely a bőr redőinek egyedi mintázatát vizsgálja. Ez a technológia gyors, költséghatékony és széles körben alkalmazott – például okostelefonok zárolásának feloldására, munkahelyi beléptetésre vagy hatósági személyazonosításra.

Hasonlóan népszerű az arcfelismerés, amely az arc meghatározó pontjait és ezek geometriai viszonyait rögzíti és hasonlítja össze a tárolt sablonokkal.



Az íriszszkennelés ennél is pontosabb megoldást kínál, mivel az írisz mintázata egyedi és életünk során alig változik. Bár az írisz- és retinaszkennelés nagyfokú megbízhatóságot nyújt, ezek a technológiák költségesek, ezért elsősorban magas biztonsági szintet igénylő alkalmazási területeken fordulnak elő.

Kevésbé elterjedt, de létező módszerek a kézgeometria, a tenyérvonalak és a kézfej vénamintázatának elemzése, amelyek bizonyos speciális beléptetőrendszerekben még mindig használatban vannak.

A viselkedési biometria az emberi tevékenység mintázatait figyeli. Ilyen például a gépelési dinamika, amely azt vizsgálja, hogyan és milyen ritmusban használja valaki a billentyűzetet – például mekkora idő telik el két leütés között, és milyen erővel történik a leütés. Ez a módszer háttérben futva képes megerősíteni a felhasználó személyazonosságát, akár már a munkamenet közben is. A dinamikus aláírás elemzése nem csupán a kézírás alakját vizsgálja, hanem annak sebességét, irányváltásait, nyomását és gyorsulását is, ezáltal hitelesebb képet ad a felhasználóról. Egyre több kutatás irányul a járásmintázat, vagyis az emberi mozgás stílusának azonosítására, amelyet akár térfigyelő kamerák, akár okosórák és mozgásérzékelős szenzorok is képesek rögzíteni. A használati mintázatok, például hogy valaki milyen sorrendben nyitja meg az alkalmazásokat, hogyan tartja a telefont, szintén szolgálhatnak viselkedésalapú biometrikus azonosításként, különösen a passzív autentikációs rendszerekben.

A modern gyakorlatban egyre elterjedtebbek a multimodális biometrikus rendszerek, amelyek egyszerre több biometrikus azonosítót kombinálnak – például ujjlenyomatot és arcfelismerést, vagy íriszt és gépelési dinamikát. Az ilyen rendszerek előnye, hogy pontosabb azonosítást biztosítanak és ellenállóbbak a támadásokkal szemben, hiszen ha az egyik jellemző nem elérhető vagy torzított, a másik még érvényes lehet. Ugyanakkor ezek a megoldások nagyobb költségekkel járnak, bonyolultabb adatvédelmi elvárásokat támasztanak, és összetettebb rendszertervezést igényelnek.

Bár a biometrikus azonosítás egyik legnagyobb előnye, hogy az azonosító nem felejthető el, és általában egyedi és állandó, ugyanakkor éppen ez ad okot a legnagyobb aggodalomra is. Egy kompromittált biometrikus sablon – például egy ellopott arckép vagy íriszminta – nem változtatható meg úgy, mint egy jelszó. Emiatt a biometrikus rendszerek tervezése és használata során kiemelt figyelmet kell fordítani az adatbiztonsági és adatvédelmi intézkedések betartására.

A biometrikus rendszerek működése

A biometrikus azonosítási rendszerek működése több, egymást követő technológiai lépésből áll, amelyek célja az egyén egyedi fizikai vagy viselkedési jellemzőinek rögzítése, átalakítása és összevetése egy korábban elmentett referenciamintával. Ezek a rendszerek nem az adott személy teljes jellemzőjét tárolják, hanem annak matematikai reprezentációját, az úgynevezett biometrikus sablont, amelyet összehasonlításra használnak.

A folyamat első lépése az adatgyűjtés, amely során a rendszer szenzorai rögzítik a biometrikus jellemzőt – például egy kamerás modul lefotózza az arcot, egy ujjlenyomat-olvasó letapogatja a bőr mintázatát, vagy egy gyorsulásmérő figyeli a járásdinamikát. Ezt az információt ezután digitalizálják, vagyis számítógépes formára alakítják, majd algoritmusok segítségével feldolgozzák és jellemzőket extrahálnak belőle. Ezekből a jellemzőkből készül el a sablon, amely nem azonos az eredeti kép vagy jelfolyam formájával – nem rekonstruálható belőle például az arc vagy az ujjlenyomat teljes képe, de a mintázat statisztikai reprezentációja alapján az összevetés lehetségessé válik.

A sablon elkészítése után azt regisztrációs (enrollment) folyamat keretében eltárolják egy adatbázisban vagy a végfelhasználó eszközén. A legtöbb rendszer úgy működik, hogy az új belépési kísérlet során ismét begyűjti a biometrikus adatot, új sablont generál belőle, majd azt összehasonlítja a korábban elmentett példánnyal. Ez az úgynevezett egyezésvizsgálat (matching).

Ennek eredményeként egy hasonlósági pontszám születik, amely alapján a rendszer eldönti, hogy az aktuális minta elég közel áll-e a tárolt sablonhoz. A hitelesítés akkor sikeres, ha a hasonlósági pontszám meghalad egy előre beállított küszöbértéket.

Kétféle alapvető összevetési módszer létezik: az azonosítás (identification) és a hitelesítés (authentication). Az azonosítás során a rendszernek azt kell meghatároznia, ki a felhasználó – tehát a begyűjtött mintát összeveti az összes tárolt sablonnal, és a legjobban egyezőt választja ki. Ezzel szemben hitelesítés esetén a felhasználó először megad egy azonosítót (pl. felhasználónevet vagy azonosító számot), és a rendszer csak az adott személyhez tartozó sablonnal hasonlítja össze az aktuális mintát.

Fontos különbséget tenni a valós idejű (online) és az előfeldolgozott (offline) rendszerek között. Az online rendszerek azonosítást végeznek valós időben, például belépés vagy fizetés előtt, míg az offline megoldások előbb rögzítik az adatokat, majd csak később elemzik azokat – ilyen lehet például egy hatósági ellenőrzés során alkalmazott biometrikus azonosítás, ahol a kiértékelés nem történik meg azonnal.

A rendszerek működésének pontosságát többféle mérőszám jellemzi. A false acceptance rate (FAR) azt mutatja meg, hogy milyen gyakran fogad el a rendszer egy illetéktelen személyt, míg a false rejection rate (FRR) azt, hogy milyen gyakran utasít el jogos felhasználót. A kettő közötti egyensúly kulcsfontosságú: ha túl szigorú a rendszer, sok jogos belépés hiúsul meg; ha túl engedékeny, akkor megnő a hamis azonosítás veszélye. A gyakorlatban gyakran alkalmazzák az equal error rate (EER) mutatót, amely azt az értéket jelzi, ahol a FAR és az FRR értéke megegyezik – ez a rendszer optimális teljesítményének egyfajta jellemzője.

A sablonok biztonságos tárolása különösen fontos kérdés. Ezeket általában titkosítva vagy hash-elve tárolják, és egyes rendszerek úgynevezett cancelable biometrics megoldásokat alkalmaznak, ahol a sablon egy előre meghatározott algoritmus szerint torzított formában kerül mentésre. Így ha egy sablon kiszivárog, az nem használható más rendszerek megtévesztésére, és új sablon generálható ugyanabból a biometrikus jellemzőből egy másik torzítási paraméterrel.

A működési mechanizmus ismerete nem csupán a fejlesztők és informatikai szakemberek számára fontos, hanem minden felhasználónak segít megérteni, hogyan történik az ő azonosítása a háttérben, és miért jelent ez egyszerre kényelmet és potenciális kockázatot.

A biometrikus azonosítás előnyei és lehetőségei

A biometrikus azonosítás egyre elterjedtebbé válása nem véletlen. Számos olyan előnyt kínál, amelyre a hagyományos azonosítási módszerek – például jelszavak vagy PIN-kódok – nem képesek. Ezek az előnyök nemcsak kényelmi szempontból jelentősek, hanem biztonsági, szervezeti és felhasználói élmény szempontból is.

Az egyik legfontosabb előnye, hogy a biometrikus azonosítók egyediek és személyhez kötöttek. Mivel a biometrikus jellemzők – például az ujjlenyomat, az írisz vagy a járásminta – genetikailag vagy neurológiailag meghatározottak, gyakorlatilag lehetetlen, hogy két különböző ember pontosan ugyanazzal a mintázattal rendelkezzen. Ez az egyediség jelentősen csökkenti a hamis pozitív azonosítások esélyét, így a rendszer megbízhatósága megnő.

További előnyt jelent, hogy a biometrikus jellemzők nem felejthetők el, és nem lehet őket könnyedén megosztani vagy ellopni a hagyományos értelemben. Míg a jelszavakat le lehet írni, tovább lehet adni, vagy egyszerűen el lehet felejteni, a biometrikus azonosító mindig „kéznél van" – szó szerint. Ez jelentősen csökkenti a felhasználói hibákból eredő biztonsági kockázatokat, például a gyenge jelszavak vagy az újrahasznosított hitelesítő adatok problémáját.

A biometrikus rendszerek további erőssége a gyorsaság és egyszerűség. Egy ujjlenyomat-leolvasás vagy arcfelismerés akár a másodperc törtrésze alatt végbemehet, jelentősen lerövidítve az azonosítási időt.

Ez különösen fontos lehet nagy áteresztőképességű rendszerekben, mint például repülőtereken, stadionokban vagy vállalati beléptető kapuknál, ahol a gyors, de biztonságos azonosítás kritikus.

A biometrikus technológiák továbbá kényelmet biztosítanak a felhasználók számára, mivel nincs szükség hosszú jelszavak megjegyzésére vagy folyamatos újragenerálására. Az ilyen típusú felhasználói élmény különösen előnyös lehet olyan helyzetekben, ahol a klasszikus hitelesítés nem praktikus – például kesztyűs kézzel dolgozók, korlátozott mozgásképességű személyek vagy idősek esetében.

Nem elhanyagolható szempont az sem, hogy a biometrikus azonosítás jól integrálható más hitelesítési mechanizmusokkal, így része lehet egy többtényezős azonosítási rendszernek (MFA). Egy rendszer például kombinálhatja az ujjlenyomatot egy jelszóval vagy egy hardveres biztonsági kulccsal, így a kompromittáció kockázata jelentősen csökkenthető. Az ilyen megközelítések különösen indokoltak magas kockázatú környezetekben, például pénzügyi tranzakciók, orvosi adatok elérése vagy állami rendszerek esetén.

A kétfaktoros hitelesítés témában készített az NBSZ NKI egy kiadványt, amelyet ezen a linken olvashat el.

Végezetül, a biometrikus rendszerek olyan lehetőségeket is megnyitnak, amelyek túlmutatnak a klasszikus beléptetésen. A technológia alkalmazható például fizetési rendszerekben, jogosultságkezelésben, hozzáférés-naplózásban, sőt folyamatos hitelesítésre is – azaz nemcsak a belépés pillanatában, hanem a teljes munkamenet alatt ellenőrizhető a felhasználó jelenléte és viselkedése.

Mindezek az előnyök azt mutatják, hogy a biometrikus azonosítás nem pusztán egy divatos újítás, hanem egy stratégiai jelentőségű technológia, amely megfelelő alkalmazás és biztonsági kontroll mellett hatékony eszköze lehet a korszerű digitális környezetek védelmének.

Kockázatok és sebezhetőségek a biometrikus azonosításban

Bár a biometrikus azonosítás kétségtelenül számos előnnyel jár, fontos megérteni, hogy e technológiák önmagukban nem feltétlenül biztonságosabbak, mint a hagyományos azonosítási módszerek. A biometrikus rendszerek sajátos kockázatokat hordoznak, amelyek technológiai, támadástechnikai és adatvédelmi szempontból is jelentősek.

Az egyik legnagyobb probléma a biometrikus jellemzők visszavonhatatlansága. Míg egy ellopott vagy kiszivárgott jelszót bármikor meg lehet változtatni, egy egyszer kompromittált ujjlenyomat, íriszminta vagy arckép már nem cserélhető le. Ez azt jelenti, hogy a biometrikus sablon elvesztése véglegessé váló kockázatot jelenthet a felhasználó számára, különösen akkor, ha ugyanazt a mintázatot több rendszer is használja.

A másik alapvető veszélyt a hamisítás és utánzás lehetősége jelenti. Számos kutatás és támadási demonstráció bizonyította, hogy egyes biometrikus rendszerek megtéveszthetők mesterséges mintákkal. Az ujjlenyomat-olvasók például sokáig érzékenyek voltak szilikonból vagy zseléből készült hamis ujjlenyomatokra, míg az arcfelismerő rendszerek gyengébb változatait meg lehetett téveszteni fotókkal vagy 3D-nyomtatott maszkokkal. Az elmúlt években a mesterséges intelligencia és a deepfake technológiák fejlődésével az ilyen támadások kifinomultabbá és veszélyesebbé váltak.

Nem elhanyagolható kockázat a sablonlopás és visszafejtés sem. A biometrikus rendszerek általában nem a nyers képet vagy hangfájlt tárolják, hanem egy sablont, amely egy algoritmus segítségével kivonatolt adatstruktúra. Ha azonban ezt a sablont egy támadó megszerzi, akkor bizonyos esetekben képes lehet azt visszafejteni vagy újraalkotni a biometrikus jellemző egy részét – különösen akkor, ha a sablon nem megfelelően titkosított vagy maszkolt. Mivel sok rendszer ugyanazt a biometrikus jellemzőt használja (például ugyanaz az ujjlenyomat több alkalmazásban), a sablon újrafelhasználása révén több rendszer is kompromittálódhat.

További gyakori támadástípus az úgynevezett „replay-támadás”, amikor a támadó egy korábban rögzített biometrikus adatot (például arcképet vagy hangmintát) újra felhasznál, hogy megtévessze a rendszert. Ennek elkerülésére egyre több biometrikus rendszer igyekszik beépíteni liveness detection (élő-jelenlét ellenőrzés) funkciókat, amelyek a felhasználó valós idejű mozgásait, reakcióit vagy élettani jeleit vizsgálják – például pislogást, szemmozgást vagy mikrorezgéseket.

A kockázatok nem korlátozódnak csupán a támadástechnikai dimenziókra. A biometrikus rendszerek sok esetben érzékenyek a működési körülményekre is. A szenzorok például tévesen működhetnek rossz fényviszonyok, fizikai sérülések vagy eszközhibák esetén. Egy arcfelismerő rendszer hibásan azonosíthat vagy megtagadhatja a hozzáférést, ha a felhasználó szemüveget, maszkot vagy sapkát visel. A fizikai változások – például egy seb az ujjlenyomaton vagy az öregedés hatásai – szintén befolyásolhatják a felismerés megbízhatóságát.

Végezetül, a biometrikus rendszerek jelentős adatvédelmi kihívásokat is felvetnek. A legtöbb biometrikus adat az érzékeny személyes adatok körébe tartozik, amelynek kezelése szigorú jogi szabályozás alá esik. A GDPR (Európai Unió Általános Adatvédelmi Rendelete) például külön kategóriában tárgyalja a biometrikus adatokat, amelyek kezeléséhez általában kifejezett hozzájárulás, biztonságos tárolás, átlátható felhasználás és korlátozott célú adatfeldolgozás szükséges. Az adatok nem megfelelő kezelése jogsértéshez és bírsághoz vezethet, emellett a felhasználók bizalmának elvesztését is okozhatja.

A felsorolt kockázatok fényében világossá válik, hogy a biometrikus azonosítás nem csodaszer, hanem egy érzékeny és nagy felelősséggel járó technológia, amelynek bevezetése és működtetése alapos tervezést, támadásmodellezést, tesztelést és folyamatos karbantartást igényel. A biztonság nem a technológiában rejlik, hanem annak körültekintő és felelős alkalmazásában.

Adatvédelem és jogi megfelelés

A biometrikus azonosítás kapcsán nem csupán technológiai kérdésekről van szó: a biometrikus adatok kezelése komoly jogi és adatvédelmi kötelezettségeket ró mindazokra, akik ilyen rendszert terveznek, üzemeltetnek vagy használnak. A biometrikus jellemzők ugyanis az különleges személyes adatok körébe tartoznak, ezért ezek gyűjtése, tárolása és felhasználása csak szigorúan meghatározott feltételek mellett történhet. E követelmények középpontjában a GDPR áll, amely külön kategóriában kezeli a biometrikus adatokat.

A GDPR 9. cikke szerint a biometrikus adatok – például egy személy ujjlenyomata, arcképe vagy íriszmintája – olyan különleges adatnak minősülnek, amelyek feldolgozása alapértelmezetten tilos, kivéve, ha azt valamilyen külön jogalap lehetővé teszi. Az egyik leggyakoribb ilyen jogalap a kifejezett hozzájárulás, amelynek önkéntesnek, egyértelműnek, tájékozottnak és konkrétnak kell lennie. Fontos megjegyezni, hogy a hozzájárulásnak visszavonhatóvá kell válnia, amely komoly kihívást jelent olyan rendszerekben, ahol a biometrikus adat maga az egyetlen azonosító – hiszen egy ujjlenyomat „visszavonása" fizikailag nem értelmezhető.

A szabályozás további kulcseleme az adatminimalizálás elve, amely kimondja, hogy a szervezetek csak olyan biometrikus adatokat gyűjthetnek és kezelhetnek, amelyek szükségesek és arányosak a konkrét cél eléréséhez.

Ez azt jelenti, hogy a biometrikus azonosítást nem lehet önmagában a kényelem vagy technológiai divat kedvéért alkalmazni: minden esetben bizonyítani kell, hogy a cél máshogy nem érhető el, vagy csak aránytalanul nagy költséggel és kockázattal.

A tárolási időtartam is szigorúan szabályozott: a biometrikus adatokat csak addig lehet őrizni, ameddig az adott célmegvalósítása indokolja. Ezt követően az adatokat véglegesen és visszafordíthatatlanul törölni kell. Ez különösen fontos az olyan rendszerek esetében, amelyek hosszú távon építenek fel felhasználói profilokat, vagy amelyeknél a regisztrációs és törlési mechanizmusok nem teljesen átláthatók.

A jogi megfelelés másik sarkalatos pontja az adatbiztonság, amely a GDPR 32. cikke szerint azt jelenti, hogy a szervezeteknek megfelelő technikai és szervezési intézkedéseket kell tenniük az adatok védelme érdekében. A biometrikus sablonokat például titkosított formában, lehetőleg decentralizált módon kell tárolni, és védeni kell a jogosulatlan hozzáféréstől, módosítástól vagy kiszivárgástól. A szabályozás szerint minden biometrikus rendszernél kockázatértékelést kell végezni a bevezetés előtt, és adathasználati nyilvántartásban kell dokumentálni, ki, mikor, milyen célból és milyen jogalapon fér hozzá ezekhez az adatokhoz.

További gyakorlati követelmény a transzparencia és elszámoltathatóság, vagyis a felhasználónak tudnia kell, hogy milyen adatot gyűjtenek róla, mire használják, kik férnek hozzá, és milyen jogai vannak az adatkezeléssel kapcsolatban. Az adatkezelőnek pedig képesnek kell lennie bizonyítani a megfelelést bármely hatósági ellenőrzés során.

Ez magában foglalja a tájékoztatási kötelezettség teljesítését, a hozzáférési kérelmek kezelését, valamint az olyan mechanizmusok bevezetését, mint a biometrikus azonosítás alternatíváinak biztosítása – például jelszó vagy kártyás belépés lehetősége azok számára, akik nem kívánnak biometrikus adatokat megadni.

Nem kizárólag az EU jogszabályai foglalkoznak ezzel a kérdéskörrel. Számos ország – például az Egyesült Államok, Kanada, Brazília vagy Ausztrália – rendelkezik saját adatvédelmi törvényekkel, amelyek eltérő módon szabályozzák a biometrikus adatok gyűjtését és kezelését. Egyes joghatóságok – különösen Kína vagy India – a tömeges biometrikus adatgyűjtést állami szinten is alkalmazzák, ami komoly etikai és emberi jogi kérdéseket vet fel, különösen a célhoz kötöttség és a hozzájárulás valódiságának hiányában.

A fentiekből világosan látható, hogy a biometrikus azonosítás nem pusztán technológiai kérdés, hanem komplex jogi, etikai és adatvédelmi kihívás is. Egy jól megtervezett biometrikus rendszer nemcsak biztonságos és hatékony, hanem összhangban van a jogszabályokkal, tiszteletben tartja az egyének autonómiáját, és elkerüli az indokolatlan adatgyűjtést és kockázatokat. A valódi biztonság ebben az esetben nemcsak a jogosulatlan hozzáférés megelőzését jelenti, hanem azt is, hogy az érintettek ellenőrzést gyakorolhassanak saját biometrikus adataik felett.

Biztonsági ajánlások a biometrikus rendszerekhez

A biometrikus rendszerek bevezetése és működtetése során a biztonság nem automatikusan biztosított: megfelelő védelem hiányában ezek a rendszerek akár kockázatosabbá is válhatnak, mint a hagyományos azonosítási eljárások. A valóban megbízható biometrikus azonosítás megvalósítása érdekében számos technikai, szervezeti és adatvédelmi intézkedésre van szükség.

Az első és legfontosabb alapelv az, hogy a biometrikus adatokat soha ne tároljuk nyers formában. Egy arckép, ujjlenyomat-felvétel vagy íriszminta digitális képe nem alkalmas biztonságos tárolásra, mivel könnyen visszafejthető, manipulálható vagy újrahasznosítható. Ehelyett a nyers adatból egy matematikai sablont kell generálni, amelyet úgy kell kialakítani, hogy ne legyen visszaalakítható az eredeti jellemzővé, és ne legyen újrafelhasználható más rendszerekben. E célra különféle sablonvédelmi technológiák léteznek, mint például a template masking, ahol a sablont egy adott kulcs vagy algoritmus torzítja, illetve a cancelable biometrics, ahol a sablon egy újragenerálható, torzított formában kerül tárolásra.

Kiemelten fontos a sablonok titkosítása, lehetőség szerint end-to-end módon – azaz már a szenzor szintjén megkezdett titkosítással. Az adatok tárolása során modern, erős kriptográfiai algoritmusokat (például AES-256, SHA-3) kell alkalmazni, és gondoskodni kell a kulcskezelés megfelelő szétválasztásáról, naplózásáról és jogosultsági szintjeiről. A titkosított adattárolás mellett javasolt az is, hogy a

biometrikus adatokat – ha lehetséges – helyileg, az eszközön tárolják, például a felhasználó mobilkészülékén vagy chipkártyán. Ez csökkenti a központi adatbázisok támadási felületét, és lehetővé teszi a decentralizált működést.

A rendszernek minden esetben tartalmaznia kell valódiságellenőrző (liveness detection) funkciót, amely biztosítja, hogy a szenzor valódi, élő embertől származó mintát dolgoz fel, és nem egy fényképet, műujjat vagy deepfake videót. A liveness detection lehet aktív – például a felhasználót megkérik, hogy pislogjon, mosolyogjon, mozgassa a fejét –, vagy passzív, amely az arckép vagy hang finom jeleiből érzékeli az élő jelenlétet. E technológia hiánya a rendszer megtévesztését különösen könnyűvé teszi.

A biztonság növelése érdekében ajánlott a biometrikus azonosítást nem önállóan, hanem többtényezős azonosítás részeként alkalmazni. A többtényezős (MFA) rendszerek a „valami, amit tudsz" (pl. jelszó), „valami, amid van" (pl. mobiltelefon) és „valami, ami vagy" (pl. biometrikus jellemző) kombinációját használják. Egy biometrikus jellemző egyedisége önmagában nem garantál védelmet a kompromittált végpont, a manipulált szenzor vagy a jelszavas rés feltörése ellen – csak más tényezőkkel kombinálva biztosíthat magas szintű védelmet.

Szervezeti szinten elengedhetetlen a hozzáférési jogosultságok szigorú szabályozása: ki férhet hozzá a biometrikus adatokhoz, milyen célból, milyen időtartamra és milyen naplózás mellett. Emellett a rendszerbe épített auditálási és naplózási mechanizmusok biztosítják, hogy minden hozzáférési kísérlet nyomon követhető legyen, és az esetleges visszaélések bizonyíthatóak maradjanak.

Ajánlott továbbá rendszeres biztonsági tesztelés – például sérülékenységvizsgálat vagy penetrációs teszt –, különösen olyan rendszerek esetén, amelyek nyilvánosan elérhetők, vagy érzékeny adatokhoz biztosítanak hozzáférést. Ezeknek a teszteknek ki kell terjedniük a szenzorok manipulálhatóságára, a sablonok sérülékenységére, az autentikációs folyamatok visszajátszhatóságára, valamint a rendszerben alkalmazott kriptográfiai védelmek helyességére.

A felhasználói oldalról nézve nem szabad megfeledkezni a tudatosítás és oktatás fontosságáról sem. A felhasználóknak érteniük kell, hogyan működik a biometrikus rendszer, milyen kockázatokkal jár az azonosító megosztása, és hogyan ismerhetik fel, ha a rendszer hibásan működik, vagy ha támadás alatt áll. Ezen túl fontos, hogy a felhasználóknak – különösen vállalati környezetben – legyen alternatív azonosítási lehetőségük abban az esetben, ha a biometrikus megoldás nem működik, vagy ha nem kívánják azt használni.

Összességében elmondható, hogy a biometrikus rendszerek akkor válhatnak biztonságos és megbízható technológiává, ha azok nem önmagukban, hanem egy átfogó kockázatkezelési stratégia részeként kerülnek bevezetésre. A megfelelő sablonvédelem, titkosítás, rendszerarchitektúra és oktatás együttesen garantálhatja, hogy a biometrikus azonosítás ne gyenge pont, hanem megerősített védelmi réteg legyen a szervezet biztonsági rendszerében.

Gyakorlati példák és támadási esetek

A biometrikus rendszerek történetében több olyan ismert támadás és kompromittáció történt, amelyek rávilágítottak arra, hogy a „csak biometria" alapú azonosítás hamis biztonságérzetet kelthet, és megfelelő védelem nélkül komoly kockázatot jelenthet.

Az egyik legnagyobb szabású és legnagyobb hatású eset az indiai Aadhaar rendszer kompromittációja volt. Az Aadhaar a világ legnagyobb biometrikus azonosítási rendszere, amely több mint 1 milliárd ember ujjlenyomatát, arcfelismerési adatait és íriszmintáját tárolja. 2018-ban kiderült, hogy több millió ember biometrikus adataihoz lehetett hozzáférni egy adminisztrációs hozzáférés feltörése után, ráadásul olyan módon, hogy az adatok egy részét nyíltan árulták a feketepiacon. A rendszer sérülékenységeinek kihasználása súlyos adatvédelmi válságot okozott, és rávilágított arra, hogy a központi tárolású biometrikus adatbázisok különösen sebezhetőek, ha nem történik meg a szigorú hozzáféréskezelés, naplózás és sablonvédelem.

Egy másik ismert eset a Samsung Galaxy S10 telefon arcfelismerő- és ujjlenyomat-olvasó rendszeréhez kapcsolódik. 2019-ben biztonsági kutatók kimutatták, hogy a készülék képes volt elfogadni olyan ujjlenyomatot is, amely nem a regisztrált felhasználóhoz tartozott, ha az illető egy védőfóliát helyezett a képernyőre. A szenzor a fólia mintázatát összetévesztette az ujjlenyomattal, és sikeresen hitelesítette a támadót.

Ez az eset jól példázza, hogy a szenzortechnológia sebezhetősége súlyosan aláásható az azonosítás megbízhatóságát.

A deepfake technológia terjedésével új támadási vektorok nyíltak meg az arcfelismerő rendszerek ellen is. Egyes kutatásokban már sikerült olyan valós időben generált videókat készíteni, amelyek a kamera számára élő, természetes arcképet utánoztak, miközben valójában nem az adott személy volt jelen. Bár a fejlett rendszerek ma már beépítenek valódiságellenőrző mechanizmusokat, ezek a támadások jól mutatják, hogy a támadói eszközök fejlődése folyamatosan új kihívások elé állítja a biometrikus biztonságot.

Kevésbé látványos, de annál súlyosabb támadástípus a biometrikus sablonok újrafelhasználása. Ha egy biometrikus sablon kikerül egy rendszerből, és más, hasonló rendszer nem védi megfelelően az adatainak egyediségét, akkor a sablont más környezetben is felhasználhatják hitelesítésre. Ez különösen akkor válik veszélyessé, ha a felhasználó több szolgáltatásban is ugyanazt a biometrikus jellemzőt használja (pl. ugyanazzal az ujjlenyomattal lép be banki alkalmazásba, belépőrendszerbe és egészségügyi platformra).

A támadások sorában érdemes megemlíteni azokat az eseteket is, ahol a rendszer hibásan azonosított valakit. 2020-ban az Egyesült Államokban egy fekete bőrű férfit tévesen tartóztattak le, miután egy arcfelismerő rendszer hamisan azonosította egy bűncselekmény gyanúsítottjaként. A rendszer nemcsak tévedett, hanem torzításokat is mutatott, mivel nem megfelelő adathalmazon lett betanítva. Ez az eset súlyosan megkérdőjelezte az arcfelismerő rendszerek alkalmazhatóságát bűnüldözésben, és rávilágított az algoritmikus torzítások súlyos következményeire.

E példák alapján jól látható, hogy a biometrikus rendszerek nem immunisak a hibára, a támadásra vagy az emberi mulasztásra. A legfontosabb tanulság, hogy egy biometrikus azonosítási rendszer nem lehet önmagában az egyetlen védelmi vonal, és csak akkor alkalmazható felelősen, ha azt kockázatértékelés, tesztelés és alternatív hozzáférési mechanizmusok egészítik ki. A való életben történt esetek azt bizonyítják, hogy a biometrikus azonosítás csak akkor válhat megbízhatóvá, ha a rendszer egészét – az érzékelőktől a sablontárolásig – biztonságtudatos módon tervezzük meg és működtetjük.

Ajánlások szervezeteknek és felhasználóknak

A biometrikus azonosítás bevezetése nem csupán technológiai döntés, hanem stratégiai és adatvédelmi kérdés is. Mielőtt egy szervezet biometrikus rendszert alkalmazna, célszerű mérlegelnie a várható előnyöket és a vele járó kockázatokat, és mindezt a jogszabályi környezettel, az érintettek bizalmával és a működési környezettel összhangban tennie.

Elsőként meg kell válaszolni a kérdést: valóban szükség van-e biometrikus azonosításra, vagy egyéb, kevésbé érzékeny technológia is elegendő? A biometrikus megoldások bevezetése akkor indokolt, ha a védendő erőforrás vagy hozzáférés magas biztonsági értékkel bír, és ha más azonosítási módszerek nem nyújtanak kellő védelmet, vagy nem felelnek meg a használati körülményeknek. Ugyanakkor a pusztán kényelmi célból történő alkalmazás – például amikor egyébként alacsony kockázatú rendszer bevezetéséről van szó– aránytalan adatvédelmi kockázatot eredményezhet.

Amennyiben a szervezet úgy dönt, hogy biometrikus azonosítást alkalmaz, az egyik legfontosabb szempont a rendszer átláthatósága. A felhasználókat részletesen és érthetően tájékoztatni kell arról, milyen adatokat gyűjt a rendszer, mire használja azokat, hol és meddig tárolja, milyen jogalapon történik az adatkezelés, és milyen jogorvoslati lehetőségek állnak rendelkezésükre. A tájékoztatásnak nem csupán formálisnak kell lennie, hanem valós, gyakorlati eligazítást kell adnia a felhasználóknak – különösen, ha érzékeny személyes adatokról van szó.

A bizalom megerősítése érdekében fontos, hogy a szervezet alternatív azonosítási módokat is biztosítson azok számára, akik valamilyen okból nem kívánják vagy nem tudják használni a biometrikus megoldást. Ez lehet például jelszóalapú bejelentkezés, hardveres token, vagy kétfaktoros azonosítás más formában. Az alternatíva biztosítása etikai és jogi szempontból is elengedhetetlen, hiszen az érintetteknek joguk van dönteni saját biometrikus adataikkezeléséről.

Ajánlott továbbá, hogy a biometrikus azonosítás ne önmagában, hanem többtényezős rendszer részeként kerüljön bevezetésre. Így a biometrikus jellemző egy további biztonsági rétegként szolgálhat, nem pedig kizárólagos belépési eszközként. Ez a megközelítés jobban védi a felhasználókat a visszaélésektől, és lehetővé teszi, hogy egy-egy tényező sérülése vagy kompromittálódása esetén más módon is hitelesíthető maradjon a felhasználó.

Fontos szem előtt tartani, hogy egy biometrikus rendszer nem zárja ki a rendszeres karbantartás és biztonsági felülvizsgálat szükségességét. A szoftvereket, érzékelőket és adatkezelési mechanizmusokat időszakosan ellenőrizni, a naplózott eseményeket pedig elemezni kell, és fel kell készülni a lehetséges incidensekre – például sablonlopás esetén elérhetővé kell tenni egy új hitelesítési útvonalat. Célszerű „incident response" tervet is készíteni kifejezetten a biometrikus rendszerekhez kapcsolódó helyzetekre.

Felhasználói oldalon a legfontosabb tanács az, hogy senki ne tekintse a biometrikus azonosítást mindenhatónak vagy megtéveszthetetlennek. A felhasználóknak érdemes tisztában lenniük azzal, hogy a biometrikus adatok különösen érzékeny információk, amelyek megosztásával hosszú távú, visszafordíthatatlan kockázatot vállalnak. Éppen ezért nem javasolt, hogy valaki ugyanazt a biometrikus azonosítót használja több különböző rendszerben, különösen, ha azok biztonsági szintje eltérő.

Felhasználóként érdemes csak akkor elfogadni biometrikus azonosítást, ha a rendszer világos és részletes tájékoztatást nyújt az adatkezelésről, lehetőséget ad az elutasításra, és megfelelő technikai védelmet nyújt. Ha ezek nem teljesülnek, a biometrikus adat megadása kockázatos és indokolatlan lehet. A tudatos felhasználói magatartás – beleértve az adatvédelmi beállítások ellenőrzését, a hozzáférési naplók követését, és az alternatív lehetőségek keresését – elengedhetetlen ahhoz, hogy a biometrikus azonosítás eszköz legyen, ne gyengeség.

Végső soron a biometrikus azonosítás alkalmazása akkor tekinthető sikeresnek, ha a rendszer nemcsak technikailag működik, hanem etikai, jogi és felhasználói szempontból is elfogadható, és hozzájárul a szervezet teljes biztonsági ökoszisztémájának megerősítéséhez.

Összegzés és jövőbeli kilátások

A biometrikus azonosítás ma már nemcsak a sci-fi filmek sajátja, hanem a hétköznapi digitális élet szerves része. Okostelefonok, beléptetőrendszerek, határátlépési pontok, banki alkalmazások – mind olyan területek, ahol az emberi test vagy viselkedés egyedi jellemzőit használják azonosításra. Az eddigiek alapján azonban világossá válik, hogy a biometrikus rendszerek nem pusztán kényelmi eszközök: érzékeny, nagy felelősséggel járó technológiák, amelyek használata komoly biztonsági, adatvédelmi és etikai kérdéseket vet fel.

Az egyik legfontosabb tanulság az, hogy a biometrikus azonosítás soha nem tekinthető önmagában teljes értékű biztonsági megoldásnak. Egyedisége és kényelme mellett ugyanis visszafordíthatatlan kompromittációs kockázattal jár, ha nem megfelelően védjük a sablonokat, nem alkalmazunk többtényezős hitelesítést, vagy figyelmen kívül hagyjuk a rendszertechnikai támadási felületeket. A valóban biztonságos biometrikus rendszer mindig összetett védelemre épül, amely tartalmaz titkosítást, élettelenség-ellenőrzést, rendszeres auditálást, hozzáférés-szabályozást és adatvédelmi megfelelést.

A felhasználói oldal szempontjából is fontos a tudatosság növelése. Mivel a biometrikus jellemzők nem megváltoztathatók, a felhasználóknak tisztában kell lenniük azzal, hogy adatuk megosztása hosszú távú kockázatot hordozhat. Tudniuk kell, mire adják a hozzájárulásukat, milyen jogok illetik meg őket, és hogyan ellenőrizhetik az adatkezelés gyakorlatát. A technológia iránti bizalom nem automatikus, hanem csak akkor alakul ki, ha a rendszerek átláthatók, igazságosak és jogszerűek.

A biometrikus technológia fejlődése ugyanakkor folyamatos. A jövőben egyre nagyobb hangsúlyt kapnak a passzív biometrikus megoldások, amelyek a felhasználó viselkedését – például egérmozgását, járásmintázatát vagy mobiltelefon-használati szokásait – figyelve végzik az azonosítást, gyakran a háttérben, megszakítás nélkül. Ezzel párhuzamosan terjednek a decentralizált azonosítási modellek, amelyek célja, hogy a biometrikus adatok ne központi adatbázisban, hanem a felhasználó eszközén maradjanak, és csak titkosított hitelesítési eredményeket osszanak meg. Az ilyen megoldások – például a zero-knowledge proof alapú autentikációk – lehetővé teszik, hogy a felhasználó úgy igazolja magát, hogy közben nem kell átadnia a tényleges biometrikus adatot.

További fontos trend a biometria és a mesterséges intelligencia összekapcsolása. A gépi tanulás és neurális hálózatok fejlődése lehetővé teszi a pontosabb és rugalmasabb azonosítást, ugyanakkor újfajta támadási lehetőségeket is nyit – például a deepfake vagy generatív modelleken alapuló megtévesztő minták használatát. Ennek megfelelően a következő évek legnagyobb kihívása az lesz, hogy a védelmi oldalt gyorsabban fejlesszük, mint a támadók eszköztárát.

Végső soron a biometrikus azonosítás jövője nem kizárólag a technológián múlik, hanem azon is, hogy képesek vagyunk-e társadalmi, jogi és szervezeti szinten felelősen integrálni ezt az eszközt a digitális világ működésébe. A siker feltétele az, hogy a biztonság, a kényelem és az adatvédelem ne egymás rovására, hanem egymással összhangban érvényesüljenek.

Források

A. O. Adewole, O. A. Adediran, M. O. Adediran (2016). Fingerprint biometric-based Access Control and Classroom Attendance Management System. https://www.researchgate.net/publication/304230297_Fingerprint_biometric_based_Access_Control_and_Classroom_Attendance_Management_System (Letöltve: 2025. június 19.)

ABI Research (2023). 6 Types of Biometrics for Identity Authentication. https://www.abiresearch.com/blog/types-of-biometrics (Letöltve: 2025. június 12.)

Aratek (2023). Exploring Biometric Authentication: From Basics to Case Studies. https://www.aratek.co/news/exploring-biometric-authentication-from-basics-to-case-studies (Letöltve: 2025. június 19.)

Bleicher, Paul (2005). Biometrics comes of age: despite accuracy and security concerns, biometrics are gaining in popularity. Applied Clinical Trials. https://www.appliedclinicaltrialsonline.com/view/biometrics-comes-age (Letöltve: 2025. június 13.)

Cao, Liling; Ge, Wancheng (2015). Analysis and improvement of a multi-factor biometric authentication scheme: Analysis and improvement of a MFBA scheme. Security and Communication Networks, 01(4), 617–625. https://doi.org/10.1002/sec.1010 (Letöltve: 2025. június 12.)

CynergyTech (n.d.). Biometric Authentication: Benefits and Challenges. https://www.cynergytech.com/stories/biometric-authentication-benefits-and-challenges/ (Letöltve: 2025. június 19.)

Datadog (n.d.). Cloud Security Management - Vulnerabilities. https://docs.datadoghq.com/security/cloud_security_management/vulnerabilities/ (Letöltve: 2025. június 19.)

Európai Parlament és Tanács (2004). 2252/2004/EK rendelet a biztonsági jellemzők és a biometrikus azonosítás szabványairól úti okmányokban. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004R2252 (Letöltve: 2025. június 13.)

European Data Protection Board (EDPB) (n.d.). Biometrics – Documents and Guidance. https://www.edpb.europa.eu/our-work-tools/our-documents/topic/biometrics_en (Letöltve: 2025. június 19.)

European Data Protection Board (EDPB) (n.d.). Guidelines, Recommendations and Best Practices. https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_hu?page=9 (Letöltve: 2025. június 19.)

European Union Agency for Cybersecurity (ENISA) (2023). Remote Identity Proofing: Attacks & Countermeasures. https://www.datanamix.com/wp-content/uploads/2023/02/ENISA-Report-Remote-Identity-Proofing-Attacks-Countermeasures.pdf (Letöltve: 2025. június 18.)

European Union Agency for Cybersecurity (ENISA) (2024). Technical Implementation Guidance on Cybersecurity Risk Management Measures, Version 1.0. https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf (Letöltve: 2025. június 16.)

Future of Privacy Forum (FPF) (2022). A Visual Guide to Practical Data De-Identification. https://fpf.org/blog/a-visual-guide-to-practical-data-de-identification/ (Letöltve: 2025. június 11.)

National Cyber Security Centre (NCSC, Egyesült Királyság) (n.d.). Using biometrics. https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/using-biometrics (Letöltve: 2025. június 13.)

National Institute of Standards and Technology (NIST) (2016). Applying Measurement Science in the Identity Ecosystem Workshop. https://www.nist.gov/system/files/applyingmeasurementscienceworkshopjan12_13_2016.pdf (Letöltve: 2025. június 19.)

National Institute of Standards and Technology (NIST) (2020). International Biometric Performance Conference: Panel on Image Quality. https://www.nist.gov/system/files/documents/2020/12/15/340_1_mansfield_panel_ibpc.pdf (Letöltve: 2025. június 19.)

National Institute of Standards and Technology (NIST) (2023). Face Recognition Vendor Test (FRVT) Results. https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt (Letöltve: 2025. június 11.)

Security Industry Association (SIA) (2020). SIA Response to NIST Data and Facial Recognition. https://www.securityindustry.org/wp-content/uploads/2020/02/SIA-NIST-data-and-facial-recognition.pdf (Letöltve: 2025. június 19.)

Sterling, Bruce (2018). Indian Aadhaar Issues. Wired. https://www.wired.com/beyond-the-beyond/2018/02/indian-aadhaar-issues/ (Letöltve: 2025. június 19.)

Thales Group (n.d.). History of Biometric Authentication. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-biometric-authentication (Letöltve: 2025. június 19.)

Villas-Boas, Antonio (2021). Passwords are incredibly insecure, so websites and apps are quietly tracking your mouse movements and smartphone swipes without you knowing to make sure it's really you. Business Insider. https://www.businessinsider.com/websites-apps-track-mouse-movements-screen-swipes-security-behavioral-biometrics-2019-7 (Letöltve: 2025. június 17.)

NEMZETI
KIBERBIZTONSÁGI
INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2025