Doktori (PhD) értekezés

(tervezet)

Koller Marco

2025

NEMZETI KÖZSZOLGÁLATI EGYETEM

Hadtudományi Doktori Iskola

Koller Marco:

Okos eszközök fejlődő irányai, az információs társadalom biztonsági kihívásai, az adatbiztonság, és a társadalmi elfogadottság tükrében

Doktori (PhD) értekezés

(tervezet)

Társ-témavezető:

Dr. Bányász Péter

……..

Témavezető:

Dr. Dobák Imre

……..

Budapest, 2025

TARTALOMJEGYZÉK

1 BEVEZETÉS ... 6
1.1 A téma aktualitása ... 6
1.2 A téma relevanciája a hadtudományban ... 10
1.3 Szakirodalmi áttekintés ... 17
1.4 Kutatási célok ... 19
1.5 Kutatási kérdések ... 21
1.6 Hipotézisek ... 22
1.7 Kutatási módszertan ... 24
1.8 Az értekezés logikai felépítése ... 26
2 Az információs társadalom és annak biztonsági kihívásai ... 28
2.1 Információs társdalom meghatározása ... 28
2.1.1 Információs társdalom fogalmi definíciói ... 28
2.1.2 Az információs társadalomtörténeti keletkezése és fejlődése ... 31
2.1.3 Az információs társadalom dimenziói és fő jellemzői ... 33
2.2 Az információs társadalom biztonsági kihívásai, annak típusai és felosztása ... 41
2.3 Technológiai és technikai kihívások ... 43
2.3.1 Az okos eszközökből és IoT eszközökből adódó biztonsági kihívások ... 45
2.3.2 Okos mobil eszközök kihívásai ... 46
2.3.3 Az okos otthoni eszközök és a privát szféra ... 48
2.3.4 Okos városok és a megfigyelés problematikája ... 49
2.3.5 Okos infrastruktúrák kiberbiztonsági kockázatai ... 51
2.3.6 Kibertámadások és kiberbűnözés ... 52
2.3.7 A biometrikus adatok kezelésének kihívásai ... 56
2.3.8 A mesterséges intelligencia és automatizáció ... 57
2.3.9 Decentralizált technológiák és kriptográfiai akadályok ... 59
2.3.10 Kihívások a kvantumszámítástechnikában ... 61
2.4 Humán forrású kihívások ... 62
2.4.1 Társadalmi-gazdasági kihívások ... 63
2.4.2 Jogi, adatvédelmi kihívások ... 63
2.4.3 Hitelesség kérdésköre és az információs műveletek, álhírek terjedése ... 65
2.4.4 Az információs műveletek típusai és a kognitív térben zajló műveletek ... 67
2.4.5 A dezinformáció típusai és evolúciója ... 70
2.4.6 Digitális kompetencia, oktatási és tudatossági hiányosságok. ... 73
Következtetések ... 75
3 Okos eszközök evolúciója és a kapcsolódó kihívások ... 78
3.1.1 Történeti betekintés eszközök kialakulása. ... 80
3.1.2 Hardveres innovációk az elmúlt évtizedben ... 82
3.1.3 Konnektivitás és hálózati technológiák ... 82
3.2 Az okos eszközök applikációinak szerepe ... 83
3.2.1 Az alkalmazások funkciója és jelentősége az okos eszközök ökoszisztémájában ... 85
3.3 Az okos eszközök alkalmazástípusainak sokszínűsége ... 87
3.3.1 Fogyasztói alkalmazások ... 87
3.3.2 Üzleti és vállalati alkalmazások ... 89
3.3.3 Speciális alkalmazások ... 90
3.4 Az okos eszközök alkalmazásainak fejlesztési trendjei és technológiái ... 92
3.4.1 Mesterséges intelligencia, gépi tanulás és algoritmusok szerepe ... 92
3.4.2 5G és későbbi hálózati technológiák ... 93
3.4.3 Edge computing ... 93
3.4.4 Blockchain és decentralizált alkalmazások (dApps) ... 94
3.4.5 Ambient computing ... 94
3.4.6 Felhasználói szemléletből fakadó tényezők ... 95
3.5 Személyazonosításra és hitelesítésre alkalmas eszközzé válás ... 97
3.5.1 A személyazonosítás főbb típusai ... 98
3.5.2 A személyi hitelesítés főbb típusai ... 99
3.5.3 A mobil azonosítás fejlődésének áttekintése ... 101
3.5.4 Mobileszköz-alapú hitelesítés ... 103
3.5.5 Nemzetközi példák ... 104
3.5.6 Hazai példa (AVDH, e-személyi, DÁP) ... 110

3.5.7 A magyar elektronikus azonosítási megoldások nemzetközi összehasonlításban 116
3.6 Okos mobil eszközök és applikációinak biztonsági kérdései és kockázatai 117
3.6.1 Kibertérben zajló támadások, támadási vektorok 117
3.6.2 Alkalmazás-specifikus biztonsági kockázatok 121
3.6.3 Excessive Permissions és adathozzáférés 121
3.6.4 Adatszivárgás és harmadik felek általi adatgyűjtés 121
3.6.5 Frissítési mechanizmusok sebezhetőségei 122
3.6.6 In-App vásárlások és pénzügyi kockázatok 122
3.6.7 Alkalmazások közötti interakciók veszélyei 122
3.6.8 Hálózati kapcsolatok és kommunikációs protokollok biztonsági kihívásai 123
3.6.9 Bluetooth kapcsolatok sebezhetőségei 124
3.6.10 IoT kommunikációs protokollok biztonsági kihívásai 124
3.6.11 További kommunikációs technológiák kockázatai 125
3.6.12 Adatbiztonsági és adatvédelmi kockázatok 126
Következtetések 128
4 Személyazonosításra és hitelesítésre alkalmas technológia jelenlegi felhasználási területei 134
4.1 Magánszférában alkalmazott technológiák 134
4.1.1 Bank és pénzügyi szektor 135
4.1.2 Ügyvédi irodák és jogi szektor 140
4.1.3 Turizmus és idegenforgalmi szektor 143
4.1.4 Közösségi média és egyéb online platformok 145
4.2 Állami szférában alkalmazott technológiák 148
4.2.1 E-közigazgatás, m-közigazgatás 149
4.2.2 Személyazonosítási és hitelesítési technológiák a digitális kormányzatban 151
4.2.3 Biometrikus hitelesítés a kormányzati alkalmazásokban 153
4.2.4 Megosztott hitelesítési ökoszisztémák 155
4.3 Személyazonosítási és hitelesítési technológiák a védelmi, biztonsági szektorban 155
4.3.1 Katonai műveletek 158
4.3.2 Bűnüldözési alkalmazások 158
4.3.3 Határellenőrzés és bevándorlás 159
4.3.4 Egészségügy 161
4.4 Jelenlegi biztonsági a mobil személyazonosítási és hitelesítési technológiák kapacsán kihívások, kockázatok 163
4.4.1 A biometrikus hitelesítés sebezhetőségei 164
4.4.2 A mesterséges intelligenciával kapcsolatos veszélyek és ellenstratégiák 164
4.4.3 Adatvédelmi és adatvédelmi kihívások 164
4.4.4 Az interoperabilitással és standardizálással kapcsolatos akadályok 166
4.4.5 Teljesítménnyel és megbízhatósággal kapcsolatos aggályok 166
4.4.6 A társadalmi elfogadással és bizalommal kapcsolatos kérdések 167
4.5 Ágazat-specifikus kihívások 168
4.5.1 Az egészségügyi hitelesítéssel kapcsolatos kérdések 168
4.5.2 A pénzügyi szolgáltatási szektor biztonsági követelményei 168
4.5.3 Ügyvédi irodák 169
4.5.4 Turizmus 169
4.5.5 Közösségi média 170
4.5.6 A közszféra kezdeményezéseinek végrehajtási kihívásai 170
4.5.7 Védelmi, biztonsági szektor 172
4.6 Mobil személyazonosítási és hitelesítési technológia társadalmi elfogadottsága a magánszférában 173
4.6.1 Társadalmi elfogadottság vizsgálata releváns videók alatti hozzászólások alapján ... 175
4.7 Mobil személyazonosítási és hitelesítési technológia társadalmi elfogadottsága az állami szférában 179
4.7.1 A korábbi magyar eSzemélyi elfogadottsága. 180
4.7.2 Határellenőrzés és bevándorlás-kezelés 180
4.7.3 Egészségügyi hitelesítési rendszerek 181
4.7.4 Társadalmi elfogadottság vizsgálata releváns videók alatti hozzászólások alapján ... 181
Következtetések 198
5 Személyazonosításra és hitelesítésre alkalmas technológia alkalmazásának jövőbeli lehetőségei 203
5.1 Államilag fejlesztett eszköz általi hitelesítés 203

5.1.1 Feltörekvő biometrikus technológiák a kormányzati alkalmazásokban 204
5.1.2 Fejlett prezentációs támadásdetektálás 204
5.1.3 Peremhálózati számítástechnika a biztonságos biometrikus adatfeldolgozáshoz 205
5.1.4 Mesterséges intelligencia integráció és folyamatos hitelesítés 205
5.1.5 Blokklánc és önszuverén identitás 206
5.2 Jövőbeli fejlesztési irányok és ajánlások 206
5.2.1 Kvantumrezisztens kriptográfia 206
5.2.2 Folyamatos hitelesítés és zéró bizalom architektúra 206
5.2.3 Befogadó tervezés és hozzáférhetőség 207
5.3 Magánszektor által fejlesztett eszköz általi hitelesítés 207
5.3.1 Okoseszköz-alkalmazások a magánszektorbeli hitelesítéshez 208
5.4 Állami és magán partnerségek és hibrid modellek, együttműködési keretrendszerek az identitás-ellenőrzéshez 211
5.4.1 A hibrid megközelítések előnyei és kihívásai 211
5.5 Stratégiák a társadalmi elfogadottság növelésére 212
5.5.1 Adatvédelmet erősítő implementációs stratégiák 213
5.6 Internetes csalások elleni 213
5.6.1 Közösségi média platform implementációs stratégiák 216
5.7 Információs műveletek elleni küzdelem 217
5.7.1 Okos eszközök biometrikus képességei és azok alkalmazása az információs műveletek elleni küzdelemben 218
5.7.2 Platformokon átívelő hitelesítési szabványok 219
5.7.3 Gyakorlati alkalmazások az információs műveletek elleni küzdelemben 219
5.7.4 Személyazonosításra és hitelesítésre alkalmas technológia jövőbeli biztonsági kockázatai 221
Következtetések és szakértői interjú eredmények 225
6 Személyi azonosításra vagy hitelesítésre alkalmas technológia felhasználásának lehetőségei és kockázatai a védelmi, biztonsági szektorban 231
6.1 Katonai szektorban történő alkalmazás 231
6.1.1 Mobilalkalmazások a katonai biometrikus azonosításban 231
6.1.2 Kockázatok és kihívások 234
6.1.3 Fejlődési trendek és jövőbeli alkalmazások 235
Következtetések és ajánlások 237
6.2 Rendészeti, rendvédelmi szektorban történő alkalmazás 238
6.2.1 Mobilalkalmazások a rendőrségi biometrikus azonosításban 239
6.2.2 Kockázatok és kihívások 241
6.2.3 Jogi és szabályozási keretek 242
6.2.4 Jövőbeli trendek és fejlesztési irányok 243
Következtetések 244
6.3 Magánbiztonsági szektorban történő alkalmazás 245
6.3.1 Mobilalkalmazások a biometrikus azonosításban 245
6.3.2 A biometrikus hitelesítés előnyei a magánbiztonsági szektorban 246
6.3.3 Mesterséges intelligencia integrációja a biometrikus rendszerekbe 246
6.3.4 Összegzés és ajánlások 247
6.4 Idegenrendészeti területen történő alkalmazás 248
6.4.1 Mobil applikációk szerepe az idegenrendészeti biometrikus azonosításban 248
6.4.2 Alkalmazási területek az idegenrendészetben 249
6.4.3 Az idegenrendészeti biometrikus azonosítás előnyei 249
6.4.4 Legjobb gyakorlatok és ajánlások 250
Következtetések 251
6.5 Nemzetbiztonsági területen történő alkalmazás 252
6.5.1 A biometrikus azonosítás evolúciója a titkosszolgálati munkában 252
6.5.2 Titkosszolgálati alkalmazási területek 253
6.5.3 Kockázatok és sebezhetőségek a titkosszolgálati alkalmazásban 255
6.5.4 Jövőbeli trendek és fejlesztési irányok 256
Következtetések és ajánlások 257
7 ÖSSZEGZETT KÖVETKEZTETÉSEK 259
A kutatási eredmények értékelése és a hipotézisek teljesülése 261
Következtetések 264
8 Új tudományos eredmények 266

9 Ajánlások a kutatás eredményeinek gyakorlati felhasználhatóságára 268
További kutatási irányok 268
10 Ábra jegyzék 270
11 Felhasznált irodalom 270
12 Publikációs jegyzék 290

1 BEVEZETÉS

Az információs társadalom egyik vívmánya az internet és a nagy mennyiségű adathoz, információhoz való gyors, szinte azonnali hozzáférés. A technológia, a technológiai fejlődés, valamint az ember és gép közötti kölcsönhatások növekvő száma napjaink társadalmának szerves részévé vált, alapvetően átalakítva mindennapi életünket. Az ember-gép interfész technológia elsődleges funkciója a felhasználók és eszközök közötti kommunikáció biztosítása, amely megteremti a hatékony interakció lehetőségét. Ahogy Castells rámutat, ez az új technológiai paradigma nemcsak eszközöket, hanem új társadalmi struktúrákat is létrehoz, amelyek komplex hatással vannak a társadalmi kapcsolatrendszerre és a hatalmi viszonyokra.[1] Az okos eszközök (lényegében olyan eszköz, ami képes az internetre csatlakozni, más eszközökkel kommunikálni és különböző szoftverek segítségével speciális feladatokat végrehajtani, mint például okos telefonok, táblagépek, robotporszívók, okos órák. (A fogalmat részletesen a későbbiek során fogom kifejteni.) Ennek a technológiai paradigmának kiváló példái, amelyek fokozatos elterjedése és a mindennapi életbe való integrálódása révén különböző állami és nem állami szereplők értékes információkat gyűjthetnek az egyének szokásairól, mozgásáról, társadalmi kapcsolatairól, vagy akár egészségügyi állapotáról is.

1.1 A téma aktualitása

A téma aktualitása kapcsán kiemelendő, hogy a digitális eszközök fejlődési üteme az elmúlt évtizedben exponenciálisan gyorsult, amit a Gartner adatai is bizonyítanak, mert a felmérésük alapján 2025-re a világ népességének mintegy 75%-a legalább napi szinten interaktál valamilyen okos eszközzel.[2] Ez előbbi alátámasztja azt, hogy az okos eszközök működésének, fejlődési irányainak, valamint társadalmi, biztonsági és adatvédelmi hatásainak alaposabb megértése, azok vizsgálata kiemelt témakör. Nemeslaki András és kutatótársai kiemelték, hogy az infokommunikációs eszközök penetrációja

[1] Manuel Castells, *Communication Power* (New York: Oxford University Press, 2009).
[2] Inc Gartner, *Gartner Forecasts Worldwide Connected Devices to Total 41.6 Billion in 2025* (Gartner Press Release, 2023).

drámai mértékben változtatja meg a társadalmi működést, ami együtt jár az állami szerepvállalás revíziónak szükségességével is[3] , így szükséges a téma esetleges állami szerepvállalásának konzisztens monitorozása, elemzése. Különös figyelmet érdemelnek az okos eszközök és az azokra letölthető applikációk által nyújtott funkciók és azok folyamatos evolúciója. Eklatáns példaként említhetők az okos telefonok mobilbanki alkalmazásai, amelyek átalakították a pénzügyi szolgáltatások igénybevételének módját. Ezek az alkalmazások lehetővé teszik a felhasználók számára, hogy banki ügyeiket bárhol, bármikor intézhessék, ugyanakkor kihívásokat is jelenthetnek. Pap Zoltán szerint a mobilbanki alkalmazásokkal kapcsolatban nem csupán technikai jellegű biztonsági kockázatok vannak, hanem társadalmi és pszichológiai aspektusokkal is rendelkeznek, mivel a felhasználók gyakran nem megfelelően mérlegelik a kényelmi szempontok és a biztonsági követelmények közötti egyensúlyt.[4]

Az egyre gyorsuló ütemben digitalizálódó társadalmakban az okos eszközök és alkalmazások nemcsak a magánszektorban jelennek meg és növekedik a szerepük, hanem a közszférában is fokozatosan felértékelődik a jelentőségük. Mivel a kényelmi faktor egyre inkább a mindennapunk egyik meghatározó része, így a különböző szolgáltatásokhoz való könnyű, akár távoli hozzáférés érdekében szükséges a biztonság szavatolása. Az e-kormányzati megoldások és az elektronikus ügyintézés fejlődése felhasználóbarát, gyors és hatékony alternatívákat kínál az állampolgárok számára a hagyományos, személyes jelenlétet igénylő ügyintézéssel szemben.[5] Ezek a megoldások a jövőben tovább fejlődhetnek a távazonosításon alapuló, teljes mértékben digitalizált ügyintézés irányába, amely új típusú kockázatokat vethetnek fel. Budai Balázs Benjamin kutatásai rámutatnak, hogy a magyar közigazgatásban is egyre nagyobb teret nyer a digitális transzformáció, ami az ügyintézési folyamatok teljes újragondolása mellett szükségszerűen a biztonságos elektronikus azonosítási megoldások fejlesztését is szükségessé teszi.[6] Tehát a digitális átalakulás nemcsak a magánszféra világát formálta át, hanem a munkavégzést is. Az Eurostat adatai szerint az Európai Unióban a rendszeresen vagy alkalmanként távmunkában dolgozók aránya még 2019-ben 14,4% volt,

[3] András Nemeslaki – László Duma – Tamás Szántai (2019): A digitális transzformáció szervezeti kihívásai, *Vezetéstudomány* 50, sz. 7–8 (é. n.): 77–88.
[4] Pap Zoltán, „A mobilalkalmazások biztonsági kockázatai", *Biztonságtudományi Szemle* 2, sz. 4 (2020): 65–78.
[5] O.E.C.D., „Digital Government Index: 2022 Results", *OECD Public Governance Policy Papers*, sz. 11 (2022).
[6] Budai Balázs Benjámin, *Az e-közigazgatás elmélete* (Budapest: Akadémiai Kiadó, 2018).

ami 2021-re a COVID-19 okozta pandémiás válság a legszigorúbb lezárási fázis után, közel 10 százalékponttal emelkedett. Ha csak a rendszeresen távmunkában dolgozókat nézzük, ez az arány 2019-ben 5,5%-ról 2021-ben 13,5%-ra nőtt.[7] A COVID-19 nem csak a távmunka és home office lehetőség fokozott elterjedését eredményezte, hanem új igényként merült fel mind állami, mind nemzetközi szinten a személyazonosság és különböző jogosultságok (például egészségügyi státusz) gyors és megbízható ellenőrzése.

Korábbi publikációmban már felvetettem, hogy középtávon egy megfelelően biztonságos és felhasználóbarát mobilalkalmazás valószínűleg fokozatosan átveheti vagy kiegészítheti a hagyományos személyazonosító okmányok szerepét, hasonlóan ahhoz a folyamathoz, amely a bankkártyák esetében már megfigyelhető. Ez a prognózis még a Digitális Állampolgárság Program (DÁP) és a kapcsolódó jogszabályi keretrendszer kidolgozása előtt született, de az azóta megfigyelhető fejlődési irányok visszaigazolják ezt a feltételezést. Kiss Attila elemzése szerint a fizikai igazolványok digitális megfelelői számos előnyt kínálnak, de egyben új típusú kockázatokat is hordoznak, amelyek kezelése multidiszciplináris megközelítést igényel.[8] A témakör szempontjából mindenképpen fontos rámutatni a digitális identitás és a digitális állampolgárság kérdéskörére. Krasznay Csaba és Simon Béla kutatásai alapján a digitális identitások kezelése és védelme stratégiai jelentőségű kérdéssé vált, amely alapvetően meghatározza egy ország kiberbiztonságának és digitális szuverenitásának szintjét.[9] A digitális állampolgárság koncepciója is egyre fontosabbá válik a modern városi környezetben, ahol a kormányok és helyi önkormányzatok új digitális megoldásokat vezetnek be az azonosítás-ellenőrzésre és az állampolgári részvétel ösztönzésére. Ez magában foglalja a szolgáltatásnyújtás innovatív digitális módjait, az engedélyek online kérelmezésétől a szociális juttatások igényléséig és az elektronikus adóbevallásig.[10] Az okos városokban az okos eszközökön keresztüli személyi hitelesítés elengedhetetlen lesz a közle-

[7] Eurostat (2021): Remote work in Europe before and after the pandemic. https://www.europeandatajournalism.eu/cp_data_news/remote-work-in-europe-before-and-after-the-pandemic/ (Letöltve: 2025. április 15.)
[8] Kiss Attila, „Elektronikus személyazonosítás és digitális identitás", *Infokommunikáció és Jog* 73 (2019): 33–38.
[9] Simon Csaba Krasznay – Béla, „A digitális identitás problémái", *Nemzet és Biztonság* 13, sz. 3 (2020): 105–17.
[10] European Commission, „Digital Compass: The European Way for the Digital Decade", 2021.

kedéstől az egészségügyi szolgáltatásokig terjedő városi szolgáltatásokhoz való hozzáféréshez. A digitális identitáskezelő rendszerek egyaránt jelentenek kényelmi előnyöket és biztonsági kihívásokat, különösen, amikor a mindennapi városi élethez nélkülözhetetlen szolgáltatások igénybevételét szabályozzák.[11] Németh Zoltán kutatásai alapján az okos városok fejlesztése során kiemelt figyelmet kell fordítani a kiberbiztonságra, mivel a városi infrastruktúra digitalizálása új sebezhetőségeket teremthet, amelyek kihasználása súlyos következményekkel járhat a lakosság biztonságára nézve.[12] Ezen kockázatok megjelenésével állami és nem állami szereplők is számolhatnak, amely kihasználhatnak, akár anyagi előny kovácsolása, vagy az adott társadalom befolyásolása – akár félelemkeltés által – érdekében, így a különböző kibertéri műveletek célpontjai lehetnek ezen infrastruktúrák. Jelen felvetés is alátámasztja kutatási témám aktualitását, továbbá hadtudományi relevanciáját.

A kibertérben elkövetett bűncselekmények, az innovatív csalási formák, a titkosított kommunikációs csatornák terjedése, valamint a dezinformációs kampányok komoly kihívás elé állítják a hagyományos állami struktúrákat. Ugyanakkor ezek a változások lehetőségeket is teremtenek az állami feladatok (közigazgatás, bűnüldözés, egészségügy, gazdaságfejlesztés) hatékonyabb ellátására.[13] Szádeczky Tamás kutatásai alapján kijelenthetjük, hogy a kiberbűnözés és az információs rendszerek elleni támadások nemcsak az egyént, hanem a kritikus infrastruktúrák biztonságát és a nemzetgazdaság stabilitását is veszélyeztethetik, ami szükségessé teszi a jogszabályi környezet és a védelmi mechanizmusok folyamatos fejlesztését.[14] A hazai kiberképességek fejlesztése terén kiemelt figyelmet érdemel álláspontom szerint nem csupán a hagyományos közigazgatási szervek, hanem rendvédelmi, beleértve a nemzetbiztonsági szolgálatok és a honvédségi képességeinek evolúciója, lehetősége e téren. Témaválasztásom oka, a fentiekben kifejtettek szerint az, hogy az okos eszközök fejlődése, annak irányai nem csupán a hétköznap életünkre van hatással, hanem az államigazgatásra, az állam és a polgári lakosság viszonyára, továbbá az egyes fegyveres szervek munkavégzésére, tevékenységére is. Ezek vizsgálata, kutatása fontos, hiszen az új típusú technológiák

[11] Smart Cities World, „Global Smart Cities Market to Reach $2.5 Trillion by 2026", *Market Analysis Report*, 2023.
[12] Németh Zoltán, „Az okos városok biztonsági kihívásai", *Belügyi Szemle* 68, sz. 2 (2020): 89–106.
[13] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023* (The Hague, European Union Agency for Law Enforcement Cooperation, 2023).
[14] Szádeczky Tamás, „Információbiztonsági szabályozások és az EU" (Budapest, NKE, 2020).

kapcsán esetlegesen megjelenő kockázatok előzetes felismerése stratégiai jelentőségű lehet, figyelemmel arra, hogy ilyen esetekben célravezetőbb a proaktív szemlélet, ellenben a reakcióssal.

1.2 A téma relevanciája a hadtudományban

Egy átlagos okos eszköz-használó esetében már annak tudatosulása is előrelépésnek tekinthető, ha megértik, hogy egy alkalmazás telepítése és használata előtt mérlegelniük kell, mennyi és milyen minőségű információval rendelkeznek az adott szoftverről, milyen kockázatokkal járhat a telepítése, ezáltal csökkentve a váratlan és kellemetlen következmények esélyét. Nem is említve magát az okos eszközt, annak hardveres felépítését, és az azzal kapcsolatos tudás meglétét, mivel egyes eszközök (Huawei) kapcsán felmerült már annak a lehetősége, hogy hardveres szinten van benne olyan kiskapu építve, amely lehetővé teszi azt, hogy arra fel nem jogosított személyek információkat kapjanak az eszközről és annak használójáról.[15] Ez egyfajta belső kockázatelemzésnek is tekinthető. Figyelembe kell venni, hogy a kockázat értékelése kontextus függő. Különböző szervezetek vagy személyek számára eltérő jelentéssel és fontossággal bír, így az úgynevezett nem átlagos felhasználóknak (például állami döntéshozók, nemzetbiztonsági védelem alá eső személyek, és intézmények dolgozói[16]) még nagyobb körültekintéssel kell eljárniuk az okos eszközök beszerzésekor és az alkalmazások telepítésekor, mivel egy magas rangú személy esetében. A kártékony szoftver telepítése nemcsak személyes kockázatot, hanem nemzeti biztonsági és akár nemzetbiztonsági fenyegetést is jelenthet. A nemzeti biztonság fogalmának mélyebb elemzése során látható, hogy az túlmutat a szűk értelemben vett nemzetbiztonságon. Laufer Balázs megfogalmazása szerint a nemzetbiztonság egy sokrétű társadalmi teljesítmény, amelynek biztosításában számos szerv és intézmény játszik szerepet.[17] Ez a tágabb fogalmi keret magában foglalja mindazon tényezőket, amelyek egy adott állam számára kockázatként, kihívásként vagy fenyegetésként jelenhetnek meg. Az értekezésem hadtudományi relevanciájának mélyebb megértéséhez szükséges továbbá a kockázat fogalmának tisztázása és kontextualizálása.

---

[15] Karsten Friis és Olav Lysne, „Huawei, 5G and Security: Technological Limitations and Political Responses", *Development and Change* 52, sz. 5 (2021): 1174–95, https://doi.org/10.1111/dech.12680.
[16] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról, 1. § (a-e) pont.
2009/2015. (XII. 29.) Korm. határozat a nemzetbiztonsági védelem alá eső szervek és létesítmények köréről, 1. melléklet 1.8-1.16. pont.
[17] Laufer Balázs, „A migráció rendészeti és nemzetbiztonsági kihívásai. PhD-értekezés" (Budapest, 2013).

A hazai, illetve nemzetközi szakmai és tudományos szakirodalomban a kockázat fogalmának számos megközelítése létezik. Resperger megfogalmazása szerint a kockázat "*azon helyzetek és körülmények összessége, amelyek az általánosan értelmezett biztonság egyes összetevőit olyan mértékben befolyásolják a lehetséges veszélyek szintjén, hogy nemzeti érdekek sérülhetnek, ezáltal veszteségeket okozva.*"[18] Ez a definíció a kockázatot biztonsági politikai, hadtudományi és nemzetbiztonsági szempontból értelmezi, egy hármas kategorizálási rendszerben helyezve el, ahol a kockázat a kihívás és a fenyegetés között helyezkedik el a potenciális veszélyesség skáláján. Bár Resperger meghatározása elsősorban hatásalapú megközelítést alkalmaz, véleményem szerint a kockázat fogalmának teljesebb megragadásához a hatás nagysága mellett figyelembe kell venni a bekövetkezés valószínűségét és az esetleges megakadályozás, illetve védekezés nehézségét is. Haig Zsolt és Várhegyi István kiberbiztonsági kutatásai is megerősítik, hogy a technológiai fejlődéssel összefüggő kockázatok értékelése során nem elegendő csupán a lehetséges következményeket vizsgálni, hanem a fenyegetések, sebezhetőségek és valószínűségek komplex összefüggésrendszerét kell feltárni.[19] Egy másik megfogalmazás szerint a kockázat "a kockázati esemény hatásának a szervezetre gyakorolt fontossága, ha az bekövetkezik", míg a kockázati esemény "olyan esemény, amely várhatóan hatással lesz a szervezetre (a vezetők által kitűzött célok elérésére vagy a követelmények teljesítésére), de még nem következett be."[20] Az ISO 31000 szabvány alapján a kockázat a szervezeti célokra gyakorolt bizonytalanság hatásaként értelmezhető. E meghatározások alapján megállapítható, hogy a kockázat egy bizonytalansági tényezőt jelöl, amely bekövetkezése esetén negatív hatással van valamilyen védendő értékre. Kutatásom szempontjából kiemelendő a Magyarország kiberbiztonságáról szóló törvény, amely értelmező rendelkezésében a tételes felsorolásnál nevesíti a kockázat fogalmát, ami *„a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának, bekövetkezési valószínűségének és az ez által okozott kár nagyságának a függvénye.”*[21] A fentiek alapján az értekezésem során az egyes kockázatok elemzése során figyelembe vettem az esetlegesen bekövetkezendő

[18] Resperger István, *A válságkezelés és a hibrid hadviselés* (Budapest: Dialóg Campus Kiadó, 2018).
[19] Várhegyi Zsolt Haig – István, „Információs műveletek és hadviselés”, in *Hadtudományi Lexikon: Új kötet* (Budapest: Ludovika Egyetemi Kiadó, 2018), 502–7.
[20] Horváth Péter – Németh Edit*: Integrált kockázatkezelési rendszer alapjai*, Dialóg Campus Kiadó, Budapest, 2018. 9.o.
[21] 2024. évi LXIX törvény Magyarország kiberbiztonságáról 4 § 52. ponr

negatív esemény által a nemzeti biztonságban okozott kár nagyságát, a bekövetkezés várható valószínűségét, továbbá a védekezés, elhárítás szempontjait is.

A téma hadtudományi relevanciáját erősítik az orosz-ukrán háború tapasztalatai is, amelyek rávilágítottak az információs műveletek jelentőségére a 21. századi hadviselésben. Az okos eszközök és alkalmazásaik – különösen a személyazonosításra vagy hitelesítésre szolgáló technológiák – fejlődése elkerülhetetlenül nemzetbiztonsági kockázatokat és kihívásokat is magában hordoz.[22] Krasznay Csaba elemzései szerint a kibertér a modern konfliktusok ötödik dimenziójává vált, amelyben az információs hadviselés eszköztára folyamatosan bővül és diverzifikálódik.[23] Napjaink egyik kulcsfontosságú kérdése a hitelesség és megbízhatóság, amely nemcsak társadalmi szempontból alapvető fontosságú, hanem hadtudományi relevanciával is bír. A 2014-es krími annexió óta Oroszország fokozatosan beépítette az információs hadviselést stratégiai eszköztárába, azzal a nyilvánvaló céllal, hogy megossza az ellenséges társadalmakat és aláássa a nyugati demokratikus intézményekbe vetett bizalmat.[24] A nyugati országok ellen irányuló dezinformációs kampányok központi elemei között szerepel a hamis narratívák terjesztése és a közösségi média manipulálása, gyakran mesterségesen létrehozott, hamis profilok felhasználásával. Az orosz típusú dezinformációs kampányok olyan összetett kihívást jelentenek, amely a demokratikus társadalmak alapvető működését is veszélyeztetheti. A hatékony védelem kialakításához elengedhetetlen, hogy a komplex biztonsági kihívásra komplex biztonsági megoldások szülessenek, amelyek egyaránt tartalmaznak technológiai innovációt, jogi szabályozást és a társadalmi ellenálló képesség erősítését célzó intézkedéseket. A hadtudomány területén a személyazonosításra és személyi hitelesítésre alkalmas alkalmazások által a jövőben esetlegesen létrehozandó validált, azaz hiteles profilok használata a közösségi médiában kulcsfontosságúvá válhat a kiberbiztonság és a stratégiai kommunikáció szempontjából is, különösen a koordinált álprofilokkal szemben folytatott védekezésben.[25] Az okos eszközök fejlődési irányai, egyes alkalmazások evolúciója kapcsán a fentiek

[22] In *NATO Strategic Communications Centre of Excellence (2022): Digital Resilience in the Age of Disinformation* (Riga, é. n.).
[23] Krasznay Csaba, *A kiberbiztonság stratégiai vetületei* (Budapest: Dialóg Campus Kiadó, 2020).
[24] Bettina Renz, „Russia and »hybrid warfare«", *Contemporary Politics* 22, sz. 3 (2016): 283–300.
[25] Erik Uszkiewicz, *Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and Its Member States* (European Parliament, 2019).

miatt a személyazonosításra és hitelesítésre alkalmas technológiák, köztük az egyes biometrikus megoldások vizsgálatát tűztem ki célul.

Bányász Péter kutatásai rámutatnak, hogy a közösségi média platformok befolyásolási potenciállal rendelkeznek, amit állami és nem állami szereplők egyaránt kihasználhatnak stratégiai céljaik elérése érdekében.[26] Ezért a közösségi médiában esetlegesen alkalmazandó hiteles profilok bevezetésének lehetősége komoly szakmai és tudományos relevanciával bír, amire jelen értekezés során bővebben is kitérek.

Megállapítható, hogy az okos eszközök és az azok applikációinak fejlődési trendjei közvetlen hatást gyakorolhatnak a nemzetbiztonsági stratégiákra és a modern hadviselés koncepcióira. különböző intelligens eszközök, szenzorok és mesterséges intelligencia (MI vagy Artificial Intelligence - AI) által vezérelt rendszerek integrációja átalakíthatja akár biztonság fogalmát, a rendőrség, nemzetbiztonság, illetve a honvédség információgyűjtés módszereit és a különböző védelmi és védekezési stratégiákat. Az International Data Corporation korábbi előrejelzése szerint 2025-re a hálózatokhoz csatlakoztatott Internet of Things (IoT) eszközök száma eléri a 41,6 milliárdot, ami exponenciálisan növeli a kiberbűnözés lehetőségeinek tárházát is.[27] Kovács László felhívja a figyelmet arra, hogy az összekapcsolt eszközök számának növekedésével párhuzamosan növekszik a támadási felület is, ami új típusú kibervédelmi megközelítéseket és technológiákat tesz szükségessé.[28]

Jelen kutatás során nem hagyható figyelmen kívül az okos eszközök fejlődése szempontjából a mesterséges intelligencia, amely nem csupán kezd a mindennapjaink szerves részéve válni, hiszen a Spirtle felmérése úgy kalkulált, hogy 2025-re a háztartások 75%-a fog AI-alapú okos eszközöket használni. A hangasszisztensek a fogyasztói elektronikai eszközök hangutasításainak 90%-át fogják kezelni[29] , hanem hadtudományi szempontból kiemelendő. A mesterséges intelligencia katonai alkalmazásának pi-

[26] Bányász Péter, „A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében", *Szakmai Szemle* 16, sz. 1 (2018): 59–77.
[27] „Worldwide Global DataSphere IoT Device and Data Forecast", 2022.
[28] Kovács László, *A kibertér védelme* (Budapest: Dialóg Campus Kiadó, 2018).
[29] Spritle (2025): 100 Game-Changing AI Statistics for 2025: Trends Shaping Our Future. Elérhető: https://www.spritle.com/blog/100-game-changing-ai-statistics-for-2025-trends-shaping-our-future/ (Letöltve: 2025. április 15.)

aca is növekedést mutat. Market.us adatai szerint a globális hadiipari mesterséges intelligencia piac bevétele 2022-ben 7,9 milliárd USD volt, amely 2023-ra 8,9 milliárd USD-re növekedett, és a Market.us adatai szerint ez a növekedési ütem folyamatosnak tekinthető.[30]

A mesterséges intelligencia az okos eszközök fejlődésének egyik legmeghatározóbb hajtóereje. A katonai alkalmazásban a fejlett szenzorokkal és elemzési kapacitással rendelkező, MI-képes ISTAR (Intelligence, Surveillance, Target Acquisition, and Reconnaissance - Hírszerzés, megfigyelés, célazonosítás és felderítés) rendszerek javítják a célazonosítást és a helyzetismeretet. Az autonóm pilóta nélküli légi rendszerek (Unmanned Aircraft System - UAS) és földi járművek magas kockázatú küldetéseket tudnak végrehajtani a kezelő személyzet veszélyeztetése nélkül.[31] A civil szférában az MI-vezérelt okos asszisztensek egyre intuitívabbá és reaktívabbá válnak. Az olyan virtuális asszisztensek, mint az Amazon Alexa, a Google Assistant és az Apple HomeKit képesek megtanulni a felhasználói szokásokat, a természetes nyelvfeldolgozás fejlődése zökkenő mentesebb ember-gép interakciókat tesz lehetővé.[32] Azonban az egyre növekvő felhasználás és a technológiai fejlődés mellett nem szabad megfeledkezni az esetleges kockázati faktorokról és azok változatosságáról, növekedéséről sem. Nyikes Zoltán kutatásai alapján az okos otthonok és az intelligens épületvezérlő rendszerek biztonsági kockázatai folyamatosan növekednek.[33]

A személyazonosításra és személyi hitelesítésre alkalmas technológiák egy fontos szegmensét képezik az okos eszközök fejlődésének, illetve kiemelt vizsgálat tárgyát képezték az értekezésem elkészítése során folytatott kutatásnak. A biometrikus azonosítás, a többfaktoros hitelesítés és a digitális identitáskezelő rendszerek alapjaiban formálják át mind a civil, mind a katonai biztonsági protokollokat. 2025-ben a digitális identitás várhatóan a biztonsági rendszerek sarokkövévé válik, különösen a zero-trust keretrendszereken belül, ahol a folyamatos hitelesítés és a felhasználói viselkedés

[30] Market.us (2025): Artificial Intelligence in Military Statistics and Facts (2025). Elérhető: https://scoop.market.us/artificial-intelligence-in-military-statistics/ (Letöltve: 2025. április 15.)
[31] Michael C. Horowitz, „Artificial Intelligence, International Competition, and the Balance of Power", *Texas National Security Review* 1, sz. 3 (2018): 36–57.
[32] PwC, „Global Artificial Intelligence Study: Exploiting the AI Revolution", 2023.
[33] Nyikes Zoltán, „Az okos otthonok IT biztonsági kihívásai", *Hadmérnök* 14, sz. 1 (2019): 212–23.

elemzése lehetővé teszi az anomális minták és a potenciális behatolások korai felismerését.[34] A zero-trust keretrendszer lényegében azt jelenti, hogy a „soha ne bízz, mindig ellenőrizz", ez jelenthet folyamatos hitelesítést, feltételes hozzáférést, dinamikus bizalomértékelést és a legkisebb jogosultság elvét alkalmazva a biztonság növelése érdekében.[35] Munk Sándor kutatásai alapján megállapítható, hogy az információs műveletek sikeres végrehajtásának egyik kulcseleme a megfelelő információs infrastruktúra és a megbízható azonosítási rendszerek kialakítása, amelyek biztosítják az információ integritását és hitelességét.[36]

A biometrikus azonosítási technikák is fejlődnek, egyre precízebbek és a korábban felmerülő azonosítási akadályokat kezdik leküzdeni. Például az arcfelismerő rendszerek fejlődése lehetővé teszi az arckifejezések finom változásainak észlelését, ami értékes információkat szolgáltathat a biztonság, az érzelem felismerés és a felhasználói élmény területén. A modern algoritmusok már maszkot vagy egyéb, a tiszta láthatóságot akadályozó felszerelést viselő személyek azonosítására is képesek, ami növeli alkalmazhatóságukat, ami hatalmas segítséget nyújthat a rendvédelem számára is. Az ultrahang-alapú ujjlenyomat-szkennelés pedig forradalmasítja az érintés nélküli hitelesítést, gyorsabbá és higiénikusabbá téve a rendszereket,[37] miközben a bőr mélyebb rétegeinek olvasásával is javítja a pontosságot, csökkentve a téves azonosítások arányát.[38] Jelen technológia a biometrikus beléptetést alkalmazó állami és a magánintézmények védelméhez hozzájárulhat. Azonban Orbók Ákos felhívja a figyelmet arra kutatása során, hogy a biometrikus azonosítási technológiák fejlődésével párhuzamosan fejlődnek az azok kijátszására irányuló technikák is, ami folyamatos innovációt tesz szükségessé az azonosítási rendszerek biztonságának fenntartásához.[39] Így jelen témakör kutatása mindenképpen relevanciával bír.

---

[34] „Zero Trust Architecture", 2020.
[35] Muhammad Liman Gambo és Ahmad Almulhem, „Zero Trust Architecture: A Systematic Literature Review", elérés 2025. május 24., https://www.authorea.com/users/887944/articles/1266894-zero-trust-architecture-a-systematic-literature-review.
[36] Munk Sándor, „Információs műveletek – információs tevékenységek", *Hadtudomány* 28, sz. 3–4 (2018): 118–29.
[37] Gambo és Almulhem, „Zero Trust Architecture".
[38] Joseph N. Pato – Lynette I. Millett, *Biometric Recognition: Challenges and Opportunities* (National Academies Press, 2010).
[39] Orbók Ákos, „Biometrikus rendszerek hitelesítési módszerei", *Hadmérnök* 13, sz. 4 (2018): 71–82.

Nemzeti biztonsági kontextusban, és katonai szempontból is kritikus éggel bírnak az adatvédelmi szempontok, mivel adott esetben egy információszivárgás veszélyeztetheti a műveleti biztonságot, felfedheti a személyi állomány tartózkodási helyét, vagy érzékeny adatokat szolgáltathat az ellenséges erőknek. Érdekes példaként említhető, mikor a Strava nevű fitnesz alkalmazás katonai létesítmények helyét leplezte le. 2018-ban a Strava által közzétett globális aktivitási térkép számos katonai létesítmény azonosítását olyan országokban, mint Szíria és Afganisztán, mivel a katonai személyzet rendszeresen használta az alkalmazást futás vagy kerékpározás közben.[40] A katonai IoT-eszközök által gyűjtött adatok, illetve nemzeti biztonság kapcsán kiemelendő intézmények dolgozóinak adatainak magas szintű védelme nemzetbiztonsági szempontból elengedhetetlen.[41] A személyazonosításra használt rendszerekben különösen értékes lehet a blockchain technológia, amely decentralizált és biztonságos természetéről ismert, várhatóan kulcsszerepet játszik majd az adatvédelem jövőjében.[42] Rajnai Zoltán és kutatótársai elemzései rámutatnak, hogy a blockchain technológia alkalmazása nemcsak a pénzügyi szektorban, hanem a közigazgatásban és a védelmi szektorban is potenciállal rendelkezik, különösen az adatok integritásának és hitelességének biztosítása szempontjából.[43]

Ahogy a fentiekben már többször is említettem a technológia fejlődésével a kockázatok, illetve az egyes támadók által alkalmazott módszerek is evolválódnak, így a kiberfenyegetések evolúciója folyamatosan új kihívások elé állítja a védelmi rendszereket. 2025-ben az egyik elsődleges kihívást várhatóan a mobil malware-ek kifinomult változatai jelentik majd, mivel a kibertér rosszindulatú szereplői a mesterséges intelligenciát és gépi tanulást felhasználva már olyan kártékony szoftvereket fejlesztenek, amelyek képesek alkalmazkodni a különböző biztonsági környezetekhez, megkerülve a hagyományos védelmi mechanizmusokat.[44] A phishing és social engineering taktikák

[40] BBC (2018): Fitness app Strava lights up staff at military bases. BBC News, 2018. január 29. Elérhető: https://www.bbc.com/news/technology-42853072 (Letöltve: 2025. április 15.)
[41] Bányász, „A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében".
[42] „Zibin Zheng – Shaoan Xie – Hong-Ning Dai – Xiangping Chen – Huaimin Wang (2018): Blockchain challenges and opportunities: A survey", *International Journal of Web and Grid Services* 14, sz. 4 (é. n.): 352–75.
[43] Ozsváth Zoltán Rajnai – Beatrix Fregan – Judit, A kiberbiztonság technológiai és módszertani támogatása – A blockchain, mint biztonságtechnológia, *Biztonságtudományi Szemle* 1, sz. 3 (2018): 61–70.
[44] E.N.I.S.A., *ENISA Threat Landscape 2023* (European Union Agency for Cybersecurity, 2023).

is egyre kifinomultabbá és személyre szabottabbá válnak. A támadók már MI-eszközöket is bevetnek a kommunikációs stílusok szimulálására, utánzására. Ezek a támadások gyakran a közösségi médiában és más online platformokon elérhető személyes adatokat használják fel, hogy testreszabott üzeneteket készítsenek a potenciális áldozatok számára.[45] Továbbá ahogyan Bányász Péter is rámutat, a közösségi média platformok által gyűjtött adatok felhasználása nemcsak kereskedelmi célokat szolgálhat, hanem lehetővé teszik a politikai befolyásolást és a célzott dezinformációs kampányok végrehajtását is.[46] A fentiekre tekintettel még inkább felértékelődik a hitelesség, illetve a hiteles felhasználói fiókok, így a biometrikus azonosítás, illetve a személyazonosításra, illetve hitelesítésre alkalmas technológia várhatóan kulcsfontosságú szerepet tölt majd be. A digitális identitási és állampolgársági rendszerek komoly relevanciával bírnak, hadtudományi, és nemzeti biztonsági szempontból nézve is, hiszen a megbízható személyazonosság-ellenőrző rendszerek kritikus fontosságúak a határbiztonság, a terrorizmus elleni műveletek és a kritikus infrastruktúra védelme szempontjából. Ugyanakkor ezek a rendszerek maguk is potenciális célpontokká válnak az ellenérdekelt szereplők számára, akik e rendszerek kompromittálásával komoly károkat okozhatnak.[47]

Összességében elmondható, hogy az okos eszközök evolúciója szükségessé teszi az adatvédelmi és biztonsági megoldások folyamatos fejlesztését, valamint az etikai és társadalmi kérdések alapos vizsgálatát. A fentiek alapján az okos eszközök és a személyazonosításra, hitelesítésre alkalmas technológiák fejlődése megállíthatatlan trend, ami nem csupán hadtudományi relevanciával bír, hanem katonai, nemzetbiztonsági és rendészeti szempontból történő vizsgálatuk szinte elengedhetetlen. A nemzetbiztonsági szervezeteknek, katonai intézményeknek és politikai döntéshozóknak proaktívan kell alkalmazkodniuk ezekhez a változásokhoz, kihasználva a bennük rejlő lehetőségeket, miközben felkészülnek az általuk hozott kihívásokra.

1.3 Szakirodalmi áttekintés

A doktori értekezésem elkészítése során a releváns szakirodalom kiválasztása kettős volt, egyrészt az okos eszközök és a személyazonosítás, valamint személyi hitelesítés

[45] Vala Ali Rohani, „Phishing Detection: A Case Analysis on Classifiers with Rules Using Machine Learning", *Journal of Theoretical and Applied Information Technology* 97, sz. 8 (2019): 2235–49.
[46] Bányász Péter, „A közösségi média, mint a nyílt forrású információszerzés forrása", *Nemzetbiztonsági Szemle* 7, sz. 2 (2019): 5–24.
[47] Kovács László, *A kibertér védelme* (Budapest: Dialóg Campus Kiadó, 2018

területén végzett tudományos vizsgálatokat kerestem, másrészt a hadtudományi, rendvédelmi és nemzetbiztonsági kontextus megteremtéséhez a tudományos szakirodalom áttekintése mellett szakértői interjúkat is készítettem. A választott tanulmányok egyaránt lefedik a technológiai, társadalmi, jogi és katonai aspektusokat, így biztosítottam a kutatásom multidiszciplináris megközelítését.

Az információs társadalom vizsgálatánál főként Castells munkásságára hagyatkoztam, ezt egészíti ki Nemeslaki András és társain által végzett tanulmányok, ami az infokommunikációs eszközök és az állami szerepvállalás szükségességét kutatják, illetve megadják a témakör hazai relevanciáját is.

Az okos eszközök és applikációinak vizsgálata során Pap Zoltán munkásságát vettem figyelembe a mobilbanki alkalmazások biztonsági és pszichológiai kérdései kapcsán. Továbbá az alkalmazások és az okos mobil eszközök kapcsán főként Bányász Péter munkásságaira támaszkodtam. A digitális állampolgárság kapcsán a vonatkozó jogszabályok, egyes országok alkalmazásainak leírásán túlmenően Budai Balázs Benjamin munkásságát vettem figyelembe. A technológiai oldalról Haig Zsolt, Nyikes Zoltán és Orbók Ákos munkái részletezik az IoT-eszközök, okos otthonok és biometrikus rendszerek biztonsági kihívásait. Továbbá az információs műveletek kapcsán Haig Zsolt által feltártak alapján dolgoztam.

A (kiber)biztonsági és nemzetbiztonsági szempontokat Krasznay Csaba, Laufer Balázs és Resperger István kutatásai alapozták meg. Munkáik rávilágítanak a digitális identitás és a nemzeti szuverenitás közötti összefüggésekre, valamint a kockázatok multidimenzionális természetére, amelyet a technológiai fejlődés folyamatosan újraértelmez. Továbbá mind biztonsági, mind technológiai szempontból Rajnai Zoltán blockchain technológiák kapcsán végzett kutatását vettem figyelembe.

A mesterséges intelligencia (AI) katonai és civil alkalmazásaira vonatkozó ismereteket a Market.us, IDC és Spirtle által közzétett piaci előrejelzések egészítik ki, amelyek a technológiai jövőkép meghatározásában játszottak szerepet. Az MI hadászati lehetőségeit és kockázatait Munk Sándor és Bányász Péter elemzései tették egyértelművé, különösen az információs műveletek és a közösségi média manipulációjának kontextusában.

A Strava-eset példája és a Rajnai Zoltán által elemzett blockchain technológiák jól demonstrálják, hogy a technikai innovációk miként válhatnak nemzetbiztonsági kockázattá – vagy éppen megoldássá – az adatvédelem és a műveleti biztonság szempontjából.

A felhasznált szakirodalom nemcsak az értekezés témájának elméleti megalapozását szolgálja, hanem azt is lehetővé teszi, hogy a technológiai trendek, társadalmi attitűdök és biztonsági kockázatok közötti kapcsolatokat komplex módon, a hadtudományi és nemzetbiztonsági keretek között lehessen vizsgálni. Ezáltal a kutatásom hozzájárul a digitális identitás, az adatbiztonság és az okos eszközök katonai alkalmazhatóságának mélyebb megértéséhez, amely a fentiekben felsorolt kutatók munkájához illeszkedik, illetve új, multidiszciplináris módon közelíti meg a témát.

1.4 Kutatási célok

A kutatásom során öt fő célt tűztem ki, amelyek együttesen átfogó képet adnak az okos eszközök fejlődési irányairól, különös tekintettel a személyazonosításra és személyi hitelesítésre, alkalmas technológiákra, azok alkalmazására, különös tekintettel a nemzeti biztonságra:

KC1. Az okos eszközök és alkalmazásaik elmúlt 10 évben történt fejlődési irányainak vizsgálata.
Ennek vizsgálata azért is volt kiemelt, mivel a dolgozatot kontextusba helyezi, a megfelelő értelmezési keret megteremtése érdekében, továbbá a kutatás elején, magát a kutatási irányokat is befolyásolta, hiszen ezen eszközök fejlődése a lehetséges jövőbeli trendeket az indikálhatja. Ebből következőleg indul ki a második kutatási cél is.

KC2. A személyazonosításra és személyi hitelesítésre alkalmas technológia fejlődési irányainak, valamint az ezekhez kapcsolódó társadalmi elfogadottság vizsgálata.
Értekezésem során külön figyelmet szenteltem az okos eszközök e fejlődési irányára, figyelemmel annak aktualitására, illetve ezen technológia jelentette lehetőségekre, illetve az esetleges rejtett kockázatokra. A személyi azonosításra és személyi hitelesítésre alkalmas technológiák esetében nem lehet elmenni a biometrikus adatok mellett, illetve azok felhasználásáról az említett technológiák kapcsán. Azonban akármennyi

lehetőséget (vagy kockázatot) rejt magában egy adott technológia, ha az nem kerül széles körben használatra annak társadalmi elutasítottsága miatt, akkor annak alkalmazása irreleváns lehet.[48]

KC3. A személyazonosításra és személyi hitelesítésre alkalmas technológia jelenlegi és jövőbeni felhasználási területeinek kutatása.
A fentiekhez kapcsolódóan a személyazonosításra és személyi hitelesítésre alkalmas technológiák vizsgálata során szükséges megállapítani a jelenlegi felhasználási területeket az esetleges lehetőségek és kockázatok feltárása érdekében. Továbbá a jövőbeni felhasználási lehetőségek a fejlődési irányokból következnek, azonban külön szegmenst érdemelt a témakör a lehetséges jövőbeni kockáztok és alkalmazási lehetőségek és felhasználási területek miatt, legyen szó polgári vagy katonai szektorról.

KC4. A nevezett technológia jelenlegi és jövőbeni potenciális kockázatainak feltárása, típusaik kategorizálása, az ellenük való védekezési stratégiák feltárása.
Az értekezés elkészítése során fontosnak tartottam a vizsgált technológia feltérképezéséhez kapcsolódóan a feltárt kockázatok besorolását, kategorizálását, azok jobb megértése és az esetleges elhárítási, illetve védekezési stratégiák felállítása érdekében.

KC5. A hiteles profilok létrehozásának irányai, a közösségi médiában való társadalmi elfogadottságuk vizsgálata.
A kutatásom egyik sarkalatos pontja a közösségi média felületeken létező és a jövőben létrehozható olyan profilok vizsgálata, amely hitelesítve kerültek vagy valamilyen szempont vagy technológia által. Ezen profilok alkalmazásának lehetőségei és kockázatai mellett, a megjelenésük és bevezetésük kapcsán felmerülő társadalmi elfogadás, vagy éppen ellenállás szintén kardinális kérdéskör. Hiszen bármennyi lehetőség lehet akár a különböző dezinformációs kampányok, vagy csalások elleni védekezésben az ilyen hiteles profiloknak, ha azokat nem használjak széles körben az alacsony elfogadottság miatt.

[48] Wenyi Zhang, Hengtian Zhang, és Zhouyang Deng, „Public Attitude and Media Governance of Biometric Information Dissemination in the Era of Digital Intelligence", *Scientific Reports* 15, sz. 1 (2025. január 18.): 2419, https://doi.org/10.1038/s41598-025-86603-w.

1.5 Kutatási kérdések

A kutatási célok elérése érdekében a következő kutatási kérdéseket fogalmaztam meg, a hipotézisek felállítása, illetve az értekezés elkészítése közben ezeket vettem kiemelten figyelembe:

KK1. Az okos eszközök fejlesztésének szempontjából prioritást élvező fejlesztési iránynak tekinthető-e a személyazonosításra és személyi hitelesítésre alkalmas technológiák fejlesztése?

Az okos eszközök és applikációinak vizsgálata során több aktuális tendencia vizsgálható lett volna. A választott résztéma hadtudományi relevanciájának feltárása érdekében szükséges volt annak megismerése, hogy a személyi azonosításra, illetve hitelesítésre alkalmas fejlődési irány prioritást élve-e akár csak az evolúció általános szempontjából, vagy éppen az esetleges hadtudományi kötődés miatt.

KK2. Melyik a társadalmilag elfogadottabb: az állam által vagy a magáncégek által fejlesztett hitelesítésre és azonosításra alkalmas technológia?

A társadalmi elfogadottság terén felmerülő kérdés, hogy az elfogadottságot, vagy esetlegesen az elutasítottságot mennyire befolyásolja az, hogy az adott technológiát állami cég, vagy éppen egy magánvállalat fejlesztette, üzemeli, vagy maga a technológia jobban befolyásolja ezt, mint a fejlesztés háttere.

KK3. Milyen lehetséges alkalmazási területei lehetnek ennek a technológiának, különösen a közszférában?

Értekezésem elkészítése során a személyazonosításra és személyi hitelesítésre alkalmas okos eszköz technológiák kapcsán kérdésként merült fel, hogy ezek alkalmazása az állami szektoron belül hol lehetnek relevánsak, a technológiában rejlő potenciál kiaknázásában érdekelt lehet-e a rendvédelem, vagy éppen a honvédség.

KK4. Lehetnek-e a hitelesített közösségi média fiókokból eredő kockázatok? Hogyan tudják ezt különböző szereplők kihasználni?

Kérdésként merült a már létező, illetve az esetlegesen jövőben létrehozandó hitelesített közösségi média profilok kapcsán, hogy az esetleges lehetőségeken túlmenően milyen kockázatok jelenhetnek meg. Ezen kockázatok túlmutatnak-e a lehetőségeken, illetve az egyes hiteles profilok esetén megjelenő kockázatok az átlagos felhasználó vagy pedig speciális attribútummal rendelkező felhasználók esetén (fegyveres szervek tagjai,

kiemelt állami szereplők) milyen mértékű, az esetleges kockázatok meghaladják-e a várt hasznosságot.

KK5. Mennyire lenne népszerű a társadalomban a hitelesített profilok kötelező alkalmazása?
Ezen kérdéskör szorosan kapcsolódik a fentiekben felsoroltakhoz, leginkább a társadalom relációira való fókusz jelenti. Felmerül annak a lehetősége, hogy a hiteles profilok lehetőségei túlmutatnak a kockázatokon, azonban a várható pozitív eredmények csak kötelező bevezetés esetén lennének számottevőek, azonban ez a társdalom általi elutasítottsághoz vezethet. A kérdéskör boncolása segítséget nyújthat akár a különböző döntéshozók részére az egyes technológiai vagy jogi megoldások kötelező bevezetésének esetleges hatásainak megértéséhez,

1.6 Hipotézisek

A kutatási kérdések alapján hat hipotézist állítottam fel, amelyeket a kutatás során alkalmazott módszertan segítségével fogok megerősíteni vagy cáfolni:

H1. Az okos eszközök és alkalmazásaik fejlődése folyamatos, a fejlődés irányát nehéz meghatározni, azonban szinte biztosra vehető a személyi hitelesítésre alkalmas applikációk egyre dominánsabb jövőbeli szerepe.

Az első kutatási cél (KC1) az okos eszközök és alkalmazásaik elmúlt 10 évben történt fejlődési irányainak vizsgálatára irányul. Ebből a célból következik az első kutatási kérdés (KK1), amelyhez szorosan kapcsolódik a H1 hipotézis. Ez a hipotézis logikusan következik a kutatási kérdésből, mivel feltételezi, hogy bár az általános fejlődési irányok nehezen meghatározhatók, a személyi hitelesítési technológiák mégis kiemelkedő szerepet fognak játszani.

H2. A személyazonosításra, illetve személyi hitelesítésre alkalmas applikációknak több fejlesztési iránya is van, társadalmilag az állami fejlesztési irány a preferáltabb.

A második kutatási cél (KC2) a személyazonosításra és személyi hitelesítésre alkalmas technológia fejlődési irányainak, valamint az ezekhez kapcsolódó társadalmi elfogadottság vizsgálatára összpontosít. Ebből a célból következik a második kutatási kérdés (KK2). Ez a kérdés a társadalmi elfogadottság terén merül fel, vizsgálva, hogy az elfogadottságot vagy esetlegesen az elutasítottságot mennyire befolyásolja az, hogy az adott technológiát állami cég vagy éppen egy magánvállalat fejlesztette, üzemeli, vagy maga a technológia jobban befolyásolja ezt, mint a fejlesztés háttere, ehhez a kérdéshez kapcsolódik a H2 hipotézis. Ez a hipotézis a kutatási kérdésre adott előzetes válaszom. Álláspontom alapján a magánszektor, kifejezetten a Meta-t ért különböző botrányok miatt[49] az állami fejlesztés elfogadottabb lehet, mint a magánvállalati, továbbá korábbi saját metaadatokkal kapcsolatos kutatásomban feltárt kérdőíves felmérés alapján erre a következtetésre jutottam.[50]

H3. A személyazonosításra, illetve személyi hitelesítésre alkalmas applikációkban alapvetően több a lehetőség, mint a kockázat.

A harmadik kutatási célom (KC3) a személyazonosításra és személyi hitelesítésre alkalmas technológia jelenlegi és jövőbeni felhasználási területeinek kutatására irányul. Ebből a célból adódik a harmadik kutatási kérdés (KK3) Ehhez a kutatási kérdéshez két hipotézis is kapcsolódik. A H3 hipotézis az egyik.

H4. A személyazonosításra, illetve személyi hitelesítésre alkalmas applikációk előre vetítik a különböző kibertérben történt bűncselekmények evolúcióját, továbbá új típusú, a hagyományos közegben történő bűncselekményeket tud tovább fejleszteni, megváltoztatni. (Pl.: embercsempészet esetén)

A negyedik kutatási cél (KC4) a nevezett technológia jelenlegi és jövőbeni potenciális kockázatainak feltárására, típusaik kategorizálására, az ellenük való védekezési stratégiák feltárására összpontosít. Ebből következik a negyedik kutatási kérdés (KK4): "Lehetnek-e a hitelesített közösségi média fiókokból eredő kockázatok? Hogyan tudják

[49] Luis Aguiar és mtsai., „Facebook Shadow Profiles" (arXiv, 2022. július 19.), https://doi.org/10.48550/arXiv.2202.04131.
[50] Marco Koller és András Kerti, „Az okoseszközök applikációi által gyűjtött metaadatokkal való visszaélések kockázati szemléletmód általi, felhasználói szintű lehetséges visszaszorítása", *Hadmérnök* 16, sz. 4 (2021): 145–56, https://doi.org/10.32567/hm.2021.4.11.

ezt különböző szereplők kihasználni?" A kapcsolódó H4 hipotézis abból a felismerésből következik, hogy a lehetőségek általában mindig különböző kockázatokat vetítenek előre.

H5. A hiteles profilok alkalmasak lehetnek az internetes bűnözés és dezinformációs kampányok visszaszorítására, továbbá a védelmi szektorban is felhasználható lehet.

Jelen hipotézis kapcsolódik még a KC3-hoz és a KK3-hoz

H6. Bár a közösségi média használat személyi hitelesítéshez való kötése képes lenne csökkenteni az online térben elkövetett rosszindulatú cselekményeket (pl.: online zaklatás, csalás, stb.), kötelezővé tétele nem lenne elfogadott.

Az ötödik kutatási cél (KC5) a hiteles profilok létrehozásának irányai, a közösségi médiában való társadalmi elfogadottságuk vizsgálatára irányul. Ebből a célból következik az ötödik kutatási kérdés (KK5). A kapcsolódó jelen hipotézis a kutatási kérdésből logikusan következik, elismerve a technológia potenciális hasznait, ugyanakkor előrevetítve a társadalmi ellenállást a kötelező bevezetéssel szemben.

1.7 Kutatási módszertan

A kutatási módszertan kidolgozásánál figyelembe vettem, hogy az információbiztonsági kutatások területén nincs egyetlen, általánosan elfogadott módszertani hagyomány. Ahogy Van Niekerk és von Solms rámutatnak: "az információbiztonsági kutatók a nagyon technikai jellegűtől a 'puhább', ember-központú területekig terjedő kutatási tevékenységeket végezhetnek".[51] Ennek megfelelően a kutatás során mind kvantitatív, mind kvalitatív módszereket alkalmazok, biztosítva a komplex kutatási kérdések átfogó vizsgálatát.

A H1 hipotézis vizsgálatához forráselemzést végeztem, amely mellett a H3 hipotézishez is kapcsolódó szakértői interjúkat is végrehajtottam. A szakértői interjúk kérdőívét

[51] Johan Van Niekerk – Rossouw von Solms, „The State of Information Security Research: A South African Perspective", in *Christiaan Kroeze Szerk.: Information Security in the Knowledge Economy* (University of Pretoria, 2013), 55–62.

a nemzetközi szakirodalomban már alkalmazott kérdések adaptálásával állítom össze, ezáltal biztosítva a kutatási eredmények nemzetközi összehasonlíthatóságát.[52]

A H2 és H6 hipotézis vizsgálatának módszertana a Technológia Elfogadási Folyamat (TAP) modell adaptációján alapul, ötvözve a narratív hálózatelemzést, a Python-alapú szövegbányászatot és a Gephi vizualizációs technikákat, melynek során a releváns videók alatti hozzászólásokat fogom vizsgálni. Ez a módszer lehetővé teszi a társadalmi attitűdök mélyreható elemzését és vizualizációját.

A H3 és H4 hipotézis vizsgálatához a nemzetközi szakirodalomban alkalmazott kérdéseket használok a szakértői interjúkban, majd ezeket a CATWOE modell alapján elemzem. A CATWOE modell (Customers, Actors, Transformation process, Worldview, Owners, Environmental constraints) lehetővé teszi a különböző érdekeltek szempontjainak figyelembevételét, ami különösen fontos az okos eszközök biztonsági kérdéseinek vizsgálatakor.

A H5 hipotézis szakértői interjúkat folytattam[53] a védelmi szektorban és az információbiztonság területén dolgozók körében. A kérdéseket a nemzetközi vagy hazai szakirodalomból adaptáltam, ezáltal biztosítva a kutatási eredmények összehasonlíthatóságát. [54] Majd a válaszokat a CRAMM (CCTA Risk Analysis and Management Method) modell alapján elemeztem.

A kutatás során alkalmazott módszertanok kombinációja biztosítja a kutatási kérdések átfogó vizsgálatát és a hipotézisek megbízható tesztelését. A kvalitatív és kvantitatív módszerek integrációja, valamint a különböző adatforrások triangulációja növeli a kutatás érvényességét és megbízhatóságát.

---

[52] "Smart Healthcare Readiness Index Measurement In Bandung City" (Hidayat, 2019) c. műben, "A Multi-Feature User Authentication Model Based on Mobile App Interactions" (Ashibani, 2020) c. műben, illetve Social Media in Teaching-Learning Process: Investigation of the "Use of Whatsapp in Teaching and Learning in University of Port Harcourt" (Abraham, 2019) c. műben szereplő interjúkat vettem alapul.

[53] Simon Béla, „A kiberbűncselekmények nyomozásának új kihívásai”, *Belügyi Szemle* 66, sz. 7–8 (2018): 106–15.

[54] Digitization, Cybersecurity and Risk Management in the Oil and Gas Sector in the post COVID world: A Systematic Review" c. (Afzaal, 2023) mű, a dezinformációval kapcsolatos kérdések a "Consensus on the role of culture in restraining financial crime: a systematic literature review" (Maulidijah, 2023.) c. mű alapján készült. A specifikus kérdések esetében "Disinformation and social bot operations in the run up to the 2017 French presidential election." (Ferrara, 2017) c. művét vettem alapul, tovbbá saját kérdésekkel egészítettem ki.

1.8 Az értekezés logikai felépítése

Az értekezés szerkezete logikusan követi a kutatási célokat és a megfogalmazott hipotéziseket. Az egyes fejezetek fokozatosan építik fel a témakör átfogó elemzését, az elméleti alapoktól a gyakorlati alkalmazásokig és jövőbeli kilátásokig. Az első fejezetben az információs társadalom biztonsági kihívásait vizsgálom, különös tekintettel a technikai és az emberi eredetű kihívásokra. Itt definiálom az információs társadalom fogalmát, áttekintést nyújtok a téma tudományos kutatottságáról, majd részletesen elemzem a különböző típusú biztonsági kihívásokat, beleértve az okos eszközökből adódó biztonsági kockázatokat és a hitelesség kérdését a digitális térben.

A második fejezetben az okos eszközök fejlődésének evolúcióját elemzem, kezdve egy történeti áttekintéssel, majd részletesen bemutatva az alkalmazások szerepét és típusait. Külön figyelmet szentelek a személyazonosításra és hitelesítésre alkalmas eszközök fejlődésének, összehasonlítva a nemzetközi és hazai példákat. A fejezet részét képezi az okos eszközök és alkalmazások adatbiztonsági kérdéseinek és kockázatainak elemzése.

A harmadik fejezetben a személyazonosításra és hitelesítésre alkalmas technológia jelenlegi felhasználási területeit tekintem át, mind a magán-, mind a közszférában. A magánszférán belül részletesen elemzem a bankszektor, az ügyvédi irodák, a turizmus és a közösségi média területén alkalmazott megoldásokat. A közszféra vonatkozásában az e-közigazgatás, m-közigazgatás, a védelmi szféra és az egészségügy területére fókuszálok. A fejezet kitér a jelenlegi biztonsági kihívásokra és kockázatokra, valamint a technológia társadalmi elfogadottságára mindkét szférában, tekintettel arra, hogy a digitális technológiák közszférában történő alkalmazásának sikere mértékben függ az állampolgárok bizalmától is.[55]

A negyedik fejezetben a személyazonosításra és hitelesítésre alkalmas technológia alkalmazásának jövőbeli lehetőségeit vizsgálom. Elemzem a fejlődés lehetséges irányait és azok társadalmi elfogadottságát, összehasonlítva az államilag fejlesztett és a magáncégek által fejlesztett megoldásokat. Külön figyelmet fordítok a közösségi médiában történő felhasználás lehetőségeire, valamint az internetes csalások és információs

[55] Király Péter György, „A digitális állami szolgáltatások felhasználói élménye”, *Pro Publico Bono – Magyar Közigazgatás* 9, sz. 1 (2021): 60–77.

műveletek elleni küzdelemben játszott szerepére. A fejezet zárásaként a hitelesítésre alkalmas technológia jövőbeli biztonsági kockázatait tárgyalom.

Az ötödik fejezetben a védelmi, biztonsági szektorban történő felhasználás lehetőségeit és kockázatait elemzem, külön kitérve a katonai, rendészeti, magánbiztonsági, idegenrendészeti és nemzetbiztonsági területek sajátosságaira. Ez a fejezet különösen fontos a téma hadtudományi relevanciájának szempontjából, hiszen részletesen feltárja a technológia potenciális alkalmazási területeit és kihívásait a nevezett szektorban.

Az értekezést összegzés, rövidítések jegyzéke, ábrajegyzék és részletes irodalomjegyzék zárja, amely tartalmazza a felhasznált hazai és nemzetközi szakirodalmat, jogszabályokat és egyéb forrásokat. Ez a logikai felépítés biztosítja, hogy az értekezés átfogó és strukturált elemzést nyújtson az okos eszközök fejlődési irányairól, különös tekintettel a személyazonosításra és hitelesítésre, alkalmas technológiákra, azok biztonsági kihívásaira, adatvédelmi vonatkozásaira és társadalmi elfogadottságára. A kutatás eredményei várhatóan hozzájárulnak a témakör tudományos megértéséhez, és gyakorlati jelentőséggel bírnak a technológia jövőbeli fejlesztése és alkalmazása szempontjából.

2 AZ INFORMÁCIÓS TÁRSADALOM ÉS ANNAK BIZTONSÁGI KIHÍVÁSAI

Az információs társadalom kialakulása a 21. század egyik meghatározó társadalmi-gazdasági átalakulását eredményezte, amelynek középpontjában az információ áll. A digitális technológiák rohamos fejlődése új lehetőségeket teremtett a gazdasági szereplők, az állam, valamint az egyének számára, ugyanakkor számos biztonsági kockázatot is magában hordoz. Ebben a fejezetben áttekintem az információs társadalom főbb jellemzőit, valamint részletesen elemzem a biztonsági kihívásokat, amelyek jelentkezhetnek. Különös figyelmet fordítok a fenyegetések sokszínűségére, A fejezet célja, hogy átfogó képet adjon az információs társadalom biztonsági kérdéseiről, megalapozva ezzel az értekezés további elemzéseit.

2.1 Információs társdalom meghatározása

Maga az információs társadalom gondolata a modern társadalomtudományi diskurzus egyik meghatározó fogalmaként jelent meg, ami befolyást gyakorolt és jelenleg is gyakorol az akadémiai, kormányzati, sőt a közgondolkodásra is. Azonban a fogalom értelmezése korántsem egységes, számos, gyakran eltérő definíció és megközelítés létezik. Az információs társadalom jelenségét technológiai, gazdasági, foglalkoztatási, térbeli vagy kulturális dimenziókon keresztül is elemezhetjük, ami jól érzékelteti a koncepció komplexitását.[56]

2.1.1 Információs társdalom fogalmi definíciói

Az információs társadalom definiálása összetett feladat, mivel a különböző tudományterületek képviselői eltérő perspektívákból vizsgálják a jelenséget, annak különböző aspektusait hangsúlyozzák.[57] A fogalom összetettségét jól mutatja, hogy a különböző megközelítések gyakran csak a jelenség részleges vetületeit ragadják meg, azonban a fogalom komplex megértéséhez ezen megközelítések szintézisére van szükség.[58] Ebben az alfejezetben bemutatom a különböző tudományterületek által meghatározott

[56] Castells Manuel, *Az információ kora: Gazdaság, társadalom és kultúra. I. kötet: A hálózati társadalom kialakulása* (Budapest: Gondolat-Infonia, 2005).
[57] Pintér Róbert, *Az információs társadalom: Az elmélettől a politikai gyakorlatig* (Budapest: Gondolat-Új Mandátum, 2007).
[58] Karvalics László Z., „Információs társadalom – mi az? Egy kifejezés jelentése, története és fogalomkörnyezete", in *Róbert Pintér szerk.: Az információs társadalom* (Budapest: Gondolat-Új Mandátum, 2007), 29–47.

fogalmakat, az információs társdalom, mint definíció megértését elősegítve, megalapozva a fejezet további részeinek komplexebb és érthetőbb megközelítését.

Masuda, aki az információs társadalom koncepciójának egyik úttörője volt, úgy határozta meg azt, mint "olyan újszerű társadalmi keret, amelyben az információ megszerzése, nem pedig az anyagi javak birtoklása hajtja a fejlődést és átalakulást, az információs és kommunikációs technológiák pedig alapvető elemként szolgálnak".[59] Masuda megközelítése kiemeli az információnak a központi szerepét a társadalmi fejlődésben, és hangsúlyozza, hogy az információs társadalomban az emberi intellektuális kreativitás virágzik, szemben a korábban, amikor az anyagi javak dominanciájával. Hilbert 2015-ös definíciója szerint "az információs társadalom olyan társadalom, amelyben az információ létrehozása, elosztása, felhasználása, integrálása és manipulálása gazdasági, politikai és kulturális tevékenységet képez. Elsődleges katalizátorai a digitális információs és kommunikációs technológiák, amelyek információrobbanást idéztek elő, és alapvetően megváltoztatták a társadalmi szerveződés minden aspektusát, beleértve a gazdaságot, az oktatást, az egészségügyet, a hadviselést, a kormányzást és egyéb területeket".[60]Ez a meghatározás kiemeli a digitális technológiák kulcsfontosságú szerepét és az információs tevékenységek társadalomformáló hatását, hangsúlyozva azok összetett befolyását a társadalomra és annak minden alrendszerére.

Cronin tömör megfogalmazásában az információs társadalom "olyan társadalom, amelyben a munka intellektualizálódott"[61] , ezzel a munkavégzés jellegének átalakulását helyezi a középpontba, ahol a tudásalapú tevékenységek egyre inkább felváltják a fizikai munkavégzést.

A magyar tudományos szakirodalomban Bakonyi Péter definíciója az információs társadalmat "az információs és kommunikációs technológiák forradalmi fejlődése és konvergenciája által előidézett társadalmi átalakulások" összességeként határozza

[59] Yoneji Masuda, *The Information Society as Post-Industrial Society* (Tokyo: Institute for the Information Society, 1980).
[60] Martin Hilbert, „Digital Technology and Social Change: The Digital Transformation of Society from a Historical Perspective", *Dialogues in Clinical Neuroscience* 17, sz. 3 (2015): 347–60, https://doi.org/10.31887/DCNS.2015.17.3/mhilbert.
[61] Blaise Cronin, „The Transition to Information Society", *Aslib Proceedings* 35, sz. 2 (1983): 56–61, https://doi.org/10.1108/eb050865.

meg.[62]Bakonyi kiemeli, hogy az információs társadalomban "az információ előállítása, terjesztése és felhasználása válik a gazdaság és társadalom elsődleges erőforrásává", továbbá hangsúlyozza, hogy ebben a társadalmi formációban "az emberek közötti kommunikáció és interakció intenzívebbé válik", valamint "a modernizáció, társadalmi innováció és globalizáció, mint kedvező folyamat dominánssá válik".[63]

Manuel Castells megfogalmazása szerint az információs társadalom "olyan társadalmi struktúra, amelyet a digitális technológiák hálózatba kapcsolása jellemez, amelyek információt generálnak, feldolgoznak és terjesztenek. Ez egy tudásalapú gazdaságot foglal magában, ahol a munkafolyamatok integrálódnak az információs technológiával és a kommunikációs hálózatokkal".[64] Castells később ezt a koncepciót továbbfejlesztette a hálózati társadalom fogalmává, amelyet részletesebben a későbbiekben tárgyalunk. Z. Karvalics László, a téma ismert magyar kutatója az információs társadalmat fejlődési folyamatként értelmezi, amelyben az információ termelése, áramlása, felhasználása, feldolgozása, tárolása és továbbítása válik a gazdasági-társadalmi újratermelés meghatározó tényezőjévé".[65] Nyíri Kristóf, a magyar filozófiai gondolkodás kiemelkedő alakja továbbá hangsúlyozza, hogy "az információs társadalom olyan történelmi korszakváltást jelent, amely alapjaiban formálja át a társadalom valamennyi alrendszerét, a gazdaságot, a politikát, a kultúrát és az oktatást egyaránt".[66]

A definíciók szerteágazóak, mint ahogy láthatjuk, de az alábbi közös pontok jelennek meg:

- Az információ előtérbe kerülése,
- Az információs és kommunikációs technológiák alapvető szerepe a társadalmi változásban,
- A gazdaság, társadalom, kultúra, oktatás és politika átalakulása,
- A tudásalapú tevékenységek előtérbe kerülése a fizikai munkával szemben,

[62] Bakonyi Péter, „Az információs társadalom meghatározása”, in *Információs társadalom és jogrendszer* (Budapest: MTA Társadalomkutató Központ, 2000).
[63] Bakonyi.
[64] Manuel Castells, *The Rise of the Network Society*, Second (Oxford: Wiley-Blackwell, 2010).
[65] Z Karvalics Z. és László, „Információ, tudás, társadalom, gazdaság, technológia: egy egységes terminológia felé”, *Információs Társadalom* 5, sz. 4 (2005): 7–17.
[66] Nyíri Kristóf, „Az információs társadalom és a történelmi-kulturális hagyomány”, *Világosság* 42, sz. 7–9 (2001): 31–37.

- A hálózatosodás, digitalizáció, globalizáció, innováció és intenzívebb emberi kommunikáció, mint meghatározó folyamatok,
- Az információs társadalom egy folyamat és nem lezárt állapot,

Így a fenti szerzők definíciói alapján egyértelműen kijelenthető, hogy az információs társadalom egy összetett, több tudományterület által vizsgált fogalom. Ezek közös metszőpontjai alapján az információs társadalom úgy definiálható kutatásom szempontjából, mint egy olyan társadalmi formáció, aminek a jellemzője az információ előállítása, terjesztése, feldolgozása, felhasználása, megosztása és manipulálása. És ezek a tényezők a gazdasági, társadalmi, politikai és kulturális működés elsődleges mozgatórugói. Az információs társdalom alapját képzi az IKT fejlődése, ami új struktúrákat és folyamatokat eredményeznek a társadalomban. A hagyományos) gazdasági és társadalmi modelleket felváltja a tudás- és információalapú gazdaság, ahol az intellektuális tevékenységek, a hálózati működés és a digitális kompetenciák a meghatározók. Az információs társadalom nem csak a technológiai fejlődés eredménye, hanem egy társadalmi, gazdasági és kulturális átalakulás, ami áthatja az élet minden területét.

2.1.2 Az információs társadalomtörténeti keletkezése és fejlődése

Tekintettel a fogalom sokszínűségére, az információs társadalom, mint definíció nem köthető egyetlen konkrét időponthoz vagy személyhez, sokkal inkább egy evolúciós folyamatként lehet rá tekinteni, amit a különböző gondolkodók munkásságából és a társadalmi, gazdasági és technológiai változások megfigyeléséből és elemzéséből táplálkozott.[67] Egyes kutatók szerint az információs társadalom gyökerei a második világháború időszakáig nyúlnak vissza. A fogalom fejlődésének állomása az 1950-es évek közepére tehető. Dr. Tattay Levente szerint "1956-57-re teszik azoknak a mélyreható gazdasági, politikai és társadalmi változásoknak a kezdetét, amelyek átvezettek a modern információs társadalom szférájába. 1956-ban készült el az első tranzisztorokkal működő számítógép. Az információs munkakörben foglalkoztatottak száma az USA-ban először haladta meg az 50%-ot. 1957-ben jelent meg az ember - a szovjet Gagarin - a világűrben, amely miatt az USA hatalmas volumenű katonai fejlesztéseket indított el. Gagarin szputnyikja a hiányzó technológiai katalizátornak bizonyult".[68] Ezek az

[67] Armand Mattelart, *The Information Society: An Introduction* (London: Sage Publications, 2003).
[68] Tattay Levente, „Az információs társadalom és az Európai Unió", *Külgazdaság* 46, sz. 6 (2002): 76–97. „Az információs társadalom és az Európai Unió", *Külgazdaság* 46, sz. 6 (2002): 76–97.

események katalizálták azokat a technológiai fejlesztéseket, amelyek később az információs társadalom infrastrukturális alapját képezték.

Az információs társadalom fogalmának megjelenése szorosan köthető továbbá a fentiekben már említett, a fogalom megalkotójának tekintett, japán Yoneji Masuda professzor munkásságához. Masuda az 1960-as években kezdte el használni a fogalmat. [69] Az információs társadalom koncepciójának fejlődésében szerepet játszott Fritz Machlup amerikai közgazdász munkássága is. Machlup 1962-ben "bevezette a tudásipar fogalmát. Öt szegmenst különböztetett meg a tudás szektorán belül: oktatás, kutatás és fejlesztés, tömegmédia, információ technológiák és információ szolgáltatások. Ezen a felosztáson alapulva úgy számolta, hogy 1959-ben az USA GNP-jének 29%-át állította elő a tudásiparban.[70]

A fogalom fejlődésének következő fontos állomása Daniel Bell munkássága volt, aki az 1970-es években dolgozta ki a posztindusztriális társadalom koncepcióját, amely szorosan kapcsolódik az információs társadalom fogalmához, amely részleteit a későbbiekben fejtem ki. De előzetesen annyi leszögezhető, hogy Bell felismerte a szolgáltatási szektor és a tudásalapú tevékenységek növekvő szerepét a gazdaságban, valamint előre jelezte az ipari társadalom utáni társadalmi formáció kialakulását, amelyben A tudás és az információ válik a legfontosabb erőforrássá.[71] Az 1980-as és 1990-es években az információs társadalom koncepciója fokozatosan beépült a politikai diskurzusba is. Tattay Levente szerint "az Európai Közösség hivatalos dokumentumai közül elsőként az ún. Bengemann jelentés 1994-ben említette az információs társadalmat".[72] Ez jelzi, hogy a fogalom ekkor már nem csak a tudományos diskurzus része volt, hanem a politikai döntéshozatalban is megjelent, elismerve ezzel az információs társadalom koncepciójának jelentőségét társadalom alakulásában. Magyarországon az információs társadalommal kapcsolatos első kormányzati stratégia 1995-ben jelent meg, amely Glatz Ferenc történész, az MTA akkori elnökének vezetésével készült, és

[69] Masuda, *The Information Society as Post-Industrial Society*.
[70] Fritz Machlup, *The Production and Distribution of Knowledge in the United States* (Princeton: Princeton University Press, 1962).
[71] Daniel Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting* (London: Heinemann, 1974).
[72] Tattay, „Az információs társadalom és az Európai Unió”.

amelyben már explicit módon megjelent az információs társadalom koncepciója, mint stratégiai fejlesztési irány.[73]

Az 1990-es években és a 2000-es évek elején az információs társadalom koncepciója tovább fejlődött, és Manuel Castells munkássága révén egy új dimenzióval gazdagodott: a hálózatiság dimenziójával. Castells információs technológiai paradigmájában "az információ mellett a hálózati logika áthatósága, rugalmassága és konvergenciája a központi elem".[74].

Az információs társadalom fogalmának történeti fejlődése egy komplex folyamat, amely az 1940-es évektől napjainkig tart, és amelyben különböző tudományterületek képviselői – közgazdászok, szociológusok, filozófusok, technológiai szakemberek – egyaránt szerepet játszottak. A fogalom folyamatosan bővült, árnyalódott, új dimenziókkal gazdagodott, miközben a technológiai, gazdasági és társadalmi változások újabb és újabb impulzusokat adtak a koncepció fejlődésének.

2.1.3 Az információs társadalom dimenziói és fő jellemzői

Webster 2006-ban megjelent "Theories of the Information Society" című művében az információs társadalom öt különböző megközelítését azonosította: a technológiai, gazdasági, foglalkoztatási, térbeli és kulturális megközelítéseket.[75] Ez a kategorizálás jól mutatja, hogy az információs társadalom fogalma mennyire sokrétű és komplex, különböző tudományterületek és elméleti tradíciók perspektívájából értelmezhető. Az alábbiakban Webster felosztása alapján közelítem meg az információs társadalom egyes dimenzióit.

Technológiai dimenzió

A technológiai dimenzió az információs társadalom egyik legnyilvánvalóbb aspektusa. Ez a megközelítés az információs és kommunikációs technológiák fejlődését tekinti

[73] Glatz Ferenc, *Magyarország az ezredfordulón. Stratégiai kutatások a Magyar Tudományos Akadémián* (Budapest: MTA, 1995).
[74] Castells, *Az információ kora: Gazdaság, társadalom és kultúra. I. kötet: A hálózati társadalom kialakulása*.
[75] Frank Webster, *Theories of the Information Society* (London: Routledge, 2006), https://doi.org/10.4324/9780203962824.

az információs társadalom kialakulása fő mozgatórugójának, az a technológiai áttöréseket és fejlődés meghatározza a társadalmi átalakulásokat.[76] Az információs társadalom technológiai dimenziójában tehát központi szerepet játszik a digitális technológiák fejlődése.[77]

Azonban a technológiai dimenzió az információs társadalom korai diskurzusában játszik inkább kiemelt szerepelt, amikor még a technológiai determinizmus szemlélete dominált.[78] Bár a későbbi elméletek már árnyaltabban látják a technológia és a társadalom viszonyát, a technológiai dimenzió továbbra is meghatározó szerepet játszik az információs társadalom koncepciójában a mai napi Azonban információs társadalom nem redukálható pusztán a technológiai fejlődésre, bár kétségtelen, hogy ez az egyik legfontosabb dimenziója. Z. Karvalics László megfogalmazásában: "A technológiai determinizmus csapdája, ha az információs társadalmat kizárólag a technológiai fejlődés eredményeként értelmezzük, figyelmen kívül hagyva azokat a komplex társadalmi, gazdasági és kulturális folyamatokat, amelyek kölcsönhatásban állnak a technológiai változásokkal."[79]

Álláspontom alapján bár nem kizárólagosan technológiai determinizmus, ami formálja az információs társadalmat, de valóban az egyik fő mozgatórugója, illetve katalizátora lehet. Vita tárgyát képezheti, hogy maga társadalom fogyasztási szokásai alakultak ki az olyan mikro tartalom-közvetítő platformok, mint a TikTok, vagy maga a platform alakította ki ezt fajta rövid, tömör és sokszínű tartalmak iránti igényt. Azonban mindenképpen arra lehet következtetni, hogy ez a két dolog egymást gerjesztő tényező, így az információs társadalom dimenziói esetében is véleményem szerint egymást gerjesztő folyamatokról beszélhetünk.

---

[76] Bakonyi, „Az információs társadalom meghatározása".
[77] Hilbert, „Digital Technology and Social Change: The Digital Transformation of Society from a Historical Perspective".
[78] Pintér Róbert, „Úton az információs társadalom megismerése felé", in *Pintér Róbert (szerk.), Az információs társadalom: Az elmélettől a politikai gyakorlatig* (Budapest: Gondolat-Új Mandátum, 2007), 11–28.
[79] Karvalics, „Információs társadalom – mi az? Egy kifejezés jelentése, története és fogalomkörnyezete".

Gazdasági dimenzió

Az információs társadalom gazdasági dimenziója az információ és a tudás gazdasági szerepének felértékelődésére utal. Az információs társadalom elmélete szerint maga a társadalomban az információ előállítása, elosztása, terjesztése, használata és kezelése többkomponensű tevékenység (gazdasági, politikai és kulturális tevékenység). Az információs társadalom rendelkezek közgazdasági társfogalommal, ami a tudásgazdaság, ami szerint az tudás gazdasági hasznosításán keresztül vezeti le az értékek létrejöttét.[80] Az információs társadalom gazdasági dimenziójában az információ és a tudás nem kizárólag a termelés egy katalizátoraként, elemeként jelenik meg, hanem kiemelendő, hogy önálló gazdasági ágazatok épülnek rá. Fritz Machlup már az 1960-as években felismerte ezt a tendenciát, amikor bevezette a tudásipar fogalmát, és kimutatta, hogy az Egyesült Államok GNP-jének egy részét már ekkor a tudásszektorban állították elő.[81] Ez a megközelítés jól mutatja, hogy az információs társadalomban a tudás nem csupán absztrakt fogalomként értelmezendő, hanem olyan erőforrásként, amely közvetlenül befolyásolja a gazdasági teljesítményt.[82]

Manuel Castells az információs kapitalizmus fogalmát használja a jelenlegi gazdasági rendszer leírására. Castells szerint az információs kapitalizmusban az információ generálása, feldolgozása és átvitele a termelékenység és a hatalom alapvető forrásaivá váltak[83]

Foglalkoztatási dimenzió

Az információs társadalom foglalkoztatási dimenziója szorosan összefügg a gazdasági dimenzióval, és a munkaerőpiac szerkezetének átalakulására utal. Ahogy Cronin megfogalmazta az információs társadalom "olyan társadalom, amelyben a munka intellektualizálódott".[84] Ez a meghatározás jól rávilágít arra, hogy az információs társadalomban a fizikai munka helyett egyre inkább az intellektuális, tudásalapú tevékenységek válnak dominánssá. A Távközlési és Gazdasági Kutatóintézet (RITE) által meghatá-

[80] Peter F. Drucker, *The Age of Discontinuity; Guidelines to Our Changing Society* (New York: Harper & Row, 1969).
[81] Machlup, *The Production and Distribution of Knowledge in the United States*.
[82] Alvin Toffler, *The Third Wave* (New York: Bantam Books, 1980).
[83] Manuel Castells, „The Rise of the Network Society, The Information Age: Economy", *Society and Culture* I (1996).
[84] Cronin, „The Transition to Information Society".

rozott kritériumok között is szerepel, hogy információs társadalomról akkor beszélhetünk, ha "a szolgáltatási szektorban dolgozók aránya meghaladja a teljes munkaerő 50 százalékát".[85] Ez az arány jelzi, hogy a gazdaság szerkezetváltásával párhuzamosan a foglalkoztatási struktúra is átalakul, és az ipari termelésben dolgozók helyett a szolgáltatási szektorban, ezen belül is főként az információs tevékenységekben foglalkoztatottak aránya növekszik.

Az információs társadalom foglalkoztatási dimenziójának fontos jellemzője az is, hogy a munkaerőpiacon egyre nagyobb teret kapnak az úgynevezett transzverzális készségek, amelyek különböző munkakörökben és ágazatokban is alkalmazhatók, mint például a kritikus gondolkodás, a problémamegoldás, a kreativitás és a digitális készségek.[86] Ezek a készségek lehetővé teszik a munkavállalók számára, hogy alkalmazkodni tudjanak a gyorsan változó munkaerő-piaci követelményekhez, és sikeresen helyt álljanak a tudásalapú gazdaságban. Megjegyzendő, hogy a fentiek hiánya nem csupán adott esetekben információbiztonsági kockázatot hordozhat magában, hanem ezek hiánya az adott személy integrálódásának ellehetetlenedését jelenti az információs társadalomban.

Térbeli dimenzió

Az információs társadalom térbeli dimenziója a tér és az idő szerepének átalakulására utal az információs technológiák által lehetővé tett új kommunikációs formák révén.[87] Manuel Castells hálózati társadalom koncepciója különösen hangsúlyozza ezt a dimenziót. A térbeli dimenzió átalakulása azt jelenti, hogy az információs társadalomban a fizikai távolságok fontossága csökken, a különböző helyszínek közötti kommunikáció és interakció könnyebbé és gyorsabbá válik, ami új lehetőségeket teremt a gazdasági, társadalmi és kulturális tevékenységek szervezésében. Csizmadia Zoltán, a hálózatkutatás hazai képviselője kiemeli: "A digitális hálózatok révén olyan együttműködési és koordinációs formák jönnek létre, amelyek korábban elképzelhetetlenek voltak a fizikai távolságok korlátai miatt."[88]

---

[85] Gazdasági Kutatóintézet Távközlési, *Az információs társadalom indikátorai. Dokumentumismertetés* (Tokyo: RITE, 1990).
[86] Bizottság Európai, *Új készségek és munkahelyek menetrendje* (Brüsszel: Európai Bizottság, 2010).
[87] Castells, „The Rise of the Network Society, The Information Age: Economy".
[88] Csizmadia Zoltán, „Társadalmi kapcsolatok a magyar–szlovák–osztrák határtérségben", *Tér és Társadalom* 18, sz. 4 (2004): 103–16.

Ez a megközelítés rámutat arra, hogy az információs társadalomban a tér fogalma kibővül, és a fizikai tér (hagyományos értelemben a földrajzi helyzet, távolságok és anyagi infrastruktúrák által meghatározott terület) mellett megjelenik a virtuális vagy hálózati tér is. A hálózati tér Castells szerint a digitális hálózatok által létrehozott, időbeli és térbeli korlátokat lebontó struktúra. (Pl.: A globális tőzsdepiacok működése, ahol a világ különböző pontjain a valós idejű tranzakciók függetlenek a fizikai távolságoktól.) A hálózati térben a térbeli távolságok pedig elvesztik jelentőségüket, az egyének és közösségek új típusú kapcsolatokat alakíthatnak ki, a fizikai valóságban történt elhelyezkedésüktől. függetlenül.[89] Azonban ki kell emelni, hogy a fizikai tér relativizálódása nem azt jelenti, hogy az elveszti égét, hanem hogy új kapcsolatba kerül az adott személy a hálózati és virtuális terekkel. Ezt tökleletesen be lehet mutatni egy fiktív példával, például egy budapesti székhelyű vállalat alkalmazottai naponta kommunikálnak indiai kollégákkal internetes alapú hívásokon keresztül (hálózati tér), de a gyártás fizikai telephelyeken (Budapest, vagy más magyarországi település) zajlik.

Kulturális dimenzió

Az információs társadalom kulturális dimenziója a kulturális gyakorlatok és értékek átalakulására utal. A kulturális dimenzió átalakulása magában foglalja a tudás szerkezetének, a kulturális termékek előállításának és fogyasztásának, valamint a kulturális identitások alakulásának változásait.[90] Az információs társadalomban a kulturális termékek egyre inkább digitális formában jelennek meg, ami megváltoztatja előállításuk, terjesztésük és fogyasztásuk módjait és szokásait. Dessewffy Tibor és Láng László szerint az információs társadalom kulturális dimenziójában központi szerepet játszik a "digitális kultúra", amely "nem csupán a digitális technológiák által közvetített kulturális tartalmakat jelenti, hanem azt a sajátos életmódot, értékrendet és közösségi gyakorlatokat, amelyek az információs társadalomban kialakulnak".[91] A digitális kultúra tehát nem egyszerűen a hagyományos kultúra digitális formában való megjelenése, hanem egy új kulturális forma, amely sajátos logikával, értékekkel és gyakorlatokkal rendelkezik.

---

[89] Mészáros Rezső, *Kibertér. A földrajzi tudás új dimenziói* (Szeged: Hispánia Kiadó, 2003).
[90] György Péter, *Memex: A könyvbe zárt tudás* (Budapest: Magvető, 2001).
[91] Dessewffy Tibor és Láng László, „A figyelemgazdaság: Az új média és a digitális kapitalizmus”, *Replika* 92–93 (2015): 159–81.

Az információs társadalom kulturális dimenziójának fontos jellemzője a kulturális termelés és fogyasztás demokratizálódása is. Az internet és a digitális technológiák elterjedésével a kulturális tartalmak előállítása és terjesztése már nem csupán a hivatalos kulturális intézmények és a média privilégiuma, hanem az egyének és közösségek számára is elérhetővé válik.

Az információs társadalom és kapcsolódó koncepciók

Az információs társadalom fogalma nem izoláltan létezik a társadalomtudományi diskurzusban, hanem szorosan kapcsolódik számos más, a modern társadalmat leíró koncepcióhoz. Ezek a kapcsolódó fogalmak részben átfedésben vannak az információs társadalom koncepciójával, részben pedig annak különböző aspektusait vagy alternatív értelmezéseit jelentik.[92]

Tudástársadalom

Az információs társadalom és a tudástársadalom (knowledge society) koncepciója szorosan összefonódik a szakirodalomban. A tudástársadalom koncepciója szerint nem egyszerűen az információ mennyisége és áramlása a meghatározó, hanem az információ tudássá alakításának képessége, valamint a hasznosítása. A tudástársadalom fogalma tehát az információs társadalom egy specifikus értelmezési kerete, amely a tudás szerepét.[93]

Posztindusztriális társadalom

Az információs társadalom és a posztindusztriális társadalom fogalma szintén szorosan összekapcsolódik. "Az információs társadalmat az ipari társadalom örökösének is tekintik. Szorosan kapcsolódik a posztindusztriális társadalom (Daniel Bell), a posztfordizmus, a posztmodern társadalom, a tudástársadalom és a hálózati társadalom (Manuel Castells) fogalmaihoz". A posztindusztriális társadalom fogalmát Daniel Bell dolgozta ki az 1970-es években, és "a tudásközpontú posztindusztriális társadalom eljöttét jósolta meg".[94] Bell koncepciója szerint a posztindusztriális társadalomban a szolgál-

[92] Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting*.
[93] Nico Stehr, *Knowledge Societies* (London: Sage, 1994).
[94] Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting*.

tatási szektor válik dominánssá az ipari termelés helyett, és a társadalom szervezésében a tudás és az információ játszik központi szerepet. Bell öt dimenzióban határozta meg a posztindusztriális társadalom jellemzőit:

(1) a gazdasági szektorban a javak termeléséről a szolgáltatásokra történő átállás,

(2) a foglalkozási struktúrában a szakképzett és műszaki szakemberek dominanciája,

(3) a társadalom az elméleti tudás központi szerepe,

(4) a jövőbeli orientáció a technológia ellenőrzésére és értékelésére, és

(5) a döntéshozatal új intellektuális technológiáinak létrejötte.[95]

A posztindusztriális társadalom fogalma tehát az információs társadalom egy olyan értelmezési kerete, amely a társadalom gazdasági szerkezetváltására helyezi a hangsúlyt, kiemelve az ipari termelésről a szolgáltatásokra való átállást, valamint a tudás és az információ növekvő szerepét a gazdasági és társadalmi folyamatokban.

Posztmodern társadalom

Jean-François Lyotard, a posztmodern gondolkodás egyik képviselője, "A posztmodern állapot" című művében explicit kapcsolatot teremt a posztmodern társadalom és az információs technológiák között. Az információs társadalom és a posztmodern társadalom fogalma között is találunk kapcsolódási pontokat. A posztmodern társadalom koncepciója a modern társadalom utáni társadalomra utal, amelyben megkérdőjeleződnek a modernitás értékei, és helyettük a pluralizmus és a relativizmus válik jellemzővé.[96] Az információs társadalom és a posztmodern társadalom közötti kapcsolat abban rejlik, hogy az információs technológiák fejlődése és az információ központi szerepe hozzájárul a társadalom fragmentálódáshoz, a különböző értékrendek párhuzamos létezéséhez, valamint a hagyományos nézetek megkérdőjeleződéséhez. Az információs társadalom és a posztmodern társadalom tehát részben átfedésben vannak, bár a két fogalom különböző aspektusokra helyezi a hangsúlyt: míg az információs társadalom az információ és a technológia szerepét emeli ki, addig a posztmodern társadalom a kulturális és értékrendbeli változásokat hangsúlyozza.

[95] Bell.

[96] Lyotard Jean-François, *A posztmodern állapot*, szerk. Jürgen Habermas, Jean-François Lyotard, és Richard Rorty (Budapest: Századvég, 1993).

Hálózati társadalom

Az információs társadalom és a hálózati társadalom fogalma különösen szorosan összekapcsolódik, különösen a fentiekben már sokszor idézett Manuel Castells munkássága révén. A hálózati társadalom fogalma az információs társadalom egy olyan értelmezési kerete, amely a hálózatok szervező erejét hangsúlyozza, így maga a hálózati társadalom koncepciója az információs társadalom egy olyan specifikus értelmezése, amely a társadalmi, gazdasági és kulturális folyamatok hálózatos szerveződését emeli ki.[97]

A hálózati társadalom egyik jellemzője, hogy a hálózatok nem csupán a technológia, hanem a társadalmi szerveződés alapvető formáivá válnak. Ahogy Barabási Albert-László, a hálózatelmélet egyik vezető kutatója fogalmaz: "A hálózatok mindenütt jelen vannak. Az agy idegsejtek hálózata, a társadalmak emberek hálózatai, az internet pedig számítógépek hálózata. A sejtek kémiai reakciók hálózatai, a vállalatok emberek és erőforrások hálózatai."[98] Ez a megközelítés jól mutatja, hogy a hálózati szemlélet nemcsak a technológia, hanem az élet számos területén alkalmazható elemzési keret.

Az információs társadalom fogalmának és jellemzőinek áttekintése alapján látható, hogy egy rendkívül összetett, a társadalom valamennyi alrendszerét érintő jelenségről van szó, a különböző dimenziói – a technológiai, gazdasági, foglalkoztatási, térbeli és kulturális dimenzió – egymással szoros kölcsönhatásban alakítják a 21. századi társadalmak fejlődését.

Az információs társadalom koncepciója nem értelmezhető egyetlen, egységes elméleti keretben, hanem különböző, egymással részben átfedésben lévő, részben vitatkozó elméletek és megközelítések együttesen adhatnak átfogó képet erről a komplex jelenségről. A tudástársadalom, a posztindusztriális társadalom, a posztmodern társadalom és a hálózati társadalom koncepciói az információs társadalom különböző aspektusait emelik ki, és együttesen járulnak hozzá a jelenkori társadalmi változások megértéséhez. Az információs társadalom kutatása folyamatos reflexiót igényel, amely képes követni a gyors változásokat, az interdiszciplináris megközelítés, amely integrálja a

[97] Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting*.
[98] Barabási Albert-László, *Behálózva. A hálózatok új tudománya* (Budapest: Magyar Könyvklub, 2003).

különböző tudományterületek – szociológia, közgazdaságtudomány, politikatudomány, filozófia, pszichológia, informatika – perspektíváit, különösen fontos az információs társadalom komplex jelenségeinek megértésében. Végső soron az információs társadalom alakítása nem determinisztikus folyamat, hanem kollektív társadalmi és politikai döntések, értékválasztások és cselekvések eredménye. Az információs társadalom jövője nem pusztán technológiai, hanem alapvetően társadalmi, kulturális és politikai kérdés, amely aktív társadalmi párbeszédet és részvételt igényel.

Hadtudományi szempontból ez a rész azért releváns, mert az információs társadalom új stratégiai környezetet teremt a katonai, rendészeti és nemzetbiztonsági szervek számára. Az információs térben való működés, az adatalapú döntéshozatal és a kiberképességek alkalmazása mind olyan jelenségek, amelyek csak a társadalom digitális átalakulásának megértésén keresztül érthetők meg. A kutatásban ez a fejezet egyfajta alapozó szerepet tölt be. Az információs társadalom sajátosságainak feltárása lehetővé teszi, hogy a későbbi fejezetekben tárgyalt technológiák és azok társadalmi, jogi, valamint hadtudományi vonatkozásai komplex módon kerüljenek bemutatásra.

2.2 Az információs társadalom biztonsági kihívásai, annak típusai és felosztása

Az információs társadalom kialakulása számos előnnyel és lehetőséggel jár, ugyanakkor kihívásokat és problémákat is felvet. Az alábbiakban részletesen elemzem az információs társadalom kihívásait a nemzetközi és magyar tudományos szakirodalom alapján. Azonban itt szeretném előzetesen megjegyezni, hogy személyes álláspontom alapján az információs társadalom egyik legfontosabb problémája jelenleg digitális megosztottság (digital divide), amely nem csupán technikai eszközökhöz való hozzáférésben, hanem digitális készségek és kritikai médiaműveltség hiányában is megnyilvánul. A Nemzeti Média- és Hírközlési Hatóság 2024-es adatai szerint Magyarországon a háztartások 16%-a még mindig nem rendelkezik internet előfizetéssel.[99] Ahogy a korábbiakban is utaltam rá a digitális analfabetizmus összességében az információs társadalomból való kirekesztést okozza, továbbá mint, ahogy a későbbiekben kifejtem jelen probléma több másikat is indukál. Az általam elvégzett interjúkban is felmerült

[99] „Az elektronikus hírközlési piac fogyasztóinak vizsgálata, 2024 – háztartási felmérés", elérés 2025. június 15., https://nmhh.hu/cikk/251638/Az_elektronikus_hirkozlesi_piac_fogyasztoinak_vizsgalata_2024__haztartasi_felmeres.

nem egyszer, több a témában releváns szakmai tapasztalattal rendelkező bár külön területen dolgozó szakértő véleménye alapján az egyik legnagyobb probléma a kritikai gondolkodás hiánya, az ebből fakadó biztonságtudatossági problémák, amely más kockázat elhárításában is tényezőként szerepel.

Az információs társadalom fejlődésének történeti kontextusa három fő szakaszra osztható: a kezdeti szakasz (1970-1990), a növekedési szakasz (1990-2010) és a működési szakasz (2010-napjainkig). Az információs társadalom jelenlegi fejlődési szakaszában, a big data, a mesterséges intelligencia és az IoT-alapú automatizálás játszik domináns szerepet, eközben az információk társadalmi hatása olyan szintet ért el, ami már befolyásolhatja a választásokat, az egészségügyi rendszereket és a katonai műveleteket is.[100]

Az információs társadalom kihívásainak kezelése komplex, többdimenziós megközelítést igényel, amely magában foglalja a megfelelő jogi és szabályozási keretek kialakítását, az oktatási rendszerek reformját, a társadalmi párbeszéd erősítését, valamint az egyéni és közösségi adaptációs stratégiák támogatását, mivel maga az információs társadalom biztonsági kérdései is összetettek, egyidejűleg érintik a társadalmi, gazdasági, technikai és politikai szférákat. Az információs társadalom biztonsági kérdéseinek elemzésekor fontos felismerni, hogy a technológiai fejlődés előrehaladtával a kockázatok összetettsége is növekszik. Miközben a hagyományos kihívások csökkenhetnek, úgy új és összetettebb fenyegetések jelenhetnek meg, amelyek gyakran következményekkel járhatnak, amelyek hosszú távú hatásai csak később jelentkeznek.[101]

A biztonsági kihívásokat többféle metodika szerint ki lehet elemezni egy részről a kockázat fogalmánál ismertettek szerint elemezhető a bekövetkezendő esemény valószínűsége, a bekövetkezés várható ideje (azonnali, középtávú, hosszú távú), vagy az okozott kár nagysága szerint, illetőleg az érintett entitások nagysága szerint is (egyéni, szervezeti, nemzeti, nemzetközi). Továbbá társadalomtudományi szempontból sem lenne elvetendő a különböző társadalmi rétegekre (pl.: korosztályok) gyakorolt hatások szerinti vizsgálat. A lenitekben véleményem szerint a kihívások komplex jellege

[100] Klaus Schwab, *The Fourth Industrial Revolution* (Geneva: World Economic Forum, 2016), https://doi.org/10.2307/j.ctt20krxh8.
[101] World Economic Forum, *Global Risks Report* (Geneva: World Economic Forum, 2024).

ellenére a lehető legegyszerűbb rendszerezési elvet követtem, amely során a kihívások eredete alapján vizsgáltam. A két fő kategória technikai és humán eredetű kihívások. Ezeket a kategóriákat a feltárt kockázatok különböző alcsoportokra bontottam a könnyebb átláthatóság kedvéért az alábbiak szerint: A technológiai **és** technikai kihívásokon belül: Az okos eszközökből és IoT eszközökből adódó biztonsági kihívások, Kibertámadások és kiberbűnözés, A biometrikus adatok kezelésének kihívásai, A mesterséges intelligencia és automatizáció¸ Decentralizált technológiák és kriptográfiai akadályok, Kihívások a kvantumszámítástechnikában. A humán kategória főbb alpontjai pedig: Társadalmi-gazdasági akadályok, Politikai és jogi (adatvédelmi) kihívások, Hitelesség kérdésköre és az információs műveletek, álhírek terjedése, Digitális kompetencia, oktatási és tudatossági hiányosságok.

2.3 Technológiai és technikai kihívások

Alapvetően technológiai és technikai akadályok közé tartoznak az információs társadalom infrastruktúrájához, eszközeihez és rendszereihez kapcsolódó különböző biztonsági problémák. Ezek a következőket foglalják magukban

- Az IoT-eszközök biztonsági problémái: Többrétű jelen problémakör is, de kifejezetten releváns, mivel ezen eszközök növekvő elterjedése szélesíti a támadási felületet. 2025-re 75 milliárd IoT-eszköz használatát prognosztizálták, amelyek része nem megfelelő titkosítást alkalmaz.[102]
- Technológiai sebezhetőségek: A hardverekben és szoftverekben, különösen az operációs rendszerekben rejlő hibák és biztonsági hiányosságok, amelyeket az esetleges támadó, felek kihasználhatnak. A kibertámadások, többek között a zsarolóvírusok, világszerte gazdasági károkat okoznak, évente mintegy 6 billió dollár értékben[103] , mondhatni egy teljes iparág épült ki erre a tevékenységre jövedelmezősége miatt.[104]
- Infrastrukturális sebezhetőségek: A kritikus információs infrastruktúrák (beleértve az energiahálózatokat, banki rendszereket és közlekedési rendszereket) gyengeségei, amelyek kibernetikai támadásoknak lehetnek kitéve. Az EU

[102] National Institute Standards és Technology, *Special Publication: CRYSTALS-Kyber Implementation* (Gaithersburg, MD: NIST, 2024).
[103] Cybersecurity Ventures, *Global Cybercrime Damage Report* (Northport, NY: Cybersecurity Ventures, 2024).
[104] World Bank Group, *The Role of Cybersecurity in Economic Performance* (World Bank, 2023), http://documents1.world-bank.org/curated/en/099092324164526526/pdf/P178769189c7360111ac1f1185e04824dec.pdf.

NIS2 szabályozása kiberbiztonsági követelményeket határoz meg a kritikus létesítmények számára.[105] Egyes kutatások szerint már egyes közösségi média platformok is kritikus infrastruktúrának számíthatnak.[106] [107] [108] Szénási Imre tanulmányában a kritikus rendszerelemek típusait vizsgálva megemlíti, hogy a második típusú kritikus infrastruktúrák "teszik lehetővé az egymással való összeköttetést és az együttműködés képességét", és ide sorolja a világhálót és a különböző kommunikációs hálózatokat, bár nem nevezi meg konkrétan a közösségi médiát, de a leírás alapján a közösségi média platformok is értelmezhetők e kategória részeként.[109]

- Kriptográfiai kihívások: A hagyományos titkosítási technikák (pl. RSA) sebezhetővé a válna jövőben a kvantumszámítástechnika megjelenésével. A NIST által jóváhagyott CRYSTALS-Kyber algoritmus kvantumrezisztens titkosítást kínál ennek kiküszöbölésre.[110] Jól látható a kutatások alapján hogy a kvantumszámítástechnikának a hadtudományban is kiemelt szerepe van, az információs fölény megszerzése iránt folytatott küzdelemben.

A következőkben az előbbi szempontok mentén, de az érthetőség kedvéért tagoltabban mutatom be a technikai jellegű kihívások és problémák rendszerét, a biztonsági fenyegetéseknél részletezett felosztás szerint. Azonban az okos eszközökből és IoT eszközökből fakadó biztonsági kihívásokat jelen fejezetben csak zanzásítva, tömören fogom bemutatni tekintettel arra, hogy egy külön fejezetben részletekbe menően foglalkozok az okos eszközök evolúciójával, jelenleg és jövőbeli kockázataival. A következő alrészeknél az okos eszközök tipizálásánál az adott eszközök kiterjedtsége, nagysága alapján osztottam fel a kategóriákat, amelyek közül kiemelten a későbbiekben az okos mobil eszközökkel fogok foglalkozni. Az alábbi kategóriák kerültek meghatározásra:

- okos mobil eszköz
- okos otthoni eszközök

---

[105] European Commission, *NIS2 Directive: EU Cybersecurity Framework* (Brussels: European Commission, 2022).
[106] Szénási Sándor, „Kritikus infrastruktúrák, kritikus információs infrastruktúrák – új kihívások a nemzetbiztonság számára", *Felderítő Szemle* 10, sz. 3–4 (2011): 157–72.
[107] Laura Petersen és mtsai., „Public Expectations of Social Media Use by Critical Infrastructure Operators in Crisis Communication", in *Proceedings of the 14th ISCRAM Conference*, 2017, 521–30, https://idl.iscram.org/files/laurapetersen/2017/2040_LauraPetersen_etal2017.pdf.
[108] „»Is Social Media Critical Infrastructure?«", elérés 2025. április 17., https://www.linkedin.com/pulse/social-media-critical-infrastructure-alex-sharpe.
[109] Szénási, „Kritikus infrastruktúrák, kritikus információs infrastruktúrák – új kihívások a nemzetbiztonság számára".
[110] Standards és Technology, *Special Publication: CRYSTALS-Kyber Implementation*.

- okos város
- okos infrastruktúra

Jól látható, hogy a legkisebb elemtől haladtam a legnagyobbig. Míg egy darab okos mobil eszközt alapvetően egy ember használja, az okos otthoni eszközt már egy háztartást, az okos várost, már egy település, az okos infrastruktúrát pedig egy nagyobb régió. Tekintettel arra, hogy a kutatásom során leginkább vizsgált rész a személyazonosításra és hitelesítésre történő alkalmasság, abból fakadó előnyök és hátrányok ezért az egyéni eszközök, az okos mobil eszközöket kutattam részleteiben.

2.3.1 Az okos eszközökből és IoT eszközökből adódó biztonsági kihívások

Az IoT eszközök hálózati forgalma passzív, az okos eszközöké aktív és adaptív[111], ami azt jelenti a legrövidebben, hogy amíg az IoT eszközök adatgyűjtésre fókuszálnak, addig az okos eszközök ezen adatok alapján automatizált műveleteket hajtanak végre[112] A különbség alapvetően az adatfeldolgozás szintjéből és a hálózati viselkedésből adódik. Az IoT eszközök adatgyűjtőként működnek, míg az okos eszközök intelligens döntéshozatalra és adaptív válaszokra képesek Az IoT eszközök rohamos elterjedése alapvetően átalakítja mindennapi életünket, ugyanakkor számos biztonsági kihívást is teremt. Ezek az eszközök pervazív adatgyűjtést tesznek lehetővé, gyakran a felhasználók tudta vagy beleegyezése nélkül.[113].

Az IoT eszközök biztonsági kihívásai közé tartozik, hogy sok esetben a biztonsági funkciók implementálását feláldozzák a költségek csökkentése érdekében.[114] A gyártók a piacra kerülés gyorsaságát és a funkcionalitást helyezik sokszor előtérbe a biztonság rovására, amely gyakorlat különösen veszélyes. A felhasználók gyakran nincsenek tisztában az IoT eszközök biztonsági kockázataival, és nem alkalmazzák a szükséges alapvető biztonsági intézkedéseket sem, mint az alapértelmezett jelszavak

---

[111] „A Survey of Smart Home IoT Device Classification Using Machine Learning-Based Network Traffic Analysis | IEEE Journals & Magazine | IEEE Xplore", elérés 2025. április 17., https://ieeexplore.ieee.org/document/9881503.
[112] „Mi az IoT (eszközök internetes hálózata)? | Microsoft Azure", elérés 2025. április 17., https://azure.microsoft.com/hu-hu/resources/cloud-computing-dictionary/what-is-iot.
[113] Muhammad Madyan és mtsai., „The Impact of Top Management Education from Reputable Universities on Corporate Capital Structure: Evidence from Indonesia", *Global Business Review*, 2023. augusztus 1., 09721509231182525, https://doi.org/10.1177/09721509231182525.
[114] Madyan és mtsai.

megváltoztatása vagy éppen a rendszeres szoftverfrissítés, különös tekintettel az operációs rendszerekre. telepítése. A Mozilla Foundation "Privacy Not Included" jelentése szerint számos népszerű IoT eszköz nem felel meg az alapvető biztonsági és adatvédelmi követelményeknek.[115] Ezen biztonsági követelmények olyan alapelvek, mint a "privacy by design" (beépített adatvédelem) és a "privacy by default" (alapértelmezett adatvédelem), vagy a „security by design", amely azt jelenti, hogy a biztonság nem utólagos javítással valósul meg, hanem az adott rendszert minden szinten (hardver, szoftver, adatátvitel, üzemeltetés, stb.), előrelátóan tervezik meg, a legtöbb kockázat minimalizálásával.[116]

Az IoT eszközök biztonsági kihívásai között különösen problematikus a botnet-hálózatok létrehozásának lehetősége. A botneteket alkotó, előzetesen már meghackelt, kompromittált IoT eszközök felhasználhatók túlterheléses (DDoS) támadásokra, amelyek gazdasági károkat okozhatnak. Az Akamai "State of the Internet / Security Report" szerint az IoT eszközök elterjedésével a botnet-alapú DDoS támadások ereje növekedett.[117] Tekintettel arra, hogy az okos eszközök típusai rendkívül szerteágazóak lentebb a felhasználás helye szerinti biztonsági kihívások alapján fogom prezentálni a detektált kockázatokat.

2.3.2 Okos mobil eszközök kihívásai

Az okos mobil eszközök technikai biztonsági kihívásai napjainkban egyre összetettebbek és sokrétűbbek, mivel ezek az eszközök a mindennapi életünk szerves részévé váltak, és számos érzékeny adatot kezelnek. Az egyik probléma az operációs rendszerek sérülékenysége. Bányász Péter rámutat arra, hogy különösen az Android nyílt forráskódú jellege miatt a rendszer gyakran tartalmaz olyan biztonsági réseket, amelyeket a támadók kihasználhatnak. Az ilyen sérülékenységek, mint például a Wi-Fi protokollokban felfedezett KRACK-típusú hibák, lehetővé teszik a jogosulatlan hozzáférést a felhasználók adataihoz. A helyzetet tovább súlyosbítja, hogy sok gyártó késve adja ki a szükséges biztonsági frissítéseket, így a felhasználók hosszabb ideig ki vannak téve a fenyegetéseknek.[118]

---

[115] Mozilla Foundation, *Privacy Not Included Report* (San Francisco: Mozilla Foundation, 2023).
[116] „OWASP Application Security Verification Standard (ASVS) | OWASP Foundation", elérés 2025. május 24., https://owasp.org/www-project-application-security-verification-standard/.
[117] Akamai, *State of the Internet/Security Report* (Cambridge, MA: Akamai Technologies, 2024).
[118] Bányász Péter, „Az okos mobil eszközök biztonsága", *Hadmérnök* XIII, sz. 2 (2018): 360–72.

A rosszindulatú szoftverek, például a kémprogramok is komoly veszélyt jelentenek az okos mobil eszközökre. Kadëna Esmeralda kiemeli, hogy ezek a káros programok elsősorban az Android platformot célozzák, mivel ezen az operációs rendszeren lehetőség van alkalmazások külső forrásból történő telepítésére is. A támadók gyakran nulladik napi támadásokat (zero-day exploitokat) használnak ki, vagyis olyan, még nem javított sérülékenységeket, amelyek révén távoli hozzáférést szerezhetnek az eszközök felett.[119]

Az okos mobil eszközök esetében, tekintettel mobilis jellegükre, ahogy a neve is mutatja, gyakran csatlakoznak nyilvános Wi-Fi hálózatokhoz, amelyek nem megfelelően védettek. Ogundele Israel Oludayo és munkatársai rámutatnak, hogy a gyenge titkosítási protokollok, mint például a WEP, könnyen feltörhetők, és így a támadók lehallgathatják vagy módosíthatják az adatforgalmat. Ez különösen veszélyes lehet, ha a felhasználó érzékeny adatokat, például banki információkat továbbít.[120]

Az okos mobil eszközök egyre gyakrabban kapcsolódnak IoT rendszerekhez is, ami újabb biztonsági kihívásokat vet fel, ahogy az a fentiekben is részletezésre került. Külön kiemelendő ezen a téren az okos mobil eszközök alkalmazásai, amelyek rendkívül sokrétűek így sokrétű információt használnak fel, amely kapcsán a későbbiekben egy részletes elemzést mutatok be. Végül, de nem utolsósorban, az okos mobil eszközök fizikai elvesztése vagy ellopása is kockázatot jelent. Ha az eszközökön nincs megfelelő titkosítás vagy jelszavas védelem, akkor a támadók könnyen hozzáférhetnek a rajtuk tárolt adatokhoz. Ami különösen veszélyes a munkahelyi telefonok esetében, mert ha még konkrét érzékeny adat nem is szerepel az adott eszközben és alkalmazásaiban, az eszköz kapcsolatait, esetlegesen a névjegyzék alapján a felhasználó munkahelyi kapcsolati hálózatát is fel lehet deríteni, ami különösen a nemzetbiztonsági szolgálatok, illetve valamilyen fedést alkalmazó rendvédelmi munkatársak vagy felderítői tevékenységet végző katonák esetében aggályos.

[119] Esmeralda Kadëna, „Smartphone Security Threats", 2017.
[120] O. I. Oludayo és mtsai., „A review of smartphone security challenges and prevention", *International Research Journal of Innovations in Engineering and Technology* 7, sz. 5 (2023): 234235.

Összességében tehát az okos mobil eszközök technikai biztonsági kihívásai több rétegűek: az operációs rendszer sérülékenységeitől és a rosszindulatú szoftverektől kezdve a hálózati kapcsolatokon és IoT-integráción át egészen a fizikai biztonságig terjednek. Ezeknek a kockázatoknak a kezelése komplex, folyamatos odafigyelést és naprakész technológiai megoldásokat igényel.

2.3.3 Az okos otthoni eszközök és a privát szféra

Az okos otthoni eszközök, beleértve a biztonsági kamerákat, okos hangszórókat és okos TV-ket, lehetővé teszik az otthonok folyamatos megfigyelését.[121] Ezek az eszközök állandóan gyűjtik és elemzik a felhasználók viselkedésével kapcsolatos adatokat, ami súlyos privát szféra sérülését okozhatja. A privát szféra, vagy magánszféra védelme alapvető emberi jog, amelyet az Alaptörvény is *garantál, „Mindenkinek joga van a magán- és családi élet, az otthon, a kapcsolattartás és a jó hírnév tiszteletben tartásához.*"[122] Ez egy olyan szinten alapvető emberi jog, hogy többek között az Európai Unió Apajogi Chartája, és az Európai Emberi Jogi Egyezmény is deklarálja. Magyarországon a magánszférát a 2013. évi V. törvény a Polgári Törvénykönyvről 2:44. § (1) bekezdése határozza meg, amely alapján „*a magánélet, a magánlakás és a magántitok védelmét különösen sérti, aki más magánéletével, magánlakásával kapcsolatban illetéktelenül adatot gyűjt, más magánéletének vagy magánlakásának sérthetetlenségét illetéktelenül megsérti, más magántitkát illetéktelenül közérdekűvé teszi vagy felhasználja.*"[123] Megállapítható, hogy a magánszféra vagy más néven privát szféra az életnek azon része, amelyben egy személy úgymond elkülönülhet mindenkitől, kvázi egy olyan környezet betekinteni csak az érintett hozzájárulásával lehetséges.[124] Azért is fontos a privát szféra védelme a fentiek alapján mivel egy alapvető emberi jog, amelynek korlátozása összetett kérdéskör már csak állami szereplők szempontjából is, nem beszélve a különböző nem állami, szolgáltatók ilyen jellegű visszaéléseiről.

---

[121] Ştefan-Alexandru Catană és Andreea Barbu, „THE UNITED STATES OF AMERICA'S MOST VALUABLE BRANDS IN THE PERIOD 2021-2023", *Towards Increased Business Resilience:Facing Digital Opportunities and Challenges*, 2023, 169–74, https://doi.org/10.56177/11icmie2023.32.
[122] Magyarország Alaptörvénye VI Cikk (1)
[123] 2013. évi V. törvény a Polgári Törvénykönyvről 2:44. § (1)
[124] „A magánszféra védelmének büntetőjogon kívüli eszközrendszere – Ügyészek lapja", elérés 2025. május 24., https://ugyeszeklapja.hu/?p=3185.

A hangvezérelt virtuális asszisztensek, mint az Amazon Alexa vagy a Google Assistant, folyamatosan „hallgatóznak”, hogy felismerjék az aktiváló parancsszavakat, így potenciálisan minden beszélgetést rögzíthetnek.[125] Ezek az eszközök távolról is feltörhetők, lehetővé téve a hackerek számára, hogy lehallgassák a családi beszélgetéseket vagy megfigyeljék a mindennapi tevékenységeket, amely kiemelten veszélyes lehet védett személyek, vagy védett intézmények munkatársainak szempontjából.

Az okos otthoni eszközök használata során a felhasználók gyakran szembesülnek a biztonság és a kényelem közötti kompromisszummal. A kényelmi funkciók és a felhasználói élmény javítása érdekében a felhasználók hajlamosak elfogadni a magánélet bizonyos mértékű feladását, gyakran anélkül, hogy teljes mértékben tisztában lennének a kockázatokkal. Ez a jelenség, amelyet a szakirodalom "privacy paradox"-nak nevez, kihívást jelent az okos otthoni eszközök biztonságos használatában.[126]

A fizikai biztonság és a privát szféra összefonódása az okos otthoni eszközök esetében problematikus.[127] Ezek az eszközök növelhetik a fizikai biztonságot (például az okos biztonsági rendszerek révén) a különböző funkcióikkal, de új sebezhetőségeket is teremtenek. Az okos zárak, garázsajtók vagy riasztórendszerek feltörése lehetővé teheti a fizikai betörést, ami a hagyományos bűnelkövetés digitális térbe történő evolúciójaként is értelmezhető.

2.3.4 Okos városok és a megfigyelés problematikája

Az okos városok (smart cities) fejlesztésének mozgatórugója az urbanizációs kihívások kezelése és célja, hogy a digitális és információs technológiák integrálásával javítsák az életminőséget, a szolgáltatások hatékonyságát, illetve az erőforrás-felhasználást.[128] Kutatásom során ki kell emelni, hogy a smart city koncepcióval foglalkozok, nem az intelligent city-vel, amely bár mindkettő magyar nyelvben okos városként él,

---

[125] Gary Liu és Nathan Malkin, „PoPETs Proceedings — Effects of Privacy Permissions on User Choices in Voice Assistant App Stores”, elérés 2025. április 17., https://petsymposium.org/popets/2022/popets-2022-0116.php.

[126] „Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior - ScienceDirect”, elérés 2025. április 17., https://www.sciencedirect.com/science/article/abs/pii/S0167404818303031.

[127] Catană és Barbu, „THE UNITED STATES OF AMERICA’S MOST VALUABLE BRANDS IN THE PERIOD 2021-2023”.

[128] Dániel Tokody és Imre Mezei, „Okos, fenntartható és biztonságos városok”, *KÖZTES-EURÓPA Társadalomtudományi folyóirat* IX (2017. december 31.).

de fogalmilag más jelölnek. [129] A smart city esetében a technológia- és adatvezérelt fejlesztés általi a városi működés optimalizálizáció a cél, rövid és középtávú eredményekkel, míg az intelligent city esetében a tudásalapú gazdaságon, az emberi, társadalmi tőke fejlesztésén és kreatív ökoszisztémák kialakításán van a hangsúly és hosszabb távú eredményekkel számol. [130]

Az okos városok fejlesztése során a polgárok helyzetéről és tevékenységeiről több információhoz való hozzáférés, ami az okos városok kényelmi faktorának része, kompromittálhatja a magánéletet.[131] A városi környezetben elhelyezett szenzorok, kamerák és egyéb adatgyűjtő eszközök révén a polgárok élete folyamatosan monitorozhatóvá válik, ami adatvédelmi aggályokat vehet felt fel. Továbbá az okos városokban alkalmazott technológiák, mint például az arcfelismerő kamerák, helymeghatározó rendszerek és forgalomfigyelő szenzorok, lehetővé teszik a kormányzati és magánszereplők számára, hogy részletes információkat gyűjtsenek a polgárok mozgásáról, szokásairól és viselkedéséről. Ezek az adatok felhasználhatók a városi szolgáltatások optimalizálására, de visszaélésekre is alkalmat adhatnak, különösen az autoriter rendszerekben. Erre kiváló példa Kína Szociális Kredit Rendszere, amely egy kormány által vezérelt pontozási rendszerként viselkedésalapú jutalmazást és büntetést alkalmaz.[132] A rendszer a polgárok viselkedésének folyamatos megfigyelésén alapul, és jutalompontokat vagy büntetéseket oszt ki különböző társadalmi, gazdasági és politikai viselkedésformák szerint. Ez a rendszer kritikákat kapott a tömeges megfigyelés és a szólásszabadság korlátozása miatt.[133]

---

[129] Mahnoor Inam, „Smart City vs. Intelligent City: Key Differences and Similarities", *Minnovation Technologies* (blog), 2024. július 9., https://minnovation.com.au/smart-cities-2/smart-city-vs-intelligent-city-key-differences-and-similarities/.
[130] Messaoud Sadi és Siham Bestandji, „The Digital City, Smart City or Intelligent City?A Review of the Literature for the Choice of an Appropriate Terminology", *International Journal of Innovative Studies in Sociology and Humanities* 7 (2022. november), https://doi.org/10.20431/2456-4931.071116.
[131] Anisha V. Patel és mtsai., „Abstract B056: Inflammatory Dietary Pattern and Risk of Multiple Myeloma in US Black Women", *Cancer Epidemiology, Biomarkers & Prevention* 32, sz. 12_Supplement (2023. december 1.): B056–B056, https://doi.org/10.1158/1538-7755.DISP23-B056.
[132] Esther Nyandoya Azinga és M. Kamaara, „INFLUENCE OF LEADERSHIP STYLES ON EMPLOYEES TURNOVER IN THE INSURANCE INDUSTRY IN KENYA", 2019, https://www.semanticscholar.org/paper/INFLUENCE-OF-LEADERSHIP-STYLES-ON-EMPLOYEES-IN-THE-Azinga-Kamaara/28d5e124b25730f204a670d7838cffab25ad488e.
[133] Sipp D, „Millennium Ends Takeda's US Shopping Spree", *PubMed*, elérés 2025. május 2., https://pubmed.ncbi.nlm.nih.gov/18536661/.

Az okos városok fejlesztésében kulcsfontosságú a privát szféra védelme és a megfigyelés átláthatósága. Az olyan alapelvek, mint a "privacy by design" (beépített adatvédelem)[134] és a "privacy by default" (alapértelmezett adatvédelem)[135] alkalmazása segíthet az okos városok fejlesztése során felmerülő adatvédelmi kihívások kezelésében.[136]

2.3.5 Okos infrastruktúrák kiberbiztonsági kockázatai

„Az okos infrastruktúra olyan infrastruktúra, amely modern IKT rendszereket, például szenzortechnológiát és mesterséges intelligenciát használ autonóm folyamatirányításra. Ezek az infrastruktúrák technikai, társadalmi és zöld (ökológiai) elemekből állnak, amelyeket szorosan integrálnak a városi vagy országos környezetbe."[137] Az okos (társadalmi-technológiai) infrastruktúrák kiberbiztonsági kockázatai többrétűek. A hálózati komplexitás (ahol az egymással kölcsönhatásban lévő eszközök számának növekedésével bővül a potenciális támadási felület), az integráció összetettsége, az adatok heterogenitása (amikor a különböző típusú információk, köztük a bizalmas információk feldolgozása és tárolása vonzó célponttá teszi őket a kiberbűnözők számára), valamint a környezet dinamizmusa (az okos társadalmi-technológiai infrastruktúrák folyamatosan fejlődnek és alkalmazkodnak, ami megnehezíti biztonságuk biztosítását) mind kockázatot jelentenek.[138] A kritikus infrastruktúrák, mint például az energiahálózatok, vízellátás, közlekedési rendszerek és egészségügyi létesítmények, egyre inkább

[134] az adatvédelem és a magánszféra védelme a technológiák teljes életciklusa során, a tervezés korai szakaszától kezdve, a bevezetésen, használaton és végső selejtezésen át be van ágyazva

[135] a rendszerek és szolgáltatások alapbeállításai automatikusan a lehető legmagasabb szintű adatvédelmet biztosítják, anélkül, hogy a felhasználónak külön lépéseket kellene tennie ennek érdekében. Ez az elv szorosan kapcsolódik az adatminimalizálás, a célhoz kötöttség és a szükségesség elveihez: csak a legszükségesebb adatokat szabad gyűjteni, feldolgozni, tárolni és hozzáférhetővé tenni, és mindezt csak a meghatározott cél érdekében

[136] „Ježová", *Regional Law Review* (blog), elérés 2025. április 17., http://rlr.iup.rs/archives/year-2020/jezova/.

[137] *GRIN - Defining Smart Infrastructure. Smart Technical, Social, and Green Infrastructures in Cities and at the Federal Level and Beyond*, elérés 2025. április 17., https://www.grin.com/document/1190660.

[138] Zaimah Abdullah és mtsai., „CEO, CFO, and Board Attributes' Effect on Fair Value Agriculture Disclosure", *Cogent Business & Management* 10, sz. 3 (2023. december 11.): 2275867, https://doi.org/10.1080/23311975.2023.2275867.

függenek az információs és kommunikációs technológiáktól, ami növeli sebezhetőségüket a kibertámadásokkal szemben.[139] Az energiahálózatok digitalizációja és az intelligens mérőórák bevezetése új biztonsági kockázatokat teremtett.[140] A SWIFT rendszer elleni 2016-os támadás során 81 millió dollárt loptak el a Bangladesi Központi Banktól, ami a pénzügyi infrastruktúra kockázatait illusztrálja.[141] A WannaCry ransomware támadás 2017-ben súlyosan érintette a brit Nemzeti Egészségügyi Szolgálatot (NHS), ami jól példázza a kritikus infrastruktúrák sebezhetőségét.[142] A Colonial Pipeline ransomware támadás 2021-ben a legnagyobb amerikai üzemanyag-vezeték leállását okozta, ami több államban üzemanyaghiányhoz, pánikvásárláshoz és szövetségi vészhelyzet kihirdetéséhez vezetett.[143] De közelmúltból még meg lehet említeni a Schneider Electric elleni 2024-ben történt HellCat ransomware támadást is A Schneider Electric, mint vezető energia- és ipari automatizálási vállalat, 2024 novemberében harmadszor vált sikeres ransomware-támadás áldozatává 18 hónapon belül.[144]

2.3.6 Kibertámadások és kiberbűnözés

A NIST definíciója alapján *„kibertámadás minden olyan rosszindulatú tevékenység, amely információs rendszerek erőforrásainak vagy magának az információnak az összegyűjtésére, megzavarására, megtagadására, lerontására vagy megsemmisítésére irányul.”*[145] A fogalomból is látszik, hogy a kibertámadások egy széles kört felölelő

[139] Nannan Cui és mtsai., „Quality Assessment of TikTok as a Source of Information About Mitral Valve Regurgitation in China: Cross-Sectional Study”, *Journal of Medical Internet Research* 26 (2024. augusztus 20.): e55403, https://doi.org/10.2196/55403.
[140] R. Herzlinger, „A Managed Care Memoir: A Physician’s Whistle-Stop Journey”, 2004, https://www.semanticscholar.org/paper/A-Managed-Care-Memoir%3A-A-Physician's-Whistle-Stop-Herzlinger/37d127bb2a80fe299c2a6d5f13b8d9287fd3c74f.
[141] Tamara Teplova, Mariya Gubareva, és Nikolai Kudriavtsev, „Social Sentiment and Exchange-Specific Liquidity at a Eurasian Stock Exchange Outside of US Market Hours”, *Eurasian Economic Review* 13, sz. 3–4 (2023. december): 753–802, https://doi.org/10.1007/s40822-023-00245-9.
[142] Patrick Callahan és mtsai., „1086-P: Humanistic Burden of Type 1 Diabetes in U.S. Adults across Different Age Cohorts—A Qualitative Interview Study”, *Diabetes* 72, sz. Supplement_1 (2023. június 20.): 1086-P, https://doi.org/10.2337/db23-1086-P.
[143] Raphael Nyonyoh, „Ransomware and the Vulnerability of Critical Infrastructure: A National Security and Economic Analysis”, elérés 2025. május 25., https://journalajeba.com/index.php/AJEBA/article/view/1759.
[144] Anna Ribeiro, „Resecurity Warns of Increased Cyber Threats to Energy and Nuclear Facilities from Hacktivists and Nation-States”, *Industrial Cyber* (blog), 2025. április 18., https://industrialcyber.co/utilities-energy-power-water-waste/resecurity-warns-of-increased-cyber-threats-to-energy-and-nuclear-facilities-from-hacktivists-and-nation-states/.
[145] CSRC Content Editor, „Cyber Attack - Glossary | CSRC”, elérés 2025. május 25., https://csrc.nist.gov/glossary/term/cyber_attack.

rosszindulatú műveletek összessége, amely kapcsán megjegyzendő, hogy ezek folyamatosan változnak és alkalmazkodnak az ellenintézkedésekhez, úgymond az adaptációjuk és evolúciójuk folyamatos. A kibertámadások osztályozása több szempont szerint is lehetséges, a legáltalánosabb megközelítések a támadási vektorok, a célpontok típusai, a működési és információs hatások, valamint a védekezési stratégiák szerinti kategorizálásra épülnek [146] A következőkben a támadási vektorok alapján történő rendszerzés szerint mutatom be a kibertámadásokat, tekintettel arra, hogy az előbbiekben és a későbbiekben is a célpontok, hatások és védekezési stratégiák sokkal részletesebben lesznek kifejtve. A támadási vektorok szerinti osztályozás megkülönböztetünk:

1. Klasszikus támadási vektorok

- Rosszindulatú szoftverek (malware): A rosszindulatú szoftvereket, amelyek közé sorolhatók a vírusok, férgek, trójai programok, zsarolóvírusok (ransomware), kémprogramok (spyware) és reklámprogramok (adware) Ezek a kódok gyakran álcázott fájlokként vagy e-mail mellékletekkel kerülnek terjesztésre, és céljuk a rendszerek megbénítása vagy adatokhoz való jogosulatlan hozzáférés. [147]
- Social engineering: Az emberi tényező kihasználása, például adathalászat (phishing), vishing (hangalapú adathalászat), smishing (SMS-alapú adathalászat), pretexting, vagyis hamis indokkal történő adatkérés.[148]
- Túlterheléses támadások (Denial-of-Service (DoS) és Distributed Denial-of-Service (DDoS)): A hálózati erőforrások túlterhelésén keresztül akadályozzák szolgáltatások normál működését, gyakran botnethálózatok segítségével.[149]
- Közbeékelődéses támadás (Man-in-the-middle (MITM)): A támadó közvetítőként lép fel két fél között, például hálózati forgalom lehallgatásával, e-mail eltérítéssel vagy Wi-Fi lehallgatással, DNS spoofinggal.[150]

2. További, kiemelt aktuális támadási vektorok

A legújabb tudományos taxonómiák (pl. AVOIDIT, további támadási vektorokat különítenek el:

---

[146] „(PDF) AVOIDIT: A Cyber Attack Taxonomy", elérés 2025. április 17., https://www.researchgate.net/publication/229020163_AVOIDIT_A_Cyber_Attack_Taxonomy.
[147] „Mi az a kibertámadás? | Microsoft Biztonság", elérés 2025. április 17., https://www.microsoft.com/hu-hu/security/business/security-101/what-is-a-cyberattack.
[148] „(PDF) AVOIDIT: A Cyber Attack Taxonomy".
[149] U.o.
[150] „(PDF) AVOIDIT: A Cyber Attack Taxonomy".

- Rendszer- és alkalmazáskonfigurációs hibák (Misconfiguration): Hibás vagy hiányos beállítások (pl. nyitott portok, alapértelmezett jelszavak) kihasználása a rendszerbe való bejutásra.[151]

- Operációs rendszer maghibák (Kernel flaw: Az operációs rendszer kernelében lévő sérülékenységek kihasználása, amelyek magas szintű jogosultságot adhatnak a támadónak.[152]

- Buffer overflow: Olyan programozási hiba, amikor a támadó több adatot ír egy memóriaterületre, mint amennyit az képes kezelni, így tetszőleges kódot futtathat.[153]

- Elégtelen bemeneti ellenőrzés (Insufficient input validation): A szoftver nem ellenőrzi megfelelően a felhasználói bemenetet, így a támadó például SQL-injekcióval vagy XSS-sel (cross-site scripting) támadhat.

- Fileless malware: Olyan rosszindulatú szoftver, amely nem hagy nyomot a fájlrendszerben, hanem közvetlenül a memóriában fut, így nehezebben észlelhető.

- Nulladik napi támadás (Zero-day exploit): Olyan támadás, amely egy eddig ismeretlen vagy be nem foltozott sérülékenységet használ ki, mielőtt a gyártó javítást adna ki rá.

- Adathalászat speciális formái: Például spear phishing (célzott adathalászat), whaling (magas rangú vezetők elleni adathalászat). Jelen felsorolás nem teljes körű, ahány platform, szinte annyi típusú adahalászati módszer létezik. De kutatásom szempontjából még meg kell említenem a QR-kód alapú adathalászatot is (quishing vagy QR phishing). A támadók rosszindulatú QR-kódokat használnak, hogy a felhasználó azt beolvasva egy káros weboldalra jut, ahol a támadók adatokat próbálnak kicsalni, vagy rosszindulatú programot juttatnak az eszközére.[154] Webes támadások: Webalkalmazások és API-k sebezhetőségeit kihasználó támadások, például session hijacking, CSRF (cross-site request forgery)

---

[151] U.o.
[152] Fadi Mohsen és mtsai., „A Taxonomy for Large-Scale Cyber Security Attacks - EUDL", elérés 2025. május 2., https://eudl.eu/doi/10.4108/eai.2-3-2022.173548.
[153] Mohsen és mtsai.
[154] Timothy Vidas és mtsai., „QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks", elérés 2025. május 25., https://doi.org/10.1007/978-3-642-41320-9_4.

1. ábra Kiemelt támadási vektorok (saját szerkesztés, napkin.ai)

A kibertámadások vektorai tehát jóval túlmutatnak a klasszikus malware és adathalász támadásokon. A tudományos szakirodalom kiemeli a konfigurációs hibák, kernelhibák, memóriakezelési hibák, fileless malware, zero-day exploitok, webes sebezhetőségek, beszállítói lánc támadások és fizikai támadások jelentőségét is A kiberbűnözés gazdasági károkat okoz az információs társadalmon belül. Egyrészről közvetlen pénzügyi veszteséget okozhat a célpontok részére, beleértve az eltulajdonított pénzeszközöket, a váltságdíj-kifizetéseket és a helyreállítási költségeket.[155] Továbbá a kiberbűnözés közvetett gazdasági hatásai közé tartozik a csökkent termelékenység, a hírnév károsodása és az ügyfelek elvesztése.[156] De álláspontom alapján az kiberbűnözés felderítésének és az elhárítási technológiának a fejlesztésére szánt költségvetés is részben

[155] World Economic Forum, *Economic Impact of Global Cybercrime* (Geneva: World Economic Forum, 2023).
[156] Ponemon Institute, *Cost of a Data Breach Report* (Traverse City, MI: Ponemon Institute, 2024).

idesorolható. A Cybersecurity Ventures 2025-re a kiberbűnözés globális éves költsége 10,5 billió dollárra számította, ami növekedést jelent a 2015-ös 3 billió dollárhoz képest.[157] A globális kiberbiztonsági védelemre fordított kiadások 2022-ben meghaladták már a 150 milliárd dollárt.[158]

2.3.7 A biometrikus adatok kezelésének kihívásai

Jelen rész kiemelten releváns az értekezésem szempontjából és nem csak az információs társadalmat érintő kihívások tekintetében. Kutatásaim során az egyik legfontosabb kérdéskör az okos (mobil) eszközök, mint személyazonosításra, illetve személyi hitelesítésre alkalmas eszközök és technológia lehetőségei, kihívásai és azok esetleges társadalmi elfogadottsága. Ehhez kapcsolódóan a biometrikus adatok kezelése kulcsfontosságú kérdéskör, mivel a későbbiekben vizsgált okos eszközök a fenti „know-how"-ra alkalmas applikációi sok esetben biometrikus adatokat használhatnak, tárolhatnak az azonosításhoz vagy a hitelesítéshez. Ennek részleteit külön fejezetben tárgyalom. A biometrikus adatok – például ujjlenyomatok, arcfelismerés, írisz-szkennelés és hangminták – használata egyre elterjedtebb az azonosításban és a hitelesítésben, ami sajátos adatbiztonsági kihívásokat jelent, mivel ezen adatok személyes jellemzői egyediek és szinte megváltoztathatatlanok, ezzel növelve ezen adatok érzékenységét. Egy ellopott jelszó megváltoztatható, azonban egy kompromittált ujjlenyomat vagy arcképet nem igazán lehet módosítani.[159] Azonban itt emelném ki, hogy a deepfake és más technológiák fejlődésével lehetővé válik a biometrikus adatok manipulálása, ami új biztonsági kockázatokat teremt.[160] A biometrikus azonosítás biztonságába vetett túlzott bizalom veszélyes lehet, mivel a biometrikus rendszerek sem tökéletesen biztonságosak, és az új technológiák révén egyre több lehetőség nyílik a biometrikus adatok hamisítására vagy megszerzésére. Az általam készített interjú során az IT biztonság területén több évtizedes tapasztalattal rendelkező szakértő elmondása szerint sokszor ezek a technológiák csak a biztonság hamis illúzióját keltik.

---

[157] Ventures, *Global Cybercrime Damage Report*.
[158] Gartner, *Gartner Forecasts Worldwide Connected Devices to Total 41.6 Billion in 2025*.
[159] International Biometrics és Identity Association, *Biometric Data Security* (Washington, DC: International Biometrics and Identity Association, 2024).
[160] Péter Csizmadia, „Aging and Digitalization: Trends and Challenges", *Demography* 65, sz. 2–3 (2022): 219–40, https://doi.org/10.21543/dem.65.2-3.3.

Az arcfelismerő rendszerek és más biometrikus megfigyelőrendszerek terjedése növeli a tömeges megfigyelés lehetőségét.[161] A biometrikus adatok központi tárolása pedig vonzó célponttá teszi ezeket az adatbázisokat a kibertámadások számára. Az indiai Aadhaar rendszer 2023-as adatszivárgása 1,1 milliárd felhasználó biometrikus adatait is érintette.[162] Az Aadhaar-rendszer adatszivárgása releváns a kutatásom szempontjából, mivel rámutat arra, hogy a technológiai innovációk mellett elengedhetetlen a megfelelő jogi, szervezeti és technológiai védelem, valamint a felhasználói bizalom fenntartása.

A biometrikus adatok kezelésének szabályozása kritikus fontosságú a visszaélések megelőzése érdekében. A GDPR (az Európai Unió Általános Adatvédelmi Rendelete) és más adatvédelmi szabályozások külön kategóriaként kezelik a biometrikus adatokat, és szigorú feltételeket szabnak azok gyűjtésére és feldolgozására vonatkozóan. Azonban a szabályozási keretrendszerek gyakran lemaradnak a technológiai fejlődéshez képest, ami szabályozási vákuumot eredményezhet.

2.3.8 A mesterséges intelligencia és automatizáció

A mesterséges intelligencia és a gépi tanulási algoritmusok egyre fontosabbá válnak az információs társadalomban, azonban számos kihívás is jelentkezik velük kapcsolatban. A terület teljes és átfogó ismertetésére nem törekszem az értekezés során, figyelemmel tartalmi korlátokra, továbbá arra, hogy a terület kutatása külön disszertációs tanulmányt érdemel meg. E kategóriába az alábbi problémakörök tartoznak a teljesség igénye nélkül:

- A gépi tanulási algoritmusok átveszik és reprodukálják a képzési adatokban rejlő torzításokat és előítéleteket.[163]
- Az algoritmikus döntések torzítást mutathatnak bizonyos csoportokkal szemben, ahogy az látható a hitelbírálatoknál, az álláskeresésnél vagy a bűnügyi kockázatértékelésnél.[164]

---

[161] Semantic Scholar, *Digital Communities for Seniors Utilizing Human-Centric Technologies for an Advanced Society* (Seattle: Allen Institute for AI, 2023).
[162] Privacy International, *Investigation into Aadhaar Data Breach* (London: Privacy International, 2023).
[163] A.I.Now Institute, *Discriminatory Bias in Artificial Intelligence Systems* (New York: AI Now Institute, 2022).
[164] ProPublica, *Machine Bias* (New York: ProPublica, 2023).

- A komplex gépi tanulási algoritmusok, különösen a mély neurális hálózatok, gyakran átláthatatlan egységekként működnek, ami megnehezíti az átláthatóság biztosítását és a döntéshozatali folyamat magyarázatát.[165]
- Az algoritmusok által okozott károkért való felelősség továbbra is tisztázatlan – hogy az a fejlesztőt, az üzemeltetőt vagy a felhasználót terheli-e.[166]
- A mély tanulás fejlődése elősegítette a deepfake-ek és más szintetikus média előállítását, ami megnehezíti a valódi és a gyártott anyagok közötti különbségtételt[167] , így a deepfake technológia elterjedése fokozhatja a digitális média iránti szkepticizmust, ami az "általános hitetlenség" állapotához vezethet.[168]

Az MIT Technology Review 2024-es cikke szerint több kutatási kezdeményezés célja az AI-torzítások enyhítése, bár hatékony megoldások még nem állnak rendelkezésre.[169] A fentieken túlmenően még meg kell említeni az MI kapcsán a különböző szabályozási kihívásokat is. Amit nehezít, hogy a felelős döntéshozók az emberi jogok, az adatbiztonság, illetve az innováció előtérbe helyezése között lavíroznak, senki nem akar technológiai hátrányba kerülni, azonban az autoriter rezsimekkel ellentétben a fejlődés nem gátolhatja szabadságjogokat így az AI-technológiák szabályozásakor egy technológia-semleges keretrendszer létrehozása a cél, ami kihívás.[170] Az EU AI Act kockázatalapú megközelítést alkalmaz, különböző AI-alkalmazásokat osztályozva kockázati szintjük alapján.[171]

Az autonóm rendszerek, például önvezető autók, drónok és robotok sajátos biztonsági sebezhetőségeket mutatnak, amelyek egy része átfedésben a mesterséges intelligenciánál ismertetekkel, például az esetlegesen okozott károkért való felelősség kérdése. De jelen rendszerek kapcsán ki kell emelni a fizikai térben megvalósuló kockázatokat, hiszen egy ilyen rendszernek a valóságban is van egy outputja, így ott is tud akár fizikai

---

[165] *Standards for Explainable Artificial Intelligence* (Piscataway, NJ: IEEE, 2024).
[166] European Commission, *Proposal for the EU AI Liability Directive* (Brussels: European Commission, 2023).
[167] Stanford Internet Observatory, *Deepfakes and Disinformation* (Stanford, CA: Stanford University, 2023).
[168] Reuters Institute, *Digital News Report* (Oxford: University of Oxford, 2023).
[169] M.I.T.Technology Review, *Strategies for Mitigating AI Bias* (Cambridge, MA: MIT Technology Review, 2024).
[170] „The State of Implementation of the OECD AI Principles Four Years On", OECD, 2023. október 26., https://www.oecd.org/en/publications/the-state-of-implementation-of-the-oecd-ai-principles-four-years-on_835641c9-en.html.
[171] European Commission, *AI Act Risk Categories* (Brussels: European Commission, 2023).

kárt okozni egy meghibásodás esetén.[172] És mivel e rendszerek jellemzően a fizikai térben operálnak az innen történő befolyásolásuk is megvalósulhat, akár érzékelők megtévesztésével.[173]

2.3.9 Decentralizált technológiák és kriptográfiai akadályok

A decentralizált technológiák, köztük a blokklánc, a decentralizált autonóm szervezetek (DAO-k) és az elosztott főkönyvek (DLT), forradalmasították az adatkezelést és a tranzakciós folyamatokat. Ezek a rendszerek a decentralizáció, az adatok megváltoztathatatlansága és a kriptográfiai biztonság előnyeit hozták magukkal, azonban számos kihívás is felmerül. A tudományos szakirodalom a főbb problémák közé sorolja a kriptográfiai korlátokat, a konszenzusmechanizmusok sebezhetőségeit, a smart contractok hibái, valamint a jogi problematikát. A decentralizált rendszerek alapvető biztonsági elemei a kriptográfiai algoritmusok, amelyek az adatok integritását és titkosságát biztosítják. A nyilvános kulcsú infrastruktúrák (PKI) és a hash-függvények azonban számos kihívással szembesülnek.

Blokklánc (block-chain) technológia kihívásai

A blokklánc egy olyan decentralizált digitális főkönyv, amelyben a tranzakciós adatokat minden résztvevő (node) helyi másolatban tárolja. Nincs központi szerver vagy felügyeleti entitás, a tranzakciók nyilvánosan vagy engedélyezett környezetben osztoznak a hálózat tagjai A blokkláncok transzparens természete ütközik az olyan adatvédelmi előírásokkal, mint az általános adatvédelmi rendelet (GDPR). A zero-knowledge proof (ZKP) és a homomorf titkosítás lehetőséget kínál a tranzakciók anonimizálására, azonban ezek a módszerek számítási erőforrásokat igényelnek, ami korlátozza skálázhatóságukat. Emellett a ZKP-k komplex implementációja gyakran hibákhoz vezet, amelyek kihasználhatók.[174] A blokkláncok transzparens jellege ütközik az EU GDPR rendelkezéseivel, amelyek szerint a felhasználóknak joguk van adataik

[172] *Report on Autonomous Vehicle Safety* (Washington, DC: U.S. Department of Transportation, 2023).
[173] ENISA: "Guidelines for the Security of Autonomous Systems." 2023.
[174] McCLARKIN Emma, „JELENTÉS a blokkláncról: előretekintő kereskedelempolitika | A8-0407/2018 | Európai Parlament", elérés 2025. május 2., https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_HU.html.

törlésére ("right to be forgotten"). A blokkláncok megváltoztathatatlansága lehetetlenné teszi ezt, ami jogi konfliktusokhoz vezet.[175] A kutatások olyan megoldásokat javasolnak, mint az off-chain adattárolás vagy a merkle-fák használata bizalmas adatok anonimizálására. De maga a blokklánc technológia kutatásom szempontjából rendkívül releváns, hiszen alkalmas lehet a személyazonosításra, illetve hitelesítésre alkalmazott okos eszközök applikációi esetében nagyobb fokú kriptográfiát alkalmazni, mely lehetőségeire és esetleges kihívásaira a későbbi fejezetekben térek majd ki.

Smart contract

A smart contract-ok önállóan végrehajtható kódjai gyakran tartalmaznak hibákat, amelyek pénzügyi veszteségekhez vezetnek. A reentrancy támadások (pl. a DAO incidens 2016-ban) és az integer overflow/underflow hibák a leggyakoribbak.[176] A formális verifikáció és az automatikus kódelemzés eszközei (pl. MythX, Oyente) fejlesztése ellenére a smart contract-ok biztonsága továbbra is kritikus probléma marad.[177]

Decentralizált tároló rendszerek

A decentralizált tároló rendszerek (pl. IPFS) ugyan növelik az adatállóságot, de a Sybil-támadások (több hamis identitás létrehozása) és az adatcenzúra kockázatait is magukban hordozzák.[178] Emellett a fizikai infrastruktúra decentralizációja nem zárja ki a geográfiai koncentráció által eredményezett sebezhetőségeket, mint azt az Ethereum Classic 51%-os támadása demonstrálta.[179]

A kriptovaluták és a digitális pénzügyek veszélyei

A kriptovaluták és digitális pénzügyi rendszerek növekvő elterjedése számos egyedi kockázattal jár, amelyek a hagyományos pénzügyi rendszerektől eltérő kihívások elé állítják a felhasználókat, befektetőket és döntéshozókat. A kriptovaluták áringadozása

---

[175] Huszár V., „A decentralizáció és a blokklánc-technológia lehetőségei a katonai szférában", *Real.MTA Könyvtár*, 2020, https://doi.org/10.17625/real.mtak.109337.
[176] O. Rikken, M. Janssen, és Z. Kwee, „Governance Challenges of Blockchain and Decentralized Autonomous Organizations", *Information Polity* 24, sz. 4 (2019): 397-417, https://doi.org/10.3233/IP-190154.
[177] Z. Qadir, „Blockchain Security: Research Challenges and Opportunities", *LinkedIn*, 2024, https://www.linkedin.com/pulse/blockchain-security-research-challenges-opportunities-zohaib-qadir-x4h7f.
[178] Kovács Tamás, „Blokklánc-technológia mint a korrupció elleni küzdelem lehetséges eszköze", *Themis*, 2020, 92–128.
[179] Rikken, Janssen, és Kwee, „Governance Challenges of Blockchain and Decentralized Autonomous Organizations".

központi problémát jelent. A Bitcoin például történelmi csúcspontjait követően akár 70%-os zuhanásokon is keresztülment rövid időn belül, ami a piac spekulatív jellegét és az értékállóság hiányát hangsúlyozza. Ez nem csupán egyéni befektetők számára kockázatos, hanem destabilizáló hatással lehet a globális pénzügyi rendszerekre is.[180] Továbbá a kriptovaluták anonimitása és decentralizált jellege lehetővé teszi olyan illegális tevékenységek finanszírozását, mint a pénzmosás vagy a terrorizmus támogatása.[181] A blokklánc-technológia ugyan transzparens, de a felhasználók személyazonosságának rejtett volta megnehezíti a nyomozást.[182]

A digitális pénzügyi eszközökre vonatkozó szabályozási keretek még fejlődőben vannak. Az Európai Unióban például a GDPR előírásai ütköznek a blokkláncok megváltoztathatatlanságával, Emellett a központosított tőzsdék (pl. Mt. Gox 2014-es csődje, ahol 850 000 Bitcoin veszett el) gyakran működnek átláthatatlanul, és a befektetők nem élveznek hagyományos jogi védelmet [183] [184]

2.3.10 Kihívások a kvantumszámítástechnikában

A kvantumszámítógépek fejlődése kihívásokat jelent a meglévő kriptográfiai rendszerek számára. A kvantumszámítógép olyan számítógépes rendszer, amely a kvantummechanika elveit (pl. szuperpozíció, összefonódás, dekoherencia) használja információfeldolgozásra. A klasszikus számítógépekhez képest a kvantumszámítógépek kibővített számítási kapacitást biztosítanak exponenciális mértékben, azáltal, hogy a kvantumbitek (qubitek) szuperpozícióját és összefonódását kihasználják.[185] Ezen technológia térnyerésével a széles körben használt kriptográfiai technikák, különösen az RSA és az elliptikus görbe titkosítás, veszélyben vannak, mivel ezek feltörésére a kvantumszámítógép a megnövekedett kapacitása miatt már alkalmas.[186] Azonban jelenleg a posztkvantum algoritmusok érettsége még korlátozott, és további kutatást igényel.[187]

---

[180] International Monetary Fund, *Cryptocurrency Assets and Financial Stability* (Washington, DC: International Monetary Fund, 2023).
[181] McCLARKIN, „JELENTÉS a blokkláncról".
[182] Financial Action Task Force, *Indicators of Red Flags in Virtual Assets* (Paris: FATF, 2024).
[183] Bank International Settlements, *Regulatory Framework for Crypto-Assets* (Basel: Bank for International Settlements, 2023).
[184] Mt Gox, *Bankruptcy Proceedings of Mt. Gox, 2014-2022* (Tokyo: Tokyo District Court, 2022).
[185] „Quantum Computing Explained", *NIST*, 2025. március 18., https://www.nist.gov/quantum-information-science/quantum-computing-explained.
[186] National Institute Standards és Technology, *Report on Post-Quantum Cryptography* (Gaithersburg, MD: NIST, 2023).
[187] *Standards for Quantum-Safe Cryptography* (Sophia Antipolis: ETSI, 2023).

A kvantumszámítógépekkel felmerül a visszamenőleges dekódolás kockázata is, mert így az esetleges támadásokban az ellenérdekelt felek összegyűjthetik a titkosított adatokat, hogy azokat később kvantumszámítógépekkel fejtsék meg.[188] A NIST (Nemzeti Szabványügyi és Technológiai Intézet) 2016-ban kezdeményezte a posztkvantum-kriptográfiai algoritmusok szabványosítási folyamatát. 2022-ben a CRYSTALS-Kyber algoritmust választották a kvantumrezisztens kulcscseréhez[189] , ami egy rácson alapuló kriptográfiai algoritmus.[190] További kvantumrezisztens technológiai megoldás még a hash-alapú digitális aláírási rendszerek, mint a SPHINCS+[191], vagy a kód-alapú kriptográfiai rendszerek, mint például a Classic McEliece [192]

A kvantumtechnológia kapcsán még kiemelendő, a kvantumkulcs-elosztás és a kvantumkriptográfia, ami új lehetőségeket kínál a biztonságos kommunikációhoz, mivel lehetővé teszi egy megosztott titkos kulcs létrehozását két fél között, amely elméletileg sebezhetetlenné teszi minden típusú támadással szemben, beleértve a kvantumszámítógépekről érkező támadásokat is.[193] Azonban a kvantumkulcs-elosztás alkalmazása több akadályba ütközik, például távolsági korlátok, berendezési költségek és fizikai támadásokkal szembeni érzékenység.[194] A kvantumtechnológia, és a posztkvantum titkosítás kiemelt kérdéskor értekezésem szempontjából. A kvantumszámítástechnikával kapcsolatban a későbbi fejezetek során részleteiben jobban fogok foglalkozni, elöljáróban szeretném kifejezni, hogy ez egy kétélű penge, amely komoly lehetőségeket és kockázatokat rejt magában.

2.4 Humán forrású kihívások

Jelen kategória során a fentiekkel ellentétben nem a technológia, ami középpontba került, hanem az ember maga tekintettel arra, hogy maga az információs társadalom egyik központi eleme a technológián túlmenően a humánum, illetve ennek a kettőnek a kapcsolata. Alapvetően az egyes emberekhez köthető kihívások kapcsán meg kell jegyezni, hogy jelen felosztás a könnyebb érthetőséget szolgálja, azonban az egyes

[188] National Security Agency, *Frequently Asked Questions on Quantum Computing* (Fort Meade, MD: National Security Agency, 2023).
[189] *Standardization of Post-Quantum Cryptography* (Gaithersburg, MD: NIST, 2022).
[190] Standards és Technology, *Special Publication: CRYSTALS-Kyber Implementation*.
[191] S.P.H.I.N.C.S.+ Team, *Hash-based Signatures* (SPHINCS+ Team, 2022).
[192] McEliece Team, *Traditional McEliece Specification* (McEliece Team, 2023).
[193] *Standards for Quantum Key Distribution* (Piscataway, NJ: IEEE, 2024).
[194] *Security of QKD Implementation* (Sophia Antipolis: ETSI, 2023).

kihívások több esetben is együttesen, vagy más technológiai kockázatokkal jelentkeznek együtt, hiszen a maga a jogi, vagy adatvédelmi aspektus az ember irányából (mint jogalany vagy felhasználó) vizsgálja különböző technológiákat, de ezek mindig valamilyen technikai keretrendszert vizsgálnak, amin belül értékelhető a humánum szerepe.

2.4.1 Társadalmi-gazdasági kihívások

Az információs társadalom a társadalmi struktúrákra, gazdasági rendszerekre és kulturális tendenciákra gyakorolt hatásaiból eredhetnek kihívások. Ilyen példaképpen a digitális szakadék is.

A technológiai fejlődés egyenlőtlen eloszlása súlyosbítja a társadalmi-gazdasági egyenlőtlenségeket a világban, megfigyelhető a statisztikai adatok alapján is, hogy a fejlett országokban az információhoz való korlátlan hozzáférés kontrasztban áll a fejlődő országok infrastrukturális hiányosságaival.[195] A világ népességének 37%-a továbbra sem rendelkezik internetkapcsolattal, különösen Afrikában és Dél-Ázsiában.[196] A munkaerőpiac átalakulóban van, az automatizálás és a mesterséges intelligencia potenciálisan 800 millió munkahely megszűnéséhez vezethet 2030-ig, miközben új szakmák jelennek meg, például adatelemzők és kiberbiztonsági szakértők.[197] Itt ki kell emelni, hogy tipikusan olyan munkakörök keletkeznek, amihez szükséges az innováció és digitális tudás, míg azok a munkák, amely a fejlődő országokban végeznek, egyre inkább kiszorítja a mesterséges intelligencia, robotizáció és automatizáció.

2.4.2 Jogi, adatvédelmi kihívások

A jogi aggályok az információs társadalmon belüli irányításra, szabályozásra és a politikai rendszerekre gyakorolt hatásra vonatkoznak. A technológiai fejlődés gyakran megelőzi a jogi szabályozást, szabályozási bizonytalanságot eredményezve. Az Általános Adatvédelmi Rendelet (GDPR) szabályozza a személyes adatok kezelését az

[195] U.N.E.S.C.O., *Bridging the Digital Divide* (Paris: UNESCO, 2021).
[196] International Telecommunication Union, *Global Internet Penetration Rates* (Geneva: ITU, 2024).
[197] Bank World, *Future of Work Report* (Washington, DC: World Bank, 2023).

EU-n belül, míg a kaliforniai fogyasztói adatvédelmi törvény (CCPA) hasonló funkciókat tölt be az USA-ban.[198] [199] Egyes technológiai fejlődések megelőzik a szabályozási rendszereket, ahogy az jól látható volt a kriptovaluták esetében is ezzel egy szabályozási vákuumot létrehozva. Továbbá egyes technológiák, mint a mesterséges intelligenciáról és az okos eszközök szóló résznél írtam lehetővé teszik az egyének viselkedésének megfigyelését és szabályozását.[200] Ehhez kapcsolódik, hogy az információs korban az összegyűjtött és feldolgozott adatok mennyisége folyamatosan növekszik, ami számos adatvédelmi problémát vet fel. A nagy adathalmazok (Big Data) gyűjtése és elemzése által, az adatok összekapcsolásával a személyek azonosíthatók még anonimizált információkból is.[201] Egy nagy mennyiségű adat lehetővé teszi a profilalkotást és a viselkedés előrejelzését, ami potenciálisan visszaélésekhez vezethet.[202]

Az adatok nemzetközi mozgása problémákat vet fel a területi joghatósággal kapcsolatban. A GDPR területen kívüli hatása ezt a kérdést kívánja kezelni.[203] A különböző szabályozási keretrendszerek harmonizációja: A régiók közötti eltérő adatvédelmi megközelítések (EU, USA, Kína) kihívásokat jelentenek a multinacionális vállalatok számára.[204] Kihívások a végrehajtásban: Az adatvédelmi szabályozások végrehajtása gyakran akadályokba ütközik, különösen a nagyobb vállalatok és a határokon átnyúló adatfeldolgozás esetén.[205] Az államok szempontjából egyre nagyobb éget, kap az információs korban a digitális szuverenitás kérdésköre. A digitális szuverenitás (digital sovereignty) olyan fogalom, amely egy állam vagy szervezet képességére utal, hogy teljes ellenőrzést gyakoroljon digitális adatai, infrastruktúrái és technológiái felett, függetlenül külső befolyástól. A digitális szuverenitás fogalma a nemzetközi politika és technológiai innováció metszeteként is értelmezhető.[206]

---

[198] General Data Protection Regulation, *Official Journal of the European Union* (Brussels: European Union, 2018).
[199] *California Consumer Privacy Act (CCPA* (Sacramento: State of California, 2020).
[200] Human Rights Watch, *Surveillance in China* (New York: Human Rights Watch, 2024).
[201] *Challenges of Privacy in Big Data* (Piscataway, NJ: IEEE, 2023).
[202] *Opinion on Profiling* (Brussels: EDPS, 2022).
[203] „Article 3 GDPR", GDPRhub, elérés 2025. május 3., https://gdprhub.eu/index.php?title=Article_3_GDPR.
[204] World Economic Forum, *Global Data Governance* (Geneva: World Economic Forum, 2024).
[205] European Data Protection Board, *Guidelines on Enforcement* (Brussels: European Data Protection Board, 2023).
[206] Inc, „A digitális szuverenitás ége", *ICT Global*, 2023, https://ictglobal.hu/rovid-hirek/a-digitalis-szuverenitas-jelentosege/.

2.4.3 Hitelesség kérdésköre és az információs műveletek, álhírek terjedése

Az információs társadalomban megjelenő egyik nagyobb kihívás az információs túlterhelés (information overload) jelensége, amely megnehezíti a releváns és hiteles információk azonosítását. Ez azt jelenti, hogy exponenciálisan növekszik a rendelkezésre álló információ mennyisége, amit az egyének képtelenek hatékonyan feldolgozni és értékelni. Az információs túlterhelés kognitív és pszichológiai következményekkel jár. A folyamatos információáradat figyelemeltereléshez, döntésképtelenséghez, szorongáshoz és stresszhez vezethet.[207] Ez a jelenség befolyásolja az egyének információfogyasztási szokásait és döntéshozatali képességeit, ami hatással lehet a társadalmi és politikai részvételre is. Az egyszerűsítő heurisztikákat (pl. a legkönnyebben hozzáférhető információk elfogadása) és kognitív rövidítéseket (pl. forrás megbízhatóságának intuitív felmérése) alkalmaznak. Ez a jelenség a korlátozott információfeldolgozási kapacitásból ered, amelyet a Goette, Han és Leung (2019, 2024) kísérletei igazolnak. A kutatás szerint, amikor az információfeldolgozás nehézsége nő (pl. a korábbi információk eltűnése a képernyőről), a résztvevők kevésbé reagálnak a téves információkra.[208] A megerősítési torzítás (confirmation bias) különösen problematikus, mivel az emberek hajlamosak azokat az információkat keresni és elfogadni, amelyek megerősítik a meglévő nézeteiket, és figyelmen kívül hagyni az ellentmondó információkat.[209] Az információs túlterhelés kezelése kritikus fontosságú egyéni készség, a digitális írástudás fejlesztése, a kritikus gondolkodás és az információforrások értékelésének képessége segíthet az egyéneknek megkülönböztetni a hiteles információkat a félretájékoztatástól és a különböző kognitív térben zajló információs műveltektől. A csoportgondolkodás és a társadalmi konformitás szintén hozzájárulhat az álhírek terjedéséhez. Az emberek hajlamosak elfogadni a csoportjuk vagy közösségük által támogatott nézeteket és információkat, még akkor is, ha azok objektíven nézve kétségesek vagy tévesek.[210] Ez a jelenség különösen erős a polarizált közösségekben vagy az erős csoportidentitással rendelkező hálózatokban. A politikai polarizáció és az úgy nevezett

[207] International, *Investigation into Aadhaar Data Breach*.
[208] Lorenz Goette, Hua-Jing Han, és Benson Tsz Kin Leung, *Information Overload and Confirmation Bias* (University of Cambridge Working Paper, 2019), https://doi.org/10.17863/CAM.52487.
[209] Mediakutató, „Visszhangkamrák és szűrőbuborékok", *Médiakutató* 2020, sz. 1 (é. n.): 1–15.
[210] D. Guilbeault, D. Centola, és A. Baronchelli, „Groupthink Dynamics in Large Social Networks", *Nature Communications*, 2024, https://doi.org/10.1038/s41467-024-48034-5.

információs buborékok szoros összefüggésben vannak az álhírek terjedésével és a demokratikus diskurzus minőségének romlásával. Az online platformok algoritmusai és a felhasználói preferenciák együttesen olyan információs környezetet teremtenek, ahol a különböző politikai csoportok egyre elszigeteltebbé válnak egymástól, és eltérő "valóságokban" élnek.[211] A politikai polarizáció következményei közé tartozik a közös valóság eróziója, ami megnehezíti a társadalmi konszenzus kialakítását és a demokratikus döntéshozatalt. A médiapluralizmus és a különböző nézőpontoknak való kitettség elősegítése fontos lépés lehet.[212] Megjegyzendő, hogy felhasználók ösztönzése a különböző forrásokból származó információk fogyasztására, valamint a közös digitális terek létrehozása mind hozzájárulhat a társadalmi kohézió erősítéséhez és a demokratikus diskurzus minőségének javításához, illetve az egyéni biztonságtudatosság és az álhírek elleni rezisztencia kialakításához.

A kognitív torzítások tudatosítása és a metakognitív készségek fejlesztése (vagyis a saját gondolkodási folyamatainkról való gondolkodás képessége) segíthet az álhírek hatásának csökkentésében.[213] Az oktatási programok, amelyek a kritikus gondolkodásra és a kognitív torzítások felismerésére fókuszálnak, hozzájárulhatnak az egyének ellenállóbbá tételéhez a dezinformációval szemben.[214] A kibertérben a hitelesség percepciója gyakran nem a tartalom minőségén, hanem különböző heurisztikákon alapul. A virtuális laborköpeny-hatás szerint a felhasználók túlbecsülik a hitelesített források szakmai kompetenciáját, ha azok a saját szakterületüktől eltérő témákról nyilatkoznak.[215] A hitelesség észlelését befolyásoló tényezők között szerepel a forrás megjelenése, a felhasznált nyelv, a hivatkozások jelenléte, valamint a közösségi visszajelzések is (például like-ok, megosztások száma), azonban ezek manipulálhatók, amik lehetővé teszik a hitelesség percepciójának javítása érdekében fontos a médiaműveltség fejlesztése, a kritikus gondolkodás oktatása és a hitelesség jelzéseinek standardizálása a digitális környezetben. A platformok felelőssége is kiemelendő a hiteles tartalmak meg-

[211] Res Medias, „Az online dezinformáció és hatásai", *Medias Res Folyóirat* 7, sz. 2 (2023): 45–67.
[212] Horváth László, „Az álhír fogalma és helye a hibrid hadviselésben", *Nemzet és Biztonság* 6, sz. 1 (2023): 19–34.
[213] H. Grahn és J. Pamment, *Exploitation of Psychological Processes in Information Influence Operations* (Lund University Psychological Defence Research Institute, 2024).
[214] Pew Research Center, *Digital Divide Survey* (Washington, DC: Pew Research Center, 2023).
[215] Marsh, *Global Technology Industry Risk Study* (New York: Marsh & McLennan, 2023).

különböztetésében és előtérbe helyezésében, valamint a megbízhatatlan források megfelelő címkézésében, továbbá az oktatási intézményeknek és az államnak a szerepe is elvitathatatlan a kritikai gondolkodás kialakításában.

2.4.4 Az információs műveletek típusai és a kognitív térben zajló műveletek

Az információs műveletek egyre nagyobb szerepet játszanak a nemzetközi kapcsolatokban és a belpolitikában egyaránt. Az információs és kommunikációs technológiák intenzív fejlesztése és azok széles körű alkalmazása lehetővé teszi az ellenséges információs erőforrások és távközlési rendszerek befolyásolását és károsítását, a létfontosságú struktúrák szándékos befolyásolását, valamint egy állam gazdasági és társadalmi rendszereinek aláásását és a lakosság pszichológiai manipulálását a társadalom destabilizálása céljából.[216] Az információs műveletek olyan tevékenységek összessége, amelyek célja az információfölény megszerzése az ellenfél felett az információ és az információs rendszerek ellenőrzésével, manipulálásával vagy zavarásával. Az információs műveletek célja, hogy megzavarják vagy összezavarják az ellenség információgyűjtési, -feldolgozási és -terjesztési képességét, és ugyanakkor megvédjék a saját-jukat, azzal a végső céllal, hogy információs fölényt szerezzenek az ellenfelek felett.[217]

A kibertér és a kognitív tér integrációja lehetővé teszi, hogy ezek a műveletek mind a technikai, mind az emberi tényezőkön keresztül hatást gyakoroljanak.[218]

Technikai információs műveletek

Ezek a műveletek a kibertér fizikai és információs dimenziójára fókuszálnak, például hálózati támadásokkal, adatmanipulációval vagy elektronikai hadviseléssel. A kibertéri műveletek közé tartozik a számítógépes hálózatok infiltrációja, adatok titkosításával való zsarolás (ransomware) vagy kritikus infrastruktúrák megsemmisítése.[219] A technikai műveletek célja a fizikai károk okozása vagy az információáramlás blokkolása, de közvetve a kognitív térre is hatnak, például pánikkeltéssel vagy bizalmi rendszerek aláásásával. Annak ellenére, hogy technika jellegű kockázatról beszélünk jelen téma tárgyalása sokkal inkább ehhez az alfejezethez kapcsolódik, mert annak ellenére,

---

[216] Mandiant, *Advanced Persistent Threat Report* (Reston, VA: Mandiant, 2023).
[217] Ventures, *Global Cybercrime Damage Report*.
[218] Várhegyi, „Információs műveletek és hadviselés".
[219] Haig Zsolt, „Kibertéri kognitív befolyásolás az információs műveletekben", *Hadtudományi Szemle* 15, sz. 2 (2022): 115-130, https://doi.org/10.32563/hsz.2022.2.7.

hogy maga az alkalmazott módszer technikai jellegű a kár és a bekövetkezés helye az emberi elme. Ide tartozik a metaadatok manipulációja is, ami lehetővé teszi a tartalmak eredetének és kontextusának meghamisítását, ami alááshatja a hitelességet.[220] A hamis kontextusba helyezés (false contextualization) egy gyakori dezinformációs technika, amely során valós tartalmakat (képeket, videókat, idézeteket) a kontextusukból kiragadva, más időponthoz, helyszínhez vagy eseményhez kapcsolva terjesztenek. Ez a technika különösen hatékony lehet, mivel a tartalom maga valódi, csak a kontextusa hamis, ami megnehezíti a félretájékoztatás azonosítását.[221] A deepfake technológiák fejlődése, ahogy a fentiekben is említésre került további kihívásokat jelent a tartalmak hitelességének megítélésében. A metaadatok és a kontextus manipulációja elleni védekezés érdekében fontosak a tartalom-hitelesítési technológiák fejlesztése, a digitális aláírások és időbélyegzők alkalmazása, valamint a tartalmak eredetének nyomon követhetősége.[222] A tényellenőrző szervezetek és kezdeményezések is fontos szerepet játszhatnak a hamis kontextusba helyezett tartalmak azonosításában és a valós kontextus helyreállításában.[223]

Kognitív információs műveletek

A kognitív térben zajló műveletek közvetlenül az emberek tudati folyamatait célozzák meg, és a legnagyobb kihívást jelentnek a modern információs műveletekben,[224] ezek típusai lehetnek:

Lélektani műveletek (PSYOPS): A célja az érzelmek, hiedelmeinek és viselkedésének befolyásolása szándékosan tervezett üzenetekkel[1]. A közösségi média algoritmusai optimalizálják ezeknek az üzeneteknek az elérését, például a felhasználói figyelem irányításával (pl. clickbait címek) vagy érzelmi tartalmak priorizálásával.

Kognitív megtévesztés: A megtévesztés célja alternatív valóságok konstruálása, amelyek torzítják a célközönség helyzetértékelését.

---

[220] Amelia Acker, *Data Craft: The Manipulation of Social Media Metadata* (Data & Society, 2018).
[221] „Disinformation as a context-bound phenomenon", *Oxford Academic*, 2023, https://doi.org/10.1093/ct/qtad001.
[222] „University of Texas. Reading Metadata To Combat Disinformation", 2025.
[223] E.P.S.T.E.M., „Impact of Deepfake Technology on Social Media", 2023.
[224] H. Grahn és J. Pamment, „Exploitation of Psychological Processes in Information Influence Operations", *Working Paper* 2024, sz. 4 (2024).

Emócióalapú manipuláció: Az érzelmekkel terhelt üzenetek (pl. harag, félelem) képesek befolyásolni a kritikus gondolkodást. Például a háborús retorikában gyakran használt „ellenségkép" konstrukció direkt módon aktiválja az amygdala tevékenységét, ami racionális elemzés helyett ösztönös reakciókat vált ki.[225]

Hibrid információs műveletek: A technikai és kognitív műveletek összehangolása teszi lehetővé a legnagyobb hatékonyságot. Például kombinálja a PSYOPS-ot a kibertámadásokkal, hogy a fizikai és mentális ellenállását egyidejűleg gyengítse.[226]

Védelmi és ellenműveletek: Az információs műveletek elleni védekezés komplex stratégiákat igényel. Javaslatok közé tartozik a digitális műveltség oktatása, az algoritmustranszparencia és a kognitív rugalmasság növelése.[227]

Az információs műveletek elleni védekezés komplex feladat, amely magában foglalja a technológiai ellenintézkedéseket, a jogi és szabályozási keretrendszereket, valamint a társadalmi ellenálló képesség erősítését. A NATO Stratégiai Koncepciója külön kitér a hibrid fenyegetések és az információs műveletek elleni védekezés fontosságára.[228] A médiaműveltség fejlesztése, a kritikus gondolkodás oktatása és a demokratikus intézmények megerősítése mind hozzájárulhatnak a társadalmak ellenálló képességének növeléséhez az információs hadviselés és befolyásolási kísérletekkel szemben.

A kognitív információs műveletek célja az egyének és közösségek tudati folyamatainak befolyásolása, hogy előre meghatározott viselkedési vagy véleményváltozást érjenek el. Ezek a műveletek a kibertér és a kognitív tér szimbiózisán alapulnak, ahol technikai eszközök (pl. algoritmusok) és pszichológiai mechanizmusok (pl. kognitív torzítások) együttesen alkalmazhatók. Az álhírek és egyéb dezinformációs technikák ezen folyamatok kulcsfontosságú eszközei.[229]

---

[225] R.S. Lazarus, „Emotion and Adaptation" (Oxford University Press, 1991).
[226] N.A.T.O.Innovation Hub, „The Cognitive Warfare Concept: Enhancing NATO's Hybrid Threat Response" (NATO Innovation Hub White Paper, 2023).
[227] Haig, „Kibertéri kognitív befolyásolás az információs műveletekben".
[228] Hub, „The Cognitive Warfare Concept: Enhancing NATO's Hybrid Threat Response".
[229] Kyaw Jaw Sine Marma, „The Science of Disinformation: Cognitive Vulnerabilities and Digital Manipulation", Modern Diplomacy, 2025. február 9., https://moderndiplomacy.eu/2025/02/09/the-science-of-disinformation-cognitive-vulnerabilities-and-digital-manipulation/.

2.4.5 A dezinformáció típusai és evolúciója

A fentiekben már kifejtettem, hogy az információs műveletek egyfajta átfogó stratégiaként vannak jelen, ebben a viszonyban a dezinformáció, mint az információs műveletek egy eszköze jelenik meg, továbbá az az álhírek pedig a dezinformáció egy konkrét eszközeként. Amely magában foglalja a dezinformációt és az álhíreket is. A dezinformáció a szándékosan terjesztett, valótlan vagy félrevezető információ, amelynek célja a célközönség megtévesztése. Bányász Péter hangsúlyozza, hogy a dezinformáció eszköze az információs műveleteknek, különösen a kibertérben, ahol gyors terjedése a közösségi média algoritmusainak köszönhető, dezinformációnak az alábbi típusai lehetnek:

- Fekete propaganda: Nyíltan hamis információk, amelyek forrása rejtve marad.
- Szürke propaganda: Valós és hamis elemek keveréke, a forrás bizonytalan.
- Fehér propaganda: Hiteles forrásból származó, de szelektíven kiválasztott információk.[230]

A fentieken túlmenően a kiemelendő a félrevezető információ (misinformation), illetve a rosszindulatú kiragadott információk (malinformation). A misinformation nem szándékos tévedésből vagy tudatlanságból származó hamis információ, amely azonban ugyanúgy káros hatással lehet a társadalomra. Haig Zsolt szerint a misinformation gyakran a kognitív megtévesztés melléktermége, például amikor a felhasználók tévesen osztanak meg valótlan híreket anélkül, hogy rossz szándékuk lenne[231] A malinformation valós információ rosszindulatúan torzított kontextusba helyezése, amely célzott károkozásra szolgál. A malinformation azért is veszélyes, mert a valós adatok hitelét használja fel a célközönség megtévesztésére.[232] A fentiek alapján megállapítható, hogy a dezinformációnak egyfajta változataként lehet felfogni mind a misinformation-t, mind a malinformation-t.

Az álhír viszonya a dezinformációhoz az, hogy az előbbi az utóbbinak egy konkrét formája. Az álhírek hatékonyak a kognitív dimenzióban, mivel érzelmileg feltöltött tartalmak gyorsabban terjednek, mint a valós hírek. Az álhírek olyan mesterségesen létrehozott információk halmaza, amelyek magukat valós média tartalomnak álcázzák,

---

[230] Péter Bányász, „Dezinformáció az Ipar 4.0 kontextusában", *Hadmérnök* 19 (2024. január): 97–118, https://doi.org/10.32567/hm.2024.3.7.
[231] Haig, „Kibertéri kognitív befolyásolás az információs műveletekben".
[232] Mátyás Ináncsi és mtsai., „Empirical Studies of Russian–Ukrainian War Related Fake News, Part 1", *Hadmérnök* 18, sz. 4 (2024. május 9.): 109–28, https://doi.org/10.32567/hm.2023.4.8.

azonban az álhírek nem tartalmazzák a hírközlő médiát szerkesztő normákat és eljárásokat az információ pontosságának és hitelességének biztosítására. Céljuk a szándékosan dezinformáció, a figyelem felkeltése és félrevezetés.[233] Az álhírek felosztásánál, Melissa Zimdars ajánlását vettem figyelembe.[234] A fentiek alapján megkülönböztethetünk:

- Szatirikus hírek: humorral, iróniával túlzással, hamis információval kapcsolódik az aktuális eseményhez.
- Elfogult hírek: propagandára, bizonyos politikai nézőpontra támaszkodik, és a hír súlyosan torzított formában jelenik meg.
- Összeesküvés elméletek: ezek a jól ismert olyan híresztelések, amelyek egyes eseményeket más szemszögből vizsgálnak és összeesküvéseket vélnek felfedezni a háttérben.
- Az áltudományos hírek: az alapja olyan tény melyet a tudomány nem támasztott alá, sőt egyes esetekben ezek a hírek a tudományos eredményeket támadják.
- A kattintás vadász (Clickbait) hírek: céljuk az, hogy az adott oldalt tekintsék meg és meg osszák azt. Ezért igen félrevezető címeket és képeket használnak, amik többsége könnyen ellenőrizhető.
- Szóbeszéden alapuló hírek: alapja pletykák, amik forrása az esetek nagy részében ellenőrizetlenek.

Az elvégzett kutatások alapján a dezinformációs technikák folyamatosan fejlődnek, alkalmazkodva a változó technológiai és társadalmi környezethez. A hagyományos álhírek mellett új formák jelennek meg, mint például az erre a célra készített deepfake videók, a manipulált képek, a hamis konszenzusépítés, vagy a fél információk stratégiai terjesztése. A dezinformáció gyakran stratégiai célokkal rendelkezik, mint az információs műveletek része, például politikai kampányok befolyásolása, bizalmatlanság keltése intézmények iránt, vagy társadalmi polarizáció fokozása. A dezinformáció terjedésének sebessége az információs társadalom korában. Míg a hagyományos médiarendszerekben a gate-keeperek (szerkesztők, újságírók) szűrő szerepet töltöttek be,

---

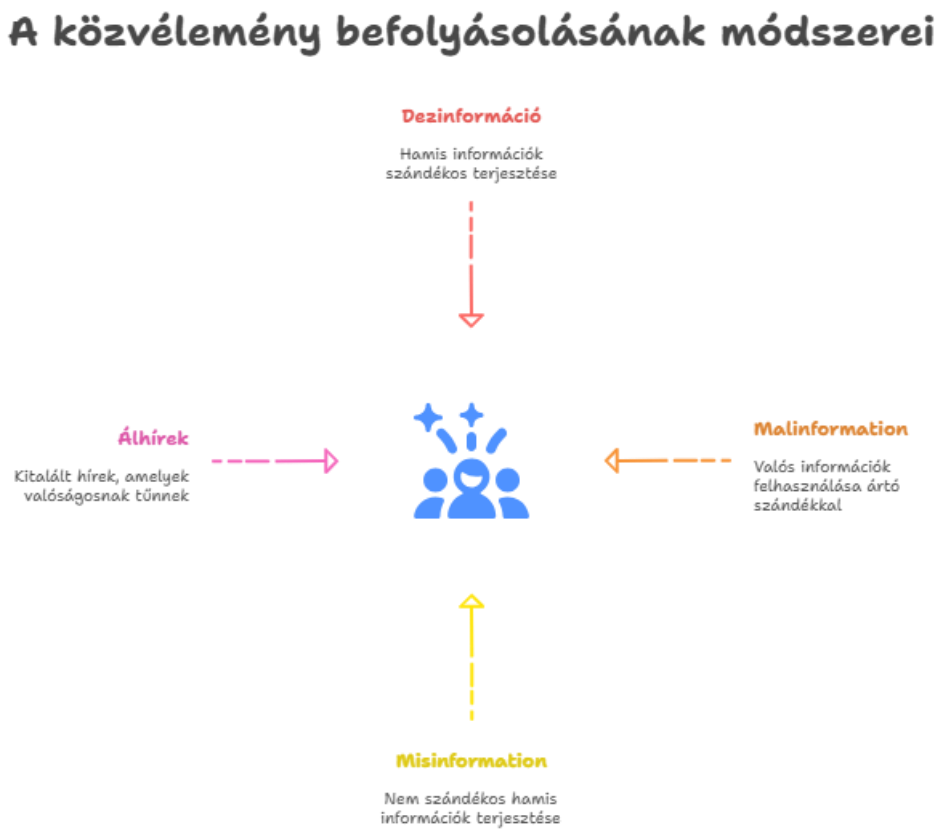
233 M. J. David at all: The science of fake news: The science of fake news, In. Science 2018, 359 szám, pp. 10941096 DOI: 10.1126/science.aao2998

234 Zimdars, Melissa: 'False, Misleading, Clickbait-y, and Satirical "News" Sources', 2016., https://docs.google.com/document/d/10eA5mCZLSS4MQY5QGb5ewC3VAL6pLkT53V_81ZyitM/edit 16 Wardle - C., Derakhshan - H., "Information disorder: Toward an interdisciplinary framework for research and policy making 2017, pp6. 6. o.

a közösségi médiában ez a funkció gyengébb, és a tartalmak szinte azonnali terjedése nehezíti az ellenőrzést és a válaszadást. A félretájékoztatás gyakran gyorsabban terjed, mint a valós információk, különösen, ha érzelmi reakciókat vált ki vagy megerősíti a meglévő hiedelmeket. A dezinformáció elleni küzdelem komplex megközelítést igényel, amely magában foglalja a szabályozási keretrendszereket, a platform-politikákat, a tényellenőrzési kezdeményezéseket, valamint a médiaműveltség és kritikus gondolkodás fejlesztését. A közösségi média platformok struktúrája és működési modellje befolyásolja, az álhírek terjedésének dinamikáját platformok algoritmusai általában A felhasználói elköteleződést maximalizálják, ami kedvez az érzelmileg stimuláló, figyelemfelkeltő tartalmaknak, függetlenül azok hitelességétől. A Reuters Institute "Digital News Report" szerint a felhasználók egyre nagyobb része tájékozódik a hírekről a közösségi médián keresztül, különösen a fiatalabb korosztályok körében.[235] A közösségi médiában az információterjedést befolyásolják a hálózati struktúrák és a felhasználói viselkedés. hitelesebbnek tekinteni azokat a tartalmakat, amelyeket sokan kedvelnek vagy osztanak meg. A közösségi média platformok felelőssége az álhírek terjedésének megakadályozásában vitatott kérdés. A platformok kezdeményezéseket indítottak a dezinformáció visszaszorítására, például tartalommoderálási irányelvek bevezetésével, tényellenőrző szervezetekkel való együttműködéssel és algoritmusaik módosításával. Ugyanakkor ezek a lépések gyakran elégtelennek bizonyulnak, és kérdéseket vetnek fel a véleménynyilvánítás szabadságával és a platform-semlegességgel kapcsolatban.

Információs műveletekben a technológiákat is kihasználva a kibertérben terjeszthetik az álhíreket, mellyel az ellenfél lakosságát is befolyásolni képesek. A konfliktusok lélektani hatása döntő fontosságúvá válik. A felek sokszor a közvetlen hatások helyett közvetett módszereket alkalmaznak egymással szemben. A műveletek gyakran egymástól elszigetelten zajlanak. Az e fajta műveleteket napjainkban leginkább hibrid hadviselésként határozzák meg.[236]

[235] Institute, *Digital News Report*.
[236] Haig Zsolt: Információs műveletek a kibertérben, Dialóg Campus Kiadó, Budapest, 2018., 174. o.



2. **ábra: Saját szerkesztés napkin.ai által**

2.4.6 Digitális kompetencia, oktatási és tudatossági hiányosságok.

A digitális szakadék, amelyet az információs és kommunikációs technológiához való hozzáférés egyenlőtlensége jellemez, akadályt jelent az információs társadalmon belül. A világ népességének egy része továbbra sem rendelkezik internetkapcsolattal. Ez az arány különösen magas a szegényebb országokban.[237] Még a hozzáféréssel rendelkezők között is eltérések mutatkoznak az internetkapcsolat sebességében és minőségében.[238] E problémát az általam készített interjúk egy IT biztonsági szakértője is kiemelte. Továbbá a megfelelő eszközökhöz (számítógép, okos telefon, táblagép) való elégtelen hozzáférés korlátozza a digitális részvételt.[239] Ezzel összefüggésben megjegyzendő digitális szolgáltatások elérhetőségének egyenlőtlensége, például e-kormányzat, e-egészségügy és e-oktatás kapcsán, ami súlyosbítja a digitális szakadékot.[240]

[237] International Telecommunication Union, *Digital Divide Report* (Geneva: ITU, 2023).
[238] Ookla, *Global Speedtest Index* (Seattle, WA: Ookla, 2024).
[239] Center, *Digital Divide Survey*.
[240] United Nations, *E-Government Survey* (New York: United Nations, 2024).

A digitális technológiához való fizikai hozzáférésen túl a digitális képességek hiánya akadályt jelent az információs társadalomban való teljes részvételhez. A digitális írástudás és a kritikus gondolkodás kulcsfontosságú készségek az információs társadalomban való hatékony részvételhez és a dezinformáció elleni védekezéshez. A digitális írástudás kutatása figyelmet kapott az elmúlt években, különösen a COVID-19 járvány hatására, amely felgyorsította a digitális átállást az oktatásban és egyéb területeken.[241]

A digitális írástudás nem csupán a technológiai eszközök használatának képességét jelenti, hanem magában foglalja az információk kritikus értékelését, az online források hitelességének megítélését, a digitális lábnyom kezelését és az online közösségekben való etikus részvételt is. A kritikus gondolkodás képessége lehetővé teszi az egyének számára, hogy elemezzék az információkat, felismerjék a kognitív torzításokat és manipulációs technikákat, valamint megalapozott következtetéseket vonjanak le.

A digitális készségek fejlesztése folyamatos kihívást jelent az oktatási intézmények számára, különösen a gyorsan fejlődő technológiai környezetben.[242] Az oktatási rendszerek fontos szerepet játszanak a digitális írástudás és kritikus gondolkodás fejlesztésében. A digitális írástudás fejlesztésére irányuló kezdeményezések globális szinten is kiemelt figyelmet kapnak. Az UNESCO "Digitális Írástudás Keretrendszere" standardokat és iránymutatásokat határoz meg a digitális írástudás oktatásához és értékeléséhez.[243] Az OECD "Skills for a Digital World" programja a digitális készségek fejlesztését támogatja a változó munkaerő-piaci igényekhez való alkalmazkodás érdekében.[244] A kritikus digitális írástudás hiánya, amely a digitális tartalom kritikus értékelésének képessége, növeli a megtévesztésre és manipulációra való fogékonyságot.[245] A digitális kompetenciák egyre fontosabbak a munkaerőpiacon, potenciálisan növelve a

[241] Grosso M, „How to Improve an Advanced Waste Management System", *PubMed*, elérés 2025. május 3., https://pubmed.ncbi.nlm.nih.gov/33977798/.
[242] „Skills for the Digital Transition", OECD, 2022. október 18., https://www.oecd.org/en/publications/skills-for-the-digital-transition_38c36777-en.html.
[243] „A global framework of reference on digital literacy skills for indicator 4.4.2 - UNESCO Digital Library", elérés 2025. május 3., https://unesdoc.unesco.org/ark:/48223/pf0000265403.
[244] „Contribution to the development of a Global Digital Literacy Skills indicator | Department of Economic and Social Affairs", elérés 2025. május 3., https://sdgs.un.org/partnerships/contribution-development-global-digital-literacy-skills-indicator.
[245] World Wide Web Consortium, *Web Content Accessibility Guidelines* (Cambridge, MA: W3C, 2023).

digitális készségekkel rendelkezők és azok között, akik nem rendelkeznek ilyen készségekkel, lévő szakadékot.[246]

A digitális technológia használata sajátos akadályokat jelent a fogyatékkal élők számára: Számos webhely és digitális szolgáltatás nem felel meg a hozzáférhetőségi szabványoknak, ezáltal korlátozza a fogyatékkal élők hozzáférését.[247] A segítő technológiák, beleértve a képernyőolvasókat, a hangfelismerő rendszereket és az alternatív beviteli eszközöket, nem kompatibilisek a mainstream technológiával.[248]

Következtetések

Az információs társadalom fogalma meghatározó keretrendszerként emelkedett ki a modern társadalomtudományi diskurzusban, hatást gyakorolva az akadémiai, kormányzati és közgondolkodásra. Az információs társadalom sokféle definíciója tükrözi annak többdimenziós természetét, amely magában foglalja a technológiai, gazdasági, foglalkoztatási, térbeli és kulturális dimenziókat Az információs társadalom koncepciójának történeti genezise nem tulajdonítható egyetlen pillanatnak vagy személynek, hanem olyan evolúciós folyamatot képvisel, amelyet különböző gondolkodók és a technológiai, valamint társadalmi változások megfigyelései tápláltak

Az információs társadalom komplexitása annak többszörös dimenzióban való megnyilvánulásából ered. Technológiai szempontból olyan paradigmaváltást képvisel, amelyet az információs és kommunikációs technológiák exponenciális fejlődése hajt. Az információs társadalom számos biztonsági kihívást hoz magával a technológiai, társadalmi-gazdasági és politikai-jogi területeken. A technológiai kihívások közé tartoznak az infrastrukturális sebezhetőségek, a kritikus információs infrastruktúrák (energiahálózatok, bankrendszerek, közlekedési rendszerek) kibertámadásoknak való kitettsége. A becslések szerint a kiberbűnözés évente körülbelül 6 billió dolláros gazdasági kárt okoz globálisan. Kriptográfiai kihívások merülnek fel, amikor a kvantumszámítástechnika veszélyezteti a hagyományos titkosítási technikákat, szükségessé

[246] E.U.Media Literacy Expert Group, *Report* (Brussels: European Commission, 2024).
[247] *Global Initiative for Inclusive Information and Communication Technologies (G3ict* (Atlanta, GA: G3ict, 2024).
[248] *ISO/IEC 30071: Accessibility Requirements for Information and Communication Technology Products* (Geneva: ISO, 2023).

téve a kvantumrezisztens titkosítási módszereket, mint például a NIST által jóváhagyott CRYSTALS-Kyber algoritmus.

A politikai és jogi kihívások közé tartoznak a szabályozási vákuumok, mivel a technológiai fejlődés gyakran megelőzi a jogi szabályozást.

Az információs társadalom fejlődése mind lehetőségeket, mind kihívásokat jelent a jövőre nézve. Az azonnali biztonsági aggályok közé tartoznak a növekvő adatvédelmi incidensek és adatvédelmi kérdések, mint például a 2023-as indiai Aadhaar rendszer adatvédelmi incidens, amely 1,1 milliárd felhasználót érintett.

Az információs társadalom interdiszciplináris kutatási potenciálja részben kiaknázatlan marad a tudományterületek közötti kommunikációs nehézségek, az eltérő módszertani hagyományok és a diszciplináris határok miatt. Az interdiszciplináris kutatási projektek támogatása, a különböző tudományterületek módszertani megközelítéseinek integrálása és a tudományterületek közötti párbeszéd erősítése fontos lépéseket jelentenek az információs társadalomkutatás előmozdításában és a globális kihívások kezelésében.

Megállapítható az információs társadalom komplex, többdimenziós jelenséget képvisel, amely az emberi élet különböző aspektusait alakítja át. Miközben példátlan lehetőségeket kínál a kommunikáció, a tudáshoz való hozzáférés és a gazdasági fejlődés terén, egyidejűleg kihívásokat jelent a biztonság, a magánélet, a társadalmi kohézió és az etikai megfontolások szempontjából. Ahogy folytatjuk ennek az átalakulásnak a navigálását, az interdiszciplináris megközelítések és a technológiai lehetőségek, valamint a társadalmi következmények gondos mérlegelése elengedhetetlen lesz egy olyan információs társadalom kialakításában, amely az emberi igényeket és értékeket szolgálja, miközben mérsékli a potenciális kockázatokat. Az álhírek terjedése a közösségi médiában súlyos fenyegetést jelent a demokratikus diskurzusra és a társadalmi kohézióra. A dezinformáció különböző típusai, a kognitív torzítások szerepe az álhírek befogadásában, valamint a politikai polarizáció és az információs buborékok kialakulása mind hozzájárulnak a probléma komplexitásához. Az információs műveletek tovább súlyosbítják a helyzetet.

Az információs társadalom biztonsági kihívásai nem csupán technológiai jellegűek, hanem a társadalmi-gazdasági vetületük is van. A kibertérben zajló támadások és a humán eredetű sebezhetőségek (pl. digitális analfabetizmus) szimbiózisa új típusú kockázatokat teremt, ahol a technikai hiányosságokat kihasználó aktorok képesek destabilizálni nemzeti intézményeket. A kritikus infrastruktúrák védelmének hiánya – például az energiahálózatok vagy egészségügyi rendszerek – közvetlenül fenyegeti a nemzetbiztonságot. A jelen fejezet és az eddigi kutatásom alapján megállapítható, hogy a kormányzati szereplőknek proaktívan kell integrálniuk a kvantumrezisztens kriptográfiát és a zero-trust architektúrákat, mivel a hagyományos védelmi mechanizmusok már nem elegendőek a modern fenyegetések leküzdésére.

3 OKOS ESZKÖZÖK EVOLUCIÓJA ÉS A KAPCSOLÓDÓ KIHÍVÁSOK

Az okos eszközök jelenleg meghatározó szerepet töltenek be mind személyes, mind szakmai tevékenységeinkben. Az okos eszközök olyan elektronikus berendezések, amelyek képesek az internethez kapcsolódni, adatokat gyűjteni és elemezni, valamint más eszközökkel kommunikálni. Fejlett számítási kapacitásuk lehetővé teszi az intelligens döntéshozatalt és a környezethez való alkalmazkodást, könnyítve ezáltal a felhasználók életét.[249]

Az okos eszközök olyan hálózatba kapcsolt készülékek, amelyek képesek információk gyűjtésére, feldolgozására és továbbítására, intelligens döntéseket hoznak, és interakcióba lépnek környezetükkel. Bányász Péter és Orbók Ákos kutatásai szerint már az 1990-es évek elején megjelentek olyan eszközök, amelyeket az "okos" jelzővel lehetett leírni.[250] Az okos eszközök széles köre magában foglalja többek között:

- Okos telefonok és táblagépek
- Okos órák és viselhető eszközök
- Okos otthoni eszközök
- Okos TV-k és médialejátszók
- Ipari IoT eszközök
- Okos járművek
- Egészségügyi okos eszközök

Azonban az I. fejezetben, az információs társadalom kihívásaiban taglalt metodika alapján megkülönböztethetünk:

- Okos mobil eszközöket
- Okos otthoni eszközöket
- Okos városok eszközeit, illetve
- Okos infrastruktúrákat

Az eszközök operációs rendszereihez készülnek kiegészítő alkalmazások, amelyek száma az adott operációs rendszer elterjedésétől függ. Az alkalmazásokat nemcsak az

[249] „Okos eszközök / Smart Devices / Okoseszköz / Smart Device / Intelligent Devices / Intelligens Eszközök / Okos Megoldások | Modern Vállalkozások Programja", elérés 2025. május 3., https://digitalisfogalomtar.vallalkozzdigitalisan.hu/okoseszkozok-smart-devices-okoseszkoz-smart-device-intelligent-devices-intelligens-eszkozok-okos-megoldasok.

[250] Bányász Péter és Orbók Ákos, *Bevezető az okos eszközök világába. In: Okos eszközök - Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2016* (Budapest: Nemzeti Közszolgálati Egyetem, 2019).

operációs rendszerek gyártói, hanem független fejlesztők is készítik, amelyek kiegészítő funkciókat vagy céleszközöket kínálnak a felhasználóknak. [251] Ezek alkalmazások típusait és fejlődését jelent fejezet későbbi részében tárgyalom részleteiben.

Jelen kutatás során az okos mobil eszközök (okos telefonok, tabletek, okos órák, stb.) és azok alkalmazásait vizsgálom részleteiben, különös tekintettel a személyazonosításra és személyi hitelesítésre alkalmas megoldásokra. Így a következőkben az okos eszközök alatt az okos mobil eszközöket, kiemelten az okos telefonokat értem.

Az általános vélekedéssel ellentétben az okos mobil eszközök fejlődéstörténete nem az Apple által 2007-ben bemutatott iPhone-nal kezdődött, annak ellenére, hogy hatalmas fordulatot hozott az okos mobileszközök fejlődésének történetében. Bányász Péter és Orbók Ákos kutatásai rámutatnak, hogy már az 1990-es évek elején megjelentek olyan eszközök, amelyeket "okosnak" lehetett nevezni.[252] A 2010-es évek elejére a mobiltelefonok már nem csupán kommunikációs eszközként működtek, hanem személyi asszisztensként, szórakoztató központként és szakmai platformként is. Az okos eszközök technológiájának fejlődése figyelemreméltó ütemben gyorsult az elmúlt évtizedben. Az okos eszközök biztonságával kapcsolatos vizsgálatok fokozott érdeklődésre tartanak számot. Bányász Péter kutatása szerint az internet és az okos mobileszközök elterjedése megváltoztatta életünket, miközben új kihívásokat is bevezetett.[253] A kibertér globális jellege számos és folyamatosan fejlődő veszélyt eredményez, ami bonyolítja a biztonsági erőfeszítéseket. Az okos eszközök biztonsági sebezhetőségei különösen magasak, mivel a programokat bárki fejlesztheti. A következő fejezetben átfogó elemzést nyújtok az okos eszközök történeti fejlődéséről, tudományos vizsgálatáról és jövőbeli irányairól, különös tekintettel az elmúlt 10 év technikai fejlesztéseire és kutatási trendjeire. Továbbá bemutatom az okos eszközök kapcsán felmerülő jelenlegi általános kihívásokat és kockázatokat hazai és nemzetközi tudományos szakirodalom forráselemzése, továbbá az IT és az IT biztonság területén dolgozó szakértőkkel készített interjúk alapján.

---

[251] „Smartphone History: From the First Smartphone to Today | Arrow.com", elérés 2025. május 3., https://www.arrow.com/en/research-and-events/articles/smartphone-history-from-the-first-smartphone-to-today.
[252] Bányász és Orbók, *Bevezető az okos eszközök világába. In: Okos eszközök - Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2016.*
[253] Bányász, „Az okos mobil eszközök biztonsága".

3.1.1 Történeti betekintés eszközök kialakulása.

A mobiltelefónia kezdetei az 1970-es évekig nyúlnak vissza. 1973-ban Dr. Martin Cooper, a Motorola mérnöke bemutatta az első működő mobiltelefonos prototípust. Ez a készülék még rendkívül kezdetleges volt a mai okos telefonokhoz képest, de megteremtette a hordozható távközlési eszközök alapjait. Az igazi áttörést az 1983-ban piacra dobott Motorola DynaTAC 8000X jelentette, amely az első kereskedelmi forgalomba került mobiltelefon volt. A "The Brick" (A Tégla) becenévre hallgató készülék csaknem 1 kilogramm súlyú volt, mindössze 30 perces akkumulátor-élettartammal rendelkezett, és 3995 dollárba került – mai értéken ez többszöröse lenne ennek az összegnek.[254]

A mobiltechnológia fejlődésében mérföldkövet jelentett az 1991-es év, amikor Finnországban elindult a 2G mobilhálózat a Globális Mobilkommunikációs Rendszeren (GSM). Ugyanebben az évben a Sony és mérnöke, Asahi Kasei kereskedelmi forgalomba hozta a könnyű és újratölthető lítium-ion akkumulátort, amely a mai napig alapvető energiaforrása az okos telefonoknak.[255] [256]

Az okos eszközök megjelenését sokan tévesen az Apple által 2007-ben bemutatott iPhone-hoz kötik, holott a fejlődés már jóval korábban kezdődött. Bányász Péter és Orbók Ákos kutatásai szerint már az 1990-es évek elején megjelentek olyan eszközök, amelyeket az "okos" jelzővel lehetett leírni. [257]

Az első valódi okos telefon prototípust 1992-ben mutatta be az IBM mérnöke, Frank Canova. A "Sweetspot" kódnevű készüléket egy számítástechnikai szakvásáron demonstrálták, bár a fogyasztói piacra csak két évvel később jutott el.[258] 1994-ben jelent meg a piacon az IBM Simon Personal Communicator, amely már érintőképernyővel rendelkezett, és a felhasználók nem csak telefonhívásokat kezdeményezhettek vele,

---

[254] „Brick Phones: '80s Mobile Tech", Newretro.Net, 2023. november 12., https://newretro.net/blogs/main/brick-phones-80s-mobile-tech.
[255] „2G Cellular Telecom is Launched on Radiolinja's Network : History of Information", elérés 2025. május 3., https://historyofinformation.com/detail.php?id=2006.
[256] Mogalahalli V. Reddy és mtsai., „Brief History of Early Lithium-Battery Development", *Materials* 13, sz. 8 (2020. április 17.): 1884, https://doi.org/10.3390/ma13081884.
[257] Bányász és Orbók, *Bevezető az okos eszközök világába. In: Okos eszközök - Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2016.*
[258] „Smartphone History: From the First Smartphone to Today | Arrow.com".

hanem faxokat és e-maileket is küldhettek, fogadhattak. Az IBM Simon emellett bevezette az első alkalmazásokat is, mint például a címjegyzéket, naptárat, számológépet, találkozó-szervezőt és jegyzettömböt.[259]

A fejlődés első állomásai között említhetjük az 1989-ben piacra dobott Grid Systems GRiDPAD táblagépét, amely formájában már hasonlított a ma ismert tabletekhez, bár még monokróm kijelzővel és beépített tollal működött.[260] Ez a készülék, bár nem terjedt el széles körben, fontos előfutára volt a későbbi táblagépeknek.

A 2000-es évek elején több platform is versengett az okos telefonok piacán: az NTT DoCoMo i-mode platformja, a BlackBerry, a Nokia Symbian rendszere és a Windows Mobile kezdett teret nyerni. Ezek az eszközök gyakran QWERTY billentyűzettel vagy rezisztív érintőképernyős bevitellel rendelkeztek, és főként az e-mail elérésre és a vezeték nélküli internetkapcsolatra helyezték a hangsúlyt.[261]

Az okos mobileszközöknél valódi paradigmaváltást az iPhone 2007-es megjelenése hozott, amely átalakította az okos telefonokkal kapcsolatos felhasználói elvárásokat. Bár az iPhone közel sem volt tökéletes, forradalmi változást indított el, amely megteremtette az igényt a könnyen kezelhető okos telefonok iránt.[262] A kapacitív érintőképernyő, a felhasználóbarát felület és az App Store koncepció bevezetése új standardot teremtett az iparágban.

A tabletek esetében szintén hasonló fejlődési folyamat figyelhető meg. Az első kereskedelmi forgalomba kerülő készülékek megjelenése után a 2010-es években széles körben elterjedtek a különböző tabletek, és egyre speciálisabb felhasználási területeken jelentek meg.[263] 2010-ben az Apple iPad megjelenése újra definiálta a táblagép kategóriát, és megnyitotta az utat a tömegpiaci elterjedés előtt.

---

[259] „Smartphone history: A complete timeline", elérés 2025. május 3., https://www.textline.com/blog/smartphone-history.
[260] Bányász és Orbók, *Bevezető az okos eszközök világába. In: Okos eszközök - Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2016*. 9. o.
[261] „A nostalgic journey through mobile operating systems, past and present.", elérés 2025. május 3., https://www.buymobiles.net/blog/a-nostalgic-journey-through-mobile-operating-systems-past-and-present/.
[262] Bányász és Orbók, *Bevezető az okos eszközök világába. In: Okos eszközök - Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2016*.
[263] Bányász és Orbók. 8-9.o.

3.1.2 Hardveres innovációk az elmúlt évtizedben

A processzortechnológia előrelépéseken ment keresztül az elmúlt évtizedben. A 2013-2014 környékén megjelent csúcskategóriás okos telefonok jellemzően 32 bites architektúrájú, négymagos processzorokat használtak, míg mára a 64 bites, akár 8-12 magos chipek váltak általánossá. A gyártási technológia is fejlődött, a 28 nanométeres folyamatról 2025-re a csúcskategóriás chipek már 3-4 nanométeres eljárással készülnek, ami nagyobb energiahatékonyságot és jobb teljesítményt tesz lehetővé.[264]

Az okos telefonok kamerái az elmúlt évtizedben olyan mértékű fejlődésen mentek keresztül, ami alapjaiban változtatta meg a mobilfotózás és videózás lehetőségeit. 2013-ban a csúcskategóriás okos telefonok jellemzően egyetlen, 8-13 megapixeles hátlapi kamerával és egy alacsonyabb felbontású előlapi kamerával rendelkeztek. Mára a legtöbb prémium kategóriás okos telefon több hátlapi kamerával rendelkezik, amelyek különböző funkciókat látnak el: ultraszéles látószög, zoom, mélységérzékelő és makró lehetőségek egyaránt elérhetők.[265]

A biometrikus azonosítás területén is fejlődés történt. Az ujjlenyomat-olvasók 2013 körül kezdtek elterjedni az okos telefonokon, először a készülékházon elhelyezve, később pedig a kijelző alá integrálva. 2017-ben az iPhone X bemutatta a Face ID arcfelismerő rendszert, amely új szintre emelte a biometrikus azonosítást a mobiltelefonokon.[266]

3.1.3 Konnektivitás és hálózati technológiák

A 4G LTE (Long Term Evolution) hálózatok 2010 körül kezdtek elterjedni, és forradalmasították a mobilinternetet a korábbi generációkhoz képest nagyobb adatátviteli sebességükkel. Az 5G technológia bevezetése 2019-2020 körül kezdődött el, és 2025-re már lefedettséget ért el világszerte. A statisztikák szerint 2024 végére várhatóan 1,9

---

[264] U.-Tech Electronics, „The Latest Innovations in Mobile Phone Technology: A Comprehensive Overview", *U-Tech Electronics* (blog), 2023. december 10., https://utech.co/blog/the-latest-innovations-in-mobile-phone-technology/.
[265] Electronics.
[266] Peter Corcoran és Claudia Costache, „Biometric Technology and Smartphones: A consideration of the practicalities of a broad adoption of biometrics and the likely impacts", *IEEE Consumer Electronics Magazine* 5, sz. 2 (2016. április): 70–78, https://doi.org/10.1109/MCE.2016.2521937.

milliárd 5G előfizetés volt aktiválva, és 2025-re az 5G hálózatok a globális népesség 65%-át fogják lefedni.[267]

Az 5G technológia három fő előnyt kínál az okos telefonok számára: nagyobb sávszélesség (akár 10-20 Gbps sebesség), alacsonyabb késleltetés (akár 1 milliszekundum), és nagyobb kapacitás (sokkal több eszköz kiszolgálása egy adott területen).[268]

A Wi-Fi technológia okos telefonok fejlődésével párhuzamosan evolválódott. A Wi-Fi 4 (802.11n) után megérkezett a Wi-Fi 5 (802.11ac), amely nagyobb sávszélességet és jobb több felhasználós támogatást kínált. A legújabb Wi-Fi 6 és Wi-Fi 6E (802.11ax) szabványok még nagyobb sebességet, jobb energiahatékonyságot és kevesebb interferenciát biztosítanak, különösen zsúfolt környezetben.[269]

3.2 Az okos eszközök applikációinak szerepe

Az okos eszközök alkalmazásai a digitális korszak meghatározó alkotóelemei, amelyek gyökeresen átalakították a felhasználók mindennapi életét, kommunikációs módjait, munkavégzését, szórakozási formáit és információszerzési gyakorlatát. Az okos eszközök hardveres platformok, amelyek valódi értékét a rajtuk futó programok adják, kiterjesztve funkcionalitásukat és potenciális felhasználási lehetőségeiket. Az alkalmazások fejlődéstörténete szorosan összefonódik az okos eszközök evolúciójával, ugyanakkor sajátos fejlődési pályát is mutat, amely az alapvető funkcióktól a kifinomult, mesterséges intelligencia által vezérelt megoldásokig terjed.

Az okos eszközök alkalmazásainak eredete az 1990-es évek elejére nyúlik vissza. Az első alkalmazások az IBM Simon készülékhez köthetők, amely 1994-ben jelent meg a piacon, és már alapvető alkalmazásokkal rendelkezett, mint például címjegyzék, naptár, számológép, találkozószervező és jegyzettömb.[270] Ezek az alkalmazások a mai programokhoz képest rendkívül kezdetlegesek voltak, előrevetítették a jövőbeli fejlesztések irányát. Az Apple által 2008-ban elindított App Store mérföldkövet jelentett

[267] „50 Top Smartphone Usage Stats To Know In 2025 – Keywords Everywhere Blog", 2025. március 12., https://keywordseverywhere.com/blog/smartphone-usage-stats/.
[268] Electronics, „The Latest Innovations in Mobile Phone Technology".
[269] Electronics.
[270] J. Laakkonen, O.M. Latvala, és A. Heikkinen, „The Mobile Application Ecosystem: A Historical and Demographic Analysis", *Journal of Theoretical and Applied Electronic Commerce Research* 16, sz. 4 (2021): 1078–96, https://doi.org/10.3390/jtaer16040061.

az alkalmazásfejlesztésben, standardizált platformot teremtve a programok terjesztésére és monetizálására.[271] Ezt követte a Google Play megjelenése 2008-ban (akkori nevén Android Market), amely hasonló lehetőségeket biztosított az Android operációs rendszert használó készülékek számára.

Az alkalmazások piaci jelentősége az elmúlt évtizedben exponenciálisan növekedett. A legfrissebb statisztikák szerint 2023-ban csupán a Google Play áruházból 111 milliárd alkalmazásletöltés történt, míg az Apple App Store-ból 39 milliárd.[272] A mobil alkalmazások globális bevétele elérte a 420 milliárd dollárt, ami 14,5%-os növekedést jelent az előző évhez képest. Ez a hatalmas gazdasági potenciál innovációs hullámot indított el, és az okos eszközök alkalmazásfejlesztése önálló iparággá vált. Racskó Péter kutatásai szerint a hazai alkalmazásfejlesztési szektor is növekedést mutat, különösen a specializált, iparág-specifikus megoldások területén.[273]

Az Európai Bizottság felmérése alapján az uniós állampolgárok naponta átlagosan 2-3 órát töltenek okostelefon-alkalmazások használatával, ami meghaladja a hagyományos web böngészéssel töltött időt.[274] Ez az időbeli eltolódás jelzi, hogy az alkalmazások váltak a digitális interakciók elsődleges platformjává. A magyar felhasználók esetében ez az arány még magasabb lehet, hiszen Magyarország mobilinternet-penetrációja meghaladja az EU-átlagot.[275] A Nemzeti Média- és Hírközlési Hatóság (NMHH) 2023-as felmérése szerint a magyar internetezők 92%-a rendelkezik okos telefonnal, és 78%-uk napi rendszerességgel használ különböző mobilalkalmazásokat.[276] A magyar felhasználók körében népszerűek a közösségi média, kommunikációs és banki szolgáltatásokkal kapcsolatos alkalmazások, összhangban a globális trendekkel. Fehér Katalin kutatásai rámutatnak, hogy a magyar felhasználók egyre nagyobb arányban

[271] Laakkonen, Latvala, és Heikkinen.
[272] „Mobile app usage - statistics & facts | Statista", elérés 2025. május 3., https://www.statista.com/topics/1002/mobile-app-usage/.
[273] Racskó Péter, „A hazai alkalmazásfejlesztési ökoszisztéma és nemzetközi versenyképessége", *Vezetéstudomány* 53, sz. 6 (2022): 35–49, https://doi.org/10.14267/VEZTUD.2022.06.04.
[274] „Digital Public Services in the Digital Economy and Society Index | Shaping Europe's Digital Future", elérés 2025. május 3., https://digital-strategy.ec.europa.eu/en/policies/desi-digital-public-services.
[275] Központi Statisztikai Hivatal, *Digitális gazdaság és társadalom, 2023* (Budapest: KSH, 2023).
[276] Hírközlési Hatóság Nemzeti Média-, *Lakossági Internethasználat Online Piackutatás 2023* (Budapest: NMHH, 2023).

használnak hazai fejlesztésű alkalmazásokat is, különösen a helyi szolgáltatásokhoz kapcsolódó területeken.[277]

3.2.1 Az alkalmazások funkciója és jelentősége az okos eszközök ökoszisztémájában

Az okos eszközök és alkalmazásaik együttesen alkotják azt a digitális ökoszisztémát. Az alkalmazások ebben a rendszerben többféle, egymást átfedő szerepet töltenek be. Funkcionális szempontból az alkalmazások kiterjesztik és személyre szabják az okos eszközök képességeit. Az alapvető operációs rendszer biztosítja a készülékek működését, az alkalmazások lehetővé teszik a specifikus feladatok végrehajtását és a felhasználói preferenciákhoz való alkalmazkodást. Pintér Róbert kutatásai szerint az alkalmazások tulajdonképpen "szoftver protézisként" funkcionálnak, kiterjesztve az emberek cselekvési lehetőségeit mind a digitális, mind a fizikai térben.[278] Ezt a jelenséget Nyíri Kristóf filozófiai megközelítésben a "kiterjesztett elme" koncepciójával hozza összefüggésbe, ahol a technológiai eszközök az emberi kognitív képességek kiterjesztéseként értelmezhetők.[279] Az alkalmazások gazdasági szerepe kettős: egyrészt önmagukban is bevételi forrást jelentenek (közvetlen letöltések, előfizetések, alkalmazáson belüli vásárlások révén), másrészt új üzleti modellek kialakítását teszik lehetővé. A hagyományos egyszeri vásárlástól az előfizetéses modelleken át a freemium megoldásokig terjedő spektrum széles monetizációs lehetőségeket kínál a fejlesztők számára. Az IDC előrejelzése szerint 2025-re a globális digitális gazdaság közel harmadát az okoseszköz-alkalmazásokhoz köthető bevételek fogják alkotni.[280] A Budapesti Corvinus Egyetem Digitális Gazdaság Kutatóközpontja által végzett elemzés szerint a magyar applikációs piac értéke 2023-ban meghaladta a 30 milliárd forintot, és továbbra is dinamikus növekedést mutat.[281]

---

[277] Fehér Katalin, „Okos eszközök és alkalmazások használata a magyar lakosság körében", *Információs Társadalom* 22, sz. 1 (2022): 43–68, https://doi.org/10.22503/inftars.XXII.2022.1.3.
[278] Pintér Róbert, „A okos telefonok mint a kiterjesztett cselekvőképesség eszközei", *Replika* 111 (2019): 63–85, https://doi.org/10.32564/111.5.
[279] Nyíri Kristóf, „Mobilkommunikáció és az elme kiterjesztése", *Magyar Tudomány* 182, sz. 5 (2021): 598–609, https://doi.org/10.1556/2065.182.2021.5.8.
[280] I.D.C., *Worldwide Digital Transformation 2022 Predictions* (Framingham: International Data Corporation, 2022).
[281] *Budapesti Corvinus Egyetem Digitális Gazdaság Kutatóközpont* (Budapest: BCE, 2023).

Az okos eszközök alkalmazásai kulcsszerepet játszanak az adatgyűjtésben és elemzésben is. Az alkalmazások folyamatosan gyűjtik és feldolgozzák a felhasználói szokásokkal kapcsolatos információkat, amelyek értékes betekintést nyújtanak a fogyasztói magatartásba. Ezek az adatok nemcsak a fejlesztők számára hasznosak a felhasználói élmény javításában, hanem a marketing és üzleti elemzés területén is. Az alkalmazások által gyűjtött adatok olyan komplex profilok létrehozását teszik lehetővé, amelyek korábban elképzelhetetlenek voltak a hagyományos piackutatási módszerekkel.[282] Ez az adatgazdagság ugyanakkor adatvédelmi és etikai kérdéseket is felvet, amelyekkel a modern adatvédelmi szabályozásnak (például a GDPR-nak) foglalkoznia kell.[283]

Társadalmi szerepüket tekintve az alkalmazások megváltoztatták a kommunikáció módját (azonnali üzenetküldő alkalmazások), az információszerzés csatornáit (hírportálok), a szórakozási szokásokat (streaming és játék alkalmazások), a vásárlási folyamatokat (e-kereskedelmi platformok), sőt még az emberi kapcsolatok kialakításának és fenntartásának módját is (társkereső és közösségi média alkalmazások).[284] Ezek a változások a társadalmi rétegződés új formáit is létrehozták, amelyek a digitális kompetenciák és hozzáférés mentén alakulnak ki.[285] Az oktatási alkalmazások pedagógiai szerepe nemcsak a formális tanulási folyamatokat egészíti ki, hanem az informális és élethosszig tartó tanulás eszközei is. A megfelelő oktatási alkalmazások használata pozitív hatással van a tanulási motivációra és a tudáselsajátítás hatékonyságára.[286] A COVID-19 pandémia során különösen felértékelődött az oktatási alkalmazások szerepe, amikor a távoktatás vált a domináns oktatási formává, továbbá a jól megtervezett oktatási alkalmazások különösen hatékonyak lehetnek a differenciált oktatásban és a speciális nevelési igényű tanulók támogatásában.[287]

---

[282] Akadémia Magyar Tudományos, *Digitális Adatok a Társadalomtudományi Kutatásban: Etikai és Módszertani Kihívások* (Budapest: MTA Társadalomtudományi Kutatóközpont, 2022).
[283] Szőke Gergely László, „Adatvédelmi kihívások az okos eszközök korában", *Infokommunikáció és Jog* 78 (2021): 15–22.
[284] Vicsek Lilla, „Digitális Szociológia: Az okostelefon-használat társadalmi hatásai Magyarországon", *Replika* 120 (2021): 7–29, https://doi.org/10.32564/120.1.
[285] Csepeli György és Prazsák Gergő, „Új társadalmi törésvonalak a digitális korban", *Társadalomtudományi Szemle* 10, sz. 2 (2020): 8–25.
[286] Molnár Gyöngyvér és Turcsányi-Szabó Márta, „Mobilalkalmazások hatása a tanulási folyamatokra: Egy longitudinális vizsgálat eredményei", *Magyar Pedagógia* 122, sz. 1 (2022): 5–33, https://doi.org/10.17670/MPed.2022.1.5.
[287] Turcsányi-Szabó Márta, „Az okos telefonok szerepe a speciális nevelési igényű tanulók oktatásában", *Gyógypedagógiai Szemle* 48, sz. 3–4 (2020): 270–86.

Az okos eszközök alkalmazásai a közigazgatásban és közszolgáltatásokban is megjelentek. Az e-kormányzati szolgáltatások mobilalkalmazás formájában történő elérhetővé tétele növeli a közszolgáltatások hatékonyságát és hozzáférhetőségét. Magyarországon ilyen például az DÁP mobilalkalmazás, amely lehetővé teszi az állampolgárok számára a különböző közigazgatási ügyek intézését okos telefonon keresztül[288] A közigazgatási mobilalkalmazások fejlesztése stratégiai jelentőségű az állami szolgáltatások modernizációjában, és hozzájárulhat az adminisztratív terhek csökkentéséhez mind az állampolgárok, mind a közigazgatási szervek számára.[289]

3.3 Az okos eszközök alkalmazástípusainak sokszínűsége

Az okos eszközök alkalmazásainak kategorizálása komplex feladat, mivel egy-egy alkalmazás gyakran több kategóriába is besorolható, és a kategóriák közötti határok egyre inkább elmosódnak. Ennek ellenére érdemes áttekinteni a főbb típusokat, hogy átfogó képet kapjunk az alkalmazások sokszínűségéről

3.3.1 Fogyasztói alkalmazások

A fogyasztói alkalmazások alkotják a legnagyobb és legdinamikusabban fejlődő kategóriát. Ezek az alkalmazások elsősorban a végfelhasználók mindennapi igényeit szolgálják ki, személyes használatra készülnek. A kategória további alcsoportokra bontható:

- **Kommunikációs alkalmazások**: Ide tartoznak az üzenetküldő (WhatsApp, Messenger, Viber), közösségi média (Facebook, Instagram, TikTok) és e-mail (Gmail, Outlook) alkalmazások. Ezek az alkalmazások képezik az okos eszközök használatának gerincét, a Deloitte 2023-as Digital Consumer Trends jelentése szerint a felhasználók naponta átlagosan 85 percet töltenek kommunikációs alkalmazások használatával.[290] A magyar felhasználók esetében ez az arány még

[288] Hajnal György és Király Gábor, „E-közigazgatási megoldások és mobilalkalmazások a magyar közszolgáltatásokban", *Vezetéstudomány* 54, sz. 2 (2023): 15–29, https://doi.org/10.14267/VEZTUD.2023.02.02.
[289] Balázs Benjámin Budai, „Mobilalkalmazások a modern közigazgatásban: fejlesztési lehetőségek és korlátok", *Új Magyar Közigazgatás* 15, sz. 1 (2022): 59–71.
[290] Deloitte, *Digital Consumer Trends 2023* (London: Deloitte LLP, 2023).

magasabb, átlagosan napi 105 perc, ami társadalmi és kulturális tényezőkkel magyarázható.[291]

- **Szórakoztató alkalmazások**: A játékok, streaming szolgáltatások (Netflix, Spotify, YouTube), e-könyv olvasók és egyéb médiafogyasztást lehetővé tevő alkalmazások tartoznak ide. Ez a kategória generálja a legnagyobb bevételt, különösen a mobiljátékok, amelyek 2023-ban 116 milliárd dolláros globális bevételt termeltek.[292]
- **Produktivitást növelő alkalmazások**: Naptárak, jegyzetelő alkalmazások, dokumentumszerkesztők, felhőalapú tárolók, amelyek segítik a felhasználókat a mindennapi feladataik szervezésében és végrehajtásában. A Microsoft Office mobilalkalmazásait több mint 500 millió felhasználó használja világszerte.[293] De ebben a kategóriában értelmezhető az elektronikus közigazgatási alkalmazások is.
- **Életmód alkalmazások**: Fitness és egészségkövetők, étkezési naplók, meditációs segítők, alvásmonitorok, amelyek a jóllétet és egészséges életmódot támogatják. . A Semmelweis Egyetem kutatása szerint ezek az alkalmazások potenciállal rendelkeznek a népegészségügyi kihívások kezelésében, különösen a krónikus betegségek megelőzésében és kezelésében.[294]
- **Utazás és navigáció**: Térképek, GPS navigáció, tömegközlekedési információs rendszerek, utazási foglalási platformok, amelyek a mobilitást segítik elő. A legjelentősebb képviselője a Google Maps, amely havonta több mint 1 milliárd aktív felhasználóval rendelkezik.[295] A hazai fejlesztésű BKK FUTÁR alkalmazás a budapesti tömegközlekedés tervezését segíti, és a felhasználók értékelése alapján kiemelkedően sikeres a közösségi közlekedési alkalmazások között.[296]
- **Vásárlás és pénzügyek**: E-kereskedelmi platformok, banki alkalmazások, pénzügyi tervezők, amelyek a gazdasági tranzakciókat támogatják. A PayPal, Revolut és hasonló fintech alkalmazások forradalmasították a pénzügyi szolgáltatások

[291] Dessewffy Tibor és Láng László, „Mobilkommunikációs szokások kulturális különbségei: összehasonlító elemzés", *Szociológiai Szemle* 32, sz. 1 (2022): 85–106, https://doi.org/10.1556/SzocSzem.2022.1.4.
[292] App Annie, *State of Mobile 2023 Report* (San Francisco: App Annie Inc, 2023).
[293] Microsoft, *Annual Report 2023* (Redmond: Microsoft Corporation, 2023).
[294] Egyetem Semmelweis, *Mobilalkalmazások szerepe a krónikus betegségek megelőzésében és menedzselésében* (Budapest: Semmelweis Egyetem, Magatartástudományi Intézet, 2022).
[295] Google, „Economic Impact Report", in *Mountain View: Google LLC*, 2023.
[296] Munkácsy András és Jászberényi Melinda, „Közösségi közlekedési alkalmazások használata Magyarországon", *Közlekedéstudományi Szemle* 71, sz. 4 (2021): 42–55, https://doi.org/10.24228/KTSZ.2021.4.4.

elérhetőségét. Magyarországi viszonylatban megállapítható, hogy a lakosság digitális pénzügyi szolgáltatásokkal szembeni bizalma az elmúlt években növekedett, ami elősegítette a fintech alkalmazások gyors elterjedését.[297]

3.3.2 Üzleti és vállalati alkalmazások

Az üzleti alkalmazások a vállalati működést, együttműködést és hatékonyságot támogatják. Ezek gyakran komplex rendszerek részét képezik és integrálódnak a vállalati infrastruktúrába:

- **Vállalati erőforrás-tervezési (ERP) alkalmazások**: Átfogó rendszerek a vállalati folyamatok (pénzügy, humán erőforrás, ellátási lánc) kezelésére. A SAP, Oracle és Microsoft ERP rendszerei mobilalkalmazások formájában is elérhetőek, lehetővé téve a távoli hozzáférést és irányítást. A magyar vállalatok körében az ERP-rendszerek mobilalkalmazásokon keresztüli használata különösen a középvállalatok körében mutat növekedést.[298]
- **Ügyfélkapcsolat-kezelő (CRM) alkalmazások**: Az ügyfelekkel kapcsolatos információk és interakciók kezelésére szolgáló rendszerek. A Salesforce és hasonló CRM platformok mobilalkalmazásai lehetővé teszik az értékesítők számára az ügyfél információk valós idejű elérését és frissítését. A CRM-rendszerek mobilalkalmazásokon keresztüli használata átlagosan 27%-kal növeli az értékesítési hatékonyságot.[299]
- **Projektmenedzsment és együttműködési alkalmazások**: A csapatmunkát és kommunikációt segítő eszközök, például a Microsoft Teams, Slack, Asana, amelyek különösen fontossá váltak a távmunka elterjedésével. A COVID-19 pandémia következtében ezen alkalmazások használata 86%-kal növekedett 2020-

[297] Kerényi Ádám, „A fintech alkalmazások elterjedése Magyarországon", *Hitelintézeti Szemle* 21, sz. 1 (2022): 43–69, https://doi.org/10.25201/HSZ.21.1.4369.
[298] Talyigás Judit, „Imre Mojzes", *Vezetéstudomány* 52, sz. 3 (2021): 60–73, https://doi.org/10.14267/VEZTUD.2021.03.05.
[299] Egyetem Budapesti Gazdasági, *CRM-rendszerek mobil használatának hatásai az értékesítési folyamatokra* (Budapest: BGE Kutatóközpont, 2022).

ban.[300] A kollaborációs platformok alkalmazása nemcsak a munkavégzés hatékonyságát növeli, hanem a szervezeti kultúrára és a munkahelyi elégedettségre is pozitív hatással van.[301]

- **Adatelemzési és üzleti intelligencia alkalmazások**: Valós idejű adatelemzést és vizualizációt biztosító eszközök, amelyek segítik a vezetői döntéshozatalt. A Tableau, Power BI és QlikView mobilalkalmazásai lehetővé teszik a fontos üzleti mutatók állandó nyomon követését.[302]
- **Iparág-specifikus alkalmazások**: Speciális ágazati igényekre szabott alkalmazások, például egészségügyi információs rendszerek, logisztikai alkalmazások, ingatlankezelő platformok. A Gartner előrejelzése szerint 2025-re a vállalati mobilalkalmazások 70%-az iparág-specifikus funkcionalitással fog rendelkezni.[303]

3.3.3 Speciális alkalmazások

A fentiek kapcsán továbbá kiemelendőek az IoT és okos otthon, továbbá a speciális szakmai alkalmazások, amelyek besorolhatóak a fenti kategóriákba, de lehetnek, átfedések illetve kissé kilógnak a tipológiából. Az IoT (Internet of Things) és okos otthon alkalmazások az összekapcsolt eszközök vezérlését és monitorozását teszik lehetővé, amelynek egyes típusai lehetnek fogyasztói (okos otthonok vezérlők) vagy éppen vállalati (energiahatékonysági alkalmazások, ipari IoT alkalmazások) felhasználásúak. A specializált szakmai alkalmazások különböző szakterületek speciális igényeit szolgálják ki, így sokszor egy fogyasztó használja, nem egy vállat, de más célokkal ilyenek:

- **Egészségügyi alkalmazások**: Az orvosok, ápolók és más egészségügyi szakemberek munkáját támogató rendszerek, amelyek lehetővé teszik a beteg-adatok biztonságos kezelését, diagnosztikai támogatást nyújtanak, vagy akár távkonzultációt tesznek lehetővé. Az okos eszközök és a big data alapú személyre szabott egészségügyi szolgáltatások kombinációja hozzájárulhat az egészség előmozdításához, a fizikai aktivitás nyomon követésével, a betegségek megelőzésével és

[300] International Data Corporation, *Worldwide Mobile Enterprise Applications Market Forecast, 2021-2025* (Framingham: IDC, 2021).
[301] Makó Csaba és Illéssy Miklós, „Technológiai változások és szervezeti innovációk kölcsönhatása: az alkalmazottak munkahely-átalakítási akciói", *Vezetéstudomány* 51, sz. 10 (2020): 59–68, https://doi.org/10.14267/VEZTUD.2020.10.05.
[302] Nemeslaki András, „Az adatvezérelt döntéshozatal szerepe a nemzetközi piacokon működő vállalatok digitális transzformációjában", *Külgazdaság* 65, sz. 5–6 (2021): 30–52.
[303] Gartner, *Market Guide for Mobile Enterprise Applications* (Stamford: Gartner Inc, 2023).

az egészségügyi adatok elemzésével,[304] a telemediciális alkalmazások akár 45%-kal is növelhetik a távoli területeken élők egészségügyi ellátáshoz való hozzáférését.[305]

- **Oktatási alkalmazások**: Tanulást támogató rendszerek, virtuális osztálytermek, adminisztrációs eszközök oktatási intézmények számára. A COVID-19 pandémia alatt az oktatási alkalmazások használata globálisan 90%-kal nőtt.[306]
- **Tudományos és kutatási alkalmazások**: Adatgyűjtést, elemzést és vizualizációt segítő eszközök kutatók számára. A mobil adatgyűjtési módszerek akár 40%-kal is növelhetik a terepen végzett kutatások hatékonyságát,[307] továbbá a tudományos mobilalkalmazások használata felgyorsíthatja az adatelemzési folyamatokat a komplex társadalomtudományi kutatásokban.[308]
- **Mérnöki és tervezési alkalmazások**: CAD/CAM rendszerek, épülettervező, gépészeti szimulációs eszközök, amelyek már okos telefonokon és tableteken is elérhetők. Az Autodesk és hasonló vállalatok mobilalkalmazásai lehetővé teszik a mérnökök számára a tervek helyszíni módosítását és valós idejű együttműködést. A mérnöki mobilalkalmazások használata átlagosan 23%-kal csökkenti a tervezési projektek átfutási idejét.[309]
- **Jogi és szabályozási alkalmazások**: Jogi adatbázisok, esetkezelő rendszerek, megfelelőségi ellenőrző eszközök. A LegalTech startupok száma az elmúlt öt évben megháromszorozódott, amelyek része mobilalkalmazásokat is fejleszt a jogi szakemberek és laikusok számára egyaránt.[310] A mesterséges intelligenciát alkalmazó jogi alkalmazások különösen hatékonyak lehetnek a rutinszerű jogi feladatok automatizálásában, ami növelheti a jogászok produktivitását.[311]

---

[304] Nagy János és Erdélyi Márk, „Okos eszközök és big data alapú megoldások az egészségmegőrzésben", *Orvosi Hetilap* 162, sz. 18 (2021): 696–705, https://doi.org/10.1556/650.2021.32064.
[305] Bogner Péter, Horváth Attila, és Berki Tímea, „Telemediciális alkalmazások hatása az egészségügyi ellátáshoz való hozzáférésre hátrányos helyzetű régiókban", *Egészségfejlesztés* 63, sz. 3 (2022): 45–57, https://doi.org/10.24365/ef.v63i3.723.
[306] U.N.I.C.E.F., *COVID-19: Are Children Able to Continue Learning during School Closures?* (New York: UNICEF, 2021).
[307] Ráthonyi-Ódor Kinga, Ráthonyi Gergely, és Bába Éva Bácsné, „Mobil adatgyűjtési módszerek hatékonyságvizsgálata terepkutatásokban", *Erdélyi Társadalom* 20, sz. 1 (2022): 121–38, https://doi.org/10.17177/77171.258.
[308] Hálózat Eötvös Loránd Kutatási, *Mobil adatgyűjtési és elemzési módszerek alkalmazása komplex társadalomtudományi kutatásokban* (Budapest: ELKH, 2023).
[309] Kovácsházy Tamás, Takács Barnabás, és Charaf Hassan, „Mérnöki mobilalkalmazások hatása a tervezési folyamatok időigényére", *Gép* 72, sz. 3 (2021): 67–76.
[310] Thomson Reuters, *Emerging LegalTech Market Analysis* (Toronto: Thomson Reuters Corporation, 2023).
[311] Ződi Zsolt, „A mesterséges intelligencia alkalmazása a jogi munkában", *Jogtudományi Közlöny* 77, sz. 1 (2022): 15–28.

- **E-közigazgatás, m-közigazgatás alkalmazásai**: Az elektronikus ügyintézés a közigazgatási ügyek elektronikus úton való elvégzését elsősorban az elektronizált, online szolgáltatásokat érthetjük (például Ügyfélkapu+). Az m-közigazgatás az e-közigazgatás részeként is tekinthető, azonban sajátosságai miatt önálló szolgáltatási rendszert képez.[312]

3.4 Az okos eszközök alkalmazásainak fejlesztési trendjei és technológiái

Az okos eszközök applikációinak jövőjét számos technológiai fejlesztés, társadalmi trend és szabályozási kérdés fogja alakítani. Ezek a tényezők együttesen határoznak majd meg egy dinamikusan fejlődő környezetet, amely mind a fejlesztőket, mind a felhasználókat új lehetőségekkel és kihívásokkal szembesíti. A technológiai fejlődés új lehetőséget nyit meg az alkalmazásfejlesztés területén.

3.4.1 Mesterséges intelligencia, gépi tanulás és algoritmusok szerepe

A mesterséges intelligencia és gépi tanulás integrációja új funkcionalitást és személyre szabott élményt biztosít. A felhasználói viselkedés elemzésével előre jelző és alkalmazkodó rendszerek, amelyek anticipálják a felhasználói igényeket (pl. következő úti cél javaslata, elgépelések automatikus javítása). A prediktív algoritmusok akár 35%-kal is csökkenthetik a felhasználók által alkalmazások használatára fordított időt, miközben növelik a felhasználói elégedettséget.[313] A chatbotok, virtuális asszisztensek és hangvezérelt interfészek, amelyek természetes kommunikációt tesznek lehetővé. Az NLP (Natural Language Processing – természetes nyelvfeldolgozás) technológiák lehetővé teszik az alkalmazások használatát fogyatékkal élők számára is.[314] Az okos eszközök interakciós lehetőségei folyamatosan bővülnek, új kommunikációs csatornákat nyitva. A Siri, Google Assistant, Alexa és hasonló rendszerek integrációja az alkalma-

[312] Peter Sasvari, „Közigazgatási informatikai alkalmazások", elérés 2025. május 3., https://www.academia.edu/30804398/K%C3%B6zigazgat%C3%A1si_informatikai_alkalmaz%C3%A1sok.
[313] Szathmáry László, Gábor András, és Bogdanov Péter, „Prediktív algoritmusok hatása a felhasználói időráfordításra és elégedettségre", *Információs Társadalom* 22, sz. 2 (2022): 46–67, https://doi.org/10.22503/inftars.XXII.2022.2.4.
[314] Galántai Zoltán, „A természetes nyelvfeldolgozás szerepe az akadálymentes digitális technológiákban", *Infokommunikáció és Jog* 73 (2021): 28–37.

zásokba új interakciós módot biztosít. A hangvezérlés különösen fontos az akadálymentesítés szempontjából, valamint olyan helyzetekben, amikor a kéz foglalt (vezetés, főzés).[315]

A felhasználói preferenciák alapján releváns tartalmakat és szolgáltatásokat javasló algoritmusok, amelyek növelik a felhasználói elégedettséget és az alkalmazásban töltött időt. A Netflix becsült adatai szerint ajánlórendszerük évente több mint 1 milliárd dollárt takarít meg a vállalatnak a megtartott előfizetések révén.[316]

Megjelent már a gesztus alapú vezérlés lehetősége is, ami kézmozdulatok, szemkövetés és egyéb non-verbális inputokat értelmez, különösen AR/VR környezetben. A magyar kutatók által fejlesztett Air Touch technológia például lehetővé teszi az eszközök érintés nélküli, levegőben történő vezérlését.[317]

3.4.2 5G és későbbi hálózati technológiák

Az 5G technológia (4G+) ultra alacsony késleltetés és nagy sávszélesség új alkalmazástípusokat tesz lehetővé, például valós idejű AR/VR élményeket, távoli sebészeti beavatkozásokat, vagy multi-player játékokat minimális késleltetéssel. Imre Sándor és munkatársai szerint az 5G és a jövőbeli 6G technológiák különösen nagy potenciállal rendelkeznek az ipari alkalmazások terén, lehetővé téve a valós idejű távoli irányítást és monitorozást.[318]

3.4.3 Edge computing

Az edge computing (peremhálózati számítástechnika) olyan elosztott számítástechnikai architektúra, amelyben az adatfeldolgozás és tárolás fizikailag közel helyezkedik el az adatforráshoz, minimalizálva a késleltetést és a sávszélesség-igényt.[319] A fogalom legszűkebb értelmezésében a felhőn kívüli, hálózati peremrétegen történő számítási

---

[315] Jonathan Vettel, „Voice User Interfaces for Accessibility: Current State and Future Directions", *International Journal of Human-Computer Interaction* 39, sz. 2 (2023): 1–15, https://doi.org/10.1080/10447318.2022.2070852.
[316] Netflix, *The Value of Recommendation Systems* (Los Gatos: Netflix Inc, 2023).
[317] Hungarian Academy Sciences, *Air Touch: Contactless Control Technology* (Budapest: MTA, 2023).
[318] Imre Sándor, Farkas Károly, és Schulcz Róbert, „5G és 6G rendszerek az ipari alkalmazások szolgálatában: követelmények és megoldások", *Híradástechnika* 78, sz. 2 (2023): 15–24.
[319] Weisong Shi és mtsai., „Edge Computing: Vision and Challenges", *IEEE Internet of Things Journal* 3, sz. 5 (2016): 637–46, https://doi.org/10.1109/JIOT.2016.2579198.

folyamatokat jelenti, különösen olyan alkalmazások esetén, amelyek valós idejű adatfeldolgozást igényelnek.[320] Az adatfeldolgozás közelebb hozása a felhasználóhoz csökkenti a késleltetést és növeli az alkalmazások teljesítményét, különösen IoT kontextusban. A Gartner előrejelzése szerint 2025-re az vállalati adatok 75%-az a felhőn kívül, edge eszközökön fog generálódni és feldolgozásra kerülni. [321]

3.4.4 Blockchain és decentralizált alkalmazások (dApps)

A blockchain technológia alkalmazása új lehetőségeket nyit meg a bizalmi rendszerek kiépítésében, digitális identitáskezelésben és decentralizált szolgáltatások nyújtásában. A decentralizált alkalmazások piaca várhatóan 200 milliárd dollárra nő 2025-re.[322] A blockchain-alapú alkalmazások értékesek lehetnek az olyan területeken, ahol a bizalom és a tranzakciók hitelessége kulcsfontosságú, például a pénzügyi szolgáltatások vagy a közigazgatás területén.[323] Jelen technológia kiemelt éggel bírhat a személyazonosításra és személyi hitelesítésre alkalmas technológiák fejlesztése és alkalmazása kapcsán.

3.4.5 Ambient computing

A mindenütt jelenlévő számítástechnika koncepciója, ahol a számítási képességek integrálódnak a környezetbe, és az okos eszközök közötti zökkenőmentes átjárhatóság valósul meg. A fényképünk készítés közben automatikusan szinkronizálódnak eszközeink között, a hűtő érzékeli a kifogyó élelmiszereket és automatikusan figyelmeztet, miközben a lakás hőmérséklete és világítása alkalmazkodik a napi rutinunkhoz.[324] Az ambient computing paradigma az emberi kognitív képességek kiterjesztésének új szintjét jelentheti, ahol a technológia és az ember között folyamatos, szinte észrevehetetlen interakció valósul meg.[325]

---

[320] „Edge Computing", *Microsoft Research* (blog), elérés 2025. május 3., https://www.microsoft.com/en-us/research/project/edge-computing/.
[321] Gartner, *Predicts 2025: Edge Computing Will Redefine Infrastructure* (Stamford: Gartner Inc, 2022).
[322] Grand View Research, *Decentralized Application Market Size, 2023-2030* (San Francisco: Grand View Research, Inc, 2023).
[323] Szádeczky Tamás, Keserű Balázs, és Mezőfi Márk, „Blockchain-alapú megoldások az e-közigazgatásban", *Információs Társadalom* 22, sz. 4 (2022): 7–26, https://doi.org/10.22503/inftars.XXII.2022.4.1.
[324] Microsoft Research, *Ambient Computing: The Next Era of Personal Technology* (Redmond: Microsoft Research, 2023).
[325] Baranyi Péter, „Az ember és a technológia kognitív fúziója", *Magyar Tudomány* 183, sz. 6 (2022): 730–43, https://doi.org/10.1556/2065.183.2022.6.4.

3.4.6 Felhasználói szemléletből fakadó tényezők

Azonban felhasználói szokások és elvárások, úgymond az adott applikáció társadalmi elfogadottsága hatással van az alkalmazásfejlesztésre: A felhasználók egyre inkább vonakodnak új alkalmazásokat letölteni, preferálva a már meglévőket vagy a beépített funkcionalitást. Ez arra ösztönzi a fejlesztőket, hogy értéknövelt, egyedi szolgáltatásokat nyújtsanak, vagy alternatív megoldásokat (mini-alkalmazások, chatbotok) keressenek.[326] A magyar felhasználók esetében is megfigyelhető ez a tendencia, különösen a 35 év feletti korosztályban, akik átlagosan kevesebb, mint 5 új alkalmazást töltenek le évente.[327] A felhasználók egyre inkább elvárják a teljesen személyre szabott élményt, amely figyelembe veszi egyéni preferenciáikat, szokásaikat és kontextusukat. Az AI-vezérelt személyre szabás már nem luxus, hanem alapelvárás sok területen.[328] Szektorban, ahol a vásárlói preferenciák erősen fragmentáltak.[329]

Az adatvédelmi botrányok és növekvő tudatosság következtében a felhasználók egyre inkább értékelik azokat az alkalmazásokat, amelyek, transzparensek az adatgyűjtési gyakorlataikkal kapcsolatban és minimalizálják a gyűjtött adatok körét.[330] A magyar felhasználók körében is növekszik az adatvédelmi tudatosság, különösen a fiatalabb, magasan képzett rétegekben.[331] Azonban az okos eszközök és alkalmazásaik nem egyenlően érhetők el minden társadalmi réteg számára, ami növelheti a már meglévő egyenlőtlenségeket. Magyarországon is fennáll a digitális szakadék, különösen a vidéki, alacsony jövedelmű háztartások és az idősebb generációk körében.[332]

Az alkalmazások addiktív természete, különösen a közösségi média és játékok esetében, mentális egészségügyi kockázatokat hordozhat. A Magyar Pszichiátriai Társaság

---

[326] App Annie, *State of Mobile 2022: App Download and Usage Trends* (San Francisco: App Annie Inc, 2022).
[327] Urbán Ágnes, „Magyar felhasználók okostelefon-használati szokásai és applikáció-telepítési preferenciái", *Médiakutató* 23, sz. 1 (2022): 9–26.
[328] Gartner, *Hyper-Personalization: The Future of Customer Experience* (Stamford: Gartner Inc, 2023).
[329] Bányai Edit, Németh Péter, és Petruska Ildikó, „A hiperperszonalizáció lehetőségei és korlátai a magyar e-kereskedelmi szektorban", *Marketing & Menedzsment* 56, sz. 2 (2022): 15–29, https://doi.org/10.15170/MM.2022.56.02.02.
[330] Deloitte, *Digital Consumer Trends 2023*.
[331] Székely Iván, Parti Katalin, és Szőke Gergely László, „Adatvédelmi tudatosság a magyar lakosság körében: reprezentatív felmérés eredményei", *Replika* 126 (2023): 103–21, https://doi.org/10.32564/126.6.
[332] Csepeli György és Prazsák Gergő, „Digitális egyenlőtlenségek Magyarországon: életkor, lakóhely és társadalmi státusz szerepe", *Információs Társadalom* 22, sz. 2 (2022): 120–40, https://doi.org/10.22503/inftars.XXII.2022.2.7.

jelentése szerint az okostelefon-függőség a magyar tizenévesek körében eléri a 25%-ot.[333] Azonban növekvő igény mutatkozik az alkalmazások részéről a kiegyensúlyozott, egészséges használat támogatására, a túlzott képernyőidő csökkentésére. Az Apple és Google is bevezetett digitális jólléti funkciókat, amelyek segítenek a felhasználóknak kontrollálni a képernyőhasználatot.[334]

A fejlődés irányait befolyásolhatja még a növekvő adatgyűjtés és elemzés etikai határainak politikai és/vagy társadalmi diskurzusa. Különösen érzékeny területek a biometrikus adatok, egészségügyi információk és a gyermekekre vonatkozó adatok kezelése.[335]

A szabályozási környezet is hatással van az alkalmazásfejlesztésre és használatra. A GDPR után számos ország vezet be hasonló vagy még szigorúbb adatvédelmi törvényeket, amelyeknek való megfelelés növekvő kihívást jelent a fejlesztők számára. A nemzetközi jelenléttel rendelkező alkalmazásoknak akár tíz különböző jogrendszer eltérő szabályainak is meg kell felelniük.[336] Növekvő szabályozói figyelem irányul továbbá az Apple és Google App Store gyakorlataira, különös tekintettel a jutalékokra és az alternatív terjesztési csatornákra. Az Európai Unió Digitális Piacok Törvénye (DMA) kötelezi a nagy platformüzemeltetőket, hogy engedélyezzék harmadik féltől származó alkalmazás-áruházak és fizetési rendszerek használatát.[337]

A fenntarthatóság növekvő fontossága új szempontokat hoz az alkalmazásfejlesztésbe. Az applikációk optimalizálása az akkumulátor-élettartam növelése és az energiafogyasztás csökkentése érdekében, amely nemcsak felhasználói előny, hanem környezeti

[333] Társaság Magyar Pszichiátriai, *A hazai okostelefon-függőség prevalenciája serdülők körében* (Budapest: Magyar Pszichiátriai Társaság, 2023).
[334] Google, „Digital Wellbeing Experiments: New Tools for Finding Balance with Technology", in *Mountain View: Google LLC*, 2022.
[335] Szőke Gergely László, „Biometrikus adatok kezelésének jogi és etikai kérdései", *Jogtudományi Közlöny* 77, sz. 3 (2022): 120–32.
[336] D.L.A. Piper, *Data Protection Laws of the World* (London: DLA Piper UK LLP, 2023).
[337] Unió Európai, „Az Európai Parlament és a Tanács rendelete a digitális piacokról (Digitális piacokról szóló jogszabály", *Az Európai Unió Hivatalos Lapja* 265, sz. 1 (2022).

szempont is.[338] Továbbá az adatközpontok energiafelhasználásának és környezeti hatásának minimalizálása a hatékonyabb felhőszolgáltatások révén. Az ICT szektor globálisan a CO2 kibocsátás 2-4%-áért felelős, és ez az arány növekszik.[339]

Az okos eszközök applikációi rendkívül sokrétű és dinamikusan fejlődő területet képviselnek, amely alapvetően meghatározza a digitális technológiák társadalmi adaptációját és hatását. A kezdeti egyszerű alkalmazásoktól eljutottunk a komplex, mesterséges intelligenciát alkalmazó rendszerekig, amelyek életünk szinte minden területén jelen vannak. Ezek az alkalmazások nemcsak a felhasználói élményt javítják, és új funkcionalitásokat biztosítanak, hanem gazdasági, társadalmi és kulturális változások katalizátorai is.

Az alkalmazástípusok széles spektruma mutatja, hogy az okos eszközök univerzális platformmá váltak, amelyek a hétköznapi kommunikációtól a specializált szakmai feladatokig számtalan területen nyújtanak megoldásokat. A technológiai fejlődés, különösen a mesterséges intelligencia, edge computing, 5G és AR/VR területén, további innovációs lehetőségeket nyit meg a fejlesztők számára. Ahogy Z. Karvalics László információtörténész fogalmaz: "Az okos eszközök alkalmazásai nem pusztán eszközök, hanem kulturális szignálok és társadalmi változások indikátorai is."[340]

3.5 Személyazonosításra és hitelesítésre alkalmas eszközzé válás

Az okos eszközökre, különösen a mobiltelefonokra fejlesztett alkalmazások figyelemreméltó fejlődésen mentek keresztül az elmúlt évtizedben, és kulcsfontosságú eszközökké váltak a személyazonosítás és hitelesítés szempontjából. Ez a folyamat nemcsak technikai innovációkat tett lehetővé, hanem forradalmasította a felhasználói élményt és új szintre emelte a biztonsági szabványokat. De mit is értünk személyazonosítás, illetve személyi hitelesítés alatt? A személyazonosítás (identification) az a folyamat, amely során meghatározzuk egy személy, eszköz vagy entitás identitását. Ez lényegé-

[338] Google, „Android Vitals: Energy Efficiency in Mobile Applications", in *Mountain View: Google LLC*, 2023.
[339] International Energy Agency, *Digitalization and Energy: The Environmental Footprint of the ICT Sector* (Paris: IEA, 2022).
[340] Karvalics László Z., „Az okos eszközök mint társadalmi változások katalizátorai", in *Információs társadalom kézikönyv* (Budapest: Gondolat Kiadó, 2021), 247–63.

ben egy kijelentés arról, hogy "ki vagyok én". Személyazonosításra alkalmas technológiának tekintjük azokat a módszereket és eszközöket, amelyek lehetővé teszik egy egyén azonosítását a megadott környezetben. Ezzel szemben a személyi hitelesítés (authentication) az a folyamat, amely során ellenőrizzük egy állított identitás valódiságát. Míg az azonosítás arra a kérdésre válaszol, hogy "ki vagyok én", a hitelesítés azt vizsgálja, hogy "hogyan bizonyítom, hogy valóban az vagyok, akinek állítom magam".[341] A hitelesítés tehát az azonosság bizonyítására szolgál. Bár a személyazonosítás és a személyi hitelesítés szorosan kapcsolódó fogalmak, és a gyakorlatban gyakran egymásra épülnek, fontos megérteni a közöttük lévő különbségeket. A személyazonosítás és a személyi hitelesítés közötti alapvető különbség a céljukban rejlik. A személyazonosítás megelőzi a hitelesítést a biztonsági folyamatokban. Először azonosítjuk magunkat (pl. felhasználónév megadásával), majd hitelesítjük ezt az identitást (pl. jelszó megadásával).

3.5.1 A személyazonosítás főbb típusai

A személyazonosításra alkalmas technológiákat több kategóriába sorolhatjuk:

Fizikai azonosító dokumentumok

A hagyományos fizikai azonosító dokumentumok, mint a személyi igazolvány, útlevél, jogosítvány, továbbra is a személyazonosítás alapvető eszközei. Ezek a dokumentumok fizikai formában tartalmazzák a személy azonosításához szükséges adatokat, valamint különböző biztonsági elemeket (hologramok, speciális nyomtatási technikák), amelyek megnehezítik a hamisítást.[342]

Elektronikus személyazonosító dokumentumok

Az elektronikus személyazonosító dokumentumok a hagyományos fizikai azonosítók továbbfejlesztett változatai, amelyek chipet tartalmaznak az adatok elektronikus tárolására. Magyarországon ilyen például az elektronikus személyazonosító igazolvány (e-

[341] „Mi az a hitelesítés? Definíció és módszerek | Microsoft Biztonság", elérés 2025. május 3., https://www.microsoft.com/hu-hu/security/business/security-101/what-is-authentication.
[342] Lászlóné dr Hazai, „Okmányvédelem, az NBSZ okmányvédelemmel kapcsolatos szakértői, hatósági tevékenysége", *Nemzetbiztonsági Szemle* 3, sz. 3 (2015. szeptember 30.): 60–100.

Személyi), amely a hagyományos személyazonosító funkción túl számos elektronikus szolgáltatást is támogatott.[343]

Biometrikus azonosítók

A biometrikus azonosítás az egyén egyedi fiziológiai vagy viselkedési jellemzőin alapul. A leggyakoribb biometrikus azonosítási módszerek közé tartozik az ujjlenyomat-azonosítás, az arcfelismerés, az írisz-szkennelés, a hangazonosítás és a retina-szkennelés.[344] A biometrikus azonosítók előnye, hogy nehezen hamisíthatók, és általában egyediek az adott személyre nézve. Ugyanakkor hátrányuk lehet a magasabb költség és a potenciálisan magasabb hibaarány bizonyos körülmények között.

Digitális azonosítók

A digitális azonosítók közé tartoznak a különböző felhasználónevek, email címek, digitális tanúsítványok és egyéb online azonosításra használt adatok. Ezek az azonosítók különösen fontosak a digitális szolgáltatások, online platformok és elektronikus közigazgatási szolgáltatások használatakor.[345]

3.5.2 A személyi hitelesítés főbb típusai

A vonatkozó szakirodalmi kutatás alapján, alapvetően a személyi hitelesítési technológiákat alapvetően az alábbi kategóriába soroljuk:

Tudásalapú hitelesítés

A tudásalapú hitelesítés során a felhasználó olyan információt biztosít, amelyet csak ő ismer. Ide tartoznak a jelszavak, PIN-kódok, biztonsági kérdések és válaszok. Ez a legelterjedtebb hitelesítési forma, azonban biztonsági szempontból sebezhetőséget jelenthet, ha a felhasználók gyenge jelszavakat választanak vagy ugyanazt a jelszót több szolgáltatáshoz is használják.[346]

---

[343] "Mi az e-Személyi igazolvány? Miért van szükség az e-Személyire." e-egeszsegugy.gov.hu, https://e-egeszsegugy.gov.hu/documents/26398/211405/eSzig/190ca028-b903-7e7a-c4a0-5e81c3cb73d9

[344] „Mi az a biometrikus azonosítás, és miért jó, ha használod?", elérés 2025. május 3., https://digipedia.hu/cikk/mi-az-a-biometrikus-azonositas-es-miert-jo-ha-hasznalod.

[345] „Digitális személyazonosítás: mi a kulcs? - GoodID white paper", elérés 2025. május 3., https://goodid.net/hu/white-paper-ugyfel-azonositas/.

[346] Bankszövetség Magyar, *Az e-Személyi használata a banki ügyintézésben – Iparági ajánlás* (Budapest: Magyar Bankszövetség, 2021).

Birtoklásalapú hitelesítés

A birtoklásalapú hitelesítés során a felhasználó olyan eszközt vagy tárgyat mutat fel, amely csak az ő birtokában van. Ide tartoznak a különböző tokenek, okos kártyák, mobileszközök és egyéb hardveres kulcsok. Például az e-Személyi használata során a kártyabirtokos a PIN-kód megadásával bizonyítja, hogy jogosult a kártyához tartozó elektronikus funkciók használatára.[347] Magyarországon jellemző példa volt a birtoklásalapú hitelesítésre az eSzemélyiM mobilalkalmazás, amely az e-Személyi funkcióit terjeszti ki okos telefonokra, lehetővé téve a kártyán tárolt adatok kezelését és az elektronikus azonosítást mobil eszközökön keresztül. Hasonlóképpen, az EESZT (Elektronikus Egészségügyi Szolgáltatási Tér) rendszeréhez kapcsolódó EESZT mobiltoken is egy birtoklásalapú hitelesítési megoldás, amely egy mobilalkalmazás által generált időalapú jelszót használ a belépéshez.

Biometrikus hitelesítés

A biometrikus hitelesítés során a felhasználó fizikai vagy viselkedési jellemzőit használjuk az azonosság megerősítésére. Ide tartozik az ujjlenyomat-ellenőrzés, az arcfelismerés, a hangazonosítás, az írisz-szkennelés és egyéb biometrikus jellemzők ellenőrzése[348] A biometrikus hitelesítés előnye, hogy nehezen hamisítható és általában felhasználóbarát, azonban hátrányai közé tartozhat a magasabb költség és a potenciális adatvédelmi aggályok. Álláspontom alapján a biometrikus hitelestés a birtoklásalapú hitelesítés egyfajta egyedi, mondhatni természetes alfaja.

Többfaktoros hitelesítés

A többfaktoros hitelesítés (MFA) az előző három kategória kombinációját jelenti, amikor a hitelesítéshez több, különböző típusú faktort használunk egyidejűleg. Például amikor egy banki tranzakció során a felhasználó megad egy jelszót (tudásalapú), majd egy mobilalkalmazáson keresztül megerősíti a tranzakciót (birtoklásalapú). A többfaktoros hitelesítés növeli a biztonságot, mivel több tényezőt kell egyszerre kompromittálni egy sikeres támadáshoz. Magyarországon példa erre az Ügyfélkapu+ rendszer, amely kétfaktoros azonosítást kínál. Ebben a rendszerben a felhasználónév és jelszó

[347] "Mi az e-Személyi igazolvány? Miért van szükség az e-Személyire." e-egeszsegugy.gov.hu, https://e-egeszsegugy.gov.hu/documents/26398/211405/eSzig/190ca028-b903-7e7a-c4a0-5e81c3cb73d9

[348] „OTP Bank - Biometrikus azonosítás is segíti a telefonos ügyintézést", elérés 2025. május 3., https://www.otpbank.hu/portal/hu/hirek/biometrikus-azonositas.

mellett egy időalapú egyszer használatos jelszót (Time-based One-Time Password, TOTP) is használnak az azonosításhoz.[349]

A személyazonosítás és személyi hitelesítés technológiái alapvető fontosságúak a digitális biztonság megteremtésében. Míg a személyazonosítás meghatározza, hogy ki az adott felhasználó, a személyi hitelesítés biztosítja, hogy a felhasználó valóban az, akinek állítja magát. A két technológiai terület közötti különbségek megértése elengedhetetlen a hatékony biztonsági rendszerek tervezéséhez és implementálásához. A modern megközelítések egyre inkább a többfaktoros hitelesítés, a biometrikus azonosítók és a decentralizált identitáskezelés irányába mozdulnak el, javítva a biztonságot és a felhasználói élményt.

3.5.3 A mobil azonosítás fejlődésének áttekintése

A mobil azonosítási technológiák lehetővé teszik a digitális személyazonosság hitelesítését mobil eszközökön keresztül. Az egyének mobilböngészőkön vagy alkalmazásokon keresztül igazolhatják személyazonosságukat, amikor távolról nyitnak bankszámlát, vagy különböző szolgáltatásokat vesznek igénybe. A COVID-19 világjárvány időszakában megnövekedett a távoli szolgáltatások iránti igény, ami az emberek körében fokozta a pénzügyi szolgáltatások mobil eszközökön történő elérésének függőségét. Ez az időszak a technológia fejlődésének figyelemreméltó felgyorsulását is eredményezte.[350] Az identitás-ellenőrző algoritmusok különféle folyamatokat alkalmazhatnak a megfelelő működés érdekében. Az elérhető megoldások között alapvető fontosságúak a dokumentum-ellenőrzési eljárások, a biometrikus adatok alkalmazása, az élőségi felismerés (liveness detection) megvalósítása és az egyszer használatos jelszavak (OTP) használata. Ezen technikák együttes figyelembevételével megbízható módon validálható a felhasználói személyazonosság.[351]

---

[349] Ügynökség Kormányzati Informatikai Fejlesztési, *Központi Azonosítási Ügynök (KAÜ) – Rendszerleírás* (Budapest: KIFÜ, 2021).
[350] „Digital Identity: Accelerating Financial Inclusion During a Crisis | Mobile for Development", elérés 2025. május 3., https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/gsma_resources/digital-identity-accelerating-financial-inclusion-during-a-crisis/.
[351] „What Is Identity Verification? | OneSpan", elérés 2025. május 3., https://www.onespan.com/topics/identity-verification.

A biometrikus azonosítás integrálása a mobilalkalmazásokba növelheti a felhasználók számára elérhető biztonságot és testreszabási lehetőségeket. Az azonosítás és hitelesítés céljából a biometria az emberek egyedi biológiai vagy viselkedési jellemzőit használja fel, így lényegesen magasabb szintű biztonságot nyújt a hagyományos jelszavas rendszerekhez képest.[352] Azonban itt kel megjegyezni, hogy ez nagyban attól is függ, hogy az adott alkalmazás hány vektort vesz figyelembe ilyenkor. A mobilalkalmazásokban alkalmazott biometrikus módszerek között megtalálható az ujjlenyomat-azonosítás, az arcfelismerés, az íriszleolvasás, valamint újabban a viselkedési biometria integrálása is. E technológiák bevezetése javítja a biztonsági intézkedéseket, miközben egyidejűleg fokozza a felhasználói élményt a bejelentkezési folyamatok egyszerűsítésével és felhasználóbarátabbá tételével. Ezt a bejelentkezési folyamat felgyorsításával érik el. A kutatások szerint a többfaktoros hitelesítés alkalmazása, amely a biometrikus elemeket különféle egyéb azonosítási technikákkal kombinálja, javítja a biztonsági intézkedéseket. Az elmúlt években számos innovatív megközelítés jelent meg a mobil azonosítás területén. 2022-ben egy kutatócsoport olyan újszerű módszert javasolt, amely a pislogás során bekövetkező bőr deformáció jelenségét használja fel. E módszer célja a személyes azonosítás megkönnyítése a szemüveghez hasonló eszközök használatával. Hét személyből álló csoportra alkalmazva ez a megközelítés 97,1%-os azonosítási pontosságot eredményezett.[353] A háromdimenziós érintésérzékelők integrálása az ujjelhelyezéssel, kapcsolatos adatokkal egyedülálló áttörésnek számít a hitelesítési technológia területén. Egy 2025-ben végzett vizsgálat kimutatta, hogy ez a speciális megközelítés 83%-os pontossági arány elérésében volt sikeres, miközben csökkentette mind a hamis pozitív, mind a hamis negatív eredmények számát.[354]

Az aktív akusztikus érzékelés területén is előrelépést értek el a kutatók egy forradalmi technológia felfedezésével, amely zökkenőmentesen beépíthető a szemüvegkeretekbe. Ez a csúcstechnológiás megoldás a felhasználó orrához kapcsolódó egyedi akusztikai

[352] „Biometric Security: Enhancing Mobile App Protection", 2025. február 21., https://nordstone.co.uk/blog/integrating-biometricsecurity-features-into-mobile-apps.
[353] Yohei Kawasaki és Yuta Sugiura, „Personal Identification and Authentication Using Blink with Smart Glasses", in *2022 61st Annual Conference of the Society of Instrument and Control Engineers (SICE)*, 2022, 1251–56, https://doi.org/10.23919/SICE56594.2022.9905842.
[354] K. Ahmad és S. Rahman, „Smartphone Authentication Based on 3D Touch Sensor and Finger Location", *Mesopotamian Journal of CyberSecurity* 8, sz. 2 (2025): 221–36.

jellemzőket használja fel az azonosítás feladatának elvégzéséhez. E technológia hatékonyságának megállapítása érdekében tizenegy főből álló csoporton végeztek tesztelési sorozatot.[355]

A digitális technológiák fejlődésével párhuzamosan egyre fontosabbá válik a személyazonosítás és a személyi hitelesítés megbízható megvalósítása. Ezek a technológiák alapvető szerepet játszanak mind a hagyományos, mind a digitális környezetben, a biztonságos adatkezelés és tranzakciók megvalósításában. Az informatikai biztonság területén két alapvető, ám gyakran összekeverhető fogalomról van szó: a személyazonosításról (identification) és a személyi hitelesítésről (authentication)

3.5.4 Mobileszköz-alapú hitelesítés

A mobileszközök alapú hitelesítésnél jellemzően az alábbi megoldásokat alkalmazzák:

1. **Eszközalapú hitelesítés**: A mobileszközök gyakran beépített biometrikus érzékelőkkel rendelkeznek, például ujjlenyomat-olvasóval és arcfelismerő kamerákkal, amelyek biztonságos hitelesítésre használhatók. Ezek az eszközszintű biztonsági funkciók integrálhatók kormányzati alkalmazásokkal, hogy zökkenőmentes, biztonságos hitelesítést biztosítsanak.[356]
2. **Mobil eID megoldások**: A kormány által kiállított személyazonosító okmányok digitális verzióit biztonságosan tárolhatják mobileszközökön, lehetővé téve az állampolgárok számára, hogy elektronikusan igazolják személyazonosságukat fizikai dokumentumok nélkül. Ezek a mobil eID megoldások tipikusan titkosítást, biztonságos elemeket és hitelesítési mechanizmusokat alkalmaznak a digitális identitás-hitelesítő adatok integritásának és biztonságának biztosítására.[357]
3. **Mobil aláírások**: A mobileszközökön elérhető digitális aláírási képességek lehetővé teszik az állampolgárok számára dokumentumok és tranzakciók jogi alá-

[355] Kaito Isobe és Kazuya Murao, „Personal Identification Method using Active Acoustic Sensing applied to the Nose pad of Eyeglasses", in *Adjunct Proceedings of the 2022 ACM International Joint Conference on Pervasive and Ubiquitous Computing and the 2022 ACM International Symposium on Wearable Computers*, UbiComp/ISWC '22 Adjunct (New York, NY, USA: Association for Computing Machinery, 2023), 345–48, https://doi.org/10.1145/3544793.3560400.
[356] „IR 8334, Using Mobile Device Biometrics for Authenticating First Responders | CSRC", elérés 2025. május 3., https://csrc.nist.gov/pubs/ir/8334/ipd.
[357] „Mobile ID -Trusted Digital ID for Governments", elérés 2025. május 3., https://www.thales-group.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/mobile-id.

írását kormányzati kontextusokban. A mobil aláírási megoldások tipikusan biztonságos hitelesítést kombinálnak kriptográfiai aláírási képességekkel a letagadhatatlanság és jogi érvényesség biztosítása érdekében.[358]

4. **QR-kódok és mobil ellenőrzés**: A QR-kódokat egyre inkább használják kormányzati szolgáltatásokban személyazonosság-ellenőrzéshez, dokumentum-hitelesítéshez és hozzáférés-ellenőrzéshez. A mobileszközök beolvashatják ezeket a kódokat biztonságos hitelesítési folyamatok kezdeményezéséhez vagy fizikai dokumentumok hitelességének ellenőrzéséhez.[359]
5. **Push hitelesítés**: Ez a megközelítés közvetlenül a felhasználó mobileszközére küldi a hitelesítési kéréseket, explicit jóváhagyást igényelve egy dedikált alkalmazáson keresztül. A push hitelesítés erősebb biztonságot nyújt a hagyományos módszereknél, mint az SMS, miközben egyszerűsített felhasználói élményt kínál.[360]
6. **Near Field Communication (NFC)**: A modern okos telefonok NFC-képességei biztonságos kommunikációt tesznek lehetővé elektronikus személyazonosító okmányokkal, mint például eID kártyák és e-útlevelek. A kormányzati alkalmazások kihasználhatják az NFC-t ezen dokumentumok olvasására és hitelességük ellenőrzésére, áthidalva a fizikai és digitális identitás ökoszisztémákat.[361]

3.5.5 Nemzetközi példák

Az okos eszközökön alapuló személyazonosító és hitelesítő rendszerek az elmúlt évtizedben fejlődésen mentek keresztül világszerte. Ezek a technológiák forradalmasították a felhasználók azonosításának módját mind a kormányzati, mind a magánszektorbeli szolgáltatások igénybevételénél. Nemzetközi példákra összpontosítva fogom bemutatni a személyazonosításra és hitelesítésre alkalmas okoseszköz-applikációkat, részletesen ismertetve a különböző országokban és szektorokban alkalmazott megoldásokat a teljesség igénye nélkül, a feldolgozott szakirodalom alapján releváns entitások kapcsán. (Relevancia alatt az adott alkalmazás Magyarországhoz való kapcsolata,

[358] Josip Stanešić és mtsai., „Digital signatures and their legal significance", *Edelweiss Applied Science and Technology* 9, sz. 1 (2025. január 9.): 403–12, https://doi.org/10.55214/25768484.v9i1.4154.
[359] „Document Verification with QR Codes: How It Works | ME-QR", elérés 2025. május 3., https://me-qr.com/page/blog/verification-of-documents-with-qr-codes.
[360] „IR 8334, Using Mobile Device Biometrics for Authenticating First Responders | CSRC".
[361] „IR 8334, Using Mobile Device Biometrics for Authenticating First Responders | CSRC", 8.

a technika kidolgozottsága, mint jó példa, vagy az esetleges visszaélések kapcsán értem.)

Európai személyazonosítási rendszerek

- **Európai Unió: eIDAS keretrendszer és a digitális identitás pénztárca**

Az Európai Unióban az elektronikus azonosításról és bizalmi szolgáltatásokról szóló rendelet (eIDAS) 2014-es elfogadása mérföldkövet jelentett a digitális identitás szabályozásában. A rendelet meghatározza a digitális aláírások, pecsétek és időbélyegzők joghatásait, valamint az elektronikus identitási rendszerek tagállamok közötti kölcsönös elismerésének feltételeit.[362] Az eIDAS 2.0, amelyet 2021-ben javasoltak és várhatóan 2024-től lép hatályba, tovább fejleszti ezt a keretet egy európai digitális identitási pénztárca bevezetésével. Ez lehetővé teszi majd az EU-állampolgárok számára, hogy digitálisan igazolják személyazonosságukat és megosszanak bizonyos személyes adatokat, attribútumokat és képesítéseket a hatóságokkal és magánvállalkozásokkal az EU egész területén. A jövőbeni eIDAS 2.0 keretrendszer tervek szerint támogatni fogja a "szelektív közzétételt" és a Zero Knowledge Proof (ZKP) alapú technológiákat, lehetővé téve a felhasználók számára, hogy csak a szükséges attribútumokat osszák meg identitásukból. Ez előrelépés a privacy-by-design megközelítés irányába a digitális identitás területén.[363]

- **Észtország: A digitális társadalom úttörője**

Észtország globálisan elismert vezető a digitális kormányzat és elektronikus azonosítási rendszerek területén. Az észt digitális azonosítási rendszer, amely a személyi igazolvány elektronikus változatán (eID) alapul, lehetővé teszi az állampolgárok számára, hogy gyakorlatilag minden kormányzati és magánszektorbeli szolgáltatást digitálisan használjanak. A 2014-ben bevezetett e-Residency program tovább bővítette a lehetőségeket: bárki a világon virtuális állampolgárrá válhat, vállalkozásokat indíthat és bankszámlákat nyithat anélkül, hogy fizikailag az országban tartózkodnak.[364] Az észt szolgáltatás különösen figyelemreméltó innovációval rendelkezik. Lehetővé teszi a

[362] European Union, *eIDAS Regulation: Trust Services and Electronic Identification* (Brussels: European Union, 2023).
[363] Union.
[364] E-Estonia. "e-Residency: The digital identity for global citizens." 2022. Retrieved from e-estonia.com

felhasználók számára, hogy bárhol a világon megújítsák fiókjukat anélkül, hogy bankfiókba kellene látogatniuk. A felhasználó okos telefonjával egyszerűen beolvassa személyazonosító okmányának chipjét a telefon érintésmentes olvasójával, majd "iProoving" technológiával igazolja személyazonosságát. Ez a technológia több mint 3 millió felhasználóval rendelkezik a balti államokban, és havonta több mint 200 millió szolgáltatás-igénybevételt tesz lehetővé.[365]

- **Svédország: BankID mint nemzeti azonosítási standard**

A svéd BankID kiemelkedő példája az eIDAS-kompatibilis elektronikus azonosítási rendszernek. A rendszert a svéd bankok egy csoportja fejlesztette ki, és mára a svéd népesség több mint 80%-a használja. A BankID okos telefonos alkalmazáson keresztül teszi lehetővé a felhasználók számára a személyazonosság igazolását és dokumentumok aláírását.[366] A BankID példája jól mutatja, hogy a magánszektor is hatékony szerepet játszhat a digitális identitás infrastruktúrájának kiépítésében, ha megfelelő szabályozási keret áll rendelkezésre. A rendszer olyan sikeres, hogy de facto nemzeti azonosítási standarddá vált, széles körben használják mind a közszolgáltatásokban, mind a magánszektorbeli tranzakciókban, például bankokban, biztosítóknál és online kiskereskedelemben.

- **Dánia: MitID rendszer**

A dán MitID rendszer egy olyan kormányzati azonosítási megoldás, amely lehetővé teszi az állampolgárok számára, hogy biztonságosan azonosítsák magukat online. A rendszer többfaktoros hitelesítést alkalmaz, és a felhasználók választhatnak a mobilalkalmazás, a hardveres token vagy a kódpapír használata között. A MitID különlegessége, hogy közös fejlesztés a dán kormány és a bankszektor között, ami biztosítja, hogy egyetlen azonosítási megoldással lehessen hozzáférni mind a kormányzati, mind a pénzügyi szolgáltatásokhoz. Ez az integráció egyszerűsíti a felhasználók életét, és növeli az elfogadottságot mindkét szektorban. [367]

---

[365] iProov, *Case Studies in Government Digital Identity* (London: iProov Ltd, 2021).
[366] F. Söderström és U. Melin, „The Swedish BankID System: An Infrastructure for Digital Citizenship", *International Journal of Electronic Governance* 11, sz. 3–4 (2019): 301–18, https://doi.org/10.1504/IJEG.2019.102929.
[367] Thomas Kingo és Diego F. Aranha, „User-centric security analysis of MitID: The Danish passwordless digital identity solution", *Computers & Security* 132 (2023. szeptember 1.): 103376, https://doi.org/10.1016/j.cose.2023.103376.

- **Egyesült Királyság: GOV.UK Verify és új megközelítések**

Az Egyesült Királyság GOV.UK Verify rendszere egy érdekes kísérlet volt a piaci alapú digitális identitás-rendszer létrehozására. A program több akkreditált identitás-szolgáltatóra épített, akik különböző technológiákat és módszereket használtak a felhasználók azonosítására. Bár a rendszer nem érte el a várt elfogadottságot, és 2023-ban lezárták, fontos tanulságokkal szolgált a digitális identitás-rendszerek tervezése és implementálása szempontjából.[368] Az Egyesült Királyság azóta új megközelítést alkalmaz, amely egy központi digitális identitás-keretrendszerre épül, de lehetővé teszi a különböző szektoroknak, hogy saját specifikus azonosítási megoldásokat fejlesszenek erre építve. A brit belügyminisztérium és a kormány digitális szolgáltatásokért felelős egysége (GDS) szorosan együttműködik a magánszektorral, hogy olyan innovatív megoldásokat fejlesszenek ki, amelyek megfelelnek a különböző felhasználói csoportok és szolgáltatások igényeinek.[369]

- **Franciaország: A France Identity**

Az alkalmazás lehetővé teszi a francia állampolgárok számára, hogy digitálisan igazolják személyazonosságukat különböző online és offline helyzetekben. Az alkalmazás a francia elektronikus személyi igazolványhoz kapcsolódik, és biztonságos módon tárolja a felhasználó személyes adatait a telefonon. A felhasználók különböző attribútumokat oszthatnak meg magukról, például az életkorukat, anélkül, hogy a teljes személyazonosságukat fel kellene fedniük.[370]

- **Németország: az AusweisApp2:**

Hasonló funkciót tölt be, lehetővé téve a német állampolgárok számára, hogy nemzeti elektronikus személyi igazolványukat (nPA) használják online azonosításra. Az alkal-

[368] „2022 Primary Assessments: Lessons Learnt", GOV.UK, elérés 2025. május 3., https://www.gov.uk/government/publications/2022-national-curriculum-assessments-lessons-learnt/2022-primary-assessments-lessons-learnt.
[369] „UK Digital Identity and Attributes Trust Framework", GOV.UK, 2024. november 25., https://www.gov.uk/government/collections/uk-digital-identity-and-attributes-trust-framework.
[370] „With France Identité, generate one-time credentials", elérés 2025. május 3., https://www.service-public.fr/particuliers/actualites/A17276?lang=en.

mazás NFC (Near Field Communication technológiát használ az igazolvány beolvasásához, és biztonságos csatornát hoz létre a szolgáltatóval az azonosítási folyamat során.[371]

Ázsiai-csendes-óceáni térség implementációi

- **Szingapúr: SingPass és a felhőalapú biometria**

Szingapúr a SingPass Mobile alkalmazáson keresztül teszi lehetővé állampolgárai számára a kormányzati szolgáltatások elérését. A 2018-ban bevezetett rendszer a felhőalapú biometrikus azonosítást használja. A felhasználók arcfelismeréssel vagy ujjlenyomattal hitelesíthetik magukat, és 2023-ra már több mint 350 állami és magánszektorbeli szervezet több mint 2000 szolgáltatását érhetik el egyetlen alkalmazáson keresztül.[372]A SingPass rendszer különlegessége, hogy a kormányzati és magánszektorbeli szolgáltatásokat egyaránt magába foglalja, a banki ügyintézéstől az egészségügyi adatok lekérdezésén át a lakásbérlésig. A rendszer teljes értékű "digitális tárcaként" funkcionál, ahol a felhasználók tárolhatják és megoszthatják digitális dokumentumaikat, például iskolai bizonyítványaikat vagy egészségügyi adataikat.[373] A 2021-ben elindított "Sign with SingPass" szolgáltatás lehetővé teszi a dokumentumok digitális aláírását, amely jogilag egyenértékű a kézzel írt aláírással. Ez a funkció tovább bővíti a rendszer használhatóságát, és segít csökkenteni a papíralapú ügyintézés szükségességét.[374]

- **India: Aadhaar és a világ legnagyobb biometrikus rendszere**

India Aadhaar rendszere a világ legnagyobb biometrikus azonosítási rendszere, amely több mint 1,3 milliárd ember adatait tartalmazza. Az egyedi 12 jegyű azonosítószám, amelyet a rendszer generál, ujjlenyomat, írisz-szkennelés és arcfelismerés alapján azonosítja a felhasználókat. Bár kezdetben csak kormányzati szolgáltatások elérésére

[371] „AusweisApp", Federal Office for Information Security, elérés 2025. május 3., https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Online-Ausweisfunktion/AusweisApp/ausweisapp.html?nn=920562.
[372] iProov, *Case Studies in Government Digital Identity*.
[373] „dpi.global/globaldpi/singapore_sndi", elérés 2025. május 3., https://www.dpi.global/globaldpi/singapore_sndi.
[374] „Singapore's Strategic Transformation as a Smart Nation ^ NTU356", HBR Store, elérés 2025. május 3., https://store.hbr.org/product/singapore-s-strategic-transformation-as-a-smart-nation/NTU356.

használták, mára bankok, telekommunikációs szolgáltatók és más magánvállalatok is alkalmazzák a személyazonosítás céljára.[375]

Az Aadhaar-ra épülő DigiLocker rendszer lehetővé teszi a felhasználók számára, hogy hivatalos dokumentumaikat digitálisan tárolják és osszák meg. Az alkalmazás nemcsak tárhely, hanem a dokumentumok hitelességét is garantálja, mivel közvetlenül a kibocsátó hatóságokkal áll kapcsolatban. Ez a megközelítés csökkenti a hamisított dokumentumok lehetőségét és egyszerűsíti az adminisztrációs folyamatokat.[376]

- **Ausztrália: myGovID alkalmazás**

Ausztráliában a myGovID alkalmazás hasonló céllal jött létre. Az alkalmazás biztonsági szintjei az egyszerű jelszó hitelesítéstől a személyazonosság erős, dokumentumalapú ellenőrzéséig terjednek, attól függően, hogy milyen szolgáltatáshoz kíván hozzáférni a felhasználó.[377] A myGovID különösen a COVID-19 járvány alatt bizonyult értékesnek, amikor az ausztrálok többsége otthonról intézte kormányzati ügyeit. Az alkalmazás lehetővé teszi a felhasználók számára, hogy biztonságosan hozzáférjenek különböző kormányzati szolgáltatásokhoz, beleértve az adóbevallást, a szociális juttatásokat és az egészségügyi szolgáltatásokat.[378]

Összegezve az okos eszközök applikációi a személyazonosítás és hitelesítés területén világszerte forradalmasították a felhasználók azonosításának módját. Az európai példák – Észtországtól Svédországon át az Egyesült Királyságig – jól mutatják a különböző megközelítéseket a digitális identitáskezelésben, míg az ázsiai-csendes-óceáni térség implementációi – különösen Szingapúr és India rendszerei – demonstrálják a nagyléptékű biometrikus identitásrendszerek lehetőségeit. A szektor specifikus implementációk a banki, kormányzati, vállalati és egészségügyi területeken jól példázzák, hogyan lehet az okos eszközökön alapuló azonosítási és hitelesítési megoldásokat különböző felhasználási esetekhez adaptálni.

---

[375] „Rebooting India", *Penguin Random House India* (blog), elérés 2025. május 3., https://www.penguin.co.in/book/rebooting-india-2/.
[376] cmeven, „Aadhaar and the Rise of Digital Public Infrastructure in India", *Reframe[Tech]* (blog), 2024. november 13., https://www.reframetech.de/en/2024/11/13/aadhaar-and-the-rise-of-digital-public-infrastructure-in-india/.
[377] „Home | myID", elérés 2025. május 3., https://www.myid.gov.au/.
[378] Adore Australia, „The Evolution and Impact of Australia's Digital ID Legislation", *Adore Australia* (blog), 2024. május 21., https://www.adoreaustralia.com.au/the-evolution-and-impact-of-australias-digital-id-legislation/.

A nemzetközi példák azt mutatják, hogy a sikeres mobilalapú identitásrendszerek nemcsak a technológiai innovációra, hanem a felhasználói élmény, az adatvédelem és a széles körű elfogadottság szempontjaira is hangsúlyt fektetnek. Ezek a rendszerek egyre inkább a mindennapi élet szerves részévé válnak, és alapvetően változtatják meg az állampolgárok és a szolgáltatók közötti interakciót.

3.5.6 Hazai példa (AVDH, e-személyi, DÁP)

A digitális átalakulás korszakában a személyazonosítás és hitelesítés technológiái kulcsfontosságú szerepet játszanak mind a közigazgatásban, mind a magánszektorban. Magyarországon az elmúlt évtizedben fejlesztések történtek ezen a területen, követve és gyakran megelőzve az európai trendeket. Az elektronikus személyazonosítási eszközök fejlődése a papíralapú dokumentumoktól a modern, többfunkciós chipkártyákon át a mobilalkalmazásokig ível, miközben folyamatosan növekszik az igény a biztonságos, felhasználóbarát és széleskörűen alkalmazható azonosítási megoldásokra. A modern személyazonosítási és hitelesítési technológiák elsődleges célja, hogy biztonságos és hatékony módszert biztosítsanak a digitális térben való megbízható azonosításra, miközben védik a személyes adatokat és megfelelnek a jogi szabályozásoknak. Mindez különösen fontos napjainkban, amikor az állampolgárok egyre több szolgáltatást vesznek igénybe online, és a digitális ügyintézés egyre inkább beépül a mindennapokba. Az elektronikus azonosítási és hitelesítési megoldások működését Magyarországon is több jogszabály szabályozza, amelyek meghatározzák a biztonsági követelményeket, az adatvédelmi előírásokat és a jogi keretet.

Az elektronikus azonosítás alapvető jogi hátterét az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (E-ügyintézési törvény) biztosítja, amely összhangban van az EU elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU rendeletével (eIDAS rendelet)
Az eIDAS rendelet meghatározza az elektronikus azonosító eszközök biztonsági szintjeit (alacsony, magas), valamint a határon átnyúló elektronikus azonosítás szabályait. Ez a rendelet biztosítja, hogy a magyar elektronikus azonosítási megoldások kompatibilisek legyenek más EU-tagállamok rendszereivel, és lehetővé teszi a határokon átnyúló elektronikus szolgáltatások igénybevételét.

A személyazonosító igazolványra vonatkozó szabályokat a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény, valamint a személyazonosító igazolvány kiadásáról és az egységes arcképmás- és aláírás-felvételezésről szóló 414/2015. (XII. 23.) Korm. rendelet tartalmazza. Ezek a jogszabályok határozzák meg az e-Személyi funkcionális és biztonsági követelményeit, valamint a kiadás és használat feltételeit. Az elektronikus aláírásra vonatkozó szabályokat szintén az E-ügyintézési törvény és az eIDAS rendelet határozza meg, amelyek definiálják a különböző típusú elektronikus aláírások (egyszerű, fokozott biztonságú, minősített) jogi státuszát és bizonyító erejét.

Jelen alfejezet átfogó képet nyújt a magyarországi személyazonosításra és hitelesítésre alkalmas technológiákról, bemutatva azok fejlődését, műszaki sajátosságait és alkalmazási területeit. Részletesen kitérünk a közelmúltban bevezetett Digitális Állampolgárság Programra (DÁP) is, amely új fejezetet nyit a magyar digitális közigazgatás történetében, integrálva a már meglévő és újonnan fejlesztett azonosítási és hitelesítési megoldásokat.

- **A személyazonosítás fejlődése Magyarországon**

A magyar személyazonosítási rendszerek története a papíralapú dokumentumoktól a komplex elektronikus megoldásokig ível. Az első személyi igazolványokat 1954-ben vezették be Magyarországon, ezek papíralapú okmányok voltak.[379] A fejlődés következő állomása az 1989-es rendszerváltás után következett be, amikor 1992-ben bevezették a kártyaformátumú, műanyag alapú személyi igazolványokat. Az elektronikus kormányzati szolgáltatások fejlődésével párhuzamosan egyre nyilvánvalóbbá vált, hogy szükség van olyan azonosítási megoldásokra, amelyek a digitális térben is megbízhatóan működnek. Az első lépés ebben az irányban a 2005-ben bevezetett Ügyfélkapu rendszer volt, amely felhasználónév és jelszó alapú azonosítást tett lehetővé az elektronikus közigazgatási szolgáltatásokhoz.[380] A biometrikus elemeket tartalmazó útlevelek 2006-os bevezetése újabb fontos mérföldkő volt, amely már az arcképet

[379] Nyúl Eszter Anna, „Nyúl Eszter Anna: Az állampolgárság elvesztett átmeneti rítusa", *Tudásmenedzsment* 21, sz. 1–2 (2020. december 30.): 170–77, https://doi.org/10.15170/TM.2020.21.1-2.13.
[380] „Elektronikus közszolgáltatásokat és ügyfélszolgálati tevékenységet összefoglaló monitoring jelentés - PDF Ingyenes letöltés", elérés 2025. május 3., https://docplayer.hu/116889065-Elektronikus-kozszolgaltatasokat-es-ugyfelszolgalati-tevekenyseget-osszefoglalo-monitoring-jelentes.html.

elektronikusan, a chipben is tárolta. 2009-ben kezdődött meg a nemzeti egységes kártyarendszer (NEK) kidolgozása, amelynek célja a különböző igazolványok (személyi igazolvány, jogosítvány, diákigazolvány stb.) egységes platformra helyezése volt.[381] Az elektronikus személyazonosító igazolvány (e-Személyi) 2016. január 1-jei bevezetése forradalmi változást hozott, mivel ez volt az első olyan magyar személyazonosító okmány, amely beépített elektronikus chipet és azonosítási funkciókat tartalmazott. Az e-Személyi lehetővé tette a digitális térben történő azonosítást és elektronikus aláírást, valamint több korábbi kártya funkcióinak integrálását. A fejlődés nem állt meg: 2020-ban megjelent az eSzemélyiM mobilalkalmazás, amely az e-Személyi funkcióit terjeszti ki okos telefonokra, lehetővé téve a kártyán tárolt adatok kezelését és az elektronikus azonosítást mobil eszközökön keresztül.[382] A legújabb fejlesztés a 2023-ban elindított Digitális Állampolgárság Program (DÁP), amely egy átfogó elektronikus azonosítási és szolgáltatási keretrendszert biztosít.[383]

- **Az elektronikus személyazonosító igazolvány (e-Személyi)**

Az elektronikus személyazonosító igazolvány (e-Személyi) 2016-os bevezetése mérföldkövet jelentett a magyar személyazonosítási technológiák fejlődésében. Az e-Személyi egy multifunkcionális intelligens kártya, amely a hagyományos személyazonosító funkción túl számos elektronikus szolgáltatást is támogat. A kártya műszaki kialakítását és biztonsági elemeit nemzetközi szabványok alapján tervezték, figyelembe véve az EU elektronikus azonosításra vonatkozó eIDAS rendeletét is. Az e-Személyi egy érintés nélküli interfészt (NFC) tartalmazó chipbe integrált adattárolási és hitelesítési megoldásokat tartalmaz. A kártya fizikailag a nemzetközi szabványoknak megfelelő, ID-1 formátumú (85,6 × 53,98 mm) polikarbonát anyagú igazolvány, amely számos biztonsági elemmel (hologram, mikro nyomtatás, OVI festék, stb.) rendelkezik az okmányhamisítások megakadályozására. A kártyán található chip három különböző alkalmazást tartalmaz:

[381] Nyilvantarto.hu. "Hogyan kell igényelni a NEK kártyát? Ismerje meg a Nemzeti Egységes Kártyarendszert." 2015. https://nyilvantarto.hu/archiv_honlap_2016/letoltes/aktakukac_uj-sag_kekkh_2015_s02x03.pdf4

[382] „Megjelent az eSzemélyiM mobil applikáció - eSzemélyi", elérés 2025. május 3., https://eszemelyi.hu/blog/megjelent-az-eszemelyim-mobilapplikacio/.

[383] „Új fejezet a digitális okmányhasználatban – Hiteles adatigazolás a DÁP alkalmazásban (3. rész) | FinTechZone", elérés 2025. május 3., https://fintechzone.hu/uj-fejezet-a-digitalis-okmanyhasznalatban-hiteles-adatigazolas-a-dap-alkalmazasban-3-resz/.

(1) az eTárolót, amely a kártya vizuálisan is megjelenő adatait tárolja elektronikusan,
(2) az eID-t, amely az elektronikus személyazonosításhoz szükséges, és
(3) az eSig-et, amely az elektronikus aláírási funkcionalitást biztosítja. A chip adatainak olvasása megfelelő jogosultságokhoz és PIN kódok ismeretéhez kötött, biztosítva a személyes adatok védelmét.[384]

- **Az eSzemélyiM mobilalkalmazás**

Az eSzemélyiM mobilalkalmazás a magyar kormány által 2020-ban bevezetett hivatalos alkalmazás, amely az elektronikus személyazonosító igazolvány (e-Személyi) funkcióinak mobileszközökön való használatát tette lehetővé. Az alkalmazás lényege, hogy az NFC-képes okos telefonok segítségével olvashatóvá és használhatóvá válnak az e-Személyi elektronikus funkciói külön kártyaolvasó eszköz nélkül is.[385] Az eSzemélyiM alkalmazás Android és iOS operációs rendszereken volt elérhető el, és a hivatalos alkalmazásboltokból (Google Play, App Store) ingyenesen letölthető. Az alkalmazás használatához NFC-funkciót támogató okos telefon és 2016. január 1. után kiállított elektronikus személyazonosító igazolvány szükséges. Az eSzemélyiM alkalmazás különösen a COVID-19 világjárvány idején értékelődött fel, amikor a személyes ügyintézések minimalizálása miatt megnőtt az elektronikus szolgáltatások iránti igény.

- **A Digitális Állampolgárság Program (DÁP)**

A Digitális Állampolgárság Program (DÁP) a magyar kormány átfogó kezdeményezése, amelynek célja a digitális állampolgárság koncepcióra építve egy egységes, felhasználóbarát keretrendszer kialakítása, amely egyesíti és továbbfejleszti a már meglévő elektronikus azonosítási és ügyintézési megoldásokat. A program 2023-ban indult el, és fokozatosan bővül új funkciókkal és szolgáltatásokkal.[386]

A DÁP alapkoncepciója, hogy az állampolgárok egyetlen digitális identitással férhessenek hozzá az állami és egyre bővülő körben a magánszektorbeli digitális szolgáltatásokhoz. Ez az egységes digitális identitás a már meglévő azonosítási eszközökre (e-

[384] Kiss, „Elektronikus személyazonosítás és digitális identitás".
[385] „Megjelent az eSzemélyiM mobil applikáció - eSzemélyi".
[386] „Tájékoztató a Digitális Állampolgárság Programról", 2025. március 11., https://dunavarsany.hu/index.php/2025/03/11/tajekoztato-a-digitalis-allampolgarsag-programrol/.

Személyi, Ügyfélkapu) épül, de kibővíti azokat új funkciókkal és integrációs lehetőségekkel A program egyik központi eleme a Digitális Állampolgárság Alkalmazás (DÁP alkalmazás), amely egy mobileszközökre optimalizált, személyre szabható felületet biztosít az állampolgárok számára. Az alkalmazás fokozatosan integrálja a különböző kormányzati mobilalkalmazásokat, beleértve az eSzemélyiM, EESZT (Elektronikus Egészségügyi Szolgáltatási Tér) és a Mobilizált Okmányok (MobilTárca/mOkmányok) alkalmazásokat[387] A DÁP keretében hangsúlyt kap a Digitális Dokumentumtár, amely lehetővé teszi hivatalos dokumentumok digitális tárolását, megosztását és hitelesítését. A rendszer támogatja a digitálisan aláírt dokumentumok kezelését, a dokumentumok időbélyegzését és a hosszú távú megőrzést is. Ez lehetővé teszi a papírmentes ügyintézést számos területen, a közigazgatástól az egészségügyön át a pénzügyi szolgáltatásokig. A DÁP részeként megvalósul az egységes digitális postaláda is, amely az elektronikus kapcsolattartás központi platformjaként szolgál az állampolgárok, vállalkozások és a közigazgatás között. Ez a rendszer lehetővé teszi a hivatalos értesítések, dokumentumok biztonságos küldését és fogadását, valamint azok nyomon követését és rendszerezését. A program tartalmazza a határon átnyúló azonosítás és hitelesítés támogatását is, összhangban az EU elektronikus azonosításról és bizalmi szolgáltatásokról szóló rendeletével (eIDAS). Ez lehetővé teszi a magyar digitális identitás használatát az EU más tagállamaiban elérhető szolgáltatásokhoz, valamint a más tagállamokban kibocsátott elektronikus azonosító eszközök elfogadását Magyarországon.[388] A DÁP újszerű megközelítése, hogy nem csupán a közszolgáltatások digitalizálására koncentrál, hanem egy nyílt platformként szolgál, amelyhez a magánszektor szolgáltatói is csatlakozhatnak. Ez lehetővé teszi, hogy például bankok, telekommunikációs cégek vagy kiskereskedelmi vállalatok is integrálhassák szolgáltatásaikat a rendszerbe, egyszerűsítve az ügyfelek azonosítását és a szolgáltatások igénybevételét. A program egyik kulcsfontosságú eleme a felhasználói élmény középpontba helyezése. A program része egy átfogó digitális kompetenciafejlesztési kezdeményezés is, amely segíti az állampolgárokat a digitális eszközök és szolgáltatások hatékony használatában[27].

[387] Urbán Anikó, „Így lettünk digitális állampolgárok! Végigcsináltuk, leteszteltük!”, https://fintechzone.hu/, 2024. október 9., https://fintechzone.hu/igy-lettunk-digitalis-allampolgarok-vegigcsinaltuk-leteszteltuk/.
[388] Kabinetiroda Miniszterelnöki, *Digitális Állampolgárság – Stratégiai koncepció és megvalósítási terv* (Budapest: MK, 2022).

- **Az Ügyfélkapu és továbbfejlesztései**

Az Ügyfélkapu a magyar kormány által 2005-ben bevezetett elektronikus azonosítási rendszer, amely az elektronikus közigazgatási szolgáltatások igénybevételéhez biztosít hitelesítést. A rendszer a legrégebbi és napjainkig az egyik legszélesebb körben használt elektronikus azonosítási megoldás Magyarországon, több mint 5 millió regisztrált felhasználóval.[389] Az Ügyfélkapu kezdetben egyszerű felhasználónév-jelszó alapú azonosítást kínált, amely a személyes regisztrációt követően volt használható. A regisztráció során az állampolgár személyazonosságát ellenőrizték, majd ezt követően kapott hozzáférést a rendszerhez. Ez a megoldás biztosította, hogy a digitális térben is megbízhatóan azonosíthatók legyenek a felhasználók.[390] Az évek során az Ügyfélkapu folyamatosan fejlődött, és új funkciókkal bővült. A 2010-es évek közepén integrálták az e-Személyi elektronikus azonosítási funkcióival, lehetővé téve, hogy a felhasználók az elektronikus személyazonosító igazolványukkal és PIN-kódjukkal jelentkezzenek be a rendszerbe. Ez magasabb biztonsági szintet jelentett, mint a hagyományos jelszavas azonosítás. 2018-ban vezették be az Ügyfélkapu+ rendszert, amely kétfaktoros azonosítást kínál. Ebben a rendszerben a felhasználónév és jelszó mellett egy időalapú egyszer használatos jelszót (Time-based One-Time Password, TOTP) is használnak az azonosításhoz. Ez növeli a biztonságot, mivel még a felhasználónév és jelszó kompromittálódása esetén is szükség van a második faktor - általában egy mobilalkalmazás által generált - kódjára a sikeres bejelentkezéshez.[391]

- **Egyéb elektronikus azonosítási és hitelesítési megoldások**

Magyarországon az e-Személyi, az eSzemélyiM és az Ügyfélkapu mellett számos más elektronikus azonosítási és hitelesítési megoldás is elérhető, amelyek különböző

Az elektronikus aláírás területén több megoldás is elérhető Magyarországon. Az e-Személyi beépített elektronikus aláírási funkcióval rendelkezik, amennyiben a felhasználó igényelte ezt a szolgáltatást. Emellett több piaci szolgáltató kínál minősített elektronikus aláírási szolgáltatásokat, amelyek megfelelnek az eIDAS rendelet követelmé-

[389] Ügynökség Kormányzati Informatikai Fejlesztési, *Az Ügyfélkapu rendszer átfogó ismertetése* (Budapest: KIFÜ, 2020).
[390] „Nánási Polgár", *Nánási Polgár* (blog), elérés 2025. május 3., https://nanasipolgar.hu/jogi-kisokos/.
[391] „Ügyfélkapu+ és az elektronikus ügyintézés szabályai: Mit érdemes tudni?", Vámprogram, elérés 2025. május 3., https://www.vamprogram.hu/hu/-/ugyfelkapu-plusz-es-az-elektronikus-ugyintezes-szabalyai-mit-erdemes-tudni-.

nyeinek. Az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) rendszeréhez kapcsolódóan elérhető az EESZT mobiltoken, amely biztonságos belépést tesz lehetővé az egészségügyi adatokhoz. A mobiltoken egy kétfaktoros azonosítási megoldás, amely az Ügyfélkapu-hitelesítés mellett egy mobiltelefonos alkalmazás által generált időalapú jelszót is használ a belépéshez. Az EESZT mobiltoken különösen a COVID-19 világjárvány idején vált népszerűvé, amikor az állampolgároknak gyakrabban kellett hozzáférniük egészségügyi adataikhoz, például teszteredményeikhez vagy oltási igazolásaikhoz. A megoldás egyszerűsíti az egészségügyi adatokhoz való hozzáférést, miközben biztosítja a megfelelő biztonsági szintet.[392]

3.5.7 A magyar elektronikus azonosítási megoldások nemzetközi összehasonlításban

A magyar elektronikus azonosítási és hitelesítési megoldások nemzetközi összehasonlításban is versenyképesek, és több területen az európai élvonalba tartoznak. Az e-Személyi és a kapcsolódó szolgáltatások összhangban vannak az EU előírásaival és a legjobb nemzetközi gyakorlatokkal. Az európai országok közül Észtország tekinthető az e-kormányzati megoldások úttörőjének, különösen a széles körben használt elektronikus személyazonosító kártya és a digitális állampolgársági koncepció révén. A skandináv országokban, különösen Svédországban és Dániában elterjedtek a bankszektorra épülő elektronikus azonosítási megoldások (BankID, NemID). Ezek a rendszerek nagymértékben integráltak a mindennapi szolgáltatásokba, és magas felhasználói elfogadottsággal rendelkeznek. Magyarországon a banki azonosítási megoldások egyelőre kevésbé integráltak a közigazgatási rendszerekkel, bár a DÁP keretében várható a szorosabb együttműködés a közszféra és a magánszektor között. Az Egyesült Királyságban a GOV.UK Verify rendszer egy több szolgáltatós modellt alkalmaz, ahol különböző magáncégek biztosítják az azonosítási szolgáltatásokat. Ez a megközelítés eltér a magyar centralizált modelltől, ahol az elektronikus azonosítási megoldásokat elsősorban az állam biztosítja és felügyeli.

[392] Központ Állami Egészségügyi Ellátó, *EESZT mobiltoken – Felhasználói kézikönyv* (Budapest: ÁEEK, 2020).

3.6 Okos mobil eszközök és applikációinak biztonsági kérdései és kockázatai

Az okos eszközök és a rajtuk futó alkalmazások példátlan kényelmet és hatékonyságot biztosítanak, ugyanakkor számos biztonsági kockázatot is hordoznak. Az alábbiakban részletesen bemutatom az okos eszközök és applikációik biztonságát érintő kihívásokat. A kibertér globális természete miatt a fenyegetések rendkívül sokrétűek és folyamatosan változnak, ami megnehezíti a hatékony védekezést.

A kibertámadások céljai rendkívül változatosak lehetnek: politikai, gazdasági, katonai vagy társadalmi célok elérése egyaránt motiválhatja a támadókat, akik lehetnek államok, terroristák, hacktivisták vagy bűnözői csoportok. Bányász Péter a kiberfenyegetéseket különböző kategóriákba sorolja, és részletesen elemzi az okos mobil eszközöket érintő új típusú kihívásokat.[393] A kiemelt fenyegetések között szerepelnek:

1. **Kártékony alkalmazások**: A malware különböző típusai (vírusok, férgek, trójai programok, ransomware, spyware) veszélyt jelentenek. Ezek gyakran legitim alkalmazásnak álcázzák magukat vagy legitim alkalmazásokba ágyazódnak be.
2. **Hálózati támadások**: Az okos eszközök folyamatos hálózati kapcsolata sebezhetővé teszi őket a man-in-the-middle támadásokkal, DOS (Denial of Service) támadásokkal vagy hálózati forgalom elemzéssel szemben.
3. **Adatlopás és adatszivárgás**: Az okos eszközök hatalmas mennyiségű személyes adatot gyűjtenek és tárolnak, ami vonzó célponttá teszi őket.
4. **Fizikai támadások**: Az eszközök fizikai hozzáférhetősége miatt fennáll a közvetlen manipuláció vagy lopás veszélye.
5. **Social engineering**: Az emberi tényezőt célzó támadások, amelyek megtévesztéssel, manipulációval veszik rá a felhasználókat biztonsági kockázatot jelentő cselekedetek végrehajtására.

3.6.1 Kibertérben zajló támadások, támadási vektorok

Tekintettel arra, hogy alapvetően az információs társadalom biztonsági kockázatai bemutatásra kerültek az I. fejezetben, köztük az okos eszközöké is, így jelen alfejezet során kifejezettem az okos mobil eszközök és applikációi során felmerülő biztonsági kihívások elemzését hajtom végre.

- **Operációs rendszer szintű sérülékenységek**

[393] Bányász, „Az okos mobil eszközök biztonsága”.

Az okos eszközök operációs rendszerei, mint például az Android, iOS, Windows vagy különböző IoT operációs rendszerek, folyamatosan fejlődnek és frissülnek a biztonsági rések javítása érdekében. Azonban a sérülékenységek felfedezése és kihasználása folyamatos versenyfutás a biztonsági szakértők és a támadók között. Az Android különösen sebezhetőnek tekinthető a fragmentáció miatt, mivel a különböző gyártók különböző verziókat használnak, és a frissítések nem mindig jutnak el minden eszközhöz időben. Az iOS biztonságosabbnak tekinthető a zárt ökoszisztéma és a gyorsabb frissítési ciklus miatt, azonban itt is rendszeresen fedeznek fel és használnak ki sérülékenységeket.

Az IoT eszközök esetében a biztonsági helyzet még aggasztóbb, mivel ezek az eszközök gyakran minimális erőforrásokkal rendelkeznek, és a gyártók nem mindig fektetnek elegendő erőforrást a biztonsági frissítésekbe. Az IoT eszközök gyakran hosszú ideig futnak elavult operációs rendszerekkel, ami biztonsági kockázatot jelent.[394]

- **Szoftverfrissítési és patchelési kihívások**

A szoftverfrissítések és biztonsági javítások (patch-ek) kulcsfontosságúak a felfedezett sérülékenységek javításához és az eszközök biztonságának fenntartásához. Azonban számos kihívás nehezíti a hatékony frissítési folyamatokat. Az egyik legnagyobb kihívás a frissítések időben történő telepítése. A felhasználók gyakran halogatják a frissítések telepítését, kiváltképpen, ha azok kellemetlenséget okoznak, például újraindítást igényelnek vagy változtatják a megszokott funkciók működését. Egy 2018-as felmérés szerint a felhasználók 33%-a halogatja a frissítések telepítését, és 11%-uk teljesen figyelmen kívül hagyja azokat[395] A vállalati környezetben a frissítések tesztelése és telepítése még összetettebb folyamat, ha az eszközök kritikus rendszerek részét képezik. A tesztelés és kompatibilitási ellenőrzések időigényesek, ami késleltetheti a frissítések telepítését, és meghosszabbíthatja a sebezhetőségi időablakot.[396]

[394] „In-App Purchase Security: Protecting Transactions and User Data | AppMaster", elérés 2025. május 3., https://appmaster.io/blog/in-app-purchase-security.
[395] „Device updates: what's stopping people from making the change? | Kaspersky official blog", elérés 2025. május 3., https://www.kaspersky.com/blog/device-updates-report/.
[396] @PatentPC, „Security Patching Habits: How Long Do Companies Delay Fixes?", PatentPC (@PatentPC, 2025. április 11.), https://patentpc.com/blog/security-patching-habits-how-long-do-companies-delay-fixes.

Az IoT eszközök esetében további kihívás, hogy sok eszköz nem támogatja az automatikus frissítéseket, vagy egyáltalán nem frissíthető. Ez különösen problémás a hosszú élettartamú eszközök esetében, amelyek évekig vagy akár évtizedekig használatban maradhatnak, és ezalatt az idő alatt számos új sérülékenység válhat ismertté.[397]

- **Supply Chain támadások**

A supply chain (ellátási lánc) támadások során a támadók a fejlesztési, gyártási vagy terjesztési folyamat valamely pontján kompromittálják a terméket vagy szoftvert. Ez a típusú támadás különösen veszélyes, mivel a támadók hozzáférést nyerhetnek a rendszerekhez még az üzembe helyezés előtt. Az egyik legismertebb példa a SolarWinds elleni támadás, amely 2020-ban vált ismertté. A támadók hozzáfértek a SolarWinds fejlesztési környezetéhez, és backdoor-t helyeztek el az Orion szoftverben, amelyet aztán több mint 18 000 ügyfélhez szállítottak ki, köztük számos kormányzati ügynökséghez és Fortune 500 vállalathoz.[398] Az okos eszközök és alkalmazásaik különösen sebezhetőek a supply chain támadásokkal szemben, mivel számos komponenst és szoftverkönyvtárat használnak különböző forrásokból. A nyílt forráskódú szoftverek és könyvtárak széles körű használata növeli a támadási felületet, mivel a támadók célba vehetik ezeket a komponenseket, tudva, hogy számos alkalmazásban használják őket. Az okos eszközök hardveres komponensei szintén sebezhetőek a supply chain támadásokkal szemben. A chipek, szenzorok és más alkatrészek gyakran különböző gyártóktól származnak, és nem mindig ellenőrzik őket alaposan a biztonsági problémák szempontjából. [399]

- **Hardverszintű sérülékenységek**

Az okos eszközök hardverszintű sérülékenységei további kihívásokat jelentenek a biztonság szempontjából. Ezek a sérülékenységek gyakran nehezebben javíthatók, mivel hardvercserét vagy módosításokat igényelhetnek. A processzor-szintű sérülékenységek, mint például a Meltdown és Spectre, különösen veszélyesek, mivel mélyebb rendszerszintű hozzáférést tesznek lehetővé. Ezek a sérülékenységek a processzorokban

[397] Conner John Bradley, „Sustainable Security: Exploring Longevity Challenges and Solutions for IoT", elérés 2025. május 3., https://carleton.scholaris.ca/items/af1b0a40-cd8a-4e1e-82d8-a374bb6e191d.
[398] „SolarWinds Supply Chain Attack", Fortinet, elérés 2025. május 3., https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack.
[399] „The Growing Threat of IoT Supply Chain Attacks", *Insights2Techinfo* (blog), 2025. február 20., https://insights2techinfo.com/the-growing-threat-of-iot-supply-chain-attacks/.

lévő spekulatív végrehajtás és gyorsítótár-mechanizmusokban lévő hibákat használják ki, és potenciálisan lehetővé tehetik az egyik alkalmazás számára, hogy hozzáférjen a másik alkalmazás memóriaterületéhez.[400]

A secure boot és a hardware root of trust (hardveralapú megbízhatóság) mechanizmusok célja, hogy megvédjék az eszközöket a boot-szintű támadásoktól és biztosítsák a firmware integritását. Azonban ezek a mechanizmusok sem tökéletesek, és esetenként megkerülhetők vagy manipulálhatók.[401]

A fizikai hozzáférésen alapuló támadások, mint például a side-channel támadások, a JTAG vagy UART debug portok használata, vagy a chip-szintű beavatkozás szintén kockázatot jelentenek, különösen az érzékeny környezetekben használt eszközök esetében. Ezek a támadások szakértői tudást és speciális eszközöket igényelnek, de bizonyos célpontok esetében a támadók hajlandóak befektetni ezekbe az erőforrásokba.[402]

- **0-day és más kifinomult támadások**

A 0-day (zero-day) sérülékenységek olyan biztonsági rések, amelyeket a támadók azelőtt használnak ki, mielőtt a fejlesztők vagy a közvélemény tudomást szerezne róluk, így nincs rendelkezésre álló javítás. Ezek a sérülékenységek különösen értékesek a támadók számára, és gyakran magas áron kereskednek velük a feketepiacon.[403]
Az állami szereplők és fejlett persistent threat (APT) csoportok gyakran rendelkeznek a 0-day sérülékenységek felfedezéséhez vagy megvásárlásához szükséges erőforrásokkal, és ezeket célzott támadásokhoz használják.[404] A Stuxnet féreg, amelyet az iráni nukleáris létesítmények ellen vetettek be, több 0-day sérülékenységet is kihasznált.[405]

---

[400] „Meltdown and Spectre", elérés 2025. május 3., https://meltdownattack.com/.
[401] „What Is »Hardware Root of Trust« in Industrial IoT?", elérés 2025. május 3., https://www.hms-networks.com/tech-blog/blogpost/hms-blog/2023/11/13/what-is-hardware-root-of-trust.
[402] Manali Kudtarkar, „JTAG: A Strong Tool for Security Testing", eInfochips, 2023. augusztus 24., https://www.einfochips.com/blog/jtag-a-strong-tool-for-security-testing/.
[403] „Demystifying The Market For Zero-Day Software Exploits", Packetlabs, 2024. május 17., https://www.packetlabs.net/post/demystifying-the-market-for-zero-day-software-exploits.
[404] „VulnCheck - Outpace Adversaries", VulnCheck, 2025. április 18., https://vulncheck.com/blog/understanding-apts.
[405] „A Guide to the Most Popular Zero-Day Attacks | CloudSEK", elérés 2025. május 3., https://www.cloudsek.com/blog/a-guide-to-the-most-popular-zero-day-attacks.

3.6.2 Alkalmazás-specifikus biztonsági kockázatok

Az okos eszközökön futó alkalmazások biztonsági kockázatokat hordoznak. Bányász Péter kutatásai rámutatnak, hogy az alkalmazások biztonsági kockázatai különösen nagyok, mivel bárki készítheti őket.[406]Az alkalmazásboltokban gyakran találhatók rosszindulatú programok, amelyek különböző módokon veszélyeztetik a felhasználók biztonságát.

3.6.3 Excessive Permissions és adathozzáférés

Az egyik legfigyelemreméltóbb biztonsági kockázat az alkalmazások túlzott jogosultságkérése. Sok alkalmazás olyan engedélyeket kér, amelyek nem szükségesek a működéséhez, például hozzáférést kér a kamerához, mikrofonhoz, helyadatokhoz vagy névjegyzékhez anélkül, hogy ezekre valóban szüksége lenne az alapvető funkciók biztosításához. A Pew Research Center kutatása szerint az Android alkalmazások átlagosan 10 különböző engedélyt kérnek, és ezek közül több mint 4 olyan, ami potenciálisan érzékeny adatokhoz biztosít hozzáférést.[407] A felhasználók többsége automatikusan megadja ezeket az engedélyeket anélkül, hogy valóban megértené a jogosultságok jelentését és következményeit.

3.6.4 Adatszivárgás és harmadik felek általi adatgyűjtés

Az alkalmazások része gyűjt adatokat a felhasználókról és továbbítja azokat harmadik feleknek, gyakran a felhasználók tudta vagy megfelelő tájékoztatása nélkül. Az Oxford Academic folyóiratban megjelent tanulmány szerint a Google Play áruházban található Android alkalmazások 88%-a tartalmaz olyan kódkönyvtárakat, amelyek harmadik felek részére gyűjtenek adatokat.[408] Ez a gyakorlat komoly adatvédelmi aggályokat vet fel, különösen mivel az adatok gyakran nem megfelelően titkosítva kerülnek továbbításra.

---

[406] Bányász, „Az okos mobil eszközök biztonsága".
[407] Monica Anderson, „Key Takeaways on Mobile Apps and Privacy", *Pew Research Center* (blog), 2015. november 10., https://www.pewresearch.org/short-reads/2015/11/10/key-takeaways-mobile-apps/.
[408] Isobel Asher Hamilton, „Oxford Researchers Exposed the Avalanche of Data Google and Facebook Can Hoover up from Apps on Your Phone", Business Insider, elérés 2025. május 3., https://www.businessinsider.com/google-and-facebook-big-data-apps-oxford-study-finds-2018-10.

3.6.5 Frissítési mechanizmusok sebezhetőségei

Ha az alkalmazás nem biztonságos forrásból tölti le a frissítéseket, vagy nem ellenőrzi megfelelően a frissítések integritását, akkor ez lehetőséget adhat a támadóknak, hogy kártékony kódot juttassanak a rendszerbe. A KRACK (Key Reinstallation Attack) nevű sérülékenység, amely 2017-ben vált ismertté, az Androidos készülékek 41%-át érintette. Segítségével többek között feltörhető volt a Wi-Fi titkosítás, valamint csomag újrajátszás, TCP kapcsolat eltérítés és HTTP tartalom beillesztés volt végrehajtható.[409] Ez jól példázza, hogy milyen komoly biztonsági kockázatokkal kell szembenéznünk az okos eszközök használata során.

3.6.6 In-App vásárlások és pénzügyi kockázatok

Az alkalmazáson belüli vásárlások (IAP) népszerűsége különösen a játékok és előfizetéses szolgáltatások esetében növekszik. Ez új veszélyeket teremt a felhasználók pénzügyi biztonságára nézve. A rosszul tervezett vagy szándékosan félrevezető IAP mechanizmusok nem tervezett kiadásokhoz vezethetnek, különösképpen, ha gyermekek használják az eszközt. Emellett egyre több csalási kísérlet célozza az IAP rendszereket. Hamis vásárlási felületek, megtévesztő "prémium" szolgáltatások és rejtett automatikus megújítások mind olyan módszerek, amelyek kiaknázzák az alkalmazáson belüli fizetési rendszerek biztonságának hiányosságait.

A pénzügyi adatok kezelése sok alkalmazás esetében nem megfelelő szintű titkosítással és védelemmel történik, ami további kockázatokat jelent. Az alkalmazások 43%-a nem használ elegendő titkosítást a pénzügyi tranzakciók során a Positive Technologies biztonsági cég jelentése szerint.[410]

3.6.7 Alkalmazások közötti interakciók veszélyei

Az Android Intent rendszerének és az iOS URL séma mechanizmusának köszönhetően az alkalmazások képesek kommunikálni egymással és megosztani adatokat. Bár ez a funkció rendkívül hasznos és kulcsfontosságú sok modern mobil élményhez, bizton-

---

[409] Bányász, „Az okos mobil eszközök biztonsága”.
[410] Positive Technologies. (2018). "FINANCIAL APPLICATION VULNERABILITIES". Positive Technologies. Retrieved May 03, 2025, from https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Fin-vulnerabilities-2018-eng.pdf

sági kockázatokat is rejt magában. A rosszindulatú alkalmazások kihasználhatják ezeket a mechanizmusokat illetéktelen adathozzáférés, jogosultság-eszkaláció vagy akár más alkalmazások funkcionalitásának manipulálása céljából. Az alkalmazások közötti visszaélések különösen veszélyesek, mivel megsértik az alkalmazások közötti biztonsági határokat, és lehetővé teszik a támadó számára, hogy egy kompromittált alkalmazáson keresztül hozzáférjen más alkalmazások adataihoz vagy funkcióihoz. [411]

3.6.8 Hálózati kapcsolatok és kommunikációs protokollok biztonsági kihívásai

Az okos eszközök állandó kapcsolatban vannak különböző hálózatokkal, ami számos biztonsági kihívást jelent. A különböző vezetékes és vezeték nélküli kommunikációs protokollok mindegyike sajátos sebezhetőségekkel rendelkezik, amelyeket a támadók kihasználhatnak. A Wi-Fi az egyik leggyakrabban használt vezeték nélküli kapcsolat az okos eszközök esetében, azonban számos biztonsági kockázatot hordoz magában. A nem megfelelően védett vagy nyílt Wi-Fi hálózatok különösen veszélyesek, mivel lehetővé teszik a támadók számára, hogy lehallgassák a kommunikációt vagy man-in-the-middle támadásokat hajtsanak végre. A már említett KRACK sérülékenység jól példázza a Wi-Fi protokollokban rejlő potenciális biztonsági réseket. Bányász Péter kutatásai szerint a biztonsági rések javításáig vezetékes ethernet kapcsolat vagy mobilinternet használata javasolt.[412] Az okos mobileszközök esetében azonban gyakran csak a mobilinternet jelenthet védelmet, ami sok esetben drága és nem biztosít elégséges adatforgalmat.

A mobilhálózatok (3G, 4G, 5G) alapvető kommunikációs csatornát jelentenek az okos eszközök számára. Bár ezek a hálózatok általában biztonságosabbak, mint a nyílt Wi-Fi hálózatok, továbbra is vannak biztonsági kihívások, különösen a régebbi hálózati protokollok esetében. A fake base station vagy "stingray" támadások során a támadók hamis bázisállomásokat hoznak létre, amelyek arra késztetik az eszközöket, hogy rajtuk keresztül kommunikáljanak, lehetővé téve a forgalom lehallgatását vagy manipu-

[411] Bodó Attila Pál és mtsai., *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2018* (Nemzeti Közszolgálati Egyetem, 2019), https://repozitorium.uni-nke.hu/xmlui/handle/20.500.12944/12817?locale-attribute=hu.
[412] Bányász, „Az okos mobil eszközök biztonsága”.

lálását. Az ilyen típusú támadások különösen veszélyesek, mivel a felhasználók általában nem észlelik őket.[413] Az 5G hálózatok számos biztonsági fejlesztést hoztak az előző generációkhoz képest, azonban az új technológiák új sebezhetőségeket is jelenthetnek. Az 5G hálózatok komplexitása és a virtualizált hálózati komponensek használata új támadási felületeket nyithat meg a kifinomult támadók számára.[414]

3.6.9 Bluetooth kapcsolatok sebezhetőségei

A Bluetooth technológia széles körben használt az okos eszközök közötti kommunikációra, különösen a viselhető eszközök, headset-ek és IoT eszközök esetében. A Bluetooth azonban számos biztonsági kihívással küzd, különösen a régebbi verziók esetében. A BlueBorne sebezhetőség, amelyet 2017-ben fedeztek fel, lehetővé tette a támadók számára, hogy távolról vegyék át az irányítást a Bluetooth-kompatibilis eszközök felett, anélkül, hogy párosítani kellene velük vagy a felhasználóknak bármilyen műveletet kellene végrehajtaniuk. Ez a sebezhetőség több milliárd eszközt érintett, beleértve okos telefonokat, táblagépeket, laptopokat és IoT eszközöket.[415] Az újabb Bluetooth verziók (5.0 és újabbak) javították a biztonsági funkciókat, azonban továbbra is fennállnak kockázatok, különösen a régebbi eszközökkel való kompatibilitás miatt.

3.6.10 IoT kommunikációs protokollok biztonsági kihívásai

Az IoT eszközök gyakran specializált, alacsony energiaigényű kommunikációs protokollokat használnak, mint például a ZigBee, Z-Wave, LoRaWAN vagy MQTT. Ezek a protokollok gyakran korlátozott biztonsági funkciókkal rendelkeznek a teljesítmény és energiahatékonyság optimalizálása érdekében.[416] Az IoT-eszközök és felhőszolgáltatások integrációja megköveteli a DTLS (Datagram Transport Layer Security) és CoAP (Constrained Application Protocol) specifikus protokollok alkalmazását, hogy a CIA (Confidentiality, Integrity, Availability) követelmények teljesüljenek.[417]

---

[413] „Fake Base Station Detection - Research on POWDER", PAWR, elérés 2025. május 3., https://advancedwireless.org/outreach/fake-base-station-detection-research-on-powder/.
[414] Mária Orsós és mtsai., „Security Operation Center Methodology for 5G Networks", *Acta Polytechnica Hungarica* 22, sz. 2 (2025): 99–118.
[415] Ben Seri és Gregory Vishnepolsky, *Unveiling Zero Day Vulnerabilities and Security Flaws in Modern Bluetooth Stacks* (Armis, Inc., White Paper, 2017).
[416] Krishnakant Soni, „IOT COMMUNICATION TECHNOLOGIES", in *IIP Series*, Chapter 2. Dr. C.V, köt. 3, Book 8, Part 9 (Raman University, India, 2024).
[417] S. Arun, V.M. Sriram, és S. Veni, *Lightweight and Secure Mutual Authentication Scheme for IoT Devices Using CoAP* (Computers, Materials & Continua, 2024).

Az IoT eszközök között megkülönböztethetünk vezetékes és vezeték nélküli kapcsolatokat. 2023-ban a 16,6 milliárd IoT kapcsolatból 0,7 milliárd volt vezetékes IoT aggregációs csomópont, ami a teljes IoT kapcsolatok 4%-át tette ki.[18] A fennmaradó 15,9 milliárd kapcsolat vezeték nélküli IoT aggregációs csomópont és vezeték nélküli IoT végpontok voltak. Ha azonban a vezetékes IoT végpontokat is figyelembe vesszük, akkor 2023-ban globálisan 23,4 milliárd vezetékes IoT végpont volt megtalálható. Az átlagos aggregációs csomóponthoz 33 vezetékes IoT végpont kapcsolódott 2023-ban, és ez az arány várhatóan 2030-ra 40 fölé emelkedik, mind az ipari, mind a fogyasztói IoT növekedése által hajtva. [418]

3.6.11 További kommunikációs technológiák kockázatai

Az NFC technológia az elmúlt évtizedben széles körben elterjedt az okos telefonokon, lehetővé téve a mobilfizetést, a gyors párosítást más eszközökkel és számos más kényelmi funkciót. Bár az NFC viszonylag biztonságos a rövid kommunikációs távolság miatt, továbbra is léteznek potenciális kockázatok, különösen a nyilvános helyeken történő használat során.[419]

Az UWB (Ultra-wideband) technológia a közelmúltban jelent meg az okos telefonokban, és rendkívül pontos helymeghatározást tesz lehetővé rövid távolságon belül. Ez különösen hasznos tárgyak követésére, precíziós navigációra beltérben és az eszközök közötti más térbeli interakciókra. A legújabb okos telefonok már támogatják a műholdas kommunikációt is vészhelyzeti helyzetekben. Ez a technológia új biztonsági kihívásokat jelent, különösen a globális lefedettség és a potenciális lehallgatási lehetőségek miatt.[420]

---

[418] IoT Analytics, „Number of Connected IoT Devices Growing 13% to 18.8 Billion Globally", report. (State of IoT, 2024).
[419] Marc Rivero, *Smartphone Users Should Be Aware of the Threats Posed by NFC Tag Tampering* (Cybersecurity Asia, 2025).
[420] FiRa Consortium, „Why Is UWB Important for Indoor Positioning? FiRa Consortium Blog", *October* 10 (2024).

3.6.12 Adatbiztonsági és adatvédelmi kockázatok

Az okos eszközök és alkalmazásaik hatalmas mennyiségű adatot gyűjtenek a felhasználókról és környezetükről. Ez számos adatbiztonsági és adatvédelmi kockázatot jelenthet. Az okos eszközök és alkalmazásaik adatgyűjtési gyakorlatai gyakran nem átláthatóak a felhasználók számára. Sok esetben a felhasználók nincsenek tisztában azzal, hogy milyen adatokat gyűjtenek róluk, hogyan használják fel ezeket az adatokat, vagy kivel osztják meg azokat. Az adatgyűjtés mértéke és mélysége eltérhet az alkalmazások között. Egyes alkalmazások csak az alapvető, működéshez szükséges adatokat gyűjtik, míg mások részletes profilt készítenek a felhasználók viselkedéséről, preferenciáiról és szokásairól. Ez utóbbi különösen jellemző a freemium és hirdetésalapú üzleti modellt használó alkalmazásokra, ahol az adatok gyűjtése és értékesítése a bevételi modell fontos része.[421]

A GDPR és más adatvédelmi szabályozások célja, hogy javítsák az adatgyűjtési gyakorlatok átláthatóságát és biztosítsák a felhasználók jogait adataik kezelésével kapcsolatban. Azonban a megfelelés szintje eltér az alkalmazások között, és sok esetben a megfelelés formális, anélkül, hogy valódi átláthatóságot biztosítana a felhasználók számára.[422]

Az okos eszközök és alkalmazásaik által gyűjtött adatok tárolása további biztonsági kockázatokat jelent. Az adatok tárolhatók lokálisan az eszközön vagy a felhőben, de mindkét esetben megfelelő biztonsági intézkedésekre van szükség a jogosulatlan hozzáférés, adatszivárgás vagy adatvesztés megakadályozására.

A lokális adattárolás esetén az eszköz elvesztése, ellopása vagy fizikai kompromittálása jelenthet kockázatot. A modern okos eszközök többsége támogatja az eszköz titkosítását, azonban a megfelelő beállítások és a rendszeres frissítések hiánya sebezhetővé teheti az eszközt és a rajta tárolt adatokat. A felhőalapú adattárolás esetén az adatok biztonságát a szolgáltató infrastruktúrájának és biztonsági gyakorlatainak minő-

[421] Wall Street Prep, „Freemium Model | Pricing Strategy + Examples", *Wall Street Prep*, 2024.
[422] J. Krämer, „The Death of Privacy Policies: How App Stores Shape GDPR Compliance of Apps", *Internet Policy Review* 13, sz. 2 (2024), https://doi.org/10.14763/2024.2.1757.

sége határozza meg. A felhőszolgáltatók általában fejlett biztonsági intézkedéseket alkalmaznak, azonban a megfelelő szolgáltató kiválasztása és a biztonságos konfiguráció beállítása továbbra is a felhasználók és vállalatok felelőssége[423]

Az okos eszközökön futó alkalmazások gyakran osztják meg az összegyűjtött adatokat harmadik felekkel, például hirdetési hálózatokkal, elemzési szolgáltatásokkal vagy más szolgáltatókkal. Ez további biztonsági kockázatokat jelent, mivel az adatok biztonságát a harmadik felek biztonsági gyakorlatai is befolyásolják. Az alkalmazásfejlesztők gyakran használnak harmadik féltől származó könyvtárakat és szolgáltatásokat, amelyek szintén gyűjthetnek és továbbíthatnak adatokat. Ezek a könyvtárak gyakran rejtett módon gyűjtenek adatokat, és a felhasználók vagy akár a fejlesztők sincsenek mindig tisztában azzal, hogy milyen adatokat gyűjtenek, és hogyan használják fel azokat. [424]A harmadik felek által gyűjtött adatok összekapcsolása és elemzése lehetővé teheti a felhasználók profilozását és nyomon követését, ami adatvédelmi aggályokat vet fel. A különböző forrásokból származó adatok kombinálása pontos képet adhat a felhasználók viselkedéséről, szokásairól és preferenciáiról, gyakran a felhasználók tudta vagy beleegyezése nélkül.[425]

Az adatvédelmi szabályozások, mint a GDPR vagy a magyar Infotörvény követelményeket támasztanak az okos eszközök és alkalmazásaik fejlesztői és üzemeltetői számára. Ezeknek a szabályozásoknak való megfelelés azonban gyakran kihívást jelent.[426] A megfelelési kihívások között szerepel az adatok gyűjtésére, tárolására és megosztására vonatkozó egyértelmű tájékoztatás biztosítása a felhasználók számára, a felhasználók hozzájárulásának megfelelő megszerzése, valamint a felhasználók jogainak biztosítása adataik hozzáféréséhez, törléséhez vagy hordozhatóságához.[427] A szabályozások folyamatosan fejlődnek és változnak, ami tovább nehezíti a megfelelést. Az új technológiák, mint például a mesterséges intelligencia vagy a biometrikus azonosítás,

[423] Sybell, „Mennyire biztonságos a felhőalapú adattárolás? Sybell Blog”, *Augusztus* 21 (2023).
[424] I.M.D.E.A. Networks, *An Analysis of Third-Party Mobile SDKs - Data Protection and Privacy* (IMDEA Networks Principal, 2024).
[425] Omar Hasan, *A Discussion of Privacy Challenges in User Profiling with Big Data Techniques* (LIRIS CNRS, 2013).
[426] C.M.S., *Data Protection and Cybersecurity Laws in Hungary* (CMS Expert Guide, 2024).
[427] Policyreviewinfo, „GDPR Compliance Is Hard" – but Is It?: 20 Hours to Overcome Privacy Issues in Mobile Apps”, *Policy Review*, 2023.

további szabályozási kihívásokat jelentenek, mivel a meglévő szabályozások nem mindig fedik le megfelelően ezeket a területeket.[428]

Következtetések

Az okos eszközök történeti fejlődése során nyilvánvalóvá vált, hogy a technológia gyors elterjedése gyakran másodlagos helyre sorolta a biztonsági megfontolásokat. A kibertér globális természete rendkívül változatos és folyamatosan fejlődő veszélyeket eredményez, megnehezítve a hatékony válaszlépések kidolgozását. A társadalomban az információs és kommunikációs technológiától való nagymértékű függőség miatt az állam és a gazdaság működése szinte lehetetlenné válik ezek nélkül, tovább súlyosbítva a meglévő biztonsági fenyegetések komplexitását.

Az alkalmazások biztonságát érintő potenciális sebezhetőségek értékelése különös figyelmet követel a túlzott jogosultságok problémakörének tekintetében. Az adatbiztonság és adatvédelem terén a fő kihívást az okos eszközök és a hozzájuk kapcsolódó alkalmazások átláthatatlan adatgyűjtési gyakorlatai jelentik. A felhasználók gyakran nincsenek tájékoztatva a róluk gyűjtött adatokról, azok felhasználásáról és a megosztásukban résztvevő entitásokról. Az adatok gyűjtése és monetizálása alapvető eleme a freemium és hirdetésalapú üzleti stratégiákat alkalmazó alkalmazások bevételi modelljének. Ez különösen nehéz akadályt jelent az ilyen alkalmazások számára.

Az operációs rendszerek sebezhetőségeinek vizsgálata arra utal, hogy az Android különösen hajlamos a gyengeségekre a fragmentáció miatt. Ez azért fordul elő, mert a különböző gyártók az operációs rendszer eltérő verzióit használják, és a frissítések nem következetesen jutnak el minden eszközhöz egyszerre. A biztonsági sebezhetőségek várhatóan elterjednek és diverzifikálódnak az 5G, a fejlett hálózati technológiák, az edge computing, a blokklánc, a decentralizált alkalmazások és az ambient computing megjelenése miatt. Ez a várható trendek és kihívások vizsgálatán alapul. A felhasználói viselkedés változásai, beleértve az alkalmazás-fáradtságot és az adatvédelem-központú perspektívák térnyerését, új dinamikát teremtenek a biztonság területén.

[428] BioID, „AI Regulations and Biometric Technology: How New Policies Are Reshaping Our Digital World", *BioID Blog*, 2025.

Ezek a technológiák újszerű lehetőségeket kínálnak a támadók számára, míg a felhasználói viselkedés változásai új dinamikát eredményeznek.

Az okos eszközök fejlődésének hadtudományi jelentősége a modern katonai műveletek digitalizálódásában rejlik A személyazonosításra és hitelesítésre alkalmas technológiák fejlődése közvetlenül érinti a katonai személyzet biztonságos azonosítását és a műveleti biztonságot, amelyre jó példa a Strava-botrány. Az alkalmazások biztonsági kockázatai, különösen a túlzott jogosultságkérések és adatszivárgás fenyegetést jelenthetnek a minősített környezetekben dolgozó személyzet számára. A supply chain támadások elemzése alapvető fontosságú a védelmi beszerzések biztonságának szempontjából. Az eszközök nemzetközi összehasonlítása pedig betekintést nyújt a különböző államok digitális képességeibe és biztonsági kultúrájába.

Konklúzióként elmondható, hogy a biztonság fokozása többszintű megközelítést igényel. Elsősorban elengedhetetlen a felhasználói tudatosság növelése, különös tekintettel az alkalmazás-jogosultsági kérelmek kritikus értékelésére és a gyakori szoftverfrissítések telepítésének szükségességére. Továbbá alapvető fontosságú, hogy a gyártók és fejlesztők már a tervezési fázisban figyelembe vegyék a biztonsági problémákat, ezt nevezik "security by design" elvnek, valamint rendszeres biztonsági értékeléseket végezzenek meglévő termékeiken. Végezetül elmondható az is, hogy átfogó jogi keretrendszerekre van szükség az innováció és a biztonság egyensúlyának megteremtéséhez, miközben biztosítják az átláthatóságot az adatgyűjtési és felhasználási módszerek terén.

A jövőben a kutatásnak és fejlesztésnek az okos eszközök és alkalmazások biztonságának javítására kell összpontosítania. Az okos eszközök és alkalmazásaik által nyújtott előnyök biztonságos élvezetének biztosításához, a kapcsolódó kockázatok mérséklése mellett, proaktív megközelítést kell alkalmazni, amely magában foglalja a számos érdekelt fél közötti együttműködést.

A CATWOE alapján kielemezett szakértői interjúk alapján megállapítható, hogy:

Ügyfelek (Customers)

A mobilalapú hitelesítési rendszerek ügyfelei rendkívül sokszínű csoportot alkotnak. Az interjúkból kirajzolódik, hogy a fiatalabb generáció (18-35 évesek) általában nyitottabb a biometrikus azonosítási megoldásokra, míg az idősebb korosztály (különösen a 60+ évesek) gyakran bizalmatlanabb. Ahogy Németh Márton fogalmaz: "Idősek nyilván jobban szeretik a személyes és papír alapú megoldásokat, kevésbé fogékonyak a technológiákra". Érdekes módon azonban az első (anonim) interjúalany határozottan kijelenti: "nem hiszek a generációs különbségekben", ami ellentmond a többi szakértő véleményének.

A vállalati felhasználók külön ügyfélcsoportot képeznek, akik számára a COVID-19 járvány katalizátorként szolgált a digitális azonosítási megoldások elfogadásában. Hugli Péter kiemeli a banki és pénzügyi szolgáltatások, valamint az e-kereskedelem területén dolgozókat, akik számára a "gyorsabb és biztonságosabb tranzakciók, csökkentett csalás kockázata" jelenti a fő előnyt[3].

A Digitális Állampolgárság Program (DÁP) kapcsán vegyes visszajelzések érkeztek. Németh Márton szerint "kezdik megszokni az emberek, örülnek, hogy nem kell kormányablaknál várni", ugyanakkor "vannak az embereknek biztonsági aggályai főleg a biometria terén".

Szereplők (Actors)

A hitelesítési rendszerek ökoszisztémájában számos szereplő működik együtt és verseng egymással:

Fejlesztők és technológiai szolgáltatók kulcsszerepet játszanak a biztonságos protokollok implementálásában. Az első interjúalany hangsúlyozza, hogy "a Security Design a biztonsági terület dolga, ez külön speciális rész", vagyis a fejlesztők elsősorban a protokollok követését végzik, nem pedig a biztonsági tervezést. Ugyanakkor Hujber Gábor szerint a fejlesztőknek "egyszerre kellene a szigorú biztonsági előírásokat és a felhasználóbarát élményt biztosítani".

Állami szervezetek felelősek a szabályozási keretrendszer kialakításáért. Az interjúkból kiderül, hogy Magyarországon két szektorban kötelező a többfaktoros hitelesítés: "pénzpiaci szektor, másik az állami szektor". Az állam szerepe a biztonságtudatosság

növelésében is meghatározó lenne, de az első interjúalany szerint "állami szinten se valósul meg a biztonságtudatosítás megfelelő mértékben".

Kiberbűnözők folyamatosan alkalmazkodnak az új védelmi mechanizmusokhoz. Németh Márton kiemeli, hogy "már sok próbálkozás van a kétfaktoros ellen is malwerek segítségével", míg Hugli Péter a "SIM swap" támadásokat említi, "ahol a támadók átveszik a felhasználó telefonszámát".

Átalakulási Folyamat (Transformation Process)

A hitelesítési rendszerek átalakulása több dimenzióban zajlik:

Technológiai fejlődés terén az 5G hálózatok szerepe ellentmondásos. Míg Hujber Gábor szerint az 5G "a személyazonosítás gyorsaságát is segíteni fogja", addig az első interjúalany határozottan állítja, hogy "az 5G jelen szempontból nem releváns". Németh Márton árnyaltabb képet fest: "Valamennyire gyorsítja, de vannak hátulütői, szilárd testeken nehezen megy át, rossz lehet a lefedettség emiatt".

Biztonsági architektúra átalakulásában a "zero trust" elv egyre nagyobb szerepet kap. Az első interjúalany szerint ez "a legfontosabb" védelmi stratégia. A folyamatos hitelesítés (continuous authentication) előnyeit mindegyik szakértő elismeri, bár Németh Márton figyelmeztet, hogy ez "költség és tárhely igényes, sok a fals pozitív"

Felhasználói magatartás változása kapcsán az első interjúalany javasolja a "kiberjogosítvány bevezetését is állami szinten, ami az internetes technológia felhasználói szintű ismereteit bizonyítaná". Ez összefügg azzal a megállapításával, hogy "a jelenlegi 18 év alatti korosztály esetében sok a funkcionális analfabéta, mind a digitális, mind a valós világban".

Világnézet (Worldview)

A szakértők világnézetében központi helyet foglal el a biztonság és kényelem egyensúlya. Az első (anonim) interjúalany szerint "egy biztos, konformitás a biztonság rovására szokott menni". Hujber Gábor hasonlóan fogalmaz: "Egyszerre kellene a szigorú biztonsági előírásokat és a felhasználóbarát élményt biztosítani"

A biometrikus adatok kezelése kapcsán eltérő megközelítések rajzolódnak ki. Németh Márton felhívja a figyelmet, hogy "magyar NIS2-es szabály, és osztályozás ilyen eljárás bevezetése esetén biometrikus adatokat tárolsz, ami már biztonságú osztályú lesz, ez nem támogatja azt, hogy szervezetek saját biometrikus rendszert működtessenek".

A technológiai determinizmus is megjelenik, különösen Németh Márton jövőképében: "Biztonsági szempontból csak romlani fog, viszont a felhasználó élmény és gyorsaság az nőni fog, ez felül fogja írni a biztonsági megoldásokat".

Tulajdonosok (Owners)

A hitelesítési rendszerek tulajdonosai között meghatározó szerepet játszanak az államok és nemzetközi szervezetek. Az interjúkból kiderül, hogy az EU eIDAS rendelete, illetve annak 2.0-ás verziója hatással van a fejlesztésekre. Németh Márton szerint "hiába van eIDAS rendelet, majd az eIDAS 2.0 megpróbálja helyretenni" a jogi keretrendszert.

A pénzügyi intézmények szintén kulcsfontosságú tulajdonosok. Az első interjúalany kiemeli, hogy "pénzpiaci szektor tekintetében rendelet írja elő SEPA szinten"[2] a többfaktoros hitelesítést. Ugyanő említi az MDM (Mobile Device Management) rendszerek fontosságát is: "A fentiek kezelésére szolgál az MDM és box in box a megoldás, a banki alkalmazások így működnek".

A mobilgyártók szerepe sem elhanyagolható. Az első interjúalany kritikusan jegyzi meg, hogy "a mobil eszköz gyártók információbiztonsági kultúrája is alacsony", ami biztonsági kockázatokat hordoz.

Környezeti Korlátok (Environmental Constraints)

A szakértők számos környezeti korlátot azonosítottak, amelyek befolyásolják a hitelesítési rendszerek fejlődését:

Technológiai infrastruktúra hiányosságai akadályt képeznek. Az első interjúalany szerint "Magyarországon rossz hálózati lefedettség és az államnak a lefedettség javítását ki kellene kényszerítenie". Hujber Gábor is említi, hogy "nem mindenhol adott a megfelelő internetkapcsolat".

Jogi szabályozás területén a GDPR és a NIS2 irányelv jelent meghatározó keretet. Németh Márton kiemeli, hogy a biometrikus adatok tárolása miatt "más biztonsági osztály" besorolás szükséges, ami megnehezíti a technológia elterjedését.

Társadalmi tényezők közül a digitális írástudás hiánya emelkedik ki. Az első interjúalany szerint "a magyar lakosság várja a védelmet, de nem fektet energiát saját védelmébe, képzésébe".

Kiberfenyegetések folyamatosan fejlődnek. Németh Márton említi az "AI segítségével" működő támadásokat[1], míg Hujber Gábor az "MFA megkerülése" és "AI alapú támadások" veszélyeire hívja fel a figyelmet.

A CATWOE elemzés alapján a mobilalapú hitelesítési rendszerek komplex ökoszisztémát alkotnak, amelyben a technológiai, jogi, társadalmi és biztonsági szempontok szorosan összefonódnak. A szakértők egyetértenek abban, hogy a többfaktoros hitelesítés elengedhetetlen, ugyanakkor eltérő véleményeket fogalmaznak meg az 5G szerepéről, a generációs különbségekről és a jövőbeli fejlődési irányokról. A sikeres implementáció kulcsa a biztonság és felhasználói élmény egyensúlyának megteremtése, valamint a felhasználók biztonságtudatosságának növelése.

A felárt ismeretek és az interjúk alapján **a** H1 hipotézis nem került megerősítésre az okos eszközök fejlődése és a személyi hitelesítés dominanciáját interjúk részben megerősítik, de árnyalják ezt az állítást:

A H3 hipotézis cáfolásra került az interjúk alapján mivel komplex a téma és nem megállapítható, hogy több a lehetőség, mint a kockázat, a kockázatok és lehetőségek egyensúlya bonyolultabb. Azonban a H4 hipotézis erősen alátámasztásra került.

4 SZEMÉLYAZONOSÍTÁSRA ÉS HITELESÍTÉSRE ALKALMAS TECHNOLÓGIA JELENLEGI FELHASZNÁLÁSI TERÜLETEI

A digitális átalakulás korában a személyazonosítás és hitelesítés alapvető biztonsági követelménnyé vált az egyének, vállalkozások és kormányzatok számára egyaránt. Az elektronikus tranzakciók végrehajtása, valamint a személyes és érzékeny adatok védelme mind olyan területek, ahol elengedhetetlen a megbízható személyazonosítás. Az okos telefonok elterjedésével (2025-re 6,9 milliárd okostelefon-felhasználó várható globálisan) a hitelesítési módszerek fejlődésen mentek keresztül, a hagyományos jelszóalapú megoldásoktól a korszerű biometrikus és eszközalapú technológiákig.[429] A globális biometrikus rendszerek piaca pedig várhatóan 42,9 milliárd dollárról (2023) 82,9 milliárd dollárra növekszik 2027-re, ami 17,9%-os összetett éves növekedési rátát jelent.[430]

Mint ahogy a fentiekben már említésre került a személyazonosítás és hitelesítés, bár szorosan összefüggő, különböző koncepciók. A személyazonosítás során egy entitás (személy vagy rendszer) identitását deklarálja, míg a hitelesítés folyamán ez az állítás ellenőrzésre kerül. A modern hitelesítési rendszerek három fő faktorra épülhetnek: tudásalapú (jelszavak, PIN-kódok), birtoklásalapú (mobileszközök, tokenek) és tulajdonságalapú (biometrikus jellemzők) tényezőkre.[431]

Jelen fejezetben a korábban bemutattok technológiák részletes, szektor specifikus elemzést fogom bemutatni, hogy az egyes területeken a személyazonosítás, illetve személyi hitelesítés, (de nem kizárólagosan személyek, hanem más entitások, mint szerződések, dokumentumok, akár közösségi média profilok hitelesítése) aktuális trendjeit alkalmazási területeiket, illetve specifikus biztonsági kihívásait.

4.1 Magánszférában alkalmazott technológiák

A bankszektor élen jár a személyazonosítás, illetve hitelesítés terén, mind a biometrikus és többfaktoros hitelesítés alkalmazásában. Az európai PSD2 irányelv erős ügyfél-

[429] „Mobile app usage - statistics & facts | Statista".
[430] „Biometric System Market Size, Share, Trends and Growth Analysis 2032", elérés 2025. május 3., https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html.
[431] „What Are the Three Authentication Factors? - Rublon", elérés 2025. május 3., https://rublon.com/blog/what-are-the-three-authentication-factors/.

hitelesítési (SCA) követelményeinek megfelelően a pénzintézetek különböző mobilalapú megoldásokat implementáltak.[432] A pénzügyi alkalmazásokban a biometrikus hitelesítés többféle módszert foglal magában: az ujjlenyomat-felismerés, amely egyedi ujjlenyomat-mintázatokat elemez, az arcfelismerő technológia, amely feltérképezi és elemzi az arcvonásokat, valamint a hangfelismerés, amely az utóbbi időben egyre elterjedtebbé válik.[433]

2025-ben a jelszónélküli hitelesítés várhatóan normává válik a mobil banki alkalmazásokban. Ennek oka, hogy a jelszavak sok esetben nem biztonságosak – 2024 második felében például 703%-kal nőtt a hitelesítő adatok adathalászatára irányuló támadások száma.[434] A jelszavak helyettesítésével biztonságos mobileszköz-alapú ellenőrzéssel a vállalkozások csökkenthetik az adathalászati kockázatokat, miközben javítják a felhasználói élményt.

4.1.1 Bank és pénzügyi szektor

A digitális bankolás korszakában a pontos személyazonosítás és hitelesítés biztosítása elengedhetetlenné vált a pénzügyi szolgáltatások biztonságos nyújtásához. A csalások megelőzése és az ügyféladatok védelme érdekében a bankszektornak biztonságos azonosítási rendszert kell alkalmaznia az ügyfelek számára, és megfelelően kell hitelesítenie a tranzakciókat. A hagyományos jelszóalapú hitelesítési módszereket felváltották a kifinomultabb biometrikus és eszközközpontú technológiák. A mobiltelefonok megjelenése óta a hitelesítési rendszerek fejlődésen mentek keresztül. A korszerű banki alkalmazások mind az azonosítási, mind a hitelesítési folyamatokat tartalmaznak, hogy biztosítsák a felhasználók biztonságát. A bankszektor élen jár a biometrikus és többfaktoros hitelesítés alkalmazásában. [435]

A biometrikus hitelesítés teljesen forradalmasította a bankok által használt azonosítási technikákat. A biometrikus technológiák egyedi fizikai vagy viselkedési jellemzőket

[432] „Thales Mobile Authentication Solutions for Digital Banking", elérés 2025. május 3., https://cpl.thalesgroup.com/access-management/digital-banking/mobile-authentication.
[433] „Top user authentication trends for 2025 | Twilio", elérés 2025. május 3., https://www.twilio.com/en-us/blog/user-authentication-trends.
[434] Harry Cheung, „Mobile Security Trends 2025: What You Need to Know and How to Stay Ahead", *IPification* (blog), 2025. január 24., https://www.ipification.com/blog/mobile-security-trends-2025-what-you-need-to-know-and-how-to-stay-ahead/.
[435] „Thales Mobile Authentication Solutions for Digital Banking".

használnak a biztonság fokozott szintjének biztosítására az azonosítás céljából. Ezek a tulajdonságok nehezen hamisíthatók. Az ujjlenyomat-felismerés a leggyakrabban használt biometrikus hitelesítési forma a mobil banki alkalmazásokban. Az ujjlenyomat-alapú azonosítás gyors és felhasználóbarát, mindazonáltal, bizonyos körülmények között kihívásokat jelenthet, például amikor az ujjak nedvesek vagy sérültek. Következésképpen az ujjlenyomat-alapú azonosítás problémákat okozhat.[436]

Az arcfelismerés az elmúlt években fejlődött a kutatók által kifejlesztett mesterséges intelligencia és mélytanulási algoritmusok fejlődésének köszönhetően. A korszerű arcfelismerő rendszerek mélytanulási algoritmusokat, infravörös képeket és háromdimenziós modelleket használnak a pontosság javítására és a hamisítás elleni védelem megerősítésére. Ezt a technológiát számos banki alkalmazásban használják, lehetővé téve az ügyfelek számára, hogy arcfelismeréssel hitelesítsék bejelentkezéseiket és tranzakcióikat.[437]

Számos korszerű biometrikus technológiát egyre inkább használnak a banki alkalmazásokban. Ilyen technológiák közé tartozik a tenyérerezet-felismerés és az írisz-felismerés. A tenyérerezet-azonosításnak sok előnye van, különösen az, hogy az érmintázat a bőr alatt helyezkedik el, ami megnehezíti a másolást, és idővel stabilabb marad más biometrikus jellemzőkhöz képest.[438]

A viselkedési biometria esetében az azonosítás a felhasználó viselkedési mintáira támaszkodik, amelyek nehezebben reprodukálhatók, mint a statikus adatok. Ez a viselkedési biometriát sokkal biztonságosabbá teszi. Ez magában foglalja a billentyűzetdinamikát (a gépelési minták tanulmányozását), a mozgásérzékelők adatait és az eszközhasználati viselkedést. Ezeknek a technológiáknak a használata lehetővé teszi a folyamatos és passzív hitelesítést, ezáltal javítva a biztonságot anélkül, hogy rontaná a felhasználói élményt. Ezt a stratégiát több pénzügyi szervezet is alkalmazza a csalárd tevékenységek megelőzésére.[439]

---

[436] Nordstone, „Integrating Biometric Security Features into Mobile Apps"", 2023, https://nordstone.co.uk/blog/integrating-biometricsecurity-features-into-mobile-apps.
[437] Apple Inc, *Face ID Security Guide* (Cupertino: Apple Inc, 2023).
[438] Amazon, *Amazon One: Palm-Based Identity Service"* (Technical Documentation, 2022).
[439] „Behavioral Biometrics in Financial Fraud Prevention"", *Journal of Banking Technology* 12, sz. 3 (2023).

Az erős ügyfél-hitelesítési folyamat és a PSD2 végrehajtása Magyarországon

Az erős ügyfél-hitelesítés (SCA) az Európai Unió 2015/2366 (PSD2) irányelve által létrehozott követelmény. Ez a kritérium szükségessé teszi legalább két, különböző kategóriákból származó hitelesítési elem használatát a pénzügyi tranzakciók során. Ez az igény felgyorsította a többfaktoros hitelesítési rendszerek elterjedését Európa-szerte, beleértve Magyarországot is.[440] A többfaktoros hitelesítés növeli a biztonságot, mivel még ha egy támadó kompromittálja is az egyik elemet, továbbra is meg kell szereznie a többi komponenst a sikeres hitelesítéshez.[441] A magyar pénzintézetek több módon is fejlesztettek megoldásokat az SCA követelményeinek teljesítésére. Ezek a megoldások magukban foglalják a biometrikus hitelesítést és a mobil alapú hitelesítési módszereket is. Az ügyfél azonosítás magyarországi alkalmazását a Magyar Nemzeti Bank (MNB) által kiadott 26/2019. számú ajánlás szabályozza részletesen. A javaslat meghatározza az SCA alkalmazást igénylő tranzakciókat és a megengedett kivételeket. A VII.19. Szakasz szabályozza a pénzügyi intézményekre alkalmazható elektronikus azonosítási módszereket, és engedélyezi a videobankos azonosítást, az okmányellenőrzést és a biometrikus felismerést. Számos bank, köztük az OTP, a K&H és az MBH Bank bevezette a videó alapú azonosítást. Ez népszerűségre tett szert a COVID-19 járvány idején, amikor a személyes ügyintézés nem volt lehetséges.

A PSD2 követelményeinek megfelelően kifejlesztett 3D Secure 2.0 protokoll kockázat alapú hitelesítést alkalmaz, és csak a magasabb kockázatúnak ítélt tranzakciók esetében kér további hitelesítést.[442] Ez a stratégia egyensúlyt teremt a biztonság és a felhasználói elégedettség között.

Jelszó nélküli hitelesítési technikák

A felhasználók gyakran gyenge jelszavakat választanak, ugyanazt a jelszót többször használják különböző platformokon, és ki vannak téve a "váll fölötti leskelődés" (shoulder surfing) támadásoknak, amikor a támadók a felhasználók megfigyelésével vagy külső rögzítő eszközök alkalmazásával gyűjtik a hitelesítési információkat.[443]A

[440] E.U. Directive, „On Payment Services in the Internal Market"", 2015. 2366 (PSD2.
[441] N.I.S.T., „Special Publication: CRYSTALS-Kyber Implementation", 2024.
[442] EMVCo, „3-D Secure 2.0 Specifications"", 2022.
[443] H.M. Sun és mtsai., „A Shoulder Surfing Resistant Graphical Authentication System"", *IEEE Transactions on Dependable and Secure Computing* 15, sz. 2 (2018).

pénzintézetek csökkenthetik az adathalász kísérletek kockázatát a jelszó nélküli hitelesítési technikák használatával. Az új megoldások szükségességét az is alátámasztja, hogy, 2024 második felében a hitelesítési adatok adathalászatára irányuló támadások 703%-os növekedést mutattak.[444]

A felhasználói hitelesítés megvalósítható a Fast Identity Online Alliance (FIDO) szabvány által létrehozott passkey módszerekkel. A passkey rendszerek szükségtelenné teszik, hogy a felhasználók jelszavakat jegyezzenek meg. Ezek a rendszerek kriptográfiai kulcspárokat használnak, ahol a privát kulcs a felhasználó eszközén tárolódik, míg a nyilvános kulcs a szerveren marad. [445]

Az IPification technológia egyedi Mobile ID kulcsot rendel minden felhasználóhoz. Ez a kulcs a SIM-kártyából, az eszközből, a telefonszámból és a kísérő hálózati adatokból áll. Ez a módszer nagyon hatékony a phishing erőfeszítések és a SIM-kártya csere ellen.[446]

A hongkongi és malajziai bankok korlátozták az SMS OTP-k használatát az online kártyás tranzakciókhoz, előnyben részesítve az eszközöket használó, fokozott biztonságot nyújtó opciókat. Ennek a trendnek a globális fennmaradása várható.[447]

Mesterséges intelligencia alkalmazása a banki hitelesítési folyamatokban

A pénzügyi azonosítási rendszerek területén a mesterséges intelligencia (MI) egyre fontosabb elemmé válik. A mesterséges intelligenciát (MI) használó biztonsági megoldások fokozott védelmet nyújthatnak a banki alkalmazások és a felhasználói adatok számára a biztonsági fenyegetések proaktív azonosításával és enyhítésével.[448] A mesterséges intelligencia rendszerek adaptálhatósága javítja a pontosságot, csökkenti a megfeleltetési torzítást, és javítja a biztonsági funkciókat, mint például az élőségi de-

[444] Cheung, „Mobile Security Trends 2025”.
[445] F.I.D.O. Alliance, *FIDO2: Web Authentication* (WebAuthn)", Technical Specification, 2022).
[446] Cheung, „Mobile Security Trends 2025”.
[447] „Top user authentication trends for 2025 | Twilio”.
[448] LinkedIn Pulse, „Top Mobile App Security Trends to Watch in 2025"”, 2023.

tektálást és a deepfake azonosítást, a megtévesztés elleni védelemre. Ezek a fejlesztések kulcsfontosságúak lesznek a jelenleg tapasztalt folyamatosan változó fenyegetések kezelésében és a biometrikus rendszerek megbízhatóságának javításában.[449]

A konvolúciós neurális hálózat (CNN) modelleket mobil banki alkalmazásokban használják az alkalmazáson belüli arcfelismerés biztosítására. A Firebase Machine Learning vision modell kezeli az arcazonosítást és az elő feldolgozást, míg a MobileFaceNet modell feldolgozza, kategorizálja és egy adatbázisban tárolható formátumra alakítja az adatokat. Az adatgyűjtési eljárás során az okos telefon elülső kamerájával valós időben négy képet készítenek minden egyedi felhasználóról az arcvonások dokumentálására.[450]

A CIB Bank 2022-es tanulmánya szerint az automatizált ellenőrzési rendszerek 98%-a támaszkodik biometrikus adatokra a tranzakciós csalások észlelésére. Ez kiemeli a mesterséges intelligencia és a biometria pénzügyi biztonságba való integrálásának szükségességét.[451]

A mesterséges intelligencia és a gépi tanulás használatával a pénzintézetek elemezhetik az ügyfelek viselkedését és preferenciáit, és ennek megfelelően alakíthatják szolgáltatásaikat. A felhasználói azonosítás a személyre szabás kulcsfontosságú eleme, amely egyre inkább automatizált és zökkenőmentes eljárássá válik.

Egy esettanulmány szerint egy közepes méretű bank áttért a hardveres tokenekről a szoftveres hitelesítésre az OneSpan Mobile Authenticator alkalmazás segítségével. Ez a váltás nem csak kényelmesebbé tette az ügyfelek számára a szolgáltatások elérését, hanem költségmegtakarítást is eredményezett a bank számára, miközben a biztonsági szint nem csökkent.[452]

---

[449] H.I.D. Global, „What's on the Horizon: 10 Biometric Trends for 2025"", 2023, https://blog.hidglobal.com/whats-horizon-10-biometric-trends-2025.
[450] S. Kumar, R.K. Singh, és A.S. Akhi, „Mobile Banking Authentication Using CNN Embedded Face Recognition"", in *IEEE International Conference on Future Networks and Distributed Systems*, 2022.
[451] C.I.B. Bank, „IFRS 2021 CIB Bank"", Annual Report, 2022, https://www.cib.hu/document/publications/CIB/2022/kozlemeny/IFRS_2021_CIB_Bank__HU-220325/IFRS_2021_CIB.
[452] „Top user authentication trends for 2025 | Twilio".

A HSBC 2016-ban bevezetett Voice ID rendszere különösen innovatív példája a biometrikus azonosítás alkalmazásának. A rendszer több mint 100 egyedi jellemzőt azonosít a felhasználó hangjában, beleértve a beszéd sebességét, a hangmagasságot és a szájüreg formáját. A technológia még akkor is képes azonosítani a felhasználót, ha náthás vagy változik a hangja az idő múlásával. A Voice ID bevezetése óta több mint 350 millió fontot sikerült megmenteni a banki csalásoktól az Egyesült Királyságban.[453]

4.1.2 Ügyvédi irodák és jogi szektor

Az ügyvédi irodák egyre növekvő nyomással szembesülnek, hogy megbízható személyazonosítási és hitelesítési technológiákat vezessenek be az ügyféladatok védelme, a szabályozási megfelelőség biztosítása érdekében. Az ügyvédi irodák – az általuk kezelt értékes és bizalmas információk miatt – kiemelt célpontok a támadók részére.

Biometrikus hitelesítés a jogi gyakorlatban

A biometrikus hitelesítési rendszerek népszerűségre tettek szert az ügyvédi irodákban, mivel képesek biztonságosabb és hatékonyabb ügyfél-azonosítást biztosítani a hagyományos módszerekhez képest. A biometrikus személyazonosság-ellenőrzés segít az ügyvédi irodáknak az ügyfél-integrációs folyamat egyszerűsítésében, csökkentve az ügyfél hitelesítéséhez szükséges időt és erőfeszítést. A biometrikus hitelesítési folyamat gyors és egyszerű, kiküszöbölve a manuális személyazonosság-ellenőrzés szükségességét, miközben akár 90%-kal is javítja az első áthaladási arányokat.[454]

A felhasználók akár 10 másodperc alatt ellenőrizhetők. Ez segít csökkenteni az adminisztratív költségeket és javítani az ügyvédi irodák hatékonyságát. A biometrikus ellenőrzések integrálódnak az Access Legal gyakorlatkezelő szoftverével, lehetővé téve az ellenőrzések megrendelését és közvetlen visszajuttatását a megfelelő ügyhöz anélkül, hogy el kellene hagyni a gyakorlatkezelő rendszert.[455] Az Access Legal biometrikus személyazonosság-ellenőrző rendszere példázza ezt a fejlődést, amely az Onfido partnerrel közösen fejlesztett mesterséges intelligencia algoritmusokat használ a felhasználók által benyújtott személyazonosító okmányok elemzésére és ellenőrzésére.

[453] Pulse, „Top Mobile App Security Trends to Watch in 2025"".
[454] „Efficiency Gains from Biometric Authentication in Legal Services"", *International Journal of Legal Technology* 8, sz. 2 (2023).
[455] Access Legal, *Biometric Identity Verification for Law Firms"* (Technical Documentation, 2023).

Ezek a kifinomult algoritmusok képesek felismerni a csalás különböző formáit, beleértve a hamis dokumentumokat, a manipulált képeket vagy a hamis személyazonosságokat, oly módon, hogy összehasonlítják a dokumentum jellemzőit kiterjedt adatbázisokkal, és gépi tanulási képességeket használnak a csalárd vagy gyanús dokumentumok azonosítására.[456] A biometrikus hitelesítés bevezetése számos előnyt kínál az ügyvédi irodák számára. Biztosítja a pontos dokumentumellenőrzést és a Know Your Customer (KYC) követelményeknek való megfelelést, lehetővé téve a gyors csalásfelderítést, prevenciót.[457]

A biometrikus hitelesítés jogi gyakorlatban történő megvalósítása általában strukturált folyamatot követ:

1. Biometrikus megrendelés elhelyezése a gyakorlatkezelő rendszerből, a Legal Bricks API-n keresztül, vagy a Legal Bricks szoftverből.
2. Hivatkozás fogadása telefonon, táblagépen vagy számítógépen.
3. Valós idejű "életjel-ellenőrzés" (liveness check) elvégzése az ügyfélen.
4. Képfelismerés használata ennek összehasonlítására a vezetői engedéllyel vagy útlevéllel.
5. Eredmények kézhezvétele 60 másodpercen belül.[458]

Ez a folyamat nemcsak biztonságosabb, hanem gyorsabb is, mint a hagyományos papíralapú azonosítási módszerek. Bár a hagyományos rendszerek alacsonyabb biztonságot nyújtanak a biometrikus rendszerekhez képest, költséghatékonyabbak és könnyebben implementálhatók és karbantarthatók. Ez arra utal, hogy a biometrikus rendszerek fokozott biztonságot kínálhatnak, de magasabb költségekkel és számítási komplexitással járnak.[459] A magyar jogi szektorban az ügyvédek 87%-a használtaz az elektronikus személyi igazolványok (eSzemélyi) által biztosított minősített elektronikus aláírásokat (QES) a szerződések hitelesítésére. A 418/2024. sz. kormányrendelet előírja az aláírások ellenőrizhetőségét, amelyet a Budapesti Ügyvédi Kamara tagjainak a "Kamarám" alkalmazás biztosít.[460]

---

[456] Legal.
[457] Legal.
[458] Bricks Legal, *Biometric Identity Verification Process"* (Technical Documentation, 2023).
[459] Kunda és Chishimba, „Authentication Scheme Applications on Smartphones: A Comparative Analysis"", *Journal of Information Security*, 2022.
[460] „Korm. rendelet, »Az elektronikus aláírások auditálhatóságáról«", 418Kr. u. 2024.

Az elektronikus azonosítási és bizalmi szolgáltatásokról szóló rendelet (eIDAS) biztosítja az elektronikus aláírások és a személyazonosság-ellenőrzés jogi keretét az Európai Unióban, meghatározva az egyszerű, fokozott és minősített elektronikus aláírások szabványait. A minősített elektronikus aláírások (QES) a legmagasabb szintű biztonságot nyújtják, és jogilag egyenértékűek a kézzel írt aláírásokkal, ami különösen értékessé teszi őket a jogi ügyleteket kezelő ügyvédi irodák számára.[461] A Miskolci Egyetem Állam- és Jogtudományi Karának kutatása kimutatta, hogy a biometrikus azonosítással integrált digitális dokumentumkezelő rendszerek bevezetése akár 60%-kal csökkentheti a dokumentum feldolgozási időt a jogi gyakorlatban, miközben fokozza a biztonságot és a megfelelőséget. A tanulmány azt is megállapította, hogy az ezeket a technológiákat bevezető cégek 35%-os csökkenést tapasztaltak a dokumentumkezeléssel kapcsolatos adminisztratív költségekben.[462]

A Ludovika Egyetem Kiberbiztonsági Kutatóintézetének 2021-es tanulmánya megállapította, hogy a magyar ügyvédi irodák mindössze 43%-a vezetett be átfogó mobil biztonsági irányelveket, amelyek magukban foglalták a titkosítást és a többfaktoros hitelesítést, ami fejlődési lehetőséget jelez a szektor mobil biztonsági gyakorlataiban.[463] A nemzetközi ügyfelekkel vagy műveletekkel rendelkező ügyvédi irodák számára az elektronikus azonosítási és hitelesítési módszerek határokon átnyúló elismerése kulcsfontosságú szempont. Az eIDAS rendelet jogi keretet biztosít az elektronikus azonosítási eszközök kölcsönös elismeréséhez az EU-tagállamok között, megkönnyítve a határokon átnyúló jogi tranzakciókat.[464] Az EU-n kívül a különböző joghatóságok eltérő követelményeket és normákat támasztanak az elektronikus azonosítással és hitelesítéssel kapcsolatban, jogi kontextusban. Az Egyesült Államok például az ESIGN törvényt és az UETA-t (Egységes Elektronikus Tranzakciós Törvény) követi, amelyek jogi elismerést biztosítanak az elektronikus aláírásoknak, de az eIDAS-tól

[461] Union, *eIDAS Regulation: Trust Services and Electronic Identification*.
[462] Jogtudományi Kar Miskolci Egyetem Állam-, „Digitális átalakulás a jogi gyakorlatban"", *Kutatási jelentés*, 2023, https://www.mjsz.uni-miskolc.hu/files/10854/4_nagyzoltan_t.
[463] Egyetem Ludovika, „A magyar ügyvédi irodák kiberbiztonsági gyakorlatai"", *Kutatási jelentés*, 2021, https://folyoirat.ludovika.hu/index.php/magyrend/article/download/6023/5107/25425.
[464] Bizottság Európai, „eIDAS rendelet: Az elektronikus azonosítás határokon átnyúló elismerése"", *Technikai útmutató*, 2020, https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=LEGISSUM%3Adigital_identity.

eltérő technikai követelményekkel.[465] A nemzetközi standardizációs erőfeszítések, például az International Organization for Standardization (ISO) és a FIDO (Fast Identity Online) Szövetség által vezetett kezdeményezések, közös keretrendszerek kialakítására törekszenek a biztonságos hitelesítés és személyazonosság-ellenőrzés terén. A FIDO2 standard például jelszómentes hitelesítési mechanizmust biztosít, amely különböző platformokon és joghatóságokban is megvalósítható, potenciális megoldást kínálva a nemzetközileg működő ügyvédi irodák számára.[466]

4.1.3 Turizmus és idegenforgalmi szektor

Miközben a globális turizmus továbbra is regenerálódik és átalakul a közelmúlt kihívásai után, az okos eszközök és alkalmazásaik hatékony eszközökké váltak a biztonság fokozására, a folyamatok egyszerűsítésére. A biometrikus hitelesítés, a mobil ellenőrzési rendszerek és a digitális személyazonosság-megoldások integrációja forradalmasítja, ahogyan a turisták kapcsolatba lépnek a szolgáltatásokkal. Az okos turizmus (smart tourism) az információs és kommunikációs technológiák integrációját jelenti az utazási élmény különböző aspektusainak optimalizálása érdekében.[467]

A biometrikus hitelesítés az okos turizmus kontextusában nemcsak a pénzügyi tranzakciókat erősíti meg, hanem kulcsszerepet játszik a korlátozott területekhez való hozzáférés ellenőrzésében, a szállodai bejelentkezések megkönnyítésében, sőt, akár az egyéni preferenciákon alapuló személyre szabott szolgáltatások lehetővé tételében.[468] A biometrikus biztonsági rendszerek turizmusban történő implementálása követi a pénzügyi technológia szélesebb trendjeit. A biometrikus ellenőrzést magukban foglaló mobil fizetési szolgáltatások gyorsabban dolgozhatják fel a tranzakciókat, miközben magasabb biztonsági standardokat tartanak fenn. Ez értékes a turisztikai kontextusokban, ahol a sorban állás kezelése és a hatékony szolgáltatásnyújtás közvetlenül befo-

[465] American Bar Association, „Electronic Signatures in Global and National Commerce Act"", *Legal Guide*, 2021.
[466] Alliance, *FIDO2: Web Authentication*.
[467] D. Buhalis és A. Amaranggana, „Smart Tourism Destinations: Enhancing Tourism Experience Through Personalisation of Services"", *Information and Communication Technologies in Tourism*, 2015.
[468] I.P. Tussyadiah és J. Pesonen, „Impacts of Peer-to-Peer Accommodation Use on Travel Patterns"", *Journal of Travel Research* 55, sz. 8 (2016).

lyásolja az ügyfelek elégedettségét. Továbbá, az érintésmentes biometrikus megoldások további fontosságot nyertek a COVID-19 világjárvány után, lehetővé téve a higiénikus hitelesítést fizikai érintkezés nélkül.[469]

A biometrikus azonosítás különösen hasznos nemzetközi utazás során, ahol a nyelvi akadályok és kulturális különbségek kihívásokat jelenthetnek. Az arcfelismerés vagy ujjlenyomat-alapú hitelesítés univerzális azonosítási módszert biztosít, amely nem igényel nyelvi készségeket vagy kulturális ismereteket, így különösen értékes a sokszínű turisztikai környezetekben, ahol a világ minden tájáról érkező látogatók találkoznak.[470]

Nem csak az ügyvédi irodák, hanem a szállásadók által is előszeretettel alkalmazott applikáció GoodID, ami egy digitális identitáskezelő rendszer, amelyet az ID&Trust Kft. fejlesztett ki, ugyanaz a vállalat, amely részt vett az e-személyi igazolványok és nemzetközi biometrikus dokumentumok (pl. japán útlevél) technológiájának kialakításában.[471] Az alkalmazás célja a személyazonosítás és hitelesítés egyszerűsítése nyilvános szolgáltatásokban (pl. szálláshelyek, bankok) és a felhasználói adatok biztonságos tárolása. A zero-knowledge architektúrával működik, ami azt jelenti, hogy a felhasználók adatait titkosított formában tárolja, és csak a felhasználó engedélyezése után továbbítja a szolgáltatóknak. A GoodID Scanner modulja lehetővé teszi okos telefonokkal történő okmányok (személyi igazolvány, útlevél) szkennelését optikai karakterfelismerés (OCR) és chipalapú adatkinyerés segítségével. A beolvasott adatok automatikusan feltöltődnek a szálláshelyek által használt Property Management System (PMS) felületére, majd a VIZA rendszerbe kerülnek továbbításra. A hibásan beolvasott adatok esetén kézi korrigálásra is lehetőség van, ami után a rendszer újraküldi az információkat.[472]

A rendszer kombinálja a birtoklásalapú (mobilkészülék) és biometrikus (arcfelismerés) hitelesítési faktorokat. A felhasználók önkiszolgáló módon azonosíthatják magu-

[469] Global, „What's on the Horizon: 10 Biometric Trends for 2025"".
[470] B. Neuhofer, D. Buhalis, és A. Ladkin, „Smart Technologies for Personalized Experiences: A Case Study in the Hospitality Domain"", *Electronic Markets* 25, sz. 3 (2015).
[471] „GoodID digitális irattárca - GoodID", elérés 2025. május 3., https://goodid.net/hu/digitalis-irattarca/.
[472] „Digitális személyazonosítás: mi a kulcs? - GoodID white paper".

kat távolról, például szálláshelyi vendégregisztráció során, anélkül, hogy fizikailag jelen lennének. A GoodID SecureBox technológiája lehetővé teszi dokumentumok elektronikus aláírását és adatok titkosított megosztását harmadik felekkel. A titkosítási kulcsokat a szolgáltatók birtokolják, így a GoodID szerverei sem hozzáférnek a nyers adatokhoz.[473] Bár a GoodID Common Criteria EAL4+ minősítéssel és ISO 27001 tanúsítvánnyal rendelkezik, a mobileszközök elvesztése vagy ellopása esetén fennáll a kockázata, hogy harmadik fél hozzáfér a titkosított adatokhoz. A biometrikus adatok tárolása speciális kriptográfiai módszerekkel történik, de a kvantumszámítógépek fejlődése hosszú távon veszélyeztetheti ezeket a mechanizmusokat. A VIZA rendszerrel való integráció miatt a GoodID működése kritikus függőségi kapcsolatban áll a központi rendszer elérhetőségével. 2023-as adatok szerint a VIZA rendszer havonta átlagosan 2-3 órás kiesést mutatott, ami késedelmeket okozott a szálláshelyeknél. Továbbá a vendégek által szkennelt okmányok minősége befolyásolja az adatpontosságot. A rosszul megvilágított vagy sérült dokumentumok esetén az OCR hibázhat, ami kézi korrekciót igényel és megnöveli az adminisztratív terhelést.[474]

4.1.4 Közösségi média és egyéb online platformok

A közösségi média platformok exponenciális növekedése mélyreható átalakulást hozott a digitális környezetben. Az okos eszközök elterjedése tovább gyorsította ezt a tendenciát, a mobilalkalmazások váltak a közösségi média interakciók elsődleges felületévé. A megbízható személyazonosság-ellenőrzés fontossága a közösségi médiában nem hangsúlyozható túl. A személyazonossághoz kapcsolódó csalások 28%-kal növekedtek az előző évhez képest a közösségi platformokon, ami az ezen a területen működő rossz szándékú szereplők növekvő kifinomultságát mutatja.[475] Ahogy a felhasználók egyre érzékenyebb személyes információkat osztanak meg ezeken a platformokon, és ahogy a közösségi média kritikus infrastruktúrává válik a politikai diskurzus, kereskedelmi tranzakciók és személyes kapcsolatok számára, így a hitelesítési mechanizmusok iránti igény kritikussá vált.

[473] „Digitális személyazonosítás: mi a kulcs? - GoodID white paper".
[474] „Digitális személyazonosítás: mi a kulcs? - GoodID white paper".
[475] „Social Media Fraud Soars 28% Amid Rising AI Tactics", Financial and Business News | Finance Magnates, 2024. október 30., https://www.financemagnates.com/forex/social-media-fraud-soars-28-amid-rising-ai-tactics/.

A legtöbb platform valamilyen formában biztosít ellenőrzést felhasználói számára – legyenek azok magánszemélyek, tartalomkészítők vagy vállalkozások. Bár az alapvető módszerek, mint a jelszavas hitelesítés továbbra is elterjedtek, a platformok folyamatosan fejlettebb ellenőrzési technikákat vezetnek be.[476]

A WhatsApp, amely világszerte több mint 2,95 milliárd aktív felhasználóval rendelkezik, olyan funkciókkal, mint a csoportos csevegések és csatornák, társadalmi platformnak tekinthető. A telefonszámok szolgálnak elsődleges azonosítóként mind az új, mind a meglévő felhasználók számára, így ez kulcsfontosságú eleme a felhasználói regisztrációs vagy újraellenőrzési folyamatoknak. A WhatsApp két ellenőrzési lehetőséget kínál: standard ellenőrzést és opcionális kétlépcsős ellenőrzést. A standard folyamatban az új felhasználónak meg kell adnia egy SMS-ben vagy telefonhívással küldött 6 jegyű regisztrációs kódot telefonszáma megerősítéséhez. Emellett a WhatsApp automatikusan is ellenőrizheti a telefonszámot SMS vagy nem fogadott hívások nélkül, együttműködve a távközlési szolgáltatókkal annak ellenőrzésére, hogy az eszközinformációk megegyeznek-e a regisztrált telefonszámmal. A regisztráció után a felhasználók tovább erősíthetik fiókbiztonságukat egy egyedi PIN létrehozásával és megerősítésével, amely a hitelesítéshez szükséges, így a puszta telefonszám-ellenőrzésen túl további biztonsági réteget adva.[477]

A Meta (korábban Facebook) átfogó ellenőrzési rendszereket vezetett be az üzleti felhasználók és tartalomkészítők számára. Havi 14,99 dollártól kezdődő előfizetésért a Meta olyan csomagokat kínál, amelyek tartalmazzák az ellenőrzött jelvényt és a személyiséglopás elleni védelmet proaktív megfigyelés révén. Ez a funkció 18 éven felüli felhasználókra korlátozódik, és csak bizonyos országokban érhető el.[478] Az identitás ellenőrzéséhez a közösségi platform kormányzati kibocsátású személyazonosító (fizikai) okmányokra támaszkodik, míg bizonyos régiókban videós szelfi ellenőrzés is elérhető további lépésként. A videókból készült pillanatképeket emberi ellenőrzésre küldhetik el, hogy összehasonlítsák azokat a benyújtott személyazonosító okmányokkal, ezzel biztosítva magasabb szintű ellenőrzési pontosságot. 2024 óta a Meta kötele-

[476] MediaKutato, „Digitális identitás vállalatvezetők döntéshozók", *MediaKutato Journal*, 2015.
[477] Cardinal, „VICA használata üzenetküldésre", *Technical Documentation*, 2022, https://www.cardinal.hu/vica-hasznalata-uzenetkuldesre/.
[478] Meta Platforms, „Identity Verification Systems Documentation", *Meta for Developers*, 2024.

zővé tette a kormányzati kibocsátású személyazonosítók) használatát politikai hirdetésekhez. Ez a rendszer állítólag 34%-kal csökkentette a hamis profilok számát a 2023-as választási ciklusban, bizonyítva a szigorúbb személyazonosság-ellenőrzési követelmények hatékonyságát érzékeny kontextusokban.[479]

A Twitter (most X) szintén bevezetett egy ellenőrzési rendszert, amely kormányzati kibocsátású személyazonosításra támaszkodik az ellenőrzési jelvényt kérő fiókok esetében. Ez a megközelítés segít megkülönböztetni a közszereplők, szervezetek és újságírók hiteles fiókjait a potenciális személyiségbitorlóktól, bár a platform kritikát kapott az ellenőrzési politikáinak következetlen alkalmazása miatt.[480]

Biometrikus hitelesítés a közösségi média alkalmazásokban

Az arcfelismerés a legszélesebb körben alkalmazott biometrikus hitelesítési módszer a közösségi média alkalmazásokban. Ez a technológia MI-támogatott képfeldolgozást alkalmaz a felhasználók azonosítására az arcvonások, mélység és infravörös minták elemzésével.[481] A megvalósítás platformonként változik, de általában magába foglalja a felhasználó arcadatainak rögzítését az eszköz előlapi kamerájával, majd összehasonlítását a korábban tárolt biometrikus sablonokkal. A Meta platformjai (Facebook és Instagram) integrálták az arcalapú hitelesítést a fiók-helyreállítási folyamataikba. Amikor egy felhasználó megpróbálja visszanyerni a hozzáférést egy zárolt fiókhoz, a rendszer kérheti egy videós szelfi folyamat elvégzését, amely elemzi az arcvonásokat a személyazonosság ellenőrzéséhez. Ez a rendszer kifinomult algoritmusokat használ, amelyek képesek észlelni az "élőséget", megelőzve a fényképekkel vagy előre rögzített videókkal történő csalási kísérleteket.[482]

Deepfake felismerés és csalás elleni intézkedések

A közösségi média platformok ma már kénytelenek ugyanolyan fejlett technológiákat kifejleszteni a manipulált tartalmak felismerésére. A TikTok Liveness Detection algo-

[479] Bizottság Nemzeti Választási, „Digitális identitás a választási folyamatokban: 2023-as elemzés", *Kormányzati jelentés*, 2024.
[480] X. Corp, „Account Verification Process Documentation", *Platform Policies*, 2023.
[481] Nordstone, „Integrating Biometricsecurity Features into Mobile Apps", *Technical Blog*, 2023, https://nordstone.co.uk/blog/integrating-biometricsecurity-features-into-mobile-apps.
[482] Meta Platforms, „Security and Account Authentication White Paper", *Meta Security Documentation*, 2024.

ritmusa az egyik legkifinomultabb megközelítést képviseli, amely 3D-s arcmodellezést és mikroexpressziók elemzését használja a mesterségesen generált tartalmak azonosítására.[483] Ezek a felismerő rendszerek az arcmozgások, pislogás és egyéb fiziológiai jelek finom mintázatait elemzik, amelyeket nehéz meggyőzően szimulálni a manipulált médiában. A kutatók által jelentett 92%-os pontossági arány demonstrálja mind a jelenlegi felismerési módszerek hatékonyságát, mind az egyre kifinomultabb deepfake-ek következetes azonosításának fennmaradó kihívásait.[484]

A Facebook hasonló technológiákat fejlesztett ki DeepFace rendszerén keresztül, amely képes azonosítani a deepfake-eket az arcvonások, megvilágítás és mozgásmintázatok következetlenségeinek elemzésével. Ezeket a rendszereket folyamatosan bővülő adatkészleteken képezik, hogy lépést tartsanak a szintetikus médiagenerálás fejlődésével.[485] A statikus biometrikus jelzéseken túl a közösségi média platformok egyre inkább alkalmazzák a viselkedési biometriát – elemezve, hogyan lépnek kapcsolatba a felhasználók eszközeikkel – a valódi és csalárd fiókhasználat megkülönböztetésére. Ezek a rendszerek figyelik a billentyűzet-dinamikát, érintési gesztusokat, görgetési mintázatokat és egyéb interakciós viselkedéseket, hogy egyedi "viselkedési ujjlenyomatot" hozzanak létre minden felhasználó számára.[486] Amikor szokatlan viselkedési mintákat észlelnek, a platformok további hitelesítési lépéseket indíthatnak, vagy ideiglenesen korlátozhatják a fiókhoz való hozzáférést, amíg a jogos tulajdonos igazolni tudja személyazonosságát. Ez a megközelítés előnyöket kínál a hagyományos hitelesítési módszerekkel szemben, mivel a viselkedési mintázatokat rendkívül nehéz pontosan reprodukálni, még akkor is, ha más hitelesítési adatok kompromittálódtak.[487]

4.2 Állami szférában alkalmazott technológiák

Több ország is fejlett elektronikus azonosítási rendszereket fejlesztett ki. Észtország e-ID rendszere lehetővé teszi az állampolgárok számára, hogy gyakorlatilag minden közszolgáltatáshoz elektronikusan férjenek hozzá, beleértve az elektronikus szavazást

[483] Fehér, „Deepfake Detection in Social Media Contexts", *Hungarian Journal of Media Studies*, 2024.
[484] Fehér.
[485] Meta Research, *DeepFace: Closing the Gap to Human-Level Performance in Face Verification* (Scientific Publication, 2023).
[486] LinkedIn, *Top Mobile App Security Trends to Watch for 2025: Protecting User Data* (LinkedIn Pulse, 2024).
[487] LinkedIn.

is.[488] Az észt X-Road platform decentralizált adatcsere-platformként szolgál, összekapcsolva a kormányzati adatbázisokat, zökkenőmentes e-kormányzati szolgáltatásokat biztosítva, amelyek révén az észtek a szolgáltatások 99%-át online érhetik el.[489] Szingapúr SingPass rendszere biometrikus hitelesítést alkalmaz, míg Németország elektronikus személyazonosító igazolványa erős kriptográfiai védelemmel rendelkezik. A mobilalkalmazások biometrikus útlevelekkel való integrációja egyre erősödő tendencia, több ország is olyan megoldásokat fejleszt, amelyek lehetővé teszik az utazók számára, hogy útlevelük digitális verzióját okos telefonjaikon tárolják. Ezek a mobil útlevél alkalmazások jellemzően biometrikus ellenőrzés (arcfelismerés) és titkosított adattárolás kombinációját használják a biztonság garantálására.[490]

Az elektronikus szavazási rendszerek egyre inkább felváltják vagy kiegészítik a hagyományos papíralapú szavazást, és speciális azonosítási és hitelesítési módszereket igényelnek a biztonság garantálása és a szavazás titkosságának megőrzése érdekében. Az elektronikus szavazási rendszerek különböző formákban valósíthatók meg, beleértve a szavazóhelyiségben történő elektronikus szavazást, az internetes szavazást és a hagyományos és elektronikus szavazási módszereket kombináló hibrid rendszereket. Észtország 2005 óta alkalmaz internetes szavazást, ahol az észt állampolgárok elektronikus azonosítójukat és digitális aláírásukat használják a szavazatok leadására. A 2019-es parlamenti választásokon a szavazatok 43,8%-át elektronikusan adták le.[491] A közelmúltban, a 2023-as parlamenti választásokon ez az arány már a szavazatok 50% körülire növekedett.[492]

4.2.1 E-közigazgatás, m-közigazgatás

Ahogy a digitális kormányzati kezdeményezések folyamatosan fejlődnek, a hagyományos e-közigazgatási szolgáltatások és a mobilalapú m-közigazgatási megoldások közötti különbség egyre ebbé válik, mivel mindkét megközelítés egyedi előnyöket és kihívásokat kínál mind a szolgáltatók, mind az állampolgárok számára. Az okoseszközalkalmazások integrálása a kormányzati szolgáltatásnyújtásba alapvetően átalakította,

[488] „Estonian E-Identity Model as a Best Practice"", *Journal of Digital Government* 4, sz. 2 (2021), https://folyoirat.ludovika.hu/index.php/aarms/article/download/6632/5446/29091.
[489] „Az észt X-Road platform", *Digital Government Study*, 2023.
[490] „Biometrikus azonosítás hatékonyságának elemzése", *Akadémiai Kiadó Journal*, 2024.
[491] „Statistics about Internet voting in Estonia | Elections in Estonia", elérés 2025. május 3., https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia.
[492] Smartmatic. (2023). Estonia. PDF. https://www.smartmatic.com/wp-content/uploads/2023/09/CS_Estonia_v0923.pdf

ahogyan az állampolgárok hozzáférnek a közszolgáltatásokhoz, igazolják személyazonosságukat és kapcsolatba lépnek a kormányzati intézményekkel. Az elektronikus személyazonosító kártyáktól és biometrikus ellenőrzési rendszerektől kezdve a kormányzati szolgáltatásokhoz való hozzáférést biztosító mobilalkalmazásokig, ezek a technológiák mélyrehatóan alakítják át az állampolgárok és kormányok közötti kapcsolatot.

- **Az e-közigazgatás meghatározása**

Az e-közigazgatás (elektronikus közigazgatás) az információs és kommunikációs technológiák (IKT) használatát jelenti a kormányzati szolgáltatások nyújtására, információcsere lebonyolítására, tranzakciók végrehajtására, valamint különálló rendszerek és szolgáltatások integrálására a kormány-állampolgár (G2C), kormány-üzleti szféra (G2B), kormány-kormány (G2G) és kormány-alkalmazott (G2E) kapcsolatokban.[493] Az OECD meghatározása szerint az e-közigazgatás "az információs és kommunikációs technológiák, különösen az internet használata a jobb kormányzás eszközeként".[494]

Az e-közigazgatás a digitális szolgáltatások és interakciók széles körét öleli fel, az információs weboldalakon és online adóbevallási rendszereken át az átfogó digitális identitás-keretrendszerekig és elektronikus szavazási platformokig. Az e-közigazgatás alapvető célja a kormányzati szolgáltatások hatékonyságának, hozzáférhetőségének és eredményességének javítása a digitális technológiák révén. Ez paradigmaváltást jelent a kormányzati szolgáltatásnyújtás hagyományos bürokratikus modelljeitől az állampolgár-központúbb, átláthatóbb és rugalmasabb megközelítések felé. Az e-közigazgatás fejlődését több szakasz jellemezte, a kormányzati információk alapvető digitalizálásától és egyszerű online szolgáltatásoktól kezdve a kifinomultabb, integrált és transzformatív digitális kormányzati ökoszisztémák felé haladva. Az ENSZ E-kormányzati Fejlettségi Indexe (EGDI) szerint a világ országai egyre inkább haladnak ezeken a

[493] „Csáki Gyula Balázs: Kérdésfelvetések az e-közigazgatás fogalmának meghatározása körében (IJ, 2008/7. (29.), 277-280. o.) | Szakcikk Adatbázis", elérés 2025. május 3., https://szakcikkadatbazis.hu/doc/1456098.
[494] „e-Government for Better Government | OECD", elérés 2025. május 3., https://www.oecd.org/en/publications/e-government-for-better-government_9789264018341-en.html.

szakaszokon keresztül, a vezető nemzetek pedig magas szintű e-kormányzati rendszereket vezetnek be, amelyek lehetővé teszik a zökkenőmentes, biztonságos és személyre szabott szolgáltatásnyújtást.[495]

- **Az m-közigazgatás meghatározása**

Az m-közigazgatás (mobil közigazgatás) az e-közigazgatás részhalmazát és fejlődését képviseli, amely kifejezetten a kormányzati szolgáltatások és információk mobileszközökön és technológiákon keresztüli nyújtására összpontosít. Kushchu és Kuscu meghatározása szerint az m-közigazgatás "az a stratégia és annak megvalósítása, amely magában foglalja mindenféle vezeték nélküli és mobil technológia, szolgáltatás, alkalmazás és eszköz felhasználását az e-közigazgatásban részt vevő felek – beleértve az állampolgárokat, vállalkozásokat és valamennyi kormányzati egységet – előnyeinek növelése érdekében".[496] Az m-közigazgatás felemelkedését a mobileszközök globális elterjedése, a mobiltechnológiák gyors fejlődése, valamint az állampolgárok növekvő elvárásai hajtották a kényelmes, hozzáférhető és reagáló képes kormányzati szolgáltatások iránt. Az m-közigazgatás olyan mobiltechnológiákat használ, mint az okos telefonok, táblagépek, viselhető eszközök, valamint a vezeték nélküli hálózatok, mobilalkalmazások és mobil-optimalizált szolgáltatások támogató infrastruktúráját, hogy közvetlenül az állampolgárok kezébe juttassa a kormányzati szolgáltatásokat. Ez a megközelítés felismeri a mobil interakciók iránti növekvő preferenciát és a mobiltechnológiák potenciálját a digitális kormányzat elfogadásának akadályainak leküzdésére, különösen azokon a területeken, ahol korlátozott a hagyományos internet-infrastruktúra.

4.2.2 Személyazonosítási és hitelesítési technológiák a digitális kormányzatban

A személyazonosítás és hitelesítés alapját képezi a biztonságos és megbízható digitális kormányzati szolgáltatásoknak. Ahogy a kormányzati szolgáltatások egyre inkább online és mobil platformokra költöznek, a felhasználók személyazonosságának megállapítása és ellenőrzése elengedhetetlenné válik a szolgáltatás integritásának biztosításához, az érzékeny információk védelméhez és a csalás megelőzéséhez. A digitális identitás kormányzati kontextusokban több kritikus funkciót szolgál. Egyrészt ellenőrizni

[495] Nations, *E-Government Survey*.
[496] I. Kushchu és H. Kuscu, „From E-Government to M-Government: Facing the Inevitable", in *Mobile Government: An Emerging Direction in E-Government. IGI Global*, 2003.

kell a hozzáférését, azaz ki férhet hozzá specifikus kormányzati szolgáltatásokhoz és információkhoz, biztosítva, hogy csak felhatalmazott személyek tekinthessenek meg érzékeny adatokat vagy végezhessenek el bizonyos tranzakciókat.[497] Természetesen fontos szerepe van a csalás megelőzési funkciónak, mivel identitás-ellenőrzés segít megelőzni a csalás különböző formáit, beleértve a személyazonosság-lopást, juttatási csalásokat és a kormányzati szolgáltatásokhoz való jogosulatlan hozzáférést.

Az ellenőrzött digitális identitások lehetővé teszik a kormányok számára, hogy személyre szabják a szolgáltatásokat az egyéni körülmények, jogosultságok és preferenciák alapján, javítva a felhasználói élményt és a szolgáltatás relevanciáját.[498] Továbbá csökkentik az ismételt személyazonosság-ellenőrzés szükségességét a különböző kormányzati szolgáltatások között, egyszerűsítve a folyamatokat és csökkentve az adminisztratív terheket mind az állampolgárok, mind a kormányzati ügynökségek számára.[499] A digitális identitásrendszerek kormányzati kontextusban történő implementálása gondos megfontolást igényel a biztonsági követelmények, adatvédelmi vonatkozások, hozzáférhetőségi aggályok és szabályozási keretrendszerek tekintetében. Ahogy a digitális kormányzati szolgáltatások fejlődnek, úgy hitelesítési technológiák is, hogy megfeleljenek ezeknek az összetett követelményeknek. A digitális kormányzatban a hitelesítés tipikusan egy vagy több következő tényezőt alkalmaz az identitás ellenőrzésére:

1. **Tudásfaktorok (**Ide tartoznak a jelszavak, PIN-kódok, biztonsági kérdések és egyéb információk, amelyeket csak a jogos felhasználónak kellene ismernie. Bár a tudásfaktorok széles körben használtak, egyre inkább felismerik, hogy önmagukban elégtelenek, a phishing, social engineering és brute force támadásokkal szembeni sebezhetőségek miatt.[500]

[497] „European Digital Identity (EUDI) Regulation | Shaping Europe's digital future", elérés 2025. május 3., https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation.
[498] „How a digital platform opens the door for value-added personalized public services", elérés 2025. május 3., https://nortal.com/insights/how-a-digital-platform-opens-the-door-for-value-added-personalized-public-services.
[499] European Commission. (2015). Study on eGovernment and the Reduction of Administrative Burden. https://ec.europa.eu/futurium/en/system/files/ged/finalreportstudyonegovernmentandthereductionofadministrativeburden.pdf
[500] Madhavi Gudavalli, D. Srinivasa Kumar, és S. Viswanadha Raju, „Securing E-Governance Services through Biometrics", *International Journal of Security and Its Applications* 8, sz. 1 (2014. január 31.): 103–12, https://doi.org/10.14257/ijsia.2014.8.1.10.

2. **Birtoklási faktorok,** Ezek fizikai eszközöket vagy tokeneket foglalnak magukban, amelyeket a felhasználó birtokol, például intelligens kártyákat, mobileszközöket, hardveres biztonsági kulcsokat vagy egyszer használatos jelszógenerátorokat (OTP). A birtoklási faktorok javíthatják a biztonságot, ha más hitelesítési módszerekkel kombinálják őket.[501]
3. **Tulajdonsági faktorok** A biometrikus hitelesítési módszerek ebbe a kategóriába tartoznak, beleértve az ujjlenyomat-felismerést, arcfelismerést, írisz-szkennelést, hangfelismerést és viselkedési biometriát. Ezek a módszerek egyedi fizikai vagy viselkedési jellemzőket használnak az identitás ellenőrzésére.[502]
4. **Helyfaktorok**: A helyalapú hitelesítés a felhasználó fizikai helyét használja, amit tipikusan GPS, IP-cím vagy mobilhálózati információkon keresztül határoznak meg, további ellenőrzési faktorként. Ez segíthet azonosítani a gyanús bejelentkezési kísérleteket nem várt helyekről.[503]
5. **Viselkedési faktorok**: Ezek az újonnan megjelenő hitelesítési módszerek a felhasználói viselkedésben megfigyelhető mintákat elemzik, például gépelési ritmusokat, gesztus mintákat vagy alkalmazáshasználati viselkedéseket, az identitás folyamatos ellenőrzésére. A viselkedési hitelesítés folyamatos ellenőrzést biztosíthat a felhasználói élmény megszakítása nélkül.

A többfaktoros hitelesítés (MFA) két vagy több ilyen faktort kombinál biztonságosabb hitelesítési folyamatok létrehozásához. A konkrétan használt faktorok kombinációja az elért információ vagy szolgáltatás érzékenységétől függ, a kritikusabb szolgáltatások tipikusan szigorúbb hitelesítést igényelnek.

4.2.3 Biometrikus hitelesítés a kormányzati alkalmazásokban

A biometrikus hitelesítés népszerűségre tett szert a kormányzati alkalmazásokban egyedi előnyei miatt a biztonság, kényelem és csalásmegelőzés területén. A biometrikus hitelesítés kormányzati implementációi közé tartoznak:

[501] E-SPIN, „The Significance of Digital Identification in E-Government Systems", *E-SPIN Group* (blog), 2023. december 8., https://www.e-spincorp.com/the-significance-of-digital-identification-in-e-government-systems/.
[502] „Using Mobile Apps in Government | IBM Center for The Business of Government", elérés 2025. május 3., https://www.businessofgovernment.org/report/using-mobile-apps-government.
[503] „Authentication Factors - Entro", elérés 2025. május 3., https://entro.security/glossary/authentication-factors/.

1. **Ujjlenyomat-felismerés**: Széles körben használják kormányzati alkalmazásokban érettsége, megbízhatósága és felhasználói elfogadottsága miatt. Az ujjlenyomat-felismerést nemzeti ID-rendszerekben, határellenőrzésben, bűnüldözésben és kormányzati szolgáltatásokhoz való biztonságos hozzáférésben alkalmazzák.[504]
2. **Arcfelismerés**: Egyre inkább alkalmazzák kormányzati kontextusokban nem invazív identitás-ellenőrzéshez. Az alkalmazások közé tartozik az automatizált határellenőrzés, megfigyelési rendszerek és mobil hitelesítés kormányzati szolgáltatásokhoz. Az arcfelismerési technológia fejlődött a mesterséges intelligencia előrehaladásával, javítva a pontosságot és a spoofing kísérletekkel szembeni ellenállást.[505]
3. **Írisz-felismerés**: Megbízhatósága és nem invazív jellege miatt magas biztonsági kormányzati alkalmazásokban használják, mint például nemzeti ID-programok és bevándorlás-ellenőrzés. Például India UIDAI rendszere több mint egymilliárd állampolgárt vett nyilvántartásba írisz-szkennelés használatával a szociális juttatásokhoz és támogatásokhoz való hozzáféréshez, demonstrálva hatékonyságát és skálázhatóságát.[506]
4. **Hangfelismerés**: Kormányzati call centerekben és hangvezérelt kormányzati szolgáltatásokban alkalmazzák, a hangbiometria természetes hitelesítési módszert kínál a telefonos és hangalapú interakciókhoz a kormányzati szolgáltatásokkal.[507]
5. **Viselkedési biometria**: Feltörekvő alkalmazások elemzik a felhasználói viselkedési mintákat, mint például a gépelési dinamikát, gesztus mintákat vagy járásfelismerést, hogy folyamatos, passzív hitelesítést biztosítsanak, ami kiegészíti más biometrikus módszereket.[508]

---

[504] „Behind Fingerprint Biometrics: How It Works and Why It Matters - 1Kosmos", elérés 2025. május 3., https://www.1kosmos.com/biometric-authentication/behind-fingerprint-biometrics-how-it-works-and-why-it-matters/.
[505] „2024 Update on DHS's Use of Face Recognition & Face Capture Technologies | Homeland Security", elérés 2025. május 3., https://www.dhs.gov/archive/news/2025/01/16/2024-update-dhss-use-face-recognition-face-capture-technologies.
[506] „Real-Time Human Authentication System Based on Iris Recognition", elérés 2025. május 3., https://www.mdpi.com/2673-4117/3/4/47.
[507] „Voice Technology for Government | Verbio Technologies", elérés 2025. május 3., https://www.verbio.com/voice-technology-for-government/.
[508] Access Legal, *Enhanced Security through Biometric Verification"* (White Paper, 2023).

4.2.4 Megosztott hitelesítési ökoszisztémák

A megosztott hitelesítési ökoszisztémák lehetővé teszik a felhasználók számára, hogy egyetlen digitális identitást használjanak különböző szolgáltatások igénybevételéhez. Ez az integrált megközelítés javítja a felhasználói élményt és csökkenti a többszörös azonosítási folyamatok szükségességét. Kanadában a SecureKey Concierge szolgáltatás lehetővé teszi a felhasználók számára, hogy banki hitelesítési adataikat használják kormányzati szolgáltatások elérésére. A rendszer szövetségi és tartományi kormányzati szolgáltatásokat egyaránt támogat, és több nagy kanadai bankkal áll partnerségben.[509] Az Új-Zélandi RealMe szolgáltatás hasonló célt szolgál, lehetővé téve a felhasználók számára, hogy egyetlen igazolt digitális identitást használjanak mind a kormányzati, mind a magánszektorbeli szolgáltatások elérésére. A rendszer két szintű szolgáltatást kínál: a "RealMe bejelentkezés" alapszintű digitális identitást biztosít, míg a "RealMe igazolt fiók" magasabb szintű identitáshitelesítést kínál, amely magában foglalja a személyes adatok hivatalos igazolását.[510]

4.3 Személyazonosítási és hitelesítési technológiák a védelmi, biztonsági szektorban

A kifinomult kiberfenyegetések, fizikai biztonsági rések és személyazonossági lopások elterjedésével a hitelesítési rendszerek nélkülözhetetlenné váltak az érzékeny információk, létesítmények és műveletek védelméhez A mobiltechnológiák, a biometrikus rendszerek és a kriptográfiai fejlesztések konvergenciája példátlan lehetőségeket teremtett a biztonság fokozására és az üzemeltetési hatékonyság javítására. A védelmi és biztonsági környezetben a személyazonosítás és a hitelesítés közötti különbségtétel kritikus. A teljes azonosítási folyamat három alapvető összetevőből áll:

- Azonosítás: Annak megállapítása, kinek állítja magát a személy
- Hitelesítés: Az állított személyazonosság ellenőrzése különböző tényezők segítségével
- Engedélyezés: Annak meghatározása, hogy a hitelesített személy milyen erőforrásokhoz és műveletekhez férhet hozzá

[509] Shared Services Canada, „SecureKey Concierge – Credential Broker Service”, transparency - other, 2017. április 26., https://www.canada.ca/en/shared-services/corporate/transparency/access-information-privacy/publications/securekey-concierge-credential-broker-service.html.
[510] „RealMe®”, New Zealand Digital government, 2025. március 19., https://www.digital.govt.nz/products-and-services/products-and-services-a-z/realme.

A három komponens integrált kezelése elengedhetetlen a modern rendszerek megfelelő biztonságának fenntartásához, különösen védelmi környezetben, ahol az érzékeny információkhoz való hozzáférést szigorúan korlátozni kell.[511] A védelmi és biztonsági szervezetek széles körben alkalmazzák a fiziológiai biometrikus technológiákat. Az ujjlenyomat-azonosítás továbbra is a legelterjedtebb biometrikus hitelesítési módszer a biztonsági alkalmazásokban. A bűnüldöző szervek mind helyhez kötött, mind mobil ujjlenyomat-olvasókat használnak műveleteikhez, létesítményekhez való hozzáféréshez és gyanúsítottak azonosításához. A fejlett olvasók optikai, kapacitív, ultrahangos vagy hő érzékelő technológiákat alkalmaznak az ujjlenyomat-minták nagy pontosságú rögzítésére még kihívást jelentő környezeti feltételek mellett is, amelyek gyakoriak a terepi műveletekben.[512] A határellenőrző hatóságok az arcfelismerést automatizált útlevél-ellenőrző kapuknál alkalmazzák, míg a bűnüldöző hatóságok a gyanúsítottak azonosítására használják nyilvános terekben és terepi műveletek során.[513] A Dubai nemzetközi repülőtér íriszszkennereket alkalmaz az utasok gyors, érintésmentes azonosítására, demonstrálva a technológia alkalmazhatóságát védelmi forgatókönyvekben.[514] [515]

A tenyérvéna-felismerés a bőrfelszín alatti érmintázatok észlelését teszi lehetővé, előnyöket kínálva védelmi alkalmazásokban, mivel ezek a mintázatok nehezen hamisíthatók és viszonylag stabilak maradnak az idő múlásával. A Fujitsu PalmSecure technológiájához hasonló rendszerek tenyérvéna-felismerést alkalmaznak hozzáférés-vezérlési rendszerekhez, amelyek alkalmazhatók fontos katonai létesítmények és eszközök védelmére.[516]

---

[511] Lan Zhou, Vijay Varadharajan, és Michael Hitchens, „Trust-Based Secure Cloud Data Storage with Cryptographic Role-Based Access Control", in *Proceedings of the International Conference on Security and Cryptography*, 2013, 370–75, https://www.scitepress.org/Papers/2013/45086/45086.pdf.
[512] „Reasons to choose 4-4-2 Fingerprint Scanners for Police Accuracy", elérés 2025. május 3., https://mantraidentity.com/Blog/Why-police-department-adopting-4-4-2-fingerprint-scanners-accuracy-speed.
[513] „Deep Face Recognition: An Easy-To-Understand Overview - viso.ai", elérés 2025. május 3., https://viso.ai/deep-learning/deep-face-recognition/.
[514] „CBP Broadens Iris Recognition at U.S. Borders", elérés 2025. május 3., https://www.bioenabletech.com/news/cbp-broadens-iris-recognition-at-u-s-borders.
[515] „Emirates launches integrated biometric path at DXB", elérés 2025. május 3., https://www.futuretravelexperience.com/2020/10/emirates-launches-integrated-biometric-path-at-dxb/.
[516] „Fujitsu boasts new integrator and distributor for palm vein biometric technology | Biometric Update", elérés 2025. május 3., https://www.biometricupdate.com/201403/fujitsu-boasts-new-integrator-and-distributor-for-palm-vein-biometric-technology.

A bűnüldöző és hírszerző ügynökségek egyre inkább alkalmazzák a viselkedési biometriát a folyamatos, passzív hitelesítéshez. A járáselemzés gyorsulásmérőket, kamerákat és gépi tanulási algoritmusokat használ az egyén egyedi mozgás- és testtartási jellemzőinek vizsgálatára. A Budapesti Műszaki és Gazdaságtudományi Egyetem kutatói vizsgálták a járáselemzés hatékonyságát a nyilvános felügyeleti rendszerekben, eredményeik alkalmazhatók a jogosulatlan személyek azonosítására korlátozott területeken.[517] A billentyűzetdinamika a gépelési mintákat elemzi, beleértve a billentyűleütések közötti időzítést, a billentyűlenyomások időtartamát és a hibamintákat. Ez a módszer lehetővé teszi a folyamatos, passzív hitelesítést hírszerzési elemzés és kiberbiztonsági műveletek során speciális hardver igénye nélkül. A billentyűzetdinamika 95%-os pontosságot érhet el a jogosult felhasználók azonosításában, ami értékes eszközzé teszi a terminálok biztonsági megsértésének értékelésére.[518] A hangfelismerés pedig egyre fontosabbá válik a biztonságos katonai kommunikációban és parancsnoki központokban.[519]

A védelmi és biztonsági szervezetek többmódú biometrikus rendszereket alkalmaznak, amelyek több biometrikus azonosítót integrálnak a biztonság és a pontosság fokozása érdekében. Ezek a rendszerek általában arcfelismerést, ujjlenyomat-szkennelést, írisszkennelést és hangfelismerést kombinálnak, hogy robusztusabb hitelesítési mechanizmusokat hozzanak létre, amelyeket nehezebb kompromittálni.[520]

A kutatások azt mutatják, hogy a többmódú rendszerek magasabb pontossági arányokat érhetnek el, mint az egyetlen biometrikus módszert alkalmazó rendszerek. Egy arc-, ujjlenyomat- és írisz-szkennelést kombináló többmódú rendszer akár 99,8%-os pontosságot is elérhet, ami meghaladja az egyes modalitások 95-98%-os pontosságát. Ez

[517] „Biometric Continuous Authentication | European Data Protection Supervisor", 2025. április 28., https://www.edps.europa.eu/press-publications/publications/techsonar/biometric-continuous-authentication_en.
[518] John Griffin, „Keystroke Dynamics: Typing as Powerful Behavioral Biometrics | Fleksy", 2022. augusztus 23., https://www.fleksy.com/blog/keystroke-dynamics-and-the-types-of-behavioural-biometrics/.
[519] Stefanie Pidgeon, „LOUD AND CLEAR", *USAASC* (blog), 2021. október 6., https://asc.army.mil/web/news-loud-and-clear/.
[520] „Multimodal Biometrics Enhancing Law Enforcement and Border Security", elérés 2025. május 3., https://www.laxton.com/blog/multimodal-biometrics-enhancing-law-enforcement-and-border-security/.

az innováció különösen értékes magas biztonsági szintű védelmi alkalmazásokban, ahol a hitelesítési hibák súlyos következményekkel járhatnak.[521]

4.3.1 Katonai műveletek

A hitelesítési rendszerek lehetővé teszik a parancsnokok számára, hogy a személyzet személyazonosságát ellenőrizzék műveletek során, mobileszközök és integrált biometrikus érzékelők segítségével. Ezek a rendszerek offline környezetben is működnek, és a kapcsolat helyreállásakor szinkronizálnak a központi adatbázisokkal. Képesek működni szélsőséges körülmények között, beleértve a sivatagi, sarkvidéki és magas páratartalmú környezeteket, amelyek kritikusak a globális katonai műveletekhez.[522] A felszerelés-engedélyezési alkalmazások szabályozzák a fegyverrendszerekhez, járművekhez és érzékeny berendezésekhez való hozzáférést. A védelmi minisztériumok olyan okoseszköz-alkalmazásokat valósítanak meg, amelyek több faktoros hitelesítést használnak, beleértve a biometriát és a hardveres tokeneket, biztosítva, hogy csak jogosult személyzet működtethessen bizonyos felszereléseket. Ezek a rendszerek naplózzák az összes hozzáférési kísérletet és használati mintát a küldetés utáni elemzés és elszámoltathatóság céljából.[523]

4.3.2 Bűnüldözési alkalmazások

A bűnüldöző szervek világszerte speciális mobil hitelesítési technológiákat alkalmaznak. A mobil ujjlenyomat-ellenőrzés lehetővé teszi, hogy a gyanúsítottakat a helyszínen azonosítsák hordozható szkennerek segítségével, amelyek okos telefonokhoz vagy táblagépekhez csatlakoznak. Ezek az eszközök kapcsolódnak az Automatizált Ujjlenyomat-azonosító Rendszer (AFIS) adatbázisaihoz, hogy gyors azonosítást biztosítsanak anélkül, hogy a rendőrségre kellene szállítani a személyeket. A tanulmányok sze-

[521] „Multimodal Biometrics Enhancing Law Enforcement and Border Security".
[522] „New wearable authentication more than a »token« gesture | Article | The United States Army", elérés 2025. május 3., https://www.army.mil/article/225197/new_wearable_authentication_more_than_a_token_gesture.
[523] „Army Authentication Tokens Not Just for Tactical Use | AFCEA International", elérés 2025. május 3., https://www.afcea.org/signal-media/cyber-edge/army-authentication-tokens-not-just-tactical-use.

rint ezek a technológiák akár 85%-kal is csökkenthetik a feldolgozási időt a hagyományos módszerekhez képest.[524] A testkamera általi hitelesítés biztosítja a videó bizonyítékok sértetlenségét biometrikus hozzáférés-vezérlés és a felvételek kriptográfiai aláírása révén. A hitelesítés mind a felvétel kezdeményezésekor, mind a bizonyítékok kezelésekor megtörténik, megakadályozva a jogosulatlan hozzáférést vagy módosítást.[525]

A mobil bűnügyi nyilvántartásokhoz való hozzáférési alkalmazások biztonságos, hitelesített hozzáférést biztosítanak a bűnügyi adatbázisokhoz a. A többfaktoros hitelesítés, beleértve a biometriát biztosítja, hogy csak jogosultak kérdezhessenek le érzékeny információkat a gyanúsítottakról vagy érdeklődésre számot tartó személyekről. Ezek a rendszerek olyan hitelesítési tényezőket is alkalmaznak, mint a helymeghatározási ellenőrzést, hogy megakadályozzák a jogosulatlan adatbázis-hozzáférést még akkor is, ha a hitelesítési adatok kompromittálódtak.[526]

4.3.3 Határellenőrzés és bevándorlás

Az automatizált határellenőrzési rendszerek (ABC) elektronikus kapukat (e-kapukat) alkalmaznak biometrikus ellenőrzési képességekkel az utasok gyorsabb és pontosabb azonosítása érdekében. Ezek a rendszerek jellemzően arcfelismerést vagy ujjlenyomat-ellenőrzést használnak, és az eredményeket biometrikus útlevelekkel vagy adatbázis-bejegyzésekkel hasonlítják össze.[527] A Budapesti Liszt Ferenc Nemzetközi Repülőtéren 2019 óta működnek ilyen automatizált kapuk.[528]

---

[524] „Mobile ID Fingerprint Technology Can Provide Rapid Results and Improve Officer Safety | National Institute of Justice", elérés 2025. május 3., https://nij.ojp.gov/library/publications/mobile-id-fingerprint-technology-can-provide-rapid-results-and-improve-officer.

[525] „How to secure body-worn cameras and protect footage from cyber threats | Pen Test Partners", elérés 2025. május 3., https://www.pentestpartners.com/security-blog/how-to-secure-body-worn-cameras-and-protect-footage-from-cyber-threats/.

[526] „Authentication Solutions for Criminal Justice Information Services", elérés 2025. május 3., https://www.hirschsecure.com/industries/authentication-solutions-for-criminal-justice-information-services.

[527] Sopra Steria. (2023). Transforming the immigration system through smartphone biometric enrolment. https://www.soprasteria.co.uk/docs/librariesprovider2/sopra-steria-uk-documents/thought-leadership/biometrics-paper-vf.pdf

[528] „Hassle-Free Border Control at Budapest Airport", *Adaptive Recognition | Image Capturing and Analytics* (blog), elérés 2025. május 3., https://adaptiverecognition.com/case-study/hassle-free-border-control-at-budapest-airport/.

A mobil dokumentum-ellenőrző alkalmazások near field communication (NFC) és optikai karakterfelismerési technológiákat alkalmaznak, lehetővé téve a határőrök számára, hogy a terepen hitelesítsék az úti okmányokat. Ezek az alkalmazások felismerhetik a hamis dokumentumokat a biztonsági jellemzők referencia adatbázisokkal való összehasonlításával és a dokumentumok és az utazók közötti biometrikus egyezések ellenőrzésével. A fejlett rendszerek képesek felismerni a kifinomult hamisításokat a mikro nyomtatás, holografikus elemek és UV-jellemzők elemzésével.[529]

A fejlett határellenőrző rendszerek egyre inkább magukban foglalják:

1. **Több modális biometria**: Több biometrikus modalitás (arcfelismerés, ujjlenyomatok, írisz) kombinálása az azonosítási pontosság és ellenálló képesség növelése érdekében.[530]
2. **Kockázatértékelő algoritmusok**: Utazói adatok elemzése a magas kockázatú személyek azonosítására, akik további ellenőrzést igényelhetnek.[531]
3. **Dokumentum-hitelesítés**: Az úti okmányok hitelességének ellenőrzése különböző biztonsági jellemzők és kriptográfiai validáció révén.[532]
4. **Figyelőlista-ellenőrzés**: Az utazók személyazonosságának összehasonlítása az érdeklődésre számot tartó személyek adatbázisaival, beleértve az ismert bűnözőket, terrorizmusgyanús személyeket és bevándorlási szabálysértőket.[533]

Ezek a technológiák hatékonyabb határfeldolgozást tesznek lehetővé a biztonság fenntartása vagy növelése mellett, lehetővé téve a határőrség számára, hogy az emberi erőforrásokat a magasabb kockázatú utazókra összpontosítsák, miközben egyszerűsítik a folyamatot az alacsony kockázatú személyek számára.

---

[529] „UK Home Office to test remote fingerprint enrolment via smartphone for entry | Biometric Update", elérés 2025. május 3., https://www.biometricupdate.com/202412/uk-home-office-to-test-remote-fingerprint-enrolment-via-smartphone-for-entry.
[530] „Secure and Wireless Multimodal Biometric Scanning Device for Passenger Verification Targeting Land and Sea Border Control | H2020", CORDIS | European Commission, elérés 2025. május 3., https://cordis.europa.eu/project/id/872878/reporting.
[531] „Artificial Intelligence at EU Borders: Overview of Applications and Key Issues | Think Tank | European Parliament", elérés 2025. május 3., https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2021)690706.
[532] I.C.A.O., „Digital Travel Credentials Technical Standards"", *Document* 9303 (2023).
[533] „Threat Screening Center — FBI", elérés 2025. május 3., https://www.fbi.gov/investigate/terrorism/tsc.

A bevándorlással kapcsolatos alkalmazások egyszerűsítik a menekültek és menedékkérők regisztrációját mobileszközökön történő biometrikus beíratás révén. Ezek a rendszerek egyedi digitális identitásokat hoznak létre a hagyományos azonosító okmányokkal nem rendelkező kitelepített személyek számára, fokozva a biztonságot, miközben felgyorsítják a humanitárius feldolgozást. A mobilalkalmazások lehetővé teszik a nyilvántartásba vételt távoli területeken, válságövezetekben és ideiglenes feldolgozó központokban.[534]

4.3.4 Egészségügy

Tekintettel arra, hogy az egészségügyi szolgáltatások egyre inkább digitális platformokra helyeződnek át, a betegek és az egészségügyi szakemberek pontos azonosítása elsődleges fontosságúvá vált az adatbiztonság biztosítása, az orvosi hibák megelőzése és az általános ellátási minőség javítása érdekében. Az egészségügyi szektorban is megjelent a biztonságos mobil azonosítás igénye. A biometrikus rendszerek magas azonosítási pontosságot érnek el, csökkentik az adminisztratív hibákat és gyorsítják a betegfelvételi folyamatokat. A mobil alkalmazások és okos eszközök egyre inkább elsődleges eszközökként jelennek meg ezen technológiák megvalósításában, kényelmes hozzáférési pontokat biztosítva mind a betegek, mind az egészségügyi szolgáltatók számára. Az egészségügyi környezetben ezek a technológiák fokozzák a betegbiztonságot, javítják a hatékonyságot és emelik a betegeknek nyújtott ellátás általános minőségét. Az egészségügyi szektorban a mobilalapú hitelesítési megoldások különösen fontosak az érzékeny egészségügyi adatok védelme szempontjából. Az egészségügyi mobilalkalmazások egyre inkább beépítik a biometrikus azonosítást és a többfaktoros hitelesítést. Az Egyesült Királyság National Health Service (NHS) alkalmazása, az NHS App, lehetővé teszi a felhasználók számára, hogy hozzáférjenek egészségügyi adataikhoz, időpontot foglaljanak, és recepteket újítsanak meg. Az alkalmazás biometrikus hitelesítést használ a felhasználó azonosítására, és többfaktoros hitelesítést az érzékeny funkciók, például az egészségügyi dokumentumok megtekintéséhez.[535]

---

[534] „Biometric Verification for Asylum Seekers - HSB Identification", elérés 2025. május 3., https://www.hsb.nl/our-solutions/border-control/biometric-verification-for-asylum-seekers/.
[535] „Passwordless Login", NHS Transformation Directorate, elérés 2025. május 3., https://transform.england.nhs.uk/key-tools-and-info/digital-playbooks/open-source-digital-playbook/passwordless-login/.

A svájci ELGA elektronikus egészségügyi nyilvántartási rendszer mobil hitelesítési komponense is figyelemre méltó. A rendszer lehetővé teszi a betegek számára, hogy mobilalkalmazáson keresztül kezeljék hozzáférési jogosultságaikat, például meghatározzák, hogy mely egészségügyi szolgáltatók férhetnek hozzá az egészségügyi adataikhoz. A hitelesítés a nemzeti e-ID kártyával és mobilalkalmazással történik, biztosítva a magas szintű biztonságot.[536] A biometrikus technológiák az egészségügyi szektorban nem csak az azonosításban, hanem a biztonságos adattovábbításban is szerepet játszanak, lehetővé téve a távoli konzultációkat és monitoring rendszereket.[537]

A globális egészségügyi rendszerek területén az elektronikus egészségügyi kártyák kulcsfontosságú eszközként szolgálnak a betegek azonosításának ellenőrzésében. Bár a Magyarországon használt TAJ kártya elsősorban azonosító eszközként szolgál, nem pedig technológiai komponenseket vagy biometrikus adatokat tartalmaz, több más nemzet fejlettebb rendszereket hozott létre. A Németországban használt elektronikus egészségügyi kártyát eGK-nak nevezik, ami az elektronikus egészségügyi kártya rövidítése. Olyan chipet tartalmaz, amely nyomon követi a biztosítási adatokat és kívánság szerint az egészségügyi információkat is. A franciaországi Carte Vitale rendszer hasonló módszert alkalmaz, intelligens kártya technológiát használva a betegazonosítás védelmére.[538]

Az egészségügyi személyzet megbízható azonosítása elengedhetetlen a betegadatok védelméhez és a bizalmas információkhoz való megfelelő hozzáférés biztosításához. Az egészségügyi ágazat dolgozói gyakran különböző hitelesítési módszereket alkalmaznak az elektronikus egészségügyi nyilvántartási rendszerekhez és más kritikus egészségügyi infrastruktúrához való hozzáféréshez. Az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) rendszer használatához Magyarországon az orvosi szakembereknek elektronikus személyazonosító kártyákat (eSzemélyi) vagy azzal egyenértékű hitelesítő adatokat kell alkalmazniuk.[539]

---

[536] „SwissID Login with Mobile ID", elérés 2025. május 3., https://trustservices.swisscom.com/en/about-us/news/en/swissid-login-with-mobile-id.
[537] Bundesministerium Gesundheit, „Die elektronische Gesundheitskarte (eGK", 2022, https://www.bundesgesundheitsministerium.de/elektronische-gesundheitskarte.html.
[538] Maladie Assurance, „La Carte Vitale: Funkcionalitások és biztonság", 2021, https://www.ameli.fr/.
[539] Infrastruktúra Nemzeti, *Elektronikus Egészségügyi Szolgáltatási Tér: Rendszerarchitektúra és funkcionalitások* (Budapest: ÁEEK, 2020).

Az egészségügyi információk, mivel személyes adatok kategóriájába tartoznak, egyéb adattípusoktól eltérő védelmet igényelnek. Az egészségügyi rendszerekben a hozzáférés szabályozásának domináns módszerei a következők:

- Az RBAC, vagy szerepalapú hozzáférés-vezérlés, egy olyan rendszer, amely a hozzáférési jogosultságokat az egészségügyi szakember szervezeten belüli kijelölt funkciójának megfelelően osztja ki a fiókjához. Ez biztosítja, hogy az egyének csak a konkrét munkaköri feladataikhoz szükséges információkhoz férjenek hozzá.
- Az attribútum-alapú hozzáférés-vezérlés, más néven ABAC, egy olyan módszertan, amely a hozzáférési jogosultságokat több tényező figyelembevételével határozza meg, mint például képesítések, részleg vagy betegkapcsolatok.
- A kontextus-alapú hozzáférés-vezérlés magában foglalja a bizalmas információkhoz való hozzáférés biztosítását kontextuális tényezők, például helyszín és idő figyelembevételével. Az 1997. évi XLVII. törvény (Eüak.) szabályozza a hozzáférés-ellenőrzést a magyarországi egészségügyi intézményekben. Ez a jogszabály előírja, hogy csak a beteg kezelésében aktívan részt vevő egészségügyi szakemberek férhetnek hozzá személyes adataihoz, és minden hozzáférést dokumentálni kell.[540]

4.4 Jelenlegi biztonsági a mobil személyazonosítási és hitelesítési technológiák kapacsán kihívások, kockázatok

A hordozható eszközök hitelesítési szolgáltatásokra való fokozott támaszkodás kiberbiztonsági sebezhetőségeket eredményezett. A rosszindulatú személyek kihasználhatják a mobil eszközök – beleértve az okos telefonokat, táblagépeket és laptopokat – egyedi biztonsági gyengeségeit. Ezek az eszközök kivételes kényelmet és hozzáférhetőséget biztosítanak különféle szolgáltatások nyújtásához. A fő fenyegetések közé tartozik a malware, az adathalász kísérletek, a közbeékelődéses támadások, az eszközlopás és a nem biztonságos vezeték nélküli hálózatok használata. Ezek a sebezhetőségek veszélyeztethetik a kritikus hitelesítési adatokat, potenciálisan pénzügyi veszteségeket és személyazonosság-lopást eredményezve.

[540] Infrastruktúra.

4.4.1 A biometrikus hitelesítés sebezhetőségei

A biometrikus azonosítás előnyöket kínál a hagyományos módszerekhez képest, egyedi biztonsági kihívásokat is jelent. A biometrikus rendszerek érzékenyek a prezentációs támadásokra vagy megtévesztési kísérletekre. Ezek a támadások során az elkövetők szintetikus biometrikus adatokat használnak a hitelesítési rendszer megtévesztésére. A magas minőségű másolatok félrevezethetik az ujjlenyomat-azonosító rendszereket, míg az arcfelismerő rendszerek sebezhetőek lehetnek a fényképek, videók vagy fejlett deepfake technológia felhasználásával végrehajtott támadásokkal szemben. A 2024-es Kiberbiztonsági Globális Rangsor aggasztó tendenciát jelez a biometrikus biztonság területén: 23%-os növekedés tapasztalható a biometrikus adatszivárgásokban 2023-hoz képest.[541] Továbbá, a mobilos csalások 15%-a tulajdonítható az NFC (near field communication) használatával végrehajtott támadásoknak, és a tanulmány kiemelte a növekvő aggodalmakat az arcfelismerés deepfake technológiával történő manipulálásával kapcsolatban. Ez problémát jelent, mivel a biometrikus adatok – a jelszavakkal ellentétben – nem változtathatók meg kompromittálódás esetén, hosszú távú biztonsági következményeket okozva.

4.4.2 A mesterséges intelligenciával kapcsolatos veszélyek és ellenstratégiák

A mesterséges intelligencia gyors fejlődése teljesen új csatateret nyitott a hitelesítési biztonság területén. A mesterséges intelligencia technológia fegyverként használható kifinomult deepfake-ek létrehozására, amelyek képesek lehetnek megtéveszteni a biometrikus ellenőrző rendszereket, a vállalatok 61%-a nem rendelkezik megfelelő védelmi intézkedésekkel a neurális hálózatok által generált hamis biometrikus adatok, úgynevezett DeepMasterPrints ellen.[542]

4.4.3 Adatvédelmi és adatvédelmi kihívások

A GDPR a biometrikus adatokat személyes adatok különleges kategóriájába sorolja. A személyes adatok gyűjtése és feldolgozása a digitális kormányzati hitelesítéshez adatvédelmi megfontolásokat vet fel, amelyeket mind technikai intézkedéseken, mind megfelelő szabályozási keretrendszereken keresztül gondosan kell kezelni. Az adatvédelem szempontjából a biometrikus adatok használata jelenti az egyik legjelentősebb

[541] *2024 Cybersecurity Global Ranking: Mobile Authentication Vulnerabilities* (International Cybersecurity Institute, 2024).
[542] PwC Hungary, „AI-Generated Biometric Threats Survey", *Market Research*, 2024.

kockázatot a mobil hitelesítésben.[543] A különleges kategóriába tartozó személyes adatoknak szigorúbb követelményeket támaszt a GDPR a szervezetekkel szemben a biometrikus adatok gyűjtése, kezelése, tárolása és védelme tekintetében. Az ELTE Egyetem 2024-ben végzett jogi kutatása szerint a mobil alkalmazások 42%-a nem felel meg teljes mértékben a biometrikus adatok kezelésére vonatkozó adatvédelmi előírásoknak.[544] Ez a nem-megfelelőség jogi és hírnévkockázatot jelent a biometrikus hitelesítést mobil alkalmazásaikban implementáló szervezetek számára. Továbbá, a biometrikus adatok különleges státusza gyakran zavart okoz a fejlesztők körében a beépített adatvédelmi elvek megfelelő implementálásával kapcsolatban. A mobil hitelesítési rendszerek egyik fő nehézsége a személyes adatok feletti felhasználói irányítás fenntartása, miközben átláthatóságot biztosítanak az adatkezelési módszerekben. Az iparági szakértőkkel folytatott beszélgetések rámutattak, hogy a kockázat túlmutat a szolgáltatók által összekapcsolt különböző profilok problémáján, aggályok merülnek fel azzal kapcsolatban is, hogy mely feldolgozott adatokat továbbíthatják harmadik feleknek.[545]

A szakértők hangsúlyozzák a jogszerű és jogosulatlan adatfeldolgozás közötti különbségtétel fontosságát, valamint a jóhiszemű és rosszindulatú adatfeldolgozás megkülönböztetését. Az illegális adatfeldolgozás azonosításának prioritása alapvető fontosságú, azonban ez megerősítést igényel az adatvédelmi hatóságok részéről. Az adatbiztonság végrehajtásának jelenlegi széttagolt módszere következetlenségeket eredményez abban, ahogyan a hitelesítési szolgáltatók a felhasználói adatokat kezelik a különböző országokban.

A nemzetközi utazás és a határokon átnyúló szolgáltatások további jogi és szabályozási kihívásokat jelentenek a hitelesítési rendszerek számára. Amikor a felhasználók megpróbálják ugyanazokat a hitelesítési módszereket használni nemzetközi szinten, nézeteltérések merülhetnek fel a különböző kormányzati szabályozások és személyazonosság-ellenőrzési követelmények miatt.

---

[543] P. Nagy és L. Kovács, „Legal and Privacy Aspects of Mobile Authentication Technologies", *AARMS Journal* 20, sz. 2 (2021): 77-94,.
[544] E.L.T.E. University, „Compliance Assessment of Mobile Applications with GDPR Requirements", *Legal Studies Journal* 35, sz. 3 (2024): 112-128,.
[545] Nagy és Kovács, „Legal and Privacy Aspects of Mobile Authentication Technologies".

4.4.4 Az interoperabilitással és standardizálással kapcsolatos akadályok

A különböző hitelesítési technikák közötti következetlenség kihívásokat jelent azok általános implementációja és felhasználói elfogadása szempontjából. Számos platform és szolgáltatás különálló, saját tulajdonú hitelesítési módszereket használ, ami töredezett felhasználói élményt és potenciális biztonsági kockázatokat eredményez az integrációs pontokon. Az Európai Unió Digitális Identitás Tárca kezdeményezése, amelynek teljes bevezetése 2026-ra várható, a protokollok standardizálását célozza mind a 27 tagállamban, valamint lehetővé teszi az offline működést és többnyelvű támogatást nyújt.[546]

A modern hitelesítési mechanizmusok integrálása a régebbi rendszerekkel számos technikai kihívást jelent. Számos vállalkozás befektetést eszközölt a meglévő infrastruktúrájába, amely esetleg nem kompatibilis a korszerű hitelesítési módszerekkel. Ez a probléma különösen gyakori a hosszú múltra visszatekintő rendszerekkel rendelkező ágazatokban, mint például a pénzügy, a kormányzat és az egészségügy.3A régebbi eszközökkel való kompatibilitási problémák további bonyodalmakat okoznak a telepítési folyamatban. A régebbi iOS-verziók, nevezetesen az iOS 13 előttiek, nem támogatják a fejlett biometrikus funkciókat, ami széttagolt felhasználói élményt eredményez a különböző eszközgenerációk között.[547] Ennek következtében a szervezetek több hitelesítési útvonal létrehozására kényszerülnek, ami növeli a komplexitást és a potenciális biztonsági sebezhetőségeket.

4.4.5 Teljesítménnyel és megbízhatósággal kapcsolatos aggályok

A hitelesítési rendszereknek egyensúlyt kell teremteniük a biztonsági követelmények és a teljesítménycélok között. A mobil eszközök korlátai, beleértve a számítási teljesítményt, az akkumulátor élettartamát és a kapcsolati problémákat, befolyásolhatják a hitelesítési rendszerek megbízhatóságát. A kutatások szerint a folyamatos hitelesítési funkciók 15-20%-kal növelhetik az energiafelhasználást, ami gyakorlati korlátot jelent a szélesebb körű használat számára.[548] A környezeti körülmények is befolyásolhatják

---

[546] „EU Digital Identity Wallet: Implementation Roadmap and Challenges", *European Commission Technical Report*, 2024.
[547] „Mobile Authentication Technologies: Compatibility Analysis", *Mobile Security Journal* 12, sz. 4 (2023): 78-92,.
[548] „Mobile User Authentication Market Report: Resource Utilization Analysis", *Research and Markets Report*, 2024.

az érintésmentes biometrikus eszközök hatékonyságát. Mivel a fényviszonyok, az időjárás és a háttérzaj hatással lehetnek a felismerési pontosságra, a fejlesztőknek figyelembe kell venniük ezeket a tényezőket a valós életben alkalmazott rendszerek tervezésekor[549]. A megbízhatósággal kapcsolatos aggályok olyan kritikus alkalmazások esetén, mint az egészségügy kiemelt figyelmet érdemelnek, hiszen ott a hitelesítési hibák súlyos következményekkel járhatnak.

4.4.6 A társadalmi elfogadással és bizalommal kapcsolatos kérdések

A szakértők azt állítják, hogy az elektronikus aláírások széles körű használata és a bennük való közbizalom nem javítható, hacsak nem integrálják őket egy átfogó folyamatba, például azonosításba vagy hitelesítésbe a szerződéskötés előtti ügyfél-ellenőrzés során.[550] Ez az elektronikus aláírások nyilvános elfogadására vonatkozik. A szakértők azzal érvelnek, hogy a távoli azonosítás társadalmi elfogadása összetett kihívást jelent, amely nem csak a biztonsági és kényelmi szinteket foglalja magában, hanem a jogi jóváhagyást is. A biometrikus azonosító rendszerek elfogadottsága eltér a különböző demográfiai csoportok és kulturális kontextusok között. Számos probléma akadályozhatja az elfogadást, beleértve az adatvédelmi aggályokat, bizonyos biometrikus modalitásokkal szembeni vallási ellenvetéseket és a technológiával szembeni általános bizalmatlanságot. A hitelesítési rendszerek tervezőinek figyelembe kell venniük ezeket a társadalmi összetevőket a technikai és jogi korlátozásokkal együtt, hogy biztosítsák a széles körű elfogadást és használatot. A biometrikus hitelesítési rendszerek, miközben fokozott biztonságot kínálnak, hozzáférhetőségi kihívásokat jelenthetnek bizonyos felhasználói csoportok számára. Az arcvonásaikat, ujjlenyomataikat vagy hangjukat érintő fizikai fogyatékossággal élő személyek nehézségekbe ütközhetnek olyan biometrikus hitelesítési rendszerek használatakor, amelyeket nem hozzáférhetőségi szempontok figyelembevételével terveztek.[551]

---

[549] „Eye-Tracking Technologies in Mobile Devices: Applications and Limitations", *Semantic Scholar Paper*, 2023.
[550] Nagy és Kovács, „Legal and Privacy Aspects of Mobile Authentication Technologies".
[551] „Estonian Electronic Voting System: Security Analysis and Voter Participation Trends", *Journal of E-Democracy* 11, sz. 4 (2020): 301-315,.

4.5 Ágazat-specifikus kihívások

Egyes kihívások generálisan jelennek meg a személyazonosításra, illetve személyi hitelesítésre alkalmas technológiák esetén, azonban vannak a fentiekben már felsorolt magán, illetve állami szektorbeli speciális kihívások, különös tekintettel a biometrikus megoldásokra is, az alábbiakban kerülnek röviden kifejtésre.

4.5.1 Az egészségügyi hitelesítéssel kapcsolatos kérdések

Az egészségügyi környezetekben működő hitelesítési rendszerek egyedi kihívásokkal szembesülnek az egészségügyi adatok érzékeny jellege és a rendszer megbízhatóság kritikus fontossága miatt. Az 1997. évi XLVII. törvény (Eüak.) előírja, hogy az egészségügyi vonatkozású adatoknak fokozott biztonsági intézkedéseket kell kapniuk, mivel személyes adatként kategorizáltak.[552] E szabályozás szerint csak a beteg kezelésében aktívan részt vevő egészségügyi személyzet jogosult a személyes adatokhoz való hozzáférésre, és minden hozzáférést dokumentálni kell.

Alapvető fontosságú a higiéniával és keresztszennyeződéssel kapcsolatos további aggályok biometrikus azonosítás egészségügyi szektorban való alkalmazásával kapcsolatban, különösen klinikai környezetben.[553] Bár a COVID-19 pandémia felgyorsította az érintésmentes biometrikus technológiák, például az arcfelismerés és hangazonosítás használatát, ezek a megoldások továbbra is kihívásokkal küzdenek a pontosság és megbízhatóság tekintetében az egészségügyi környezetekben.

4.5.2 A pénzügyi szolgáltatási szektor biztonsági követelményei

A bankszektorban a pénzügyi adatok érzékeny jellege és az anyagi veszteségek lehetősége miatt, a kiberbiztonsági fenyegetések komoly kihívást jelentenek. A pénzintézetek elsődleges célpontjai a hackereknek az általuk kezelt érzékeny információk miatt. A pénzügyi szektor különösen szigorú hitelesítési biztonsági követelményeknek van kitéve a potenciális célpontok értéke és a meglévő szabályozási kötelezettségek miatt.

---

[552] „Contactless Biometric Solutions in Healthcare: Post-COVID Implementation Analysis", *Journal of Healthcare Technology* 18, sz. 3 (2022): 225-241,.
[553] „Contactless Biometric Solutions in Healthcare: Post-COVID Implementation Analysis".

A mobil banki szolgáltatások bővülését a kiberkockázatok növekedése és azok összetettebbé válása kíséri. A hordozható eszközökre jellemző sebezhetőségek azok, amelyeket a hackerek kihasználhatnak. A fő fenyegetések közé tartoznak a rosszindulatú szoftverek és vírusok, az adathalász sémák, a közbeékelődéses (man-in-the-middle) támadások, az elektronikus eszközök lopása és a nem megfelelően védett Wi-Fi hálózatok használata. Ezek a veszélyek veszélyeztethetik a fontos pénzügyi információkat, potenciálisan pénzügyi veszteségekhez és személyazonosság-lopáshoz vezethetnek.[554]

4.5.3 Ügyvédi irodák

Az ügyvédi irodáknak megbízható adatvédelmi intézkedéseket kell bevezetniük a biometrikus adatok biztonságának biztosítása érdekében, beleértve:

1. Kifejezett hozzájárulás beszerzése az ügyfelektől a biometrikus adatok gyűjtése előtt.
2. A biometrikus adatok gyűjtésének és felhasználásának korlátozása meghatározott, legitim célokra.
3. Erős titkosítás és hozzáférés-szabályozás megvalósítása a tárolt biometrikus adatok védelme érdekében.
4. Egyértelmű adatmegőrzési irányelvek és biztonságos törlési eljárások kialakítása.
5. Rendszeres biztonsági értékelések és a biometrikus rendszerek auditálása.

A Nemzetközi Ügyvédi Kamara összehasonlító tanulmánya megállapította, hogy a több joghatóságban működő ügyvédi irodák kihívásokkal szembesülnek a konzisztens hitelesítési standardok fenntartásában, miközben megfelelnek a helyi szabályozásoknak. A tanulmány adaptív hitelesítési keretrendszerek bevezetését javasolta, amelyek alkalmazkodhatnak a különböző szabályozási követelményekhez, miközben konzisztens felhasználói élményt nyújtanak.[555]

4.5.4 Turizmus

Az okos turizmus kihívásai között kell említeni a turisták bizalmának megteremtése és az általuk alkalmazott technológiák széles körű elfogadásának biztosítása.[556] A Magyar

[554] „Journal of Digital Banking Security, »Mobile Security Threats and Countermeasures«", 2022.
[555] „International Bar Association, »Authentication Standards for Cross-Border Legal Services«", Research Report, 2023.
[556] Hungary, „AI-Generated Biometric Threats Survey".

Nemzeti Bank 2025-ös irányelvei szerint a biometrikus adatok tárolása kizárólag helyi tárolásra korlátozódik, kizárva a felhőalapú megoldásokat. Ez a megközelítés tükrözi a biometrikus adatok tárolásának biztonságával kapcsolatos növekvő aggályokat, és befolyásolhatja, hogyan valósítják meg a turisztikai vállalkozások a biometrikus hitelesítési rendszereket.[557]

4.5.5 Közösségi média

A felhasználók jellemzően több közösségi média platformon tartanak fenn jelenlétet, mindegyik saját hitelesítési követelményekkel és rendszerekkel. Ez a fragmentáció több kihívást teremt, többek között:

1. Hitelesítési fáradtság: A felhasználók frusztrációt tapasztalhatnak a különböző platformokon használt hitelesítési adatok kezelése miatt
2. Biztonsági következetlenségek: A platformok közötti változó biztonsági szabványok sebezhetőségeket teremthetnek
3. Adat duplikáció: Több platform által tárolt hasonló biometrikus adatok növelik az adatvédelmi kockázatokat
4. Széttagolt felhasználói élmény: Az egyes platformokon különböző hitelesítési folyamatok súrlódást okozhatnak

A standardizált, platformok közötti hitelesítési protokollok fejlesztése megoldhatná ezeket a kihívásokat, de példa nélküli együttműködést igényelne a versengő közösségi médiacégek között. A blokklánc-alapú identitás megoldások és önazonos identitásmodellek potenciális előrelépést kínálnak, bár a széles körű elterjedés továbbra is nehezen elérhető. [558]

4.5.6 A közszféra kezdeményezéseinek végrehajtási kihívásai

A közszolgáltatásokhoz használt hitelesítési rendszereknek alkalmazkodniuk kell a különböző szintű technikai jártassággal, eszközhozzáféréssel és fizikai képességekkel rendelkező felhasználókhoz. Ha ezeket a változókat nem kezelik megfelelően, az a digitális egyenlőtlenségek súlyosbodásához és az alapvető szolgáltatásokhoz való hozzáférés csökkenéséhez vezethet. Azonban a biometrikus implementáció kormányzati kontextusokban fontos megfontolásokat is felvet:

---

[557] Hungarian National Bank, „Guidelines for Biometric Data Storage in Financial Institutions", *Regulatory Document*, 2025.
[558] Identitycom, „Predictions for the Future of Digital Identity", *Market Analysis*, 2025.

- **Adatvédelmi aggályok**: A biometrikus adatok gyűjtése és tárolása adatvédelmi kérdéseket vet fel, amelyeket gondosan kell kezelni a megfelelő szabályozási keretrendszereken és technikai óvintézkedéseken keresztül.
- **Biometrikus adatok biztonsága**: A biometrikus sablonokat biztonságosan kell tárolni és védeni a támadásokkal szemben, mivel a kompromittált biometrikus adatokat nem lehet könnyen megváltoztatni vagy visszavonni, mint a jelszavakat.
- **Inkluzivitás és hozzáférhetőség**: A biometrikus rendszereknek alkalmazkodniuk kell az olyan egyénekhez, akiknek fizikai különbségei vagy fogyatékosságaik vannak, amelyek befolyásolhatják bizonyos biometrikus modalitások használatának képességét.
- **Kulturális és társadalmi elfogadás**: A biometrikus technológiák elfogadása különböző kulturális és társadalmi kontextusokban változik, ami érzékenységet igényel a helyi normák és aggályok tekintetében.[559]

Az azonosítási és hitelesítési technológiák implementálása az e-közigazgatásban és m-közigazgatásban kiberbiztonsági kihívásokkal szembesül, amelyeket kezelni kell a kormányzati szolgáltatások és állampolgári adatok integritásának, elérhetőségének és bizalmasságának fenntartása érdekében. A főbb kiberbiztonsági kihívások közé tartoznak:

- **Hitelesítési támadások**: Kísérletek a hitelesítési mechanizmusok kompromittálására olyan módszereken keresztül, mint a credential stuffing, adathalászat, social engineering vagy brute force támadások. Ezek a támadások arra irányulnak, hogy jogosulatlan hozzáférést szerezzenek a kormányzati rendszerekhez az identitás-ellenőrzési kontrollok megkerülésével. [560]
- **Adatszivárgási kockázatok**: Az állampolgári adatok centralizációja a kormányzati rendszerekben magas értékű célpontokat teremt adatszivárgások számára. A

[559] Sotiris Karetsos, Constantina Costopoulou, és Alexander Sideridis, „Developing a smartphone app for m-government in agriculture", *Journal of Agricultural Informatics* 5 (2014. július): 1–8, https://doi.org/10.17700/jai.2014.5.1.129.
[560] Palo Alto Networks, „What Is a Credential-Based Attack? Palo Alto Networks Cyberpedia", 2020, https://www.paloaltonetworks.com/cyberpedia/what-is-a-credential-based-attack.

hitelesítési rendszereket úgy kell tervezni, hogy megakadályozzák az ilyen érzékeny adattárolókhoz való jogosulatlan hozzáférést.[561]

- **Bennfentes fenyegetések**: A rendszerekhez legitim hozzáféréssel rendelkező kormányzati alkalmazottak vagy szerződéses partnerek visszaélhetnek privilégiumaikkal. A hitelesítési rendszereknek megfelelő hozzáférés-ellenőrzést, feladat elkülönítést és auditálási mechanizmusokat kell tartalmazniuk a bennfentes fenyegetések kockázatának csökkentésére.[562]
- **Fejlett kitartó fenyegetések (APT-k)**: Kifinomult, célzott támadások, amelyeket gyakran nemzetállamok vagy jól finanszírozott bűnszervezetek támogatnak. Ezek a támadások célozhatják kifejezetten a hitelesítési infrastruktúrát, mint útvonalat a szélesebb kormányzati rendszerekhez.[563]
- **Mobileszköz sebezhetőségek**: A mobileszközök, operációs rendszerek vagy alkalmazások biztonsági gyengeségei, amelyek veszélyeztethetik az m-közigazgatási hitelesítés integritását. Ezek a sebezhetőségek folyamatos biztonsági frissítéseket és robusztus biztonsági architektúrákat igényelnek.[564]

4.5.7 Védelmi, biztonsági szektor

A környezeti ellenállóképesség követelménye a védelmi szektorban még inkább fontos, mint máshol. A hitelesítési technológiáknak megbízhatóan kell működniük szélsőséges körülmények között, beleértve a sivatagi hőséget, a sarkvidéki hideget, a magas csatatéri páratartalmat és az elektromágneses interferenciát. A biometrikus érzékelők különösen érzékenyek a környezeti tényezőkre, ami speciális kialakítást igényel a katonai alkalmazásokhoz.[565] Az akkumulátor élettartamával kapcsolatos aggályok befolyásolják a hosszabb műveleteket, ahol a töltési lehetőségek korlátozottak.

---

[561] Magyarország Transparency International, „Korrupciós kockázatok Magyarországon: Nemzeti integritás tanulmány", 2008, https://transparency.hu/wp-content/uploads/2016/05/Korrupci%C3%B3s-kock%C3%A1zatok-Magyarorsz%C3%A1gon-Nemzeti-integrit%C3%A1s-tanulm%C3%A1ny.pdf.
[562] L. Eshelby, „Addressing Insider Threats in the Public Sector", *Open Access Government*, 2025, https://www.openaccessgovernment.org/addressing-insider-threats-in-the-public-sector/187801/.
[563] Berzsenyi D., „Különleges kiberműveletek", 2023, https://hdi.uni-nke.hu/document/hdi-uni-nke-hu/0.%20%C3%89rtekez%C3%A9s_Berzsenyi%20D%C3%A1niel.pdf.
[564] Gyaraki R., *Az információbiztonság alapjai* (Budapest: Nemzeti Közszolgálati Egyetem, 2023), https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/az_informaciobiztonsag_alapjai_konyv_kesz_2.pdf.
[565] „Biometric Data and Behavior Analysis", *World Journal of Advanced Research and Reviews* 26, sz. 01 (2025): 339–50.

Az együttműködési problémák merülhetnek fel a nemzetközi műveletekben, ahol különböző országok eltérő hitelesítési szabványokat és eljárásokat alkalmaznak. A koalíciós erőknek biztonságos módszereket kell kidolgozniuk a személyzet kereszthitelesítésére anélkül, hogy kompromittálnák saját biztonsági keretrendszereiket. A NATO és hasonló szervezetek együttműködési műveletekre alkalmas hitelesítési keretrendszereket fejlesztenek.[566] A biometrikus adatvédelmi követelmények még katonai környezetben is érvényesek, speciális protokollok szükségesek ennek az érzékeny személyes adatnak a kezeléséhez. A védelmi szervezeteknek megfelelő védelmi intézkedéseket kell bevezetniük a biometrikus adatok gyűjtésekor, feldolgozásakor és tárolásakor, hogy megakadályozzák a visszaélést vagy a jogosulatlan hozzáférést.[567]

A határokon átnyúló adattovábbítási korlátozások hatással lehetnek a nemzetközi műveletekre, mivel a különböző joghatóságok eltérő követelményekkel rendelkeznek a személyes és biometrikus adatok kezelésére vonatkozóan.[568] Továbbá joghatósági konfliktusok merülhetnek fel, amikor a műveletek több országot érintenek, amelyek eltérő törvényekkel rendelkeznek a megfigyelésre, adatgyűjtésre és hitelesítési követelményekre vonatkozóan. A feleknek egyértelmű protokollokat kell kidolgozniuk arra vonatkozóan, hogy mely szabványok alkalmazandók a különböző működési körülmények között.[569]

4.6 Mobil személyazonosítási és hitelesítési technológia társadalmi elfogadottsága a magánszférában

E technológiák társadalmi elfogadottsága nagymértékben befolyásolja azok alkalmazását és sikerességét, beleértve az érzékelt biztonságot, kényelmet, adatvédelmi aggályokat, valamint a technológiákat alkalmazó szervezetekbe vetett bizalmat. Jelen alfejezet a személyazonosítási és hitelesítési technológiák társadalmi elfogadottságának jelenlegi helyzetét vizsgálja, mind a magán-, mind a közszférára összpontosítva.

A szektorokat átívelő társadalmi elfogadást befolyásoló tényezők

[566] archTIS, „Securing Multinational Coalition Collaboration with Data-Centric Security", 2022, https://www.archtis.com/wp-content/uploads/2022/09/archTIS-Securing-Multinational-Coalition-Collaboration-with-Data-Centric-Security_9-22.pdf.
[567] „Department of Defense Office of Inspector General", 2023, https://media.defense.gov/2023/Nov/09/2003338047/-1/-1/1/DODIG-2024-016.PDF.
[568] Orrick, „DOJ Seeks to Restrict Data Transfers to »Countries of Concern«", 2024, https://www.orrick.com/en/Insights/2024/12/DOJ-Seeks-to-Restrict-Data-Transfers-to-Countries-of-Concern.
[569] Lieber Institute - West Point., „Biometrics on the Battlefield", 2024, https://lieber.westpoint.edu/biometrics-on-the-battlefield/.

Több közös tényező befolyásolja az azonosítási és hitelesítési technológiák társadalmi elfogadottságát mind a magán-, mind az állami szektorban:

Bizalom és átláthatóság

A hitelesítési technológiákat bevezető szervezetekbe vetett bizalom befolyásolja az elfogadási arányokat. Amikor a felhasználók bíznak abban, hogy adataikat felelősségteljesen és biztonságosan kezelik, nagyobb valószínűséggel fogadnak el új hitelesítési módszereket. Az adatgyűjtéssel, tárolással és felhasználással kapcsolatos átláthatóság elengedhetetlen e bizalom kiépítéséhez. A szakértői interjúk kiemelték, hogy a kockázat túlmutat a szolgáltatók által összekapcsolt különböző profilok problémáján, aggályok merülnek fel azzal kapcsolatban is, hogy mely feldolgozott adatokat továbbíthatják harmadik feleknek.[570] A szakértők hangsúlyozzák a jogszerű és jogosulatlan adatfeldolgozás közötti különbségtétel fontosságát, valamint a jóhiszemű és rosszindulatú adatfeldolgozás megkülönböztetését.

Érzékelt hasznosság és kényelem

A felhasználók nagyobb valószínűséggel fogadják el a hitelesítési technológiákat, ha világos előnyöket látnak a kényelem, időmegtakarítás vagy fokozott biztonság terén. A biztonság és használhatóság közötti egyensúly kulcsfontosságú – ha a hitelesítési eljárások túl nehézkesek, a felhasználók ellenállhatnak, a bevezetésnek vagy megkerülő megoldásokat kereshetnek. Az e-aláírások társadalmi elfogadottságával kapcsolatban a szakértők rámutattak, hogy az e-aláírások elterjedése és az irántuk való közbizalom nem növelhető, hacsak nem képezik részét egy komplex folyamatnak (azonosítás vagy hitelesítés a szerződéskötés előtti ügyfél-ellenőrzés során). A szakértők úgy vélték, hogy a társadalmi elfogadás összetett, mert nem csak a biztonságról és kényelmi szintekről szól, hanem a távoli azonosítás jogi elfogadásáról is.[571]

Demográfia és digitális jártasság

Az életkor, iskolai végzettség és digitális jártasság befolyáso0hatlja a hitelesítési technológiák elfogadását. A fiatalabb, technológiailag jártasabb felhasználók általában

[570] J. Brown, „Multi-Modal Authentication Systems: A Comprehensive Survey"", *IEEE Access* 9 (2021).
[571] Brown.

magasabb elfogadási arányokat mutatnak az innovatív hitelesítési módszerek iránt, míg az idősebb felhasználók előnyben részesíthetik az ismerős megközelítéseket.

Adatvédelmi aggályok és adatkontroll

A felhasználók adatvédelemmel és személyes adataik feletti kontrollal kapcsolatos aggályai befolyásolják hajlandóságukat az új hitelesítési technológiák elfogadására. A biometrikus adatok különösen aggályosak állandó jellegük miatt – a jelszavakkal ellentétben a biometrikus jellemzők nem változtathatók meg, ha kompromittálódnak.[572]

Biztonsági percepciók

A biztonsági kockázatok percepciói befolyásolják az elfogadást. Az adatvédelmi incidensek vagy a hitelesítési rendszerek sebezhetőségéről szóló jelentések csökkenthetik a bizalmat és elfogadást, még akkor is, ha a tényleges kockázatok minimálisak.

4.6.1 Társadalmi elfogadottság vizsgálata releváns videók alatti hozzászólások alapján

A társadalmi elfogadottság vizsgálatának részeként kvalitatív tartalomelemzésre került sor, amelyhez nyilvánosan elérhető YouTube-videók alatti felhasználói hozzászólások vettem alapul. A videók kiválasztásának szempontjai azok voltak, hogy legyen az adott videóhoz széleskörű nézettség és aktív hozzászólói közösség. A hozzászólások letöltése különböző nyilvánosan és ingyenesen elérhető YouTube komment letöltő platformot vettem igénybe, amely lehetővé tette a hozzászólások csv formátumban történő exportálását. Az adatok előfeldolgozását – beleértve a duplikátumok szűrését, az irreleváns karakterek eltávolítását és a szövegtisztítást Python környezetben végeztem el. Az eredmények vizualizációját a Gephi szoftver segítségével készítettem el.

1. videó

Videó címe: Is META Verified Worth It? I Paid to Find Out And Didn't Expect This!

Csatorna: Brandon Washington (bwashmedia)

Eredeti videó linkje: https://www.youtube.com/watch?v=DXvR_qW0fXQ

Feltöltés ideje: 2023 június 1.

Nézettség: 171,632 (2025. május 11-i állapot szerint)

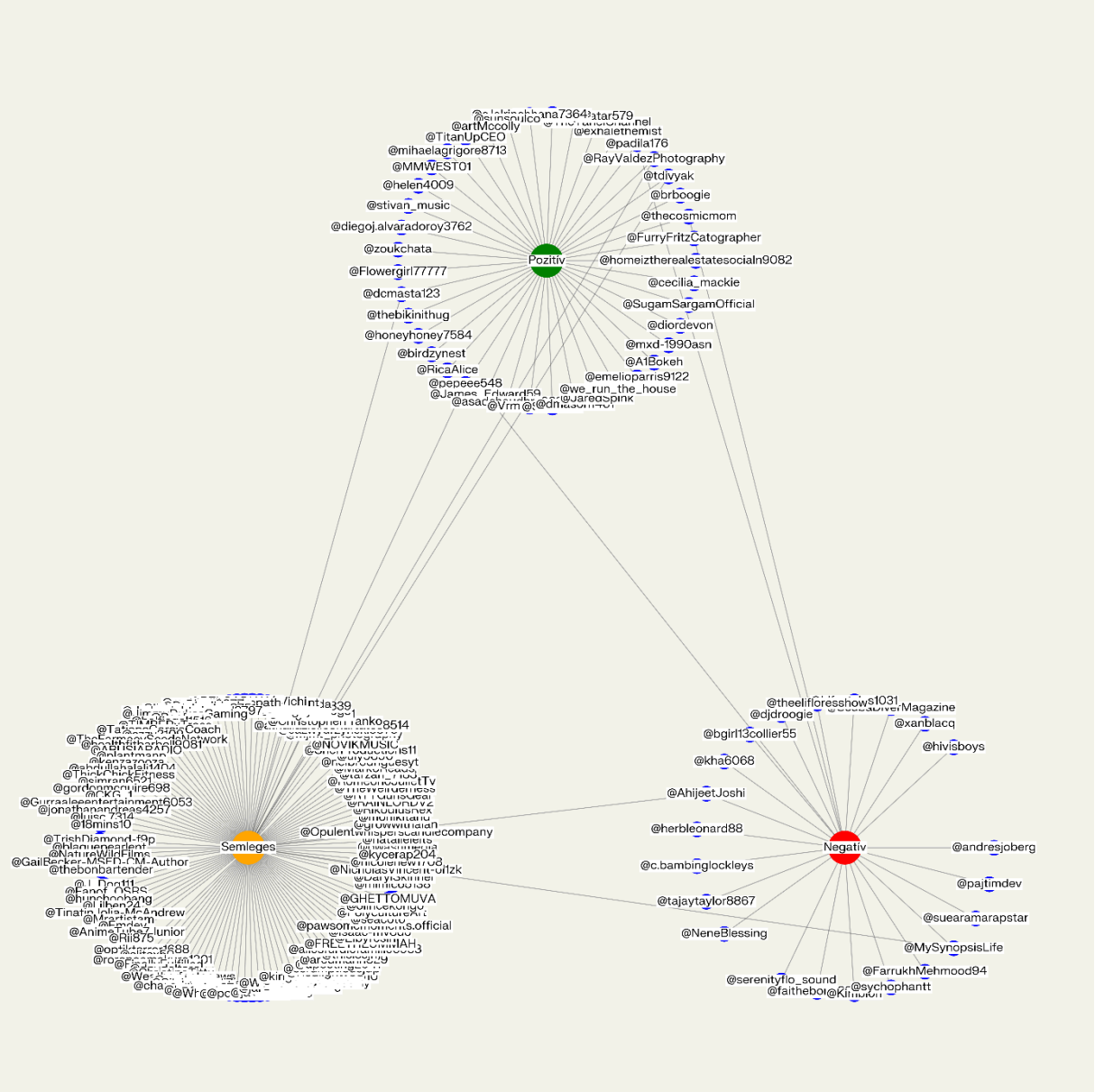
[572] Nagy és Kovács, „Legal and Privacy Aspects of Mobile Authentication Technologies".

Elemzett kommentek száma: 202 db

Szentiment analízis

A kommentek érzelmi töltetének kvantitatív elemzése a következő megoszlást mutatja:

- **Semleges**: 63.37% (128 komment)
- **Pozitív**: 24.75% (50 komment)
- **Negatív**: 11.88% (24 komment)



3. ábra: Szentiment analízis Meta 1. videó (saját szerkesztés)

Főbb témakörök

1. Üzleti érték és megtérülés 28% (57 komment)

Ez a kategória magában foglalja a Meta Verified üzleti értékével, megtérülésével és hatékonyságával kapcsolatos kommenteket.

2. Technikai kérdések és alkalmazhatóság 16% (32 komment)

Gyakorlati kérdések és technikai részletek a Meta Verified használatával kapcsolatban.

3. Adatvédelmi és biztonsági aggályok 6% (12 komment)

Ide tartoznak a személyes adatok biztonságával, adatvédelemmel kapcsolatos aggodalmak.

4. Osztálykülönbségek és társadalmi hatások 1% (2 komment)

A Meta Verified által létrehozott kétszintű felhasználói rendszer és ennek társadalmi hatásai.

5. Ügyfélszolgálati tapasztalatok 16% (32 komment)

A Meta Verified előfizetéssel járó ügyfélszolgálati élmények és problémák.

6. Egyéb 33% (67 komment)

Egyéb kategóriába sorolt kommentek, amelyek nem illeszkednek egyértelműen a fenti témakörökbe, vagy több témát is érintenek.

Összegzés

A kommentek elemzése alapján megállapítható, hogy a Meta Verified szolgáltatással kapcsolatos vélemények megosztottak. A semleges kommentek dominanciája (63.37%) arra utal, hogy sok felhasználó még ismerkedik a szolgáltatással, vagy konkrét információkat keres annak működéséről. A pozitív kommentek aránya (24.75%) meghaladja a negatív kommentek arányát (11.88%). A leggyakoribb témakör az üzleti érték és megtérülés (28.0%), ami arra utal, hogy a felhasználók elsősorban befektetésként tekintenek a szolgáltatásra, és annak hatékonyságát mérlegelik. Sokan kérdőjelezik meg, hogy a kék pipa valóban növeli-e az elérést vagy csak státuszszimbólumként szolgál.

Az elemzés alapján a Meta Verified egy olyan szolgáltatás, amely elsősorban azoknak lehet értékes, akik márkát építenek, és számukra fontos a hitelesség látszata, valamint a potenciálisan jobb ügyfélszolgálati támogatás. A hétköznapi felhasználók számára azonban a szolgáltatás értéke kérdéses, különösen a havi előfizetési díj fényében.

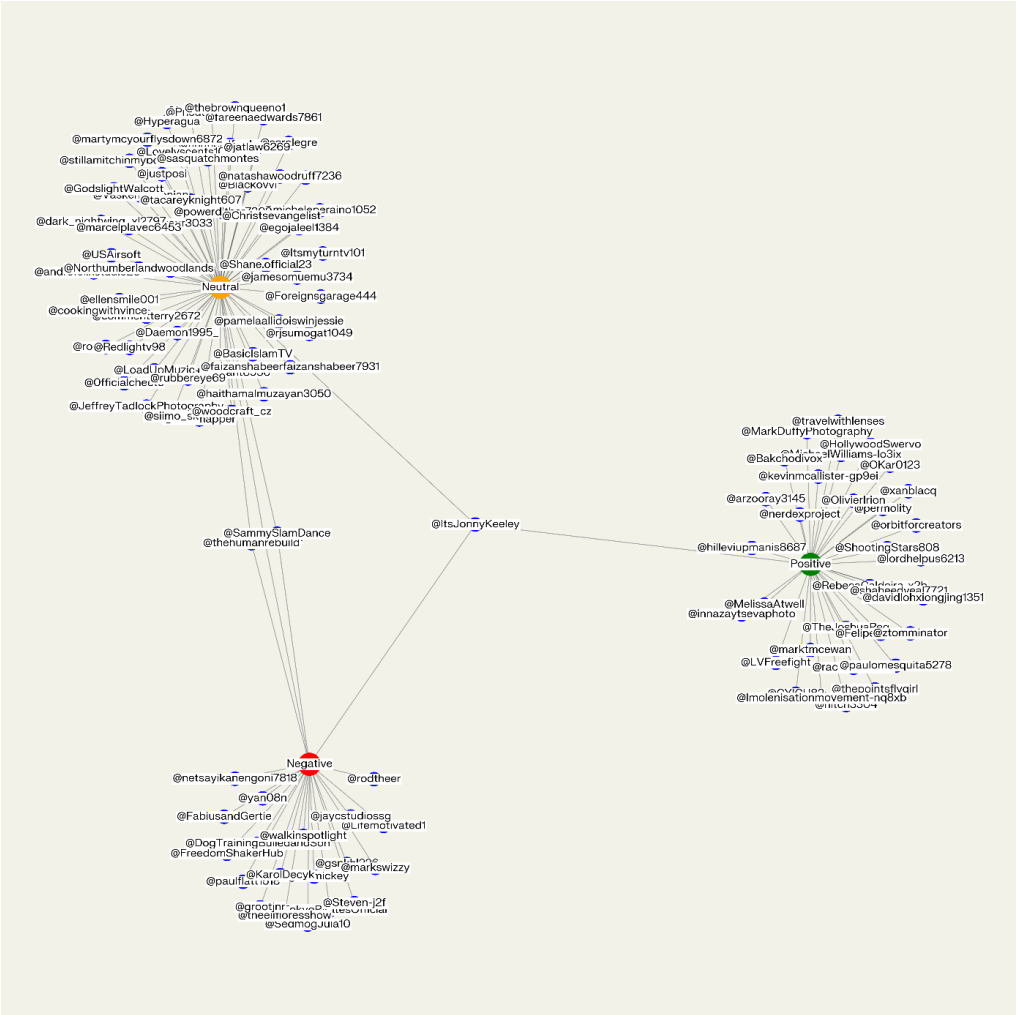
2. videó

- **Cím:** Is META Verified Worth It? I Paid to Find Out And Didn't Expect This!
- **Csatorna:** ItsJonnyKeeley
- **Eredeti videó linkje:** https://www.youtube.com/watch?v=SMFCLpUuhqY
- **Feltöltés ideje:** 2023. november 9.
- **Nézettség:** 147 000 (2025. május 11-i állapot szerint)
- **Elemzett kommentek száma:** 202

Szentiment analízis

A 202 komment szentiment szerinti eloszlása:

- **Semleges:** 139 komment (68,8%)
- **Pozitív:** 38 komment (18,8%)
- **Negatív:** 25 komment (12,4%)



4. **ábra Szentiment elemzés Meta 2. videó (saját szerkesztés)**

A Meta Verified videóhoz kapcsolódó kommentek többsége semleges, de jelentős a pozitív és negatív vélemények aránya is.

Főbb témakörök

A tematikus elemzés során a következő főbb témaköröket azonosítottam:

- **Üzleti érték és megtérülés** 15,3% (31 komment)
- **Technikai kérdések és alkalmazhatóság** 9,4% (19 komment)
- **Adatvédelmi és biztonsági aggályok** 5,9% (12 komment)
- **Ügyfélszolgálati tapasztalatok** 7,4% (15 komment)
- **Osztálykülönbségek és társadalmi hatások** 1,5% (3 komment)
- **Egyéb** 60,4% (122 komment) Ide tartoznak a rövid, általános, vagy nem egyértelműen besorolható hozzászólások.

Összegzés

A kommentek többsége semleges (68,8%), ezek főként információkérés, tapasztalat megosztás vagy rövid visszajelzés. A pozitív kommentek aránya 18,8%, ezek főként a videó készítőjét dicsérik vagy a Meta Verified szolgáltatás előnyeit emelik ki. A negatív kommentek (12,4%) között jelentős az ironikus, szarkasztikus hangvétel, illetve a csalódottságot, pénzkidobást, vagy adatvédelmi aggályokat megfogalmazó hozzászólás. A főbb témakörök közül az üzleti érték és megtérülés, valamint a technikai kérdések dominálnak. Sokan kérdőjelezik meg, hogy a Meta Verified valóban hoz-e érdemi előnyt, illetve sok a gyakorlati, ügyfélszolgálati és adatvédelmi kérdés is.

4.7 Mobil személyazonosítási és hitelesítési technológia társadalmi elfogadottsága az állami szférában

A nemzeti elektronikus azonosító rendszerek célja, hogy megbízható azonosítást biztosítsanak az állampolgárok számára a kormányzati szolgáltatásokhoz való hozzáféréshez és különféle jogi tranzakciók elvégzéséhez. Ezeket a rendszereket egyre inkább elektronikus formában valósítják meg, hatékony és biztonságos azonosítást biztosítva.

4.7.1 A korábbi magyar eSzemélyi elfogadottsága.

A G7 cikke szerint 2024 júliusának végén összesen 9 millió kártyaformátumú személyi igazolvány volt a lakosságnál, amiből 7,88 millió volt alkalmas e-aláírásra.[573] Ugyanakkor a digitális hitelesítési funkciók kihasználtsági aránya továbbra is alacsonyabb a kívánatosnál, ami a társadalmi elfogadás kihívásaira utal a széles körű terjesztés ellenére. Az elektronikus személyazonosító rendszerek elfogadottsága változik országonként és demográfiai csoportonként. Észtország e-ID rendszerét széles körben a legsikeresebb megvalósítások egyikének tekintik, magas használati aránnyal különböző szolgáltatások terén. Az észt megközelítés hangsúlyt fektet az átláthatóságra, a felhasználói kontrollra és a bizonyítható előnyökre, ami hozzájárult széles körű elfogadottságához.[574]

4.7.2 Határellenőrzés és bevándorlás-kezelés

A határellenőrzési pontokon alkalmazott biometrikus hitelesítés növekvő elfogadottságot mutat, ahogy az utazók felismerik annak előnyeit a feldolgozási sebesség és biztonság szempontjából. Az elfogadottság kihívásai között szerepelnek az adatvédelmi aggályok, különösen a biometrikus adatok gyűjtésével és tárolásával kapcsolatban. A kulturális különbségek szintén befolyásolják az elfogadottsági arányokat, eltéréseket mutatva különböző régiók között. A Nemzetközi Légi Szállítási Szövetség (IATA) adatai szerint az ázsiai-csendes-óceáni országokból érkező utazók általában magasabb elfogadási arányt mutatnak a biometrikus technológiák iránt, mint európai társaik, ami tükrözheti az adatvédelemmel és hatékonysággal kapcsolatos eltérő kulturális attitűdöket.[575]

E rendszerek társadalmi elfogadottsága általában pozitív, az utazók értékelik a csökkentett várakozási időt és az egyszerűsített folyamatokat. Egy európai határátkelőhelyeken végzett felmérés kimutatta, hogy az utazók 76%-a támogatja a biometrikus ellenőrzés használatát a fokozott biztonság érdekében, de 58%-uk aggályokat fejezett ki

[573] „Nyolc eltékozolt év után vége a személyi igazolványhoz járó e-aláírásnak - G7 - Gazdasági sztorik érthetően", elérés 2025. május 4., https://g7.hu/kozelet/20240830/nyolc-eltekozolt-ev-utan-vege-a-szemelyi-igazolvanyhoz-jaro-e-alairasnak/.
[574] „Estonian E-Identity Model as a Best Practice"".
[575] „International Border Control Association, "Biometric Authentication at Border Control: 2025 Trends and Insights", *Annual Report*, 2024.

azzal kapcsolatban, hogyan tárolják és használják biometrikus adataikat.[576] Ez jól szemlélteti a feszültséget e technológiák előnyeinek felismerése és a potenciális adatvédelmi vonatkozásokkal kapcsolatos aggályok között.

4.7.3 Egészségügyi hitelesítési rendszerek

Az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) Magyarország központi egészségügyi információs rendszere, amelyet 2017 novemberében indítottak. A betegek hozzáállása az egészségügyi hitelesítési rendszerekhez összetett és sokrétű. A hatékonysági előnyök hozzájárulnak a technológia betegek általi elfogadásához. Bár a fejlett technológiák ígéretesek technikai szempontból, társadalmi elfogadottságuk nagyban függ a technológia működéséről és az adatok védelméről szóló átlátható kommunikációtól. Az egészségügyi szolgáltatóknak egyensúlyt kell teremteniük a biztonsági előnyök és a betegek adatvédelmi aggályai között, és biztosítaniuk kell, hogy a hitelesítési rendszerek ne akadályozzák az ellátáshoz való hozzáférést, különösen a sérülékeny populációk esetében.

4.7.4 Társadalmi elfogadottság vizsgálata releváns videók alatti hozzászólások alapján

Jelen rész kapcsán ugyanazon módszer alapján dolgoztam, mint a Meta kapcsán végzett videó komment elemzésnél. Itt a kiválasztási szempont az egyes videóknál az volt, hogy mutassa be a jelenlegi magyar vonatkozású rendszert, majd az indukciós eljárások logikája mentén az Európai Unió ehhez szolgáltatott új keretét, továbbá a digitális állampolgárság, mint koncepciót vizsgáltam. Tekintettel arra, hogy az általam elvégzett szakértői interjúknál a DÁP-pal kapcsolatban nem a pozitív attitűd dominált, ezért arra az előzetes következtetésre jutottam, hogy a videók alatti kommentek során is inkább negatív hangvételű írásokat fogok találni. Ebből kiindulva a nemzetközi szakirodalomban leginkább pozitív példaként aposztrofált észt rendszert is alapul vettem, mint összehasonlítási példát. Megjegyezném, hogy a videók kiválogatása során abba a nehézségbe jutottam, hogy vagy egyáltalán nem volt a releváns videóknál komment lehetőség, vagy a felhasználók nem kommentteltek. A fentiek okán egyes esetekben alacsony mintával kellett dolgoznom.

[576] „Automated Border Control Systems: User Experience and Acceptance Factors", *International Journal of Border Security* 10, sz. 2 (2020): 156-172,.

Az alábbiakban a DÁP, az észt e-Residency és az eiDAS 2.0. társadalmi elfogadottságát vizsgáltam releváns videók alatti kommentek elemzése által az alábbiak szerint:

1. videó

Videó címe: Megszólalt a szakértő, ez a véleménye a nemrég elstartolt digitális állampolgárságról

Csatorna: ATV Magyarország

Eredeti videó linkje: https://www.youtube.com/watch?v=aIQNbfkmH58&ab_channel=ATVMagyarorsz%C3%A1g

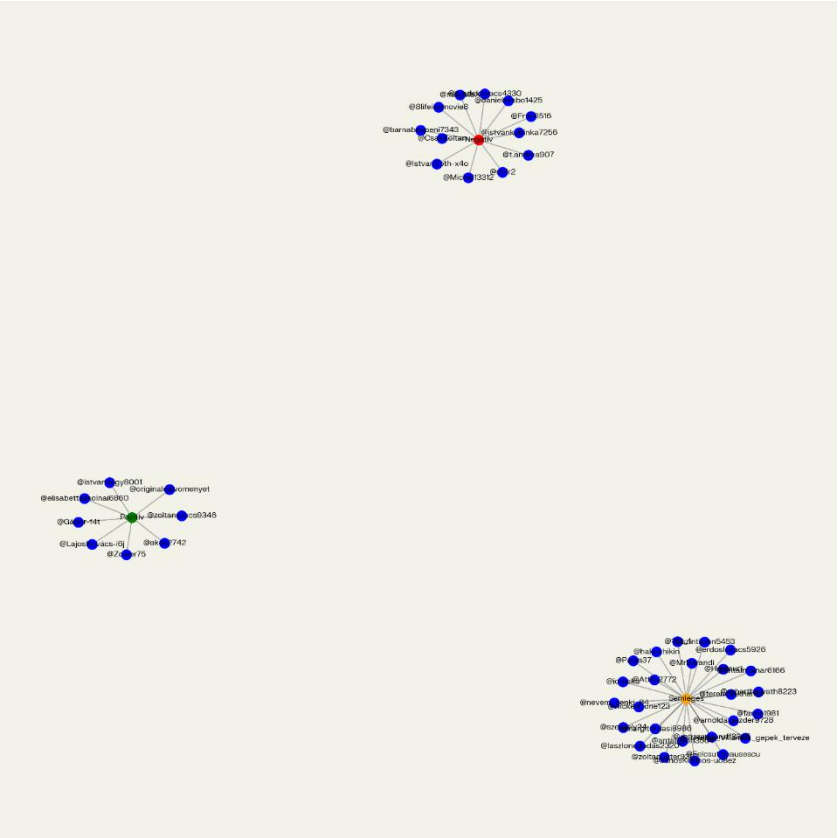
Feltöltés ideje: 2024. szeptember 8.

Nézettség: 27.199 (2025. május 11-i állapot szerint)

Elemzett kommentek száma: 49

Szentiment Analízis

- Pozitív: 14,4% (7 komment)
- Semleges: 53% (26 komment)
- Negatív: 32,6% (16 komment)



5. ábra Szentiment analízis DÁP 1. videó (saját szerkesztés)

A szentiment elemzés azt mutatja, hogy a kommentek többsége semleges vagy negatív hangvételű. A negatív kommentek aggodalmakat, kritikát vagy elutasítást tanúsítanak a DÁP-pal kapcsolatban. A pozitív kommentek száma alacsony, mindössze 14,4% (7 darab).

Témakörelemzés

A kommentek elemzése során az alábbi főbb témaköröket azonosítottam:

1. **Adatvédelmi és biztonsági aggályok 26,5% (13 komment)**

Számos komment fejez ki aggodalmakat az adatlopás, hackelés és kibertámadások lehetőségével kapcsolatban, többen azt említik, hogy a rendszer sebezhetővé teheti a személyes adatokat.

2. **Megfigyeléssel és kontrollal kapcsolatos félelmek 24,5 % (12 komment)**

Sok kommentelő a totális állami kontroll eszközének tekinti a rendszert és hasonlítják a kínai társadalmi kreditrendszerhez. Kulcsszóként jelenik meg a "Digitális rabszolgaság" és "digitális diktatúra" kifejezések-

3. **Politikai kritika 16,3 % (8 komment)**

Több komment kormányt és konkrét politikai szereplőket kritizál, illetve felmerült a választási rendszer digitalizálásának lehetősége és az ezzel kapcsolatos aggályok is.

4. **Technikai kérdések és alternatívák 14,3% (7 komment)**

Néhányan alternatív megoldásokat javasolnak (pl. személyi azonosító jel más formában). A kommentelők részéről felmerült a DÁP a kötelezővé tételének kérdése. Továbbá technikai problémákra és hiányosságokra mutatnak rá (pl. bankkártyás fizetés hiánya a közlekedésben)

5. **Ironikus és szarkasztikus megjegyzések 18,4% (9 komment)**

Számos komment használ iróniát vagy szarkazmust a téma kapcsán.

Összegzés

A kommentek általános hangvétele inkább szkeptikus és kritikus. Sokan fejezik ki aggályaikat a digitális személyazonosítás bevezetésével kapcsolatban, különösen az adatvédelem, a megfigyelés és a potenciális visszaélések tekintetében. A kommentelők jó része nem bízik a rendszer biztonságában és attól tart, hogy az állam túlzott kontrollt szerezhet az állampolgárok felett.

2. videó

Videó címe: A Digitális Állampolgár (DÁP) applikáció letöltése és a regisztráció menete-MKVKOK INFORMÁCIÓS VIDEÓ

Csatorna: Magyar Könyvvizsgálói Kamara Oktatási Központ Kft

Eredeti videó linkje: https://www.youtube.com/watch?v=GScJQe1sGWA&t=2s&ab_channel=MagyarK%C3%B6nyvvizsg%C3%A1l%C3%B3iKamaraOktat%C3%A1siK%C3%B6zpontKft.

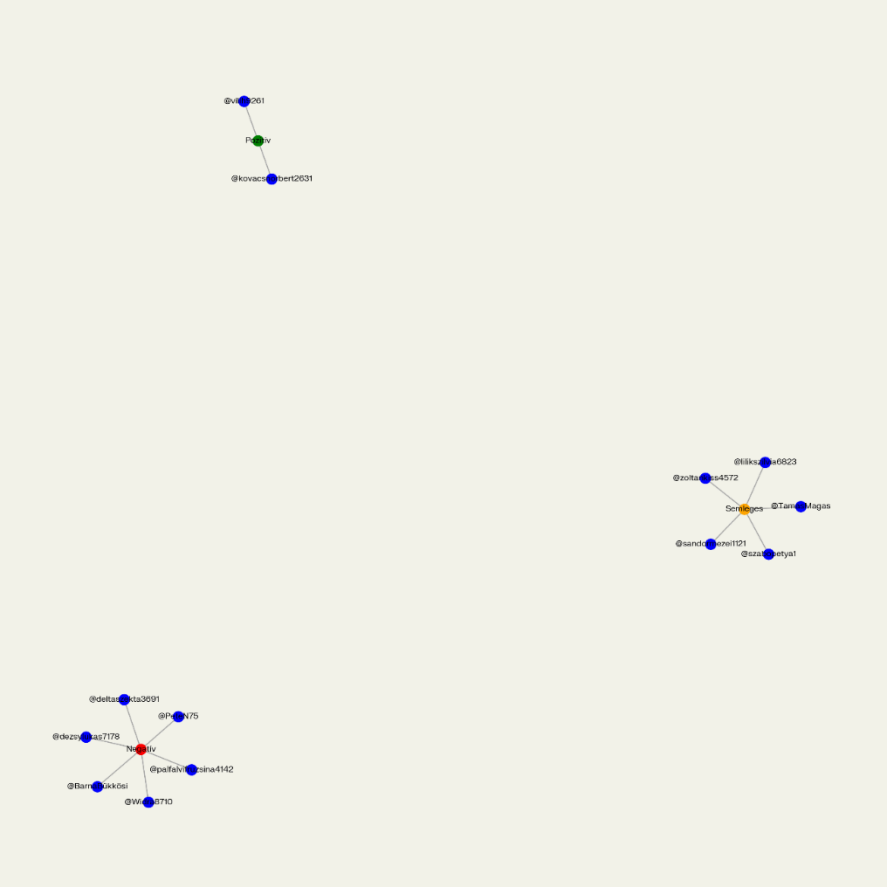
Feltöltés ideje: 2024. december 9.

Nézettség: 26,520 (2025. május 11-i állapot szerint)

Elemzett kommentek száma: 13

Szentiment Analízis

- **Pozitív**: 14,3% (2 komment)
- **Semleges**: 53,1% (7 komment)
- **Negatív**: 32,7% (4 komment)



6. ábra Szentiment analízis DÁP 2. videó (saját szerkesztés)

Megállapítható, hogy a kommentek többsége semleges vagy negatív hangvételű. A negatív kommentek gyakran tartalmaznak aggodalmakat, kritikát vagy elutasítást a bemutatott digitális személyazonosítási rendszerrel kapcsolatban. A pozitív kommentek száma alacsony, mindössze 2 darab található a teljes mintában.

Főbb Témakörök

1. **Adatvédelmi és biztonsági aggályok** 30,8% (4 komment)

Egyes kommentelők aggodalmat fejeznek ki a személyes adatok biztonságával kapcsolatban

2. **Megfigyeléssel és kontrollal kapcsolatos félelmek** 23,1% (3 komment)

A digitális állampolgárság rendszerét a magánélet és a szabadság elvesztésével társítják a kommentelők.

3. **Politikai kritika** 15,4% (2 komment)

A kormányzati rendszer kritikája fordul elő e típusban.

4. **Technikai kérdések és alternatívák** 15,4% (2 komment)

Gyakorlati használhatósággal kapcsolatos problémák is megjelennek a hozzászólások között (Pl.: "Nem olvassa be a chip-et, nem is csinál semmit")

5. **Ironikus és szarkasztikus megjegyzések** 15,4% (2 komment)

Továbbá jelen videónál is megfigyelhető az erős érzelmi elutasítás, emoji-k vagy túlzó nyelvhasználat formájában.

Összegzés

A felhasználók jelentős része technikai problémákról számol be, ami a rendszer implementációs hiányosságaira utalhat, továbbá erős negatív vélemények fogalmazódnak meg a rendszer adatvédelmi és megfigyelési aspektusaival kapcsolatban.

Megjegyzendő, hogy a pozitív kommentek jellemzően a videó hasznosságára vonatkoznak, míg a negatívak a rendszer koncepcionális vagy technikai problémáira. Tehát a pozitív kommentek nem magát a DÁP-ot minősítik, hanem az arról készült videót.

3. videó

Videó címe: Így legyél digitális állampolgár! // Könnyebb, mint gondolnád!

Csatorna: novaphone

Eredeti videó linkje: https://www.youtube.com/watch?v=nTqcNVDe8aI

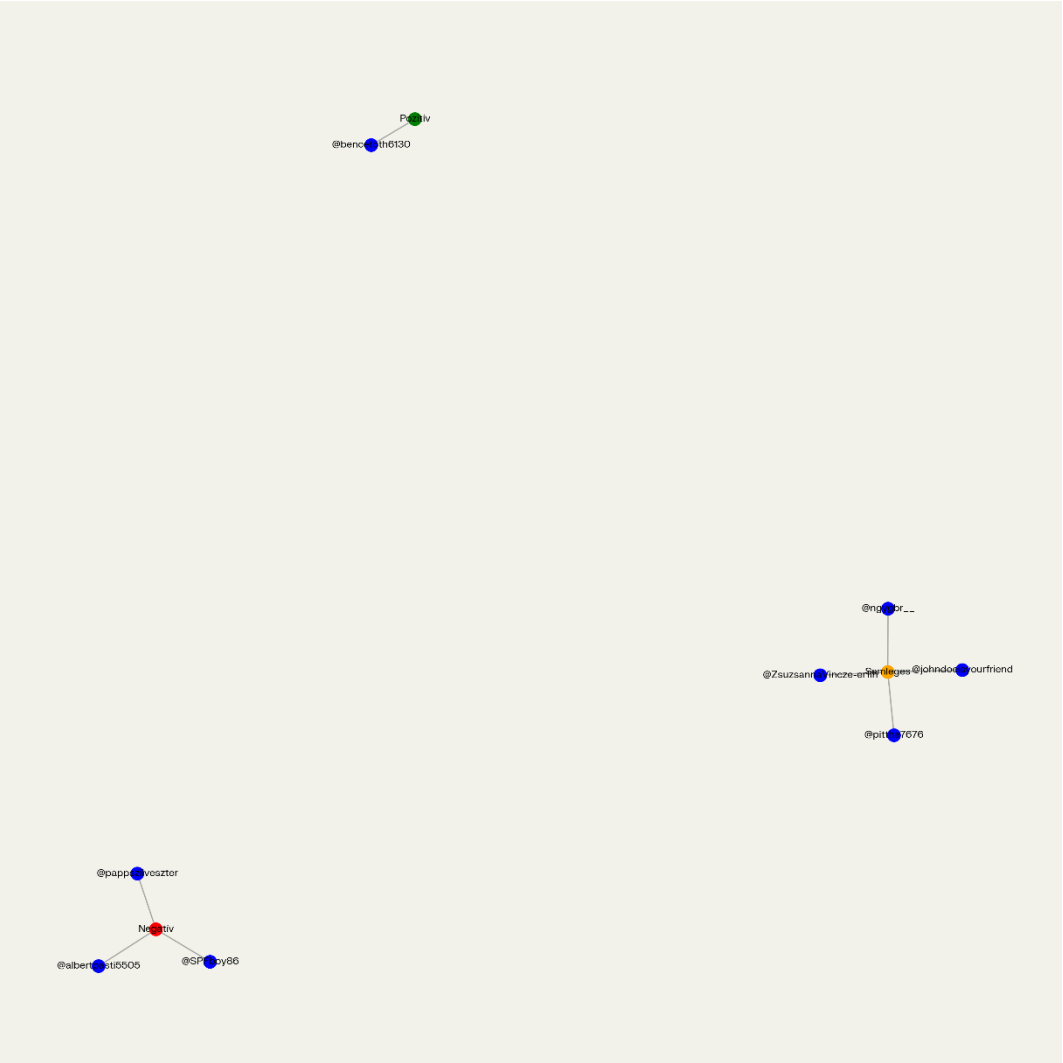
Feltöltés ideje: 2025. január 8.

Nézettség: 2,487 (2025. május 11-i állapot szerint)

Elemzett kommentek száma: 13

Szentiment Analízis

- Pozitív: 15.4% (2 komment)
- Semleges: 53.8% (7 komment)
- Negatív: 30.8% (4 komment)



7. ábra Szentiment analízis DÁP 3. videó (saját szerkesztés)

A kommentek többsége semleges hangvételű, azonban jelentős a negatív vélemények aránya is. A pozitív megnyilvánulások csak kis százalékban vannak jelen. A semleges kommentek általában információkérésre vagy tényközlésre szorítkoznak, míg a negatív kommentek főként aggodalmakat, kritikát fogalmaznak meg a digitális állampolgár platform bevezetésével kapcsolatban. A szentiment elemzés egyértelműen azt mutatja, hogy a kommentek többsége semleges vagy negatív hangvételű. A negatív kommentek gyakran tartalmaznak aggodalmakat és kritikát a DÁP-pal kapcsolatban.

Témakörelemzés

1. **Adatvédelmi és biztonsági aggályok** 30,8% (4 komment)

Jelen kategóriában a DÁP potenciális adatvédelmi kockázatai merülnek fel a kommentelők részéről, továbbá megjelenik a kormány közeli fejlesztés miatti bizalmatlanság is. Illetve az előző videókhoz hasonlóan a személyes adatok védelmével kapcsolatos félelmek.

2. **Megfigyeléssel és kontrollal kapcsolatos félelmek** 23,1% (3 komment)

Jelen témakör kapcsán megfigyelhetőek az aggodalmak a túlzott állami kontroll miatt. Kulcsszóként jelenik meg a "digitális börtön" metafora a digitális állampolgárságra-

3. **Politikai kritika** 15,4% (2 komment)

A 3. videó alatt is megjelennek a politikai kritikák, a kormányzati intézkedéseket bírálják a DÁP kötelezővé tételnek kritikája is megjelenik, továbbá egyfajta általános rendszerkritika is megjelenik.

4. **Technikai kérdések és alternatívák** (15,4% (2 komment)

Ennél témakörnél a kommentelők a regisztrációs problémákról és a technikai nehézségekről számoltak be. Továbbá felmerült az ügyfélkapu+, mint lehetséges alternatíva a DÁP-pal szemben.

5. **Ironikus és szarkasztikus megjegyzések** 15,4% (2 komment)

Ennél a videónál is hasonló arányban figyelhető meg az irónia. Cinikus hozzászólások a társadalmi befogadással és gúnyos megjegyzések a rendszer működésével kapcsolatban.

Összegzés

A digitális állampolgárság DÁP bevezetése vegyes, de inkább negatív fogadtatásra talált. A felhasználók jelentős része adatvédelmi aggályokat fogalmazott meg, és so-

kan úgy érzik, hogy a rendszert rájuk kényszerítik. Technikai problémák is felmerültek, a hozzászólók egy része alternatív megoldásokat javasol, mint például az Ügyfélkapu+ használatát. A technikai problémák mellett jelentős az adatvédelmi és szabadságjogi aggodalmak aránya, a kommentelők többsége szkeptikus a rendszerrel szemben.

Észt e-Residency kapcsán

1. videó

Videó címe: How to use your e-resident digital ID card - e-Residency tutorials

Csatorna: e-Residency

Eredeti videó linkje: https://www.youtube.com/watch?v=Y5S6ZqrT-mrw&ab_channel=e-Residency

Feltöltés ideje: 2024 november 18.

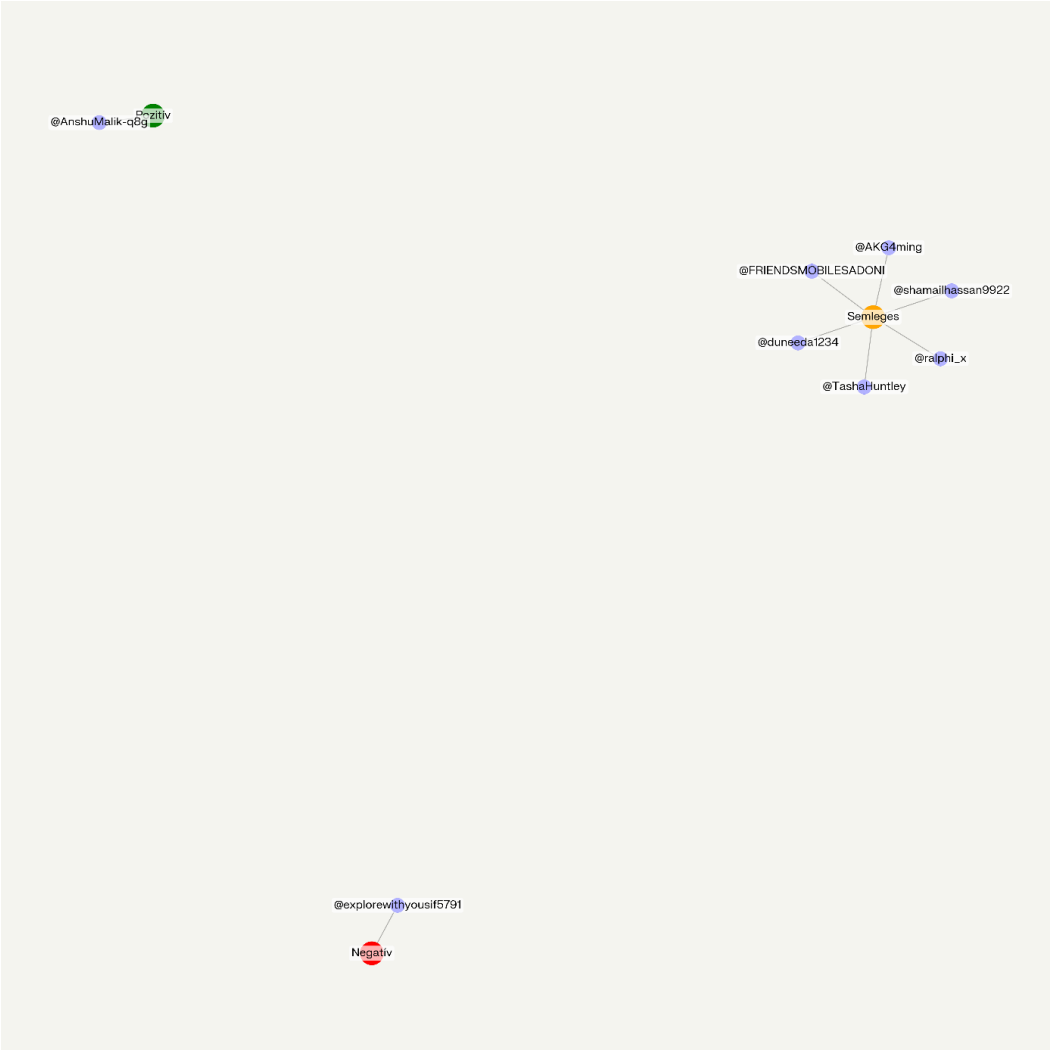
Nézettség: 3,284 (2025. május 11-i állapot szerint)

Elemzett kommentek szám: 8

Szentiment analízis

A kommentek érzelmi töltetét vizsgálva a következő megoszlást találtam:

- Pozitív: 12.5% (1 komment)
- Semleges: 75.0% (6 komment)
- Negatív: 12.5% (1 komment)



8. ábra: Szentiment analízis e-Residency 1. videó (saját szerkesztés)

A kommentek túlnyomó többsége semleges hangvételű, információkérő vagy technikai jellegű. Egy határozottan negatív komment található a mintában, amely elutasítja az e-Residency koncepcióját, míg a pozitív kommentek aránya alacsony. A gráfon egyértelműen látszik, hogy a legtöbb felhasználó a semleges szentiment kategóriához kapcsolódik, ami azt jelzi, hogy a kommentek többsége informatív vagy kérdező jellegű. Kisebb arányban találhatók pozitív hozzászólások.

Főbb témakörök elemzése

A kommentek tartalmi elemzése során az alábbi fő témaköröket azonosítottam:

1. Technikai kérdések és gyakorlati problémák 50% (4 db)

Az észt e-Residencynél az alábbi főbb problémákról számoltak be, mint a fizetési nehézségek az igénylés során, valamint kiszállítási státusszal kapcsolatos bizonytalanság, illetve hardver kompatibilitási kérdésről. (kártyaolvasó)

2. Üzleti lehetőségek és alkalmazási területek 37.5% (3 db)

Kérdések is felmerültek vállalkozásindítással, bankszámla nyitással, illetve ingatlankezeléssel kapcsolatban.

3. Adatvédelmi és kontrollal kapcsolatos aggályok 12.5% (1 db)

Jelen témakör kapcsán is megjelent a rendszer kritikája, a személyes szabadság korlátozásának kérdésköre.

Összegzés

Az elemzés alapján megállapítható, hogy az e-Residency iránt érdeklődők elsősorban gyakorlati nehézségekkel szembesülnek a szolgáltatás igénybevétele során. A kommentek jelentős része technikai problémákról számol be, ami a rendszer hozzáférhetőségét és felhasználóbarát jellegét kérdőjelezi meg. Figyelemreméltó, hogy míg az e-Residency programot innovatív, digitális határokat lebontó kezdeményezésként mutatják be, a felhasználók egy része szkeptikus, és potenciális adatvédelmi vagy szabadságjogi aggályokat fogalmaz meg.

2. videó

Videó címe: e-Residency: Everything you need to know

Csatorna: Manan Anwar

Eredeti videó linkje: https://www.youtube.com/watch?v=UxYAbXeQl14&ab_channel=MananAnwar

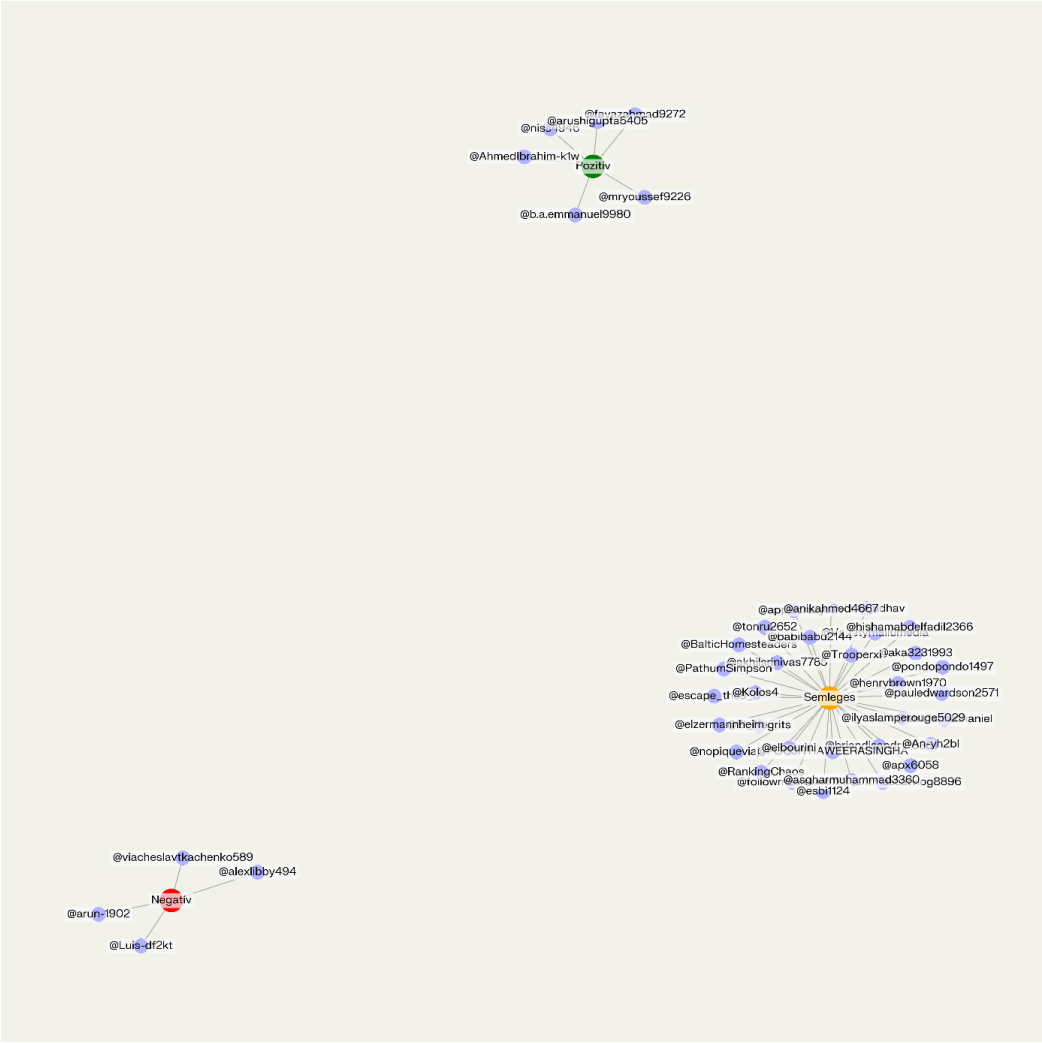
Feltöltés ideje: 2023 október 131.

Nézettség: 34,713 (2025. május 11-i állapot szerint)

Elemzett kommentek száma: 41

Szentiment analízis

- Pozitív: 12.5% (5 komment)
- Semleges: 75.0% (31 komment)
- Negatív: 12.5% (5 komment)



9. ábra Szentiment analízis e-Residency 2. videó (saját szerkesztés)

Az elemzés azt mutatja, hogy a kommentek túlnyomó többsége semleges hangvételű, elsősorban információkérő vagy tényközlő jellegű. A pozitív és negatív kommentek aránya kiegyenlített, mindkét kategória viszonylag alacsony.

Főbb témakörök

A kommentek elemzése során az alábbi főbb témaköröket azonosítottam:

1. Technikai és eljárási kérdések 51,2% (21 komment)

Ez a legnagyobb kategória, mely a program gyakorlati aspektusaira vonatkozó kérdéseket tartalmazza.

2. Üzleti felhasználás 24,4% (10 komment)

E témakör a vállalkozásindítással, üzleti lehetőségekkel kapcsolatos kérdéseket és észrevételeket tartalmazza:

3. Adatvédelmi és szabadságjogi aggályok 12,2% (5 komment)

A programmal kapcsolatos fenntartások, elsősorban az adatvédelem és a biometrikus adatok (ujjlenyomat) miatt:

4. Tartalomkérés 12,2% (5 komment)

A videó készítőhöz intézett kérések további információkért vagy segítségért:

Összegzés

Az észtországi e-állampolgárság programmal kapcsolatos YouTube-kommentek elemzése azt mutatja, hogy a nézők elsősorban gyakorlati információkat keresnek a program használatával és üzleti lehetőségeivel kapcsolatban. A kommentek többsége semleges hangvételű, információkérő jellegű, ami arra utal, hogy a téma iránt érdeklődők elsősorban tájékozódni szeretnének.

A bankszámlanyitási nehézségek jelentős akadályként jelennek meg, ami kérdéseket vet fel a program gyakorlati hasznosságával kapcsolatban. A biometrikus adatok (ujjlenyomat) követelménye szintén fenntartásokat kelt néhány kommentelőben, tükrözve a digitális identitással és adatvédelemmel kapcsolatos szélesebb társadalmi aggályokat. A programra vonatkozó érdeklődés globális jellege (különböző országokból érkező kommentek) összhangban van a digitális állampolgárság koncepciójának növekvő nemzetközi jelentőségével és a határok nélküli digitális identitás iránti igénnyel.

eiDAS 2.0. kapcsán

1. videó

Videó címe: "eIDAS 2.0 - Explained in 90 seconds"

Csatorna: IDnow

Eredeti videó linkje: https://www.youtube.com/watch?v=W14StXJPB-U

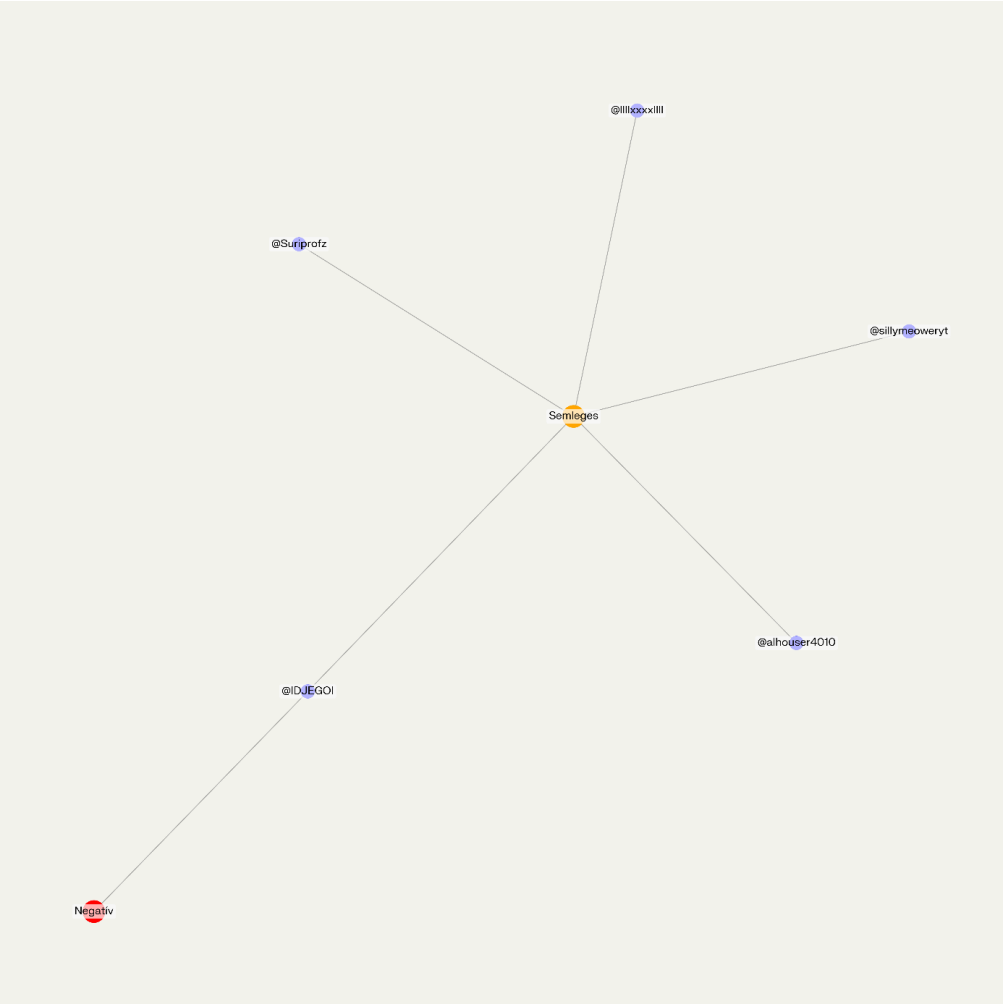
Feltöltés ideje: 2023 május 15.

Nézettség: 34,713 (2025. május 11-i állapot szerint)

Elemzett kommentek száma: 6

Szentiment analízis

- **Semleges**: 83.33% (5 komment)
- **Negatív**: 16.67% (1 komment)
- **Pozitív**: 0%



10. ábra Szentiment analízis eiDAS 2.0 1. videó (saját szerkesztés)

Főbb témakörök

1. **Technikai kérdések és alternatívák** 66.67% (4 komment)

Felmerült a nyílt forráskódú böngészők szükségességének kérdésköre, továbbá a böngészők forráskódból való fordításának nehézségei, illetve a CAA rekordok használatának lehetőségei.

2. **Adatvédelmi és biztonsági aggályok** 16.67% (1 komment)

Témakörként merült fel a kormányzati tanúsítványhatóságok (CA) kötelező elfogadásának kockázatai, illetve a külső szereplők vagy kormányzati ügynökségek általi visszaélések veszélyeinek lehetősége is. Fókuszban a felhasználók magánéletének és biztonságának veszélyeztetése.

3. **Megfigyeléssel és kontrollal kapcsolatos félelmek** 16.67% (1 komment)

A fentiekhez valamennyire kapcsolódik a kormányzati megfigyelés lehetőségének kockázata, illetve a demokrácia fokozatos leépülésének veszélye a rendszer által, továbbá néhányan a diktatórikus rendszerekhez hasonlították.

Összegzés

Az EU eIDAS szabályozás - különösen a böngészőkre vonatkozó tanúsítványhatósági követelmények aggályokat kelt a felhasználók körében. A hozzászólók többsége technikai szempontból közelíti meg a kérdést, de az adatvédelmi és megfigyelési aggályok is megjelennek. Figyelemreméltó, hogy pozitív vélemény gyakorlatilag nem található a mintában, ami arra utal, hogy a szabályozás bevezetésével kapcsolatos kommunikáció nem volt képes meggyőzni a felhasználókat annak előnyeiről.

A technikai kérdések dominanciája azt jelzi, hogy a hozzászólók jelentős része szakértő vagy technikai érdeklődésű felhasználó, akik értik a szabályozás mélyebb technikai implikációit is.

Az eIDAS szabályozással kapcsolatos YouTube-kommentek elemzése azt mutatja, hogy a technikai közösség jelentős aggályokat fogalmaz meg a szabályozás adatvédelmi és biztonsági implikációival kapcsolatban. A hozzászólók döntő többsége semleges vagy negatív véleményt fogalmaz meg, és különösen kritikusak a kormányzati tanúsítványhatóságok kötelező elfogadásának követelményével szemben.

2. videó

Videó címe: " The European Digital Identity Wallet is coming

Csatorna: DigitalEU

Eredeti videó linkje: https://www.youtube.com/watch?v=AynHulTaafk&ab_channel=DigitalEU

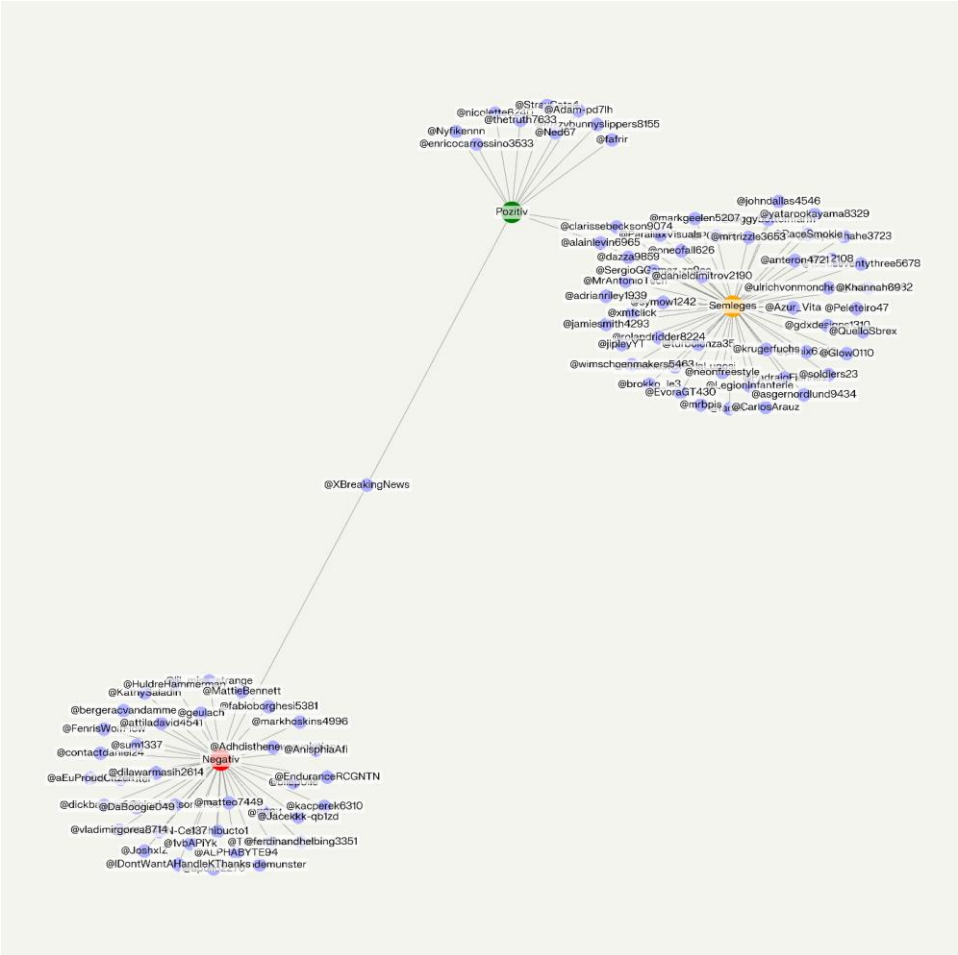
Feltöltés ideje: 2023 június 19.

Nézettség: 21,944 (2025. május 11-i állapot szerint)

Elemzett kommentek száma: 100 db

Szentiment analízis

- **Negatív**: 43.0% (43 komment)
- **Semleges**: 48.0% (48 komment)
- **Pozitív**: 9.0% (9 komment)



11. ábra Szentiment analízis eiDAS 2.0 2. videó (saját szerkesztés)

A kommentek túlnyomó többsége vagy elutasító, vagy legjobb esetben is semleges, pozitív reakciók csak elvétve fordulnak elő.

Főbb témakörök

A tartalomelemzés során öt markáns témakört azonosítottam, melyek gyakoriságát és jellemző mintázatait az alábbiakban részletezem:

1. Adatvédelmi és biztonsági aggályok 18.% (18 komment)

Ez a kategória magában foglalja a személyes adatok központosításával, tárolásával és védelmével kapcsolatos aggodalmakat.

2. Megfigyeléssel és kontrollal kapcsolatos félelmek 19% (19 komment)

A kommentek jelentős része a rendszert a túlzott állami kontroll eszközeként értelmezi.

3. Politikai kritika 8% (8 komment)

Számos komment kétségbe vonja a kezdeményezés demokratikus legitimitását.

4. Technikai kérdések és alternatívák 7% (7 komment)

Gyakorlati problémák és alternatív megoldások felvetése.

5. Ironikus és szarkasztikus megjegyzések 7% (7 komment)

Gúnyos hangnemű reakciók a videó tartalmára és a kezdeményezésre.

Összegzés

A kommentek túlnyomóan negatív vagy semleges hangvétele jól illeszkedik a korábbi tanulmányok megállapításaihoz, amelyek szerint az új technológiák, különösen a személyes szférát érintő megoldások bevezetésével szemben általában erős a kezdeti ellenállás. Az EU digitális személyazonosító kezdeményezése ellenállásba ütközik a kommentelők körében, ami összhangban van a szakirodalomban megfogalmazott aggályokkal. A negatív reakciók aránya (43%) és a semleges kommentek nagy száma (48%) azt jelzi, hogy az EU-nak hatékonyabban kellene kommunikálnia a rendszer előnyeit, valamint kezelnie a felmerülő adatvédelmi, biztonsági és hozzáférési aggályokat.

A digitális személyazonosító rendszer sikeres implementációjához elengedhetetlen lenne a szélesebb társadalmi párbeszéd, a demokratikus legitimitás erősítése és a felhasználói aggodalmak megfelelő kezelése.

Végezetül a digitális állampolgársággal, mint fogalommal kapcsolatos videó kommentjeinek elemzését fogom bemutatni, amely egy árnyaltabb képet fogalmaz meg a fenti főként semleges és negatív attitűdök mellett.

Videó címe: Make Digital Citizenship about the Do's, not the Don'ts

Csatorna: ISTE

Eredeti videó linkje: https://www.youtube.com/watch?v=tZeNr1q5QTU&ab_channel=ISTE

Feltöltés ideje: 2019. augusztus 27.

Nézettség: 67,169 (2025. május 11-i állapot szerint)

Elemzett kommentek száma: 12

Szentiment analízis

A 12 kommentből álló minta szentiment szerinti megoszlása:

- **Pozitív:** 10 komment (83%)
- **Semleges:** 2 komment (17%)
- **Negatív:** 0 komment (0%)

A kommentek túlnyomó többsége pozitív hangvételű. A semleges kommentek inkább leíró jellegűek, például: „Interesting to be a digital citizen in a digital community." Negatív szentiment nem jelent meg a mintában.

Főbb témakörök

A kvalitatív tartalomelemzés alapján az alábbi fő témakörök azonosíthatók:

1. Pozitív, cselekvésorientált digitális állampolgárság szemlélet 50% (6 komment)

A kommentelők kiemelik, hogy a videó nem a tiltásokat hangsúlyozza, hanem a helyes, kívánatos online viselkedésre fókuszál, ez a szemlélet segít a diákoknak a digitális térben való magabiztos eligazodásban.

2. Oktatási alkalmazhatóság 25% (3 komment)

A videót tanárok és oktatók is ajánlják, akik szerint a tartalom jól használható a digitális állampolgárság tanításához különböző korosztályokban.

3. Személyes élmények, közösségi élmény 8,3% (1 komment)

Több kommentelő személyes tapasztalatot oszt meg arról, hogyan használta a videót (pl. munkahelyi szünetben, playlisten, tanításban).

4. Forráskritika és hitelesség 8,3% (1 komment)

A kommentelők értékelik, hogy a videó készítője forrásokat is megjelöl, ezzel is növelve a tartalom hitelességét.

5. Nyelvi és kulturális diverzitás 8,3% (1 komment)

A kommentek között spanyol nyelvű hozzászólás is megjelenik, ami a digitális állampolgárság globális relevanciáját mutatja.

Összegzés

A kommentek alapján a vizsgált videó egyértelműen pozitív fogadtatásban részesült, különösen az oktatási közösség körében. A szentiment és témakörelemzés eredményei alapján a digitális állampolgárság témája ebben a mintában inspiráló, gyakorlatias és közösségépítő diskurzust generált.

Következtetések

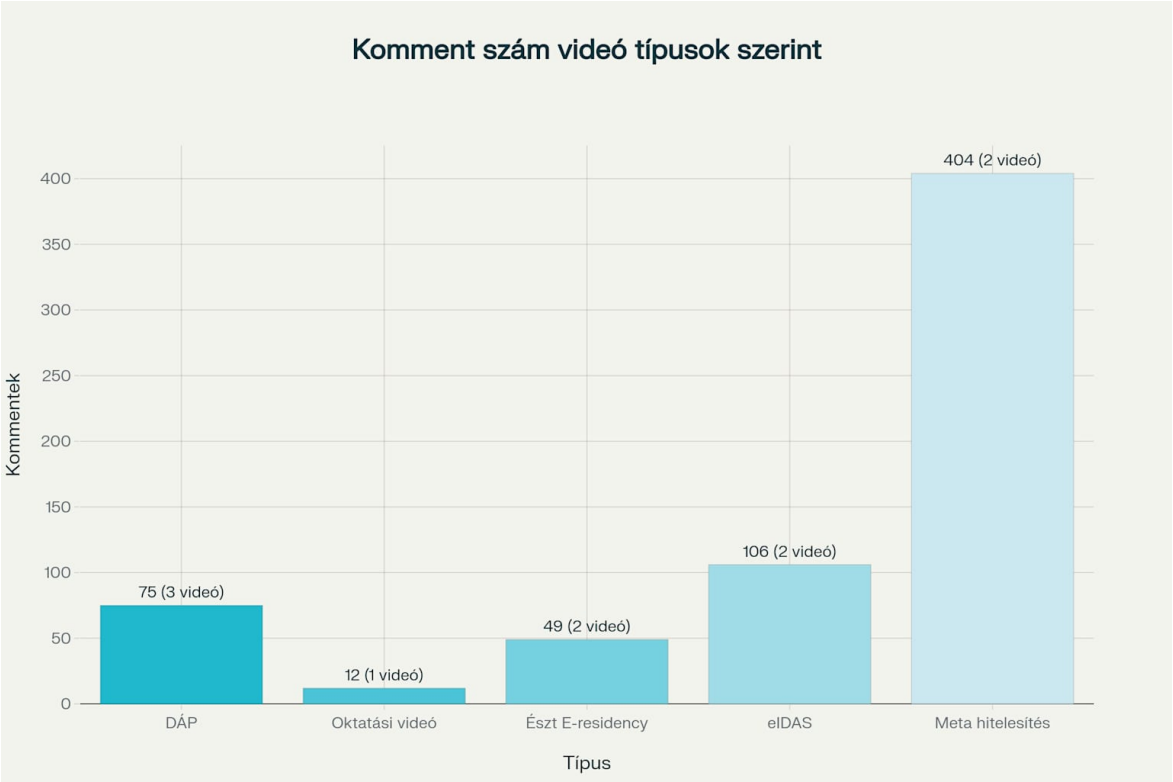
A digitális technológiák exponenciális fejlődésével a személyazonosítási és személyi hitelesítési megoldások alapvető fontosságúvá váltak mind a magán-, mind az állami szektorban. E technológiák fejlődése a hagyományos jelszóalapú módszerektől a korszerű biometrikus és eszközalapú megoldások felé tolódott, miközben az adatvédelem, a felhasználói élmény és a biztonsági követelmények közötti egyensúly megtalálása folyamatos kihívást jelent.

A rendelkezésre álló információk alapján egyértelműen kirajzolódik, hogy a biometrikus azonosítás vált az egyik legmeghatározóbb trenddé a személyazonosítási technológiák területén. A biometrikus hitelesítési módszerek – különösen az ujjlenyomat-felismerés, arcfelismerés és hangalapú azonosítás – széles körben elterjedtek szinte minden vizsgált szektorban.

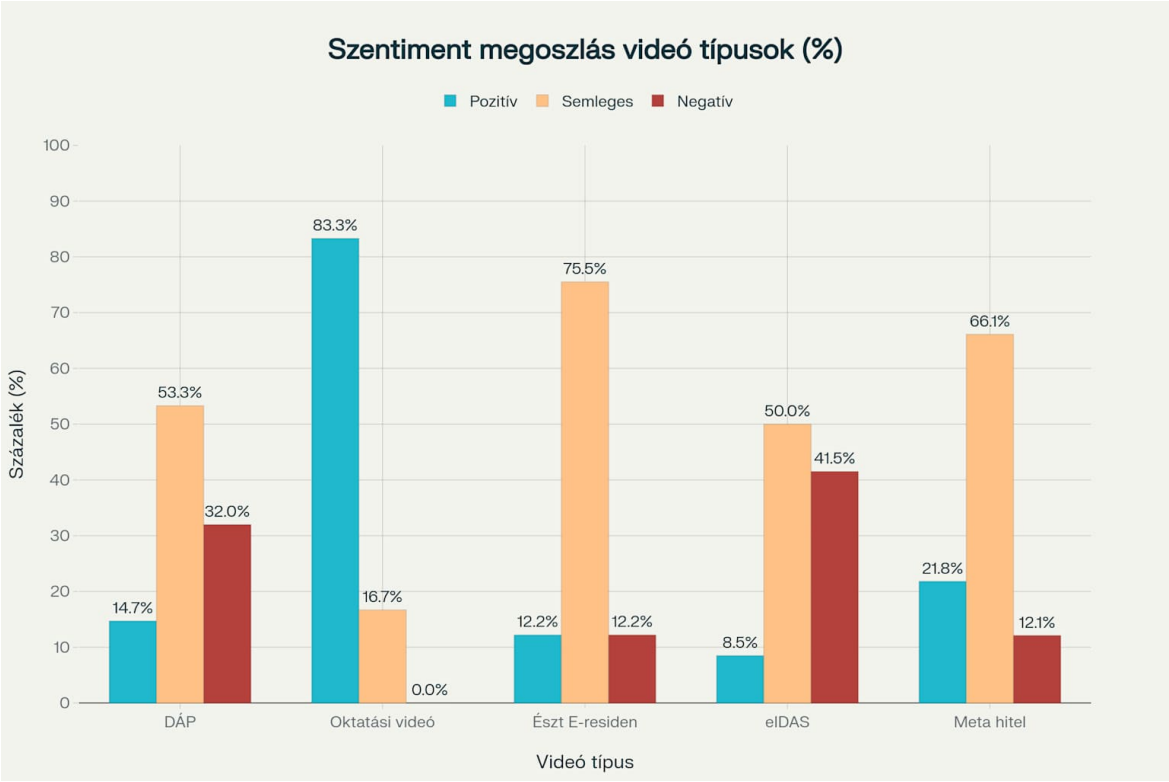
A személyazonosítási és hitelesítési technológiák alkalmazása számos előnyt kínál, ugyanakkor kihívásokkal is, de a jelenlegi kihívások ellenére több ígéretes innováció figyelhető meg a személyazonosítási és hitelesítési technológiák területén: A jövő szempontjából kritikus fontosságú lesz a biztonság és a felhasználói élmény közötti egyensúly megtalálása. A jelszómentes hitelesítés, a több modalitású biometrikus rendszerek, az önazonos identitás modellek és a kvantumrezisztens kriptográfia ígéretes megoldásokat kínálnak, amelyek fokozhatják a biztonságot anélkül, hogy rontanák a felhasználói élményt.

Végezetül, a szektorok közötti szabványosítás és együttműködés elengedhetetlen lesz a fragmentáció csökkentéséhez és a felhasználói élmény javításához. Az olyan kezdeményezések, mint az EU Digitális Személyazonosság Pénztárca, amely 2026-ra tervezi teljes bevezetését, fontos lépéseket jelentenek ebbe az irányba.

A digitális identitás technológiák YouTube videóinak kommentjei érdekes képet nyújtanak a különböző megoldások társadalmi fogadtatásáról. Az elemzés négy fő technológiai kategóriát vizsgált: a magyar DÁP rendszert, oktatási tartalmakat, az észt e-Residency programot, az EU eIDAS szabályozást, valamint a Meta hitelesítési szolgáltatását. Az összesen 646 komment mélyreható szentiment és tematikus elemzése jelentős különbségeket tárt fel az egyes technológiák megítélésében.



12. ábra YouTube videók alatti kommentszám (saját szerkesztés)



13. ábra Összesített szentiment megoszlás (saját szerkesztés)

A magyar digitális állampolgársági platform három videó alatt összesen 75 kommentet generált, ami viszonylag alacsony szám. A szentiment megoszlás kifejezetten negatív képet mutat: mindössze 11 komment (14,7%) volt pozitív, 40 komment (53,3%) semleges, míg 24 komment (32,0%) egyértelműen negatív hangvételű volt.

A tematikus elemzés aggasztó tendenciákat tár fel a DÁP társadalmi fogadtatásában. Az adatvédelmi és biztonsági aggályok dominálják a diskurzust 21 kommenttel (28,0%), ezt követik a megfigyeléssel és kontrollal kapcsolatos félelmek 18 kommenttel (24,0%). Jelentős a politikai kritika jelenléte 12 kommenttel (16,0%), valamint az ironikus és szarkasztikus megjegyzések száma 13 kommenttel (17,3%). A technikai kérdések és alternatívák csak 11 kommentet (14,7%) képviselnek, ami arra utal, hogy a felhasználók kevésbé a gyakorlati megvalósítással, mint inkább a koncepcionális elutasítással foglalkoznak.

Észt e-Residency - Pragmatikus Megközelítés

Az észt digitális rezidens program két videója alatt 49 komment született, amelyek túlnyomórészt pragmatikus megközelítést tükröznek. A szentiment megoszlás kiegyensúlyozott: 6 pozitív (12,2%), 37 semleges (75,5%) és 6 negatív komment (12,2%). A tematikus elemzés szerint a technikai és eljárási kérdések dominálják a diskurzust 21 kommenttel (42,9%), ami azt jelzi, hogy a felhasználók elsősorban a gyakorlati megvalósítás iránt érdeklődnek. Az adatvédelmi aggályok csak 5 kommentet (10,2%) tesznek ki, ami azt sugallja, hogy az észt modell nagyobb bizalmat élvez a felhasználók körében.

eIDAS

Az EU eIDAS szabályozást bemutató két videó 106 kommentet vonzott. A szentiment megoszlás kedvezőtlen: mindössze 9 pozitív (8,5%), 53 semleges (50,0%), de 44 negatív komment (41,5%) is született. A tematikus elemzés az elutasítás okait tárja fel: a megfigyeléssel és kontrollal kapcsolatos félelmek 20 kommenttel (18,9%) vezetik a listát, szorosan követve az adatvédelmi és biztonsági aggályokat 19 kommenttel (17,9%). A technikai kérdések 11 kommenttel (10,4%), a politikai kritika 8 kommenttel (7,5%) is szerepet kapnak. Ez a mintázat arra utal, hogy az EU-s digitális identitás kezdeményezés jelentős társadalmi ellenállásba ütközik.

Meta Hitelesítés

A Meta hitelesítési szolgáltatást bemutató két videó messze a legtöbb kommentet generálta: 404 darabot. A szentiment megoszlás viszonylag kiegyensúlyozott: 88 pozitív (21,8%), 267 semleges (66,1%) és 49 negatív komment (12,1%). A tematikus elemzést azonban az "Egyéb" kategória 189 kommentje (46,8%) uralja, ami a diskurzus fragmentált jellegét mutatja. Az üzleti érték és megtérülés 88 kommenttel (21,8%) a második legfontosabb téma, amit a technikai kérdések 51 kommenttel (12,6%) követnek. Az adatvédelmi aggályok csak 24 kommentet (5,9%) tesznek ki.

Oktatási Videó - Kimagasló Pozitív Fogadtatás

Az egyetlen elemzett oktatási videó ("Make Digital Citizenship about the Do's, not the Don'ts") rendkívül pozitív fogadtatásban részesült. A 12 kommentből 10 (83,3%) pozitív volt, 2 (16,7%) semleges, és egyetlen negatív vélemény sem jelent meg.
A tematikus megoszlás is egyértelműen konstruktív: a pozitív, cselekvésorientált digitális állampolgárság szemlélet 6 kommenttel (50,0%) vezeti a listát, ezt követi az oktatási alkalmazhatóság 3 kommenttel (25,0%).

A különböző digitális identitás technológiák társadalmi fogadtatásában markáns különbségek figyelhetők meg. Az oktatási tartalom kivételes pozitivitása (83,3%) éles kontrasztot képez az állami/EU-s megoldások elutasításával. A DÁP (32,0% negatív) és az eIDAS (41,5% negatív) jelentős társadalmi ellenállást váltanak ki, míg a kereskedelmi Meta szolgáltatás (12,1% negatív) pragmatikusabb megítélést kap.

A tematikus elemzés szerint az adatvédelmi és biztonsági aggályok, valamint a megfigyelési félelmek központi szerepet játszanak az állami technológiák elutasításában. A kutatás eredményei arra utalnak, hogy a digitális identitás technológiák társadalmi elfogadottsága jelentősen függ a kibocsátó intézmény megítélésétől és a kommunikációs stratégiától.

A határellenőrzési rendszerek fejlődése közvetlenül kapcsolódik a nemzetbiztonsági feladatokhoz és a terrorizmus elleni küzdelemhez. A magánszférában alkalmazott technológiák elemzése fontos a civil-katonai technológiatranszfer megértéséhez A közösségi média platformok biztonsági kihívásai különösen relevánsak az információs

műveletek és a kognitív műveletek szempontjából. A fejezet által bemutatott nemzetközi gyakorlatok összehasonlítása segíti a magyar védelmi szektor technológiai fejlesztési irányainak meghatározását.

5 SZEMÉLYAZONOSÍTÁSRA ÉS HITELESÍTÉSRE ALKALMAS TECHNOLÓGIA ALKALMAZÁSÁNAK JÖVŐBELI LEHETŐSÉGEI

A feldolgozott szakirodalom alapján a mobilalkalmazások egyre inkább digitális identitástárcaként fognak szolgálni, biztonságosan tárolva több hitelesítő adatot és zökkenőmentes hitelesítést biztosítva a szolgáltatások között. Az Európai Digitális Identitás Pénztárca kezdeményezés példázza ezt a trendet, amelynek célja, hogy 2026-ra lehetővé tegye az EU polgárai számára, hogy digitálisan azonosítsák magukat és elektronikus dokumentumokat tároljanak. A határokon átnyúló identitás megoldások is feltörekvőben vannak, a nemzetközi szabványok elősegítik a különböző nemzeti rendszerek közötti interoperabilitást. Az eIDAS rendelet Európában keretet biztosít az ilyen interoperabilitás számára, a frissített eIDAS 2.0 pedig további követelményeket vezet be a digitális identitásra vonatkozóan.[577]

A szabályozási keretek továbbra is fejlődnek, az Általános Adatvédelmi Rendelet (GDPR) szigorú követelményeket támaszt a személyes adatok kezelésére, különösen a biometrikus információkra vonatkozóan. Az EU Mesterséges Intelligencia Törvénye a biometrikus azonosító rendszereket "magas kockázatúnak" minősíti, szigorú követelményeknek vetve alá őket.[578]

5.1 Államilag fejlesztett eszköz általi hitelesítés

Mivel a hagyományos azonosítási módszereket egyre inkább felváltják a kifinomult digitális és biometrikus megoldások, a kormányok világszerte innovatív megközelítéseket vizsgálnak az okos eszközök segítségével történő személyazonosítás területén. A kormányzati azonosítási rendszerek evolúciója nem csupán technológiai váltást jelent, hanem az állampolgárok és a közszolgáltatások közötti interakció alapvető átalakulását. A biztonságot, kényelmet és bizalmat egyensúlyban tartó sikeres implementáció érdekében elengedhetetlen a technológiai lehetőségek és a társadalmi elfogadottsági kihívások megértése.

A kormányzat által fejlesztett digitális azonosítási rendszerek eltérnek összetettségükben és implementációs megközelítéseikben. A magyarországi Digitális Állampolgárság Program (DÁP) egy modern megközelítést példáz, amely 2025 januárjától váltja

[577] Union, *eIDAS Regulation: Trust Services and Electronic Identification*.
[578] European Parliament, *Artificial Intelligence Act* (Brussels: European Parliament, 2023).

fel a korábbi Ügyfélkapu rendszert. A DÁP mobilalkalmazás lehetővé teszi az állampolgárok számára, hogy biometrikus hitelesítéssel férjenek hozzá a kormányzati szolgáltatásokhoz a hagyományos felhasználónév és jelszó kombinációk helyett, amely előrelépést jelent a kormányzati azonosítási technológiákban.[579]

5.1.1 Feltörekvő biometrikus technológiák a kormányzati alkalmazásokban

A kormányzati azonosítási rendszerek egyre inkább a multimodális biometrikus megoldások felé mozdulnak, ezen rendszerek jellemzően különböző biometrikus jellemzőket kombinálnak, például ujjlenyomatokat, arcfelismerést, íriszmintákat és hangmintákat. A kutatások szerint ezeknek a modalitásoknak a kombinálása akár 80%-kal is csökkentheti a hibaarányokat az egyetlen modalitást alkalmazó rendszerekhez képest.[580] A kormányzati alkalmazások esetében, ahol a biztonság kiemelt fontosságú, ezek a fejlesztések előnyöket jelentenek.

5.1.2 Fejlett prezentációs támadásdetektálás

Ahogy a biometrikus rendszerek egyre elterjedtebbé válnak a kormányzati alkalmazásokban, úgy válnak egyre kifinomultabbá a kijátszásukra tett kísérletek is. A fejlett prezentációs támadásdetektáló (PAD) rendszerek kifinomult mesterséges intelligencia algoritmusokat alkalmaznak a finom jelek, például mikro kifejezések elemzésére, hogy hatékonyan megkülönböztessék a legitim felhasználókat a csalási kísérletektől. Ezek a rendszerek képesek észlelni és blokkolni a rögzítési ponton történő kísérleteket, biztosítva a kormányzati azonosítási folyamatok integritását.[581] Az ISO/IEC 30107 szabványok keretet biztosítanak a biometrikus prezentációs támadások felismeréséhez, a folyamatos fejlesztések pedig az életképesség-detektálásra és a spoofing elleni intézkedésekre összpontosítanak, amelyek egyre fontosabbá válnak a kormányzati implementációk számára.[582]

---

[579] „DÁP – AAM Consulting”, elérés 2025. május 4., https://aam.hu/fresh_news/dap.
[580] „Multimodal Biometric Systems: A Comparative Study”, *International Journal of Biometrics*, 2022.
[581] I.E.E.E.Transactions on, „Information Forensics and Security, "Advanced Presentation Attack Detection in Biometric Systems”, 2023.
[582] „ISO/IEC 30107, "Biometric Presentation Attack Detection Standards”, 2022.

5.1.3 Peremhálózati számítástechnika a biztonságos biometrikus adatfeldolgozáshoz

A peremhálózati számítástechnika (edge computing) biometrikus adatfeldolgozásra történő alkalmazása előnyöket kínál a közszféra implementációi számára. Az eszközön történő ellenőrzés révén, a felhőalapú feldolgozás helyett, ez a megközelítés csökkenti a késleltetést, növeli az adatvédelmet a központi szerverekre történő adatátvitel minimalizálásával, és hatékonyabb valós idejű hitelesítést tesz lehetővé. Az iparági elemzők előrejelzése szerint 2025-re a vállalatok által generált adatok több mint 75%-át a hálózat peremén dolgozzák fel, ami növekedés a 2018-as 10%-hoz képest.[583]

A kormányzati alkalmazások esetében, ahol az adatok szuverenitása és biztonsága kritikus szempont, a peremhálózati számítástechnika meggyőző megoldást kínál azáltal, hogy az érzékeny biometrikus adatokat a felhasználó eszközén tartja, ahelyett, hogy hálózatokon keresztül továbbítaná, vagy központosított adatbázisokban tárolná azokat.

5.1.4 Mesterséges intelligencia integráció és folyamatos hitelesítés

A mesterséges intelligencia és a gépi tanulás alapvetően átalakítják a kormányzati biometrikus rendszereket. A mély tanulási algoritmusok javították az arc-, ujjlenyomat- és írisz-felismerő rendszerek pontosságát. Ezen algoritmusok implementálása az elmúlt öt évben 30-40%-os javulást eredményezett a biometrikus rendszerek pontosságában.[584]

Az egyszerű időponti hitelesítésen túl a mesterséges intelligencia lehetővé teszi a folyamatos hitelesítést a viselkedési biometria révén, elemezve a felhasználók eszközhasználati mintáit. A kutatások szerint ezek a rendszerek akár 95%-os pontosságot is elérhetnek valós alkalmazásokban.[585] A kormányzati alkalmazások kihasználhatják ezeket a technológiákat érzékeny információkhoz és szolgáltatásokhoz való biztonságos hozzáférés érdekében, fenntartva a biztonságot a teljes munkamenet során, nem csak bejelentkezéskor.

[583] I.D.C., „Worldwide Edge Computing Forecast", 2021.
[584] Acuity Market Intelligence, „The Global Biometrics and Digital Identity Analyst", 2022.
[585] BehavioSec, „Behavioral Biometrics Market Analysis", 2022.

5.1.5 Blokklánc és önszuverén identitás

Több kormány is vizsgálja a blokklánc-alapú azonosítási megoldásokat, beleértve Svájc, Kanada és Hollandia kezdeményezéseit. Ezek a rendszerek megváltoztathatatlan nyilvántartást biztosíthatnak, miközben nagyobb ellenőrzést adnak az állampolgároknak személyes adataik felett, potenciálisan növelve a kormányzati azonosítási rendszerekbe vetett bizalmat.

5.2 Jövőbeli fejlesztési irányok és ajánlások

Az alábbi alfejezetben az elvégzett forráselemzés, illetve a szakértői interjúk eredményei alapján feltárt feltörekvő trendek, technológiák kerülnek bemutatásra.

5.2.1 Kvantumrezisztens kriptográfia

A kvantumszámítástechnika fejlődése kihívásokat és lehetőségeket egyaránt jelent a kormányzati hitelesítési technológiák számára. A kormányzati azonosítási rendszereknek fel kell készülniük a kvantumfenyegetésekre azáltal, hogy a nagyszabású kvantumszámítógépek megjelenése előtt kvantumrezisztens kriptográfiát implementálnak. Ez a proaktív megközelítés elengedhetetlen az állampolgári identitásadatok hosszú távú biztonságának fenntartásához.[586]

5.2.2 Folyamatos hitelesítés és zéró bizalom architektúra

A jövőbeli kormányzati azonosítási rendszerek valószínűleg túllépnek az időponti hitelesítésen a zéró bizalom architektúrákon belüli folyamatos ellenőrzés felé. Ahelyett, hogy a bejelentkezéskor egyszer hitelesítenének, a rendszerek folyamatosan ellenőrzik a felhasználó identitását a munkafolyamatok során viselkedési minták, helyszín, eszközjellemzők és egyéb kontextuális tényezők alapján. Ez a megközelítés felismeri, hogy a hitelesítés nem egyszeri esemény, hanem folyamatos folyamat, különösen az érzékeny kormányzati szolgáltatásokhoz vagy információkhoz való hozzáférés esetén.[587]

---

[586] *Transition to Post-Quantum Cryptography* (Bonn: Federal Office for Information Security, 2024).
[587] N.C.B.I., „Security, Privacy, and Usability in Continuous Authentication: A Survey", *PMC* 8434648 (2021), https://pmc.ncbi.nlm.nih.gov/articles/PMC8434648/.

5.2.3 Befogadó tervezés és hozzáférhetőség

A jövőbeli fejlesztéseknek kezelniük kell a digitális szakadékot, és alternatív hitelesítési módszereket kell biztosítaniuk a fogyatékkal élő állampolgárok, a korlátozott technológiai hozzáféréssel rendelkezők vagy az alacsony digitális műveltséggel rendelkezők számára.

A személyazonosítás és hitelesítés technológiáinak jövőjét a kormányzati szektorban a biometrikus technológiák fejlődése, a mesterséges intelligencia integrációja és az okoseszköz-alkalmazások fogják alakítani. Ezek a fejlesztések várhatóan átalakítják az állampolgár-állam interakciókat, potenciálisan biztonságosabb, kényelmesebb és személyre szabottabb kormányzati szolgáltatásokat kínálva. Azonban ezeknek a rendszereknek a sikere nem csak a technológiai kifinomultságon, hanem a társadalmi elfogadottsági tényezőkön is múlik, különösen a kormányzati intézményekbe vetett bizalmon és az észlelt adatvédelmi védelmeken. Az adatvédelmi aggályok kezelésével, a befogadó hozzáférés biztosításával és az állampolgárok számára nyújtott egyértelmű érték demonstrálásával a kormányok előmozdíthatják a széles körű elfogadáshoz szükséges bizalmat.

5.3 Magánszektor által fejlesztett eszköz általi hitelesítés

A magánszektorbeli azonosítási rendszerek evolúciója nem csupán technológiai váltást jelent, hanem alapvető átalakulást abban, ahogyan a felhasználók hitelesítik magukat és férnek hozzá a szolgáltatásokhoz. A biztonságot, a felhasználói élményt és az adatvédelmet egyensúlyban tartó stratégiák kialakításához elengedhetetlen a technológiai lehetőségek és a társadalmi elfogadási kihívások átfogó megértése. Az elmúlt évtizedben a magánszektor átalakította az azonosítási technológiák területét. A pénzügyi szolgáltatások, az egészségügy, az e-kereskedelem és a vállalati biztonság élenjáró szerepet töltött be a hagyományos jelszó-alapú rendszereken túlmutató fejlett azonosítási technológiák bevezetésében.

A biometrikus technológiák magánszektorbeli fejlesztése több egyértelmű jövőbeli fejlődési irányt mutat. A multimodális biometria – több biometrikus tényező kombinálása a biztonság és megbízhatóság növelése érdekében – az egyik legígéretesebb

megközelítést jelenti. A magánszektor olyan alkalmazásai számára, mint a banki szolgáltatások, az egészségügy és a vállalati hozzáférés-ellenőrzés, ezek a fejlesztések előnyöket jelentenek mind a biztonság, mind a felhasználói élmény szempontjából.

Ahogy a biometrikus rendszerek egyre elterjedtebbé válnak a magánszektorbeli alkalmazásokban, úgy válnak kifinomultabbá a megkerülésükre tett kísérletek is. A fejlett prezentációs támadásfelismerő (PAD) rendszerek kifinomult mesterséges intelligencia algoritmusokat alkalmaznak a mikro kifejezésekhez hasonló finom jelek elemzésére, hogy hatékonyan megkülönböztessék a legitim felhasználókat a csalási kísérletektől. Ezek a rendszerek a rögzítési ponton észlelhetik és blokkolhatják a kísérleteket, biztosítva a hitelesítési folyamat integritását.

A magánszektorbeli hitelesítés talán legérdekesebb és a legnagyobb lehetőségekkel kecsegtető fejlesztése a viselkedési biometria és a folyamatos hitelesítés felé történő elmozdulás. A hagyományos hitelesítési rendszerek csak meghatározott ellenőrzési pontokon (jellemzően bejelentkezéskor) ellenőrzik az identitást, ezzel sebezhetővé téve a rendszereket a kezdeti ellenőrzés után. A viselkedési biometrikus rendszerek folyamatosan elemzik, hogyan lépnek interakcióba a felhasználók az eszközeikkel – vizsgálva a gépelési ritmust, az érintőképernyő nyomását, a lapozási gesztusokat, a navigációs mintákat, sőt azt is, hogyan tartják az eszközt. A pénzintézetek voltak e technológia korai alkalmazói, olyan vállalatok, mint a HSBC, a JPMorgan Chase és a Barclays, viselkedési biometriát alkalmaznak a potenciálisan csalárd tevékenységek észlelésére, még akkor is, ha a helyes hitelesítő adatokat használják.

5.3.1 Okoseszköz-alkalmazások a magánszektorbeli hitelesítéshez

Digitális identitás pénztárcák

A magánszektor digitális identitás pénztárcái az azonosítási technológia egyik legígéretesebb fejlesztését jelentik. Ezek a mobilalkalmazások biztonságosan tárolnak több hitelesítő adatot, és zökkenőmentes hitelesítést tesznek lehetővé különböző szolgáltatások között. A pénzintézetek élenjárók e technológiák fejlesztésében, olyan kezdeményezésekkel, mint a FIDO (Fast Identity Online) Alliance, amely a jelszó nélküli hitelesítés szabványait népszerűsíti.[588]

[588] Alliance, *FIDO2: Web Authentication*.

Vállalati identitáskezelő platformok

A vállalati digitális identitás megoldások fejlődnek, hogy kielégítsék a távoli és hibrid munkaerő igényeit. A vállalati identitáskezelő platformok integrálódnak az emberi erőforrás rendszerekkel, a projektmenedzsment eszközökkel és a biztonsági infrastruktúrával, zökkenőmentes hozzáférést biztosítva, miközben megőrzik a robusztus biztonsági vezérlőket.

Ezek a platformok egyre inkább kontextuális és kockázatalapú hitelesítést alkalmaznak, változtatva a biztonsági követelményeket olyan tényezők alapján, mint a helyszín, az eszköz jellemzői, a hálózati feltételek és a kért erőforrás érzékenysége. Ez a dinamikus megközelítés optimalizálja mind a biztonságot, mind a felhasználói élményt azáltal, hogy csak a kockázatértékelés által indokolt esetekben alkalmaz szigorúbb követelményeket.

Mobil hitelesítő adatok és virtuális hozzáférési kártyák

A fizikai beléptető rendszerek egyre inkább integrálódnak a mobil hitelesítő adatokkal, lehetővé téve, hogy az okos telefonok helyettesítsék a hagyományos belépőkártyákat. Ezek a megoldások jellemzően közelítéses kommunikációt (NFC), Bluetooth Low Energy (BLE) vagy ultrahangos átvitelt használnak a beléptető rendszerekkel való kommunikációra, érintésmentes belépést biztosítva a létesítményekbe, miközben fenntartják vagy növelik a biztonságot.

A mesterséges intelligencia és a gépi tanulás alapvetően átalakítja a magánszektor hitelesítési rendszereit. Ezen algoritmusok javulást eredményezett a biometrikus rendszerek pontosságában. A pontosság javításán túl az MI teljesen új megközelítéseket tesz lehetővé a hitelesítésben, amelyek korábban lehetetlenek voltak. Az IBM Security kutatása szerint az MI-vezérelt adaptív hitelesítés akár 70%-kal csökkentheti a legitim felhasználók hitelesítési súrlódását, miközben 30%-kal növeli a csalási kísérletek észlelését.[589] A mesterséges intelligencia által támogatott anomália-felismerés egyre kifinomultabbá vált a szokatlan minták azonosításában, amelyek csalárd hozzáférési kísérletekre utalhatnak. Ezek a rendszerek alapvető viselkedési profilokat hoznak létre a

[589] I.B.M. Security, „The State of Authentication 2023", 2023.

legitim felhasználók számára, és jelzik azokat az eltéréseket, amelyek fiókátvételi kísérletekre utalhatnak, még akkor is, ha a helyes hitelesítő adatokat adták meg. Ez a fejlesztés a biztonsági rendszerek egyik legtöbb kihívását kezeli – a csalárd tevékenységek felismerése és a legitim felhasználói súrlódás minimalizálása közötti egyensúly megteremtését.[590]

A természetes nyelvfeldolgozással kombinált hangbiometria egy kialakulóban lévő hitelesítési csatornát képvisel, amely különösen releváns az ügyfélszolgálati alkalmazások esetében. Ezek a rendszerek természetes beszélgetés során ellenőrizhetik az azonosságot, anélkül, hogy explicit hitelesítési lépéseket vagy biztonsági kérdéseket igényelnének. pénzintézetek és távközlési szolgáltatók implementálták ezeket a technológiákat az ügyfélszolgálati interakciókban a hitelesítési súrlódás csökkentése érdekében, miközben fenntartják az erős biztonsági szintet.[591]

A hitelesíthető tanúsítványok – digitálisan aláírt igazolások egy személy identitásáról, képesítéseiről vagy jogosultságairól – standardizálódnak olyan kezdeményezéseken keresztül, mint a W3C Verifiable Credentials Data Model. Ezek a tanúsítványok kriptográfiailag ellenőrizhetők anélkül, hogy kapcsolatba kellene lépni az eredeti kibocsátóval, lehetővé téve az adatvédelmet tiszteletben tartó személyazonosság-ellenőrzést. A hitelesíthető tanúsítványok standardizálása teljesen új üzleti modelleket teremt az identitás-ellenőrzés körül. Ahelyett, hogy minden szolgáltató függetlenül ellenőrizné az ügyfél információkat, specializált identitás-ellenőrző szolgáltatók bocsáthatnak ki olyan tanúsítványokat, amelyeket a felhasználók a digitális pénztárcájukban tárolnak, és szükség esetén bemutathatnak. Ez a megközelítés csökkenti a duplikációt, javítja az adatvédelmet, és potenciálisan méltányosabb hozzáférést biztosít a szolgáltatásokhoz.[592]

---

[590] Anil Veldurthi, „The Role of AI and Machine Learning in Fraud Detection for Financial Services", *Journal of Computer Science and Technology Studies* 7 (2025. május): 757–71, https://doi.org/10.32996/jcsts.2025.7.4.88.
[591] Jean-Francois Bonastre és mtsai., „Benchmarking and Challenges in Security and Privacy for Voice Biometrics", arXiv.org, elérés 2025. június 15., https://arxiv.org/abs/2109.00281v1.
[592] Marko Jurisic, Igor Tomicic, és Petra Grd, „User Behavior Analysis for Detecting Compromised User Accounts: A Review Paper", *Cybernetics and Information Technologies* 23 (2023. szeptember): 102–13, https://doi.org/10.2478/cait-2023-0027.

A peremhálózati számítástechnika forradalmasítja a biometrikus adatfeldolgozást a magánszektor alkalmazásaiban azáltal, hogy az eszközön történő ellenőrzést teszi lehetővé a felhőalapú feldolgozás helyett. Ez a megközelítés csökkenti a késleltetést, növeli az adatvédelmet a központi szerverekre történő adatátvitel minimalizálásával, és hatékonyabb, nagy áteresztőképességű valós idejű hitelesítést tesz lehetővé. A modern okos telefonok megbízható végrehajtási környezetei izolált feldolgozási környezetet biztosítanak az érzékeny biometrikus műveletekhez. Ezek a hardverszintű biztonsági funkciók megakadályozzák a biometrikus adatokhoz való hozzáférést még akkor is, ha az eszköz operációs rendszere kompromittálódik.

5.4 Állami és magán partnerségek és hibrid modellek, együttműködési keretrendszerek az identitás-ellenőrzéshez

A köz-magán partnerségek (PPP-k) az azonosítási és hitelesítési technológiák területén meggyőző előnyöket kínál a magánszektor innovációjának és a közszféra felügyeletének kombinálásával. A Világbank szerint a hibrid digitális azonosítási rendszerek 25-40%-kal költséghatékonyabbak lehetnek, mint a kizárólag magán vagy állami rendszerek, miközben magasabb szintű innovációt és felhasználói elégedettséget biztosítanak.[593] A pénzintézetek különösen aktívak a PPP megállapodásokban, együttműködve a kormányzati ügynökségekkel az digitális identitás keretrendszerek fejlesztésében. A technológiai partnerségek, ahol magánvállalatok nyújtanak technikai megoldásokat egy kormányzati keretrendszeren belül, hatékonynak bizonyultak több régióban. A norvégiai BankID sikeres példát jelent, ahol egy magán banki konzorcium fejlesztett ki egy digitális identitás megoldást, amely nemzeti szabvánnyá vált mind a magán-, mind a közszolgáltatások számára. A rendszernek jelenleg több mint 4 millió felhasználója van – ami a norvég lakosság körülbelül 80%-a – és naponta több millió tranzakciót dolgoz fel.[594]

5.4.1 A hibrid megközelítések előnyei és kihívásai

A hibrid modellek több kulcsfontosságú előnyt kínálnak a tisztán magán vagy állami megközelítésekkel szemben:

[593] Digital Public Goods Alliance, „50-in-5 Campaign for Digital Public Infrastructure", 2023.
[594] „Nordic Innovation, "BankID Implementation Analysis: Lessons Learned", 2023.

1. A közszféra megbízhatóságának és szabályozási hatáskörének kombinálása a magánszektor innovációs képességeivel.
2. A fejlesztési költségek és a műszaki szakértelem megosztása a szektorok között.
3. Nagyobb felhasználói bázisok létrehozása, amelyek gyorsabban érik el a kritikus tömeget.
4. Következetes szabványok kialakítása a magán- és közszolgáltatásokon keresztül.
5. Befogadóbb megoldások létrehozása, amelyek különböző populációkat szolgálnak ki.

Azonban ezek a modellek egyedülálló kihívásokat is jelentenek. Az adatirányítási keretrendszereknek egyértelműen meg kell határozniuk a személyes információk védelmének felelősségét, és pontosan meg kell határozniuk az adatmegosztás korlátait. A sikeres PPP-k független felügyeleti mechanizmusokat hoznak létre az adatvédelmi előírásoknak és biztonsági szabványoknak való megfelelés biztosítására.[595]

A köz- és magánszféra ösztönzőinek összehangolása körültekintő tervezést igényel. A magánvállalatok a befektetés megtérülését és a versenyelőnyt helyezik előtérbe, míg a közszféra partnerei az univerzális hozzáférésre, a befogadásra és a hosszú távú fenntarthatóságra összpontosítanak. A fenntartható üzleti modelleknek egyensúlyba kell hozniuk ezeket a potenciálisan versengő prioritásokat.[596]

5.5 Stratégiák a társadalmi elfogadottság növelésére

Az azonosítási és hitelesítési technológiák magánszektorbeli fejlesztőinek felhasználóközpontú tervezési módszertanokat kell alkalmazniuk, amelyek a fejlesztési folyamat egészében visszajelzéseket építenek be.

Kulcsfontosságú tervezési elvek közé tartoznak:

1. Az információs követelmények progresszív közzététele
2. Minimális adatgyűjtés és a szükségesség átlátható magyarázata
3. Egyértelmű visszajelzés a hitelesítési folyamatok során
4. Különböző képességszintek és technológiai jártasság figyelembevétele

[595] Financial Action Task Force, „Public-Private Partnership in AML/CFT", 2022.
[596] „Public private partnership models (for public services)", elérés 2025. június 15., https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/public-private-partnerships?utm_source=chatgpt.com.

5. Kulturálisan érzékeny implementáció, amely tiszteletben tartja a különböző értékeket és normákat

A pénzügyi szolgáltatási vállalatok, amelyek implementálták ezeket az elveket, nemcsak magasabb elfogadási arányokról számolnak be, hanem a hitelesítéssel kapcsolatos ügyfélszolgálati megkeresések csökkenéséről is.[597]

5.5.1 Adatvédelmet erősítő implementációs stratégiák

A „privacy by design" (beépített adatvédelem) elveit a legkorábbi fejlesztési szakaszokba kell beépíteni. Ez a megközelítés az adatminimalizálást, a célhoz kötöttséget és a felhasználói kontrollt alapvető tervezési paraméterekként építi be, nem utólagos megfontolásként.[598]

Kommunikációs és oktatási kezdeményezések

Az adatkezelési gyakorlatokról szóló átlátható kommunikáció elengedhetetlen a biometrikus hitelesítésbe vetett bizalom kiépítéséhez. A vállalatoknak egyértelműen el kell magyarázniuk, hogy milyen biometrikus adatokat gyűjtenek, hogyan dolgozzák fel és tárolják azokat, és milyen konkrét biztonsági intézkedések védik ezeket az érzékeny információkat. Az oktatási kezdeményezések, amelyek segítenek a felhasználóknak megérteni a különböző hitelesítési technológiák előnyeit és korlátait, támogatják a tájékozott döntéshozatalt. Ezeknek a programoknak kezelniük kell a biometrikus biztonságról alkotott általános tévhiteket, és gyakorlati útmutatást kell nyújtaniuk a biztonságos használathoz.[599]

A független tanúsítás és a rendszeres biztonsági auditok demonstrálják a magas szintű szabványok fenntartása iránti elkötelezettséget. A harmadik fél általi validáció elismert hatóságoktól olyan hitelességet biztosít, amelyet a belső állítások önmagukban nem érhetnek el.

5.6 Internetes csalások elleni

A digitális szolgáltatások fokozott használata új lehetőségeket teremtett a hackerek számára, hogy kihasználják az azonosítási és hitelesítési rendszerek gyengeségeit. A

[597] Insider Intelligence, *Mobile Banking Adoption Report* (New York: eMarketer Inc, 2022).
[598] „Information Systems Research, "Privacy by Design: From Theory to Practice", 2022.
[599] Anthony Paul, „Biometric Data Security: Balancing Convenience with Privacy", 2024. május.

legfrissebb becslések szerint az online csalások globális veszteségei 2022-ben meghaladták a 10,3 milliárd dollárt, ami 47%-os növekedést jelent az előző évhez képest.[600] Ez az aggasztó tendencia új módszereket igényel a személyes azonosítás és ellenőrzés terén, különösen az okoseszköz-alkalmazásokon keresztül, amelyek egyedi előnyöket kínálnak a biztonság javításában, miközben biztosítják a felhasználók kényelmét. Az azonosítási és hitelesítési technológiák területe az utóbbi években átalakult, az alapvető jelszórendszerektől kezdve a fejlett többtényezős módszerekig, amelyek biometrikus és okoseszköz-funkcionalitásokat használnak. A hagyományos hitelesítési technikák elsősorban tudásalapú elemekre (a felhasználó által birtokolt információkra) támaszkodnak, mint például jelszavak és PIN-kódok. Bár ezek az eljárások évtizedek óta hagyományosak, gyengeségeket mutatnak. A mobilhitelesítés népszerűségre tett szert, mivel az okos telefonok egyre fejlettebb biometrikus érzékelőket integrálnak.

Ahogy a közösségi média platformok integrálódnak az e-kereskedelemmel, pénzügyi szolgáltatásokkal, sőt kormányzati funkciókkal is, a biztonságos, megbízható és felhasználóbarát azonosítási és hitelesítési technológiák fontossága megnőtt. A hagyományos felhasználónév-jelszó paradigma, amely hosszú ideje a digitális személyazonosság-ellenőrzés sztenderdje volt, egyre inkább elégtelennek bizonyul a kifinomult biztonsági fenyegetésekkel szemben, ami sürgető igényt teremt fejlettebb megoldásokra. A technológiai innovációk, implementációs stratégiák és társadalmi elfogadottsági tényezők feltárásával ez a tanulmány átfogó áttekintést kíván nyújtani arról, hogy ezek a technológiák hogyan alakítják át a felhasználói élményt és a platformbiztonságot a közösségi média környezetében.[601]

A közösségi média platformok kezdetben túlnyomórészt hagyományos, tudásalapú hitelesítési mechanizmusokra támaszkodtak, mint a felhasználónevek és jelszavak. Azonban ezek a módszerek sebezhetőséget mutattak különböző támadási vektorokkal szemben, beleértve az adathalászatot, a hitelesítő adatok újrafelhasználását és a brute force támadásokat. A kétfaktoros hitelesítés (2FA) és a többfaktoros hitelesítés (MFA) standard biztonsági gyakorlattá vált a közösségi média platformokon, kombinálva a

[600] Federal Bureau of Investigation, „Internet Crime Report 2022" (Federal Bureau of Investigation, 2023), https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.
[601] Pawel Szalachowski, „Password-authenticated Decentralized Identities" (arXiv, 2021. szeptember 16.), https://doi.org/10.48550/arXiv.2007.15881.

tudásalapú tényezőket (jelszavak) a birtoklásalapú tényezőkkel (jellemzően okos telefonok), és egyre inkább biometrikus tényezőket is bevonva. Ez az integráció lényegesen erősebb biztonságot nyújt, mint az egyfaktoros megközelítések, miközben a felhasználók meglévő eszközeit hasznosítja.[602]

A biometrikus technológiák fejlesztése a közösségi média hitelesítéshez több különböző jövőbeli pályát mutat. A multimodális biometria – több biometrikus tényező kombinálása a biztonság és megbízhatóság növelése érdekében – az egyik legígéretesebb megközelítést jelenti. A közösségi média platformok számára, amelyeknek egyensúlyt kell teremteniük a biztonság és a felhasználói élmény között a különböző felhasználói bázisokban, ezek a fejlesztések előnyöket kínálnak. Ahogy ezek a technológiák folyamatosan fejlődnek, a közösségi média platformok valószínűleg egyre kifinomultabb multimodális rendszereket fognak implementálni, amelyek egyidejűleg több biometrikus csatornán keresztül képesek azonosítani az identitást, így biztonságosabb, mégis súrlódásmentes hitelesítési élményeket teremtve.[603]

A közösségi médiában is egyre nagyobb teret kap a viselkedési biometria és a folyamatos hitelesítés. A hagyományos hitelesítési rendszerek csak meghatározott ellenőrzési pontokon (jellemzően bejelentkezéskor) ellenőrzik az identitást, ami a kezdeti ellenőrzés után sebezhetővé teszi a rendszereket. A viselkedési biometrikus rendszerek folyamatosan elemzik, hogyan lépnek interakcióba a felhasználók az eszközeikkel – vizsgálva a gépelési ritmust, az érintőképernyő nyomását, a görgetési gesztusokat, a navigációs mintákat, sőt azt is, hogyan tartják az eszközt. A TikTok például állítólag megkezdte a viselkedési biometria kísérletezését, hogy egyedi "viselkedési ujjlenyomatokat" hozzon létre a felhasználóknak, lehetővé téve a folyamatos ellenőrzést a felhasználói munkamenet során anélkül, hogy explicit hitelesítési műveleteket kellene végrehajtani.[604] Ez a megközelítés különösen értékes a közösségi média platformok számára, mivel lehetővé teszi a biztonsági csapatok számára, hogy potenciálisan csalárd tevékenységeket fedezzenek fel még akkor is, ha a helyes hitelesítési adatokat használják.

[602] Awais Ahmed, „Social Media Security: A Study of Password Practices and Risks”, 2025, https://doi.org/10.13140/RG.2.2.17685.44001.
[603] „Multimodal Biometric Systems: A Comparative Study”.
[604] BehavioSec, „Behavioral Biometrics Market Analysis”.

5.6.1 Közösségi média platform implementációs stratégiák

A közösségi média platformok sajátos megközelítéseket fejlesztettek ki az identitásellenőrzéshez és hitelesítéshez, gyakran átfogó ökoszisztémákat létrehozva, amelyek túlmutatnak elsődleges alkalmazásaikon. A Facebook hitelesítési rendszere például most identitásszolgáltatóként szolgál számos harmadik féltől származó alkalmazás és weboldal számára a Facebook Login segítségével, amely fejlődött, hogy biometrikus ellenőrzési lehetőségeket is magában foglaljon. Hasonlóképpen, a Google hitelesítési ökoszisztémája integrálódik a YouTube-bal és más társadalmi tulajdonságokkal, kihasználva fejlett biztonsági infrastruktúráját.[605]

Az Apple megközelítése a Face ID közösségi média alkalmazásokba integrálásával egy másik modellt képvisel, ahol a hardvergyártó biztosítja azt a hitelesítési technológiát, amelyet a társadalmi alkalmazások kihasználnak. Ez különösen sikeresnek bizonyult, a biometrikus hitelesítés elfogadási aránya az iOS közösségi média alkalmazásokon belül eléri a 91%-ot az iPhone-felhasználók körében, szemben az Android alternatívák 76%-ával.[606]

A közösségi média platformok egyre inkább implementálnak MI-vezérelt adaptív hitelesítési rendszereket, amelyek elemzik a kontextuális tényezőket a kockázati szintek meghatározásához és a hitelesítési követelmények ennek megfelelő beállításához. A magas kockázatú forgatókönyvek további ellenőrzési lépéseket indítanak el, míg az ismerős környezetben végzett rutinszerű tevékenységek minimális hitelesítést igényelhetnek. Ezek a rendszerek kifejezetten relevánsak a közösségi média platformok számára, tekintettel a változatos kontextusokra, amelyekben a felhasználók hozzáférnek szolgáltatásaikhoz – a dedikált otthoni hálózatoktól a nyilvános Wi-Fi-ig, a személyes eszközöktől a megosztott számítógépekig. A biztonsági követelmények dinamikus beállításával a kontextuális kockázati tényezők alapján a platformok optimalizálhatják mind a biztonságot, mind a felhasználói élményt.[607]

---

[605] Srivathsan G. Morkonda, Paul C. van Oorschot, és Sonia Chiasson, „Exploring Privacy Implications in OAuth Deployments" (arXiv, 2021. március 3.), https://doi.org/10.48550/arXiv.2103.02579.
[606] Apple Inc, „Face ID Security White Paper", 2023.
[607] Ahmed, „Social Media Security: A Study of Password Practices and Risks".

5.7 Információs műveletek elleni küzdelem

Az információs műveletek elleni küzdelem a digitális korszak egyik kiemelkedő kihívásává vált. Az álhírek, a kibertámadások, a személyazonosság-lopás és a dezinformációs kampányok egyre kifinomultabb formában jelennek meg, veszélyeztetve nem csupán az egyének, de intézmények, vállalatok és államok biztonságát is. A digitális technológiák fejlődésével párhuzamosan a személyazonosításra és hitelesítésre szolgáló megoldások is átalakuláson mennek keresztül, új lehetőségeket teremtve a digitális térben megjelenő fenyegetésekkel szembeni védekezésre.

A modern személyazonosítási és hitelesítési technológiák, különösen az okos eszközökön futó alkalmazások, kulcsszerepet játszhatnak az információs műveletek elleni küzdelemben. Ezek a technológiák lehetővé teszik a felhasználók megbízható azonosítását, a digitális tartalmak eredetiségének ellenőrzését, valamint a biztonságos kommunikációt és adatmegosztást, amelyek mind alapvető fontosságúak a dezinformáció és a kibertámadások elleni védekezésben. Az információs műveletek olyan összehangolt tevékenységek, amelyek célja az információ manipulálása, torzítása vagy hiteltelenítse, ezáltal befolyásolva a célközönség percepcióját, döntéseit és viselkedését. Ezek a műveletek számos formában jelenhetnek meg, beleértve a dezinformációs kampányokat, álhíreket, manipulált médiatartalmakat (deepfake), célzott kibertámadásokat és identitáslopást.[608] Az elmúlt évek tendenciái azt mutatják, hogy az információs támadások mind gyakoribbá és kifinomultabbá váltak. A Federal Bureau of Investigation (FBI) 2022-es jelentése szerint az internetes csalásokból származó globális veszteségek meghaladták a 10,3 milliárd dollárt, ami 47%-os növekedést jelent az előző évhez képest. Ez a növekedés részben az egyre kifinomultabb személyazonosság-lopási technikáknak és a célzott dezinformációs kampányoknak tulajdonítható.[609]

Az információs műveletek elleni védekezés különösen nehéz, mivel a támadók gyakran kihasználják a hagyományos azonosítási és hitelesítési módszerek gyengeségeit. A jelszó alapú rendszerek sebezhetősége közismert, a Verizon 2023-as adatbiztonsági jelentése szerint az adatvédelmi incidensek 80%-a gyenge vagy ellopott jelszavakhoz

[608] Gergely Gosztonyi és Gergely Lendvai, „Deepfake és dezinformáció – Mit tehet a jog a mélyhamisítással készült álhírek ellen?", *Médiakutató* 25, sz. 1 (2024): 29–40.
[609] Federal Bureau Investigation, „Internet Crime Complaint Center Releases 2022 Statistics", 2023. március 22., https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics.

köthető.[610] A hagyományos azonosítási módszerek korlátai miatt egyre nagyobb szükség van olyan fejlett megoldásokra, amelyek képesek megbízhatóan azonosítani a felhasználókat és hitelesíteni a digitális tartalmakat.

5.7.1 Okos eszközök biometrikus képességei és azok alkalmazása az információs műveletek elleni küzdelemben

Az okos eszközök biometrikus képességei fontos szerepet játszhatnak az információs műveletek elleni védekezésben. Ezek a technológiák nemcsak a felhasználók hitelesítésére szolgálnak, hanem lehetővé teszik a digitális tartalmak eredetének és integritásának ellenőrzését Az információs műveletek hatékony elleni küzdelemhez a folyamatos hitelesítés kulcsfontosságú. A hagyományos hitelesítési rendszerek csak meghatározott ellenőrzési pontokon (általában bejelentkezéskor) ellenőrzik az identitást, így a rendszerek sebezhetővé válnak a kezdeti ellenőrzés után. A viselkedési biometrikus rendszerek azonban folyamatosan elemzik, hogyan lépnek interakcióba a felhasználók az eszközeikkel, ami lehetővé teszi a biztonsági csapatok számára, hogy valós időben észleljék a potenciálisan csalárd tevékenységeket, még akkor is, ha a helyes hitelesítési adatokat használják.[611] Az információs műveletek során gyakran használnak hamis vagy manipulált adatokat és tartalmakat. A biometrikus rendszerek ellen irányuló prezentációs támadások (vagy spoofing) egyre gyakoribbá válnak, amelyek során hamis biometrikus mintákat mutatnak be az érzékelőnek, például fényképeket, maszkokat, előre rögzített hangmintákat vagy szintetikus ujjlenyomatokat. A mesterséges intelligencia és a gépi tanulás forradalmasítja a csalás felderítési képességeket azzal, hogy lehetővé teszi a rendszerek számára olyan minták és anomáliák azonosítását, amelyeket emberek számára lehetetlen lenne manuálisan észlelni. Az okos eszköz alkalmazások kihasználhatják ezeket a technológiákat számos kontextuális tényező és viselkedési minta egyidejű elemzéséhez, létrehozva egy átfogó kockázati profilt minden hitelesítési kísérlethez.

Az AI-vezérelt kontextuális kockázatelemzés kulcselemei közé tartozik:

1. Eszközazonosítás: A felhasználó eszközének egyedi jellemzőinek azonosítása, beleértve a hardverkonfigurációt, szoftververziókat és hálózati beállításokat.

[610] Verizon, „Data Breach Investigations Report", 2023, https://www.verizon.com/business/resources/reports/dbir/.
[611] Anvesh Gunuganti, „Behavioral Biometrics for Continuous Authentication", *Journal of Biosensors and Bioelectronics Research*, 2023. szeptember, 1–5, https://doi.org/10.47363/JBBER/2023(1)122.

2. Helymeghatározási intelligencia: A felhasználó helyzetmintáinak elemzése, gyanús hitelesítési kísérletek jelzése szokatlan helyekről vagy lehetetlen utazási forgatókönyvek esetén (például bejelentkezés két távoli helyről rövid időn belül).
3. Időbeli minták: A hitelesítési kísérletek időzítésének vizsgálata a felhasználó kialakított mintáihoz viszonyítva.
4. Interakciós minták: Annak elemzése, hogyan navigál a felhasználó az alkalmazásokban és szolgáltatásokban, beleértve a gépelési sebességet, a menüválasztási mintákat és a gesztus jellemzőit.[612]

5.7.2 Platformokon átívelő hitelesítési szabványok

A hitelesítési módszerek töredezettsége a különböző platformok és szolgáltatások között biztonsági sebezhetőségeket és súrlódást okoz a felhasználók számára. A platformokon átívelő hitelesítési szabványok fejlesztése célja, hogy kezelje ezeket a problémákat konzisztens, interoperábilis hitelesítési élményt teremtve. Ezek a szabványok konzisztens hitelesítési élményt tesznek lehetővé az eszközök és platformok között, csökkentett függőséget a jelszavaktól, egyszerűsített megfelelést a biztonsági előírásoknak és fokozott interoperabilitást a különböző szállítók megoldásai között. Ahogy ezek a szabványok tovább fejlődnek és terjednek, egységesebb megközelítést fognak létrehozni a hitelesítéshez, ami csökkentheti az internetes csalás lehetőségeit.

A platformokon átívelő szabványok különösen fontosak az információs műveletek elleni küzdelemben, mivel lehetővé teszik a megbízható identitások és hiteles tartalmak ellenőrzését különböző szolgáltatásokon és platformokon keresztül. Ez megnehezíti a rosszindulatú szereplők számára, hogy hamis identitásokat hozzanak létre vagy manipulált tartalmakat terjesszenek több platformon.[613]

5.7.3 Gyakorlati alkalmazások az információs műveletek elleni küzdelemben

Az okos eszközökön alapuló személyazonosítási és hitelesítési technológiák segíthetnek a dezinformáció, az álprofilok, a deepfake-ek és más manipulált tartalmak elleni védekezésben az alábbi gyakorlati példák mentén.

[612] Veldurthi, „The Role of AI and Machine Learning in Fraud Detection for Financial Services".
[613] F.I.D.O. Alliance, „FIDO2: Moving the World Beyond Passwords", 2023.

Deepfake és manipulált média detektálás

Az okos eszközök biometrikus és hitelesítési képességei szerepet játszhatnak a deepfake-ek és manipulált tartalmak felismerésében:

1. Élő jelek ellenőrzése: Az okos eszközökbe épített fejlett kamerák és érzékelők képesek olyan élő jeleket észlelni, amelyeket nehéz hamisítani, mint például a szemmozgás, a pupilla reakciója a fényre, vagy a bőr színváltozásai a pulzussal.
2. Eszközeredet-ellenőrzés: A készülékbe épített hardveres biztonsági modulok használhatók annak igazolására, hogy egy adott médiatartalom az adott eszközről származik, és nem manipulálták utólag.
3. Kontextuális információk ellenőrzése: Az okos eszközök érzékelői által gyűjtött metaadatok, mint a helymeghatározás, időbélyeg és eszközadatok, használhatók a tartalmak eredetiségének ellenőrzésére.
4. Többfaktorú tartalomhitelesítés: A különböző biometrikus és környezeti adatok kombinálása magasabb szintű bizonyosságot adhat egy tartalom hitelességéről.[614]

Kutatások szerint az élő arcdetekciós technológiák, amelyek vizsgálják a vérkeringéshez kapcsolódó arcszínváltozásokat (fotopletizmográfiai jelek), akár 97%-os pontossággal képesek megkülönböztetni az élő arcokat a deepfake videóktól.[615] Ezek a technológiák integrálhatók az okos telefonok és más eszközök kameraalkalmazásaiba.

Bot- és álprofildetektálás közösségi médiában

A közösségi média botok és álprofilok az információs műveletek gyakori eszközei, amelyeket dezinformáció terjesztésére, bizonyos témák látszólagos népszerűségének manipulálására, vagy célzott zaklatásra használnak. Az okoseszköz-alapú hitelesítési technológiák segíthetnek az ilyen fiókok azonosításában és korlátozásában.

A biometrikus és viselkedési hitelesítés használatával a közösségi médiaplatformok:

1. Ellenőrizhetik a felhasználók valódiságát regisztrációkor vagy magas kockázatú műveletek esetén
2. Folyamatosan figyelhetik a fiókhasználati mintákat a botszerű vagy gyanús tevékenységek észlelésére

[614] Xiao Feng, Hua Ma, és Yijie Sun, „DeepFake Detection with Remote Heart Rate Estimation Using 3D CentralDifference Convolution Attention Network", *Recent Advances in Computer Science and Communications* 16, sz. 7 (2023. szeptember): e010323214186, https://doi.org/10.2174/2666255816666230301091725.
[615] Feng, Ma, és Sun.

3. Detektálhatják a koordinált, nem hiteles viselkedést, amely információs műveletekre utalhat
4. Megnehezíthetik a támadók számára nagy mennyiségű hiteles fiók létrehozását

A viselkedési biometria különösen ígéretes ezen a területen. Egy tanulmány szerint a gépelési dinamika elemzése, a navigációs minták és az eszközhasználati szokások kombinálása 91%-os pontossággal képes megkülönböztetni a valódi humán felhasználókat a botoktól.[616] Ezek a technológiák már beépültek számos platform biztonsági rendszereibe.

Digitális tartalomhitelesítés és eredetigazolás

Az okos eszközökbe épített hitelesítési technológiák fontos szerepet játszhatnak a tartalmak provenienciájának biztosításában és a manipuláció megelőzésében vagy észlelésében. Az okos eszközök képességei a következő módokon használhatók tartalomhitelesítésre: az eddig felhasznált szakirodalmak alapján

1. Digitális aláírások: A készülék biztonságos elemében tárolt kriptográfiai kulcsok használata tartalmak digitális aláírására, igazolva azok eredetét.
2. Hardveralapú tartalomjegyezés: Az eszköz fizikai jellemzőin alapuló egyedi digitális vízjelek beágyazása a tartalomba annak forrásaként.
3. Decentralizált hitelesítés: Block chain alapú megoldások használata a tartalom létrehozásának és módosításainak átlátható, megváltoztathatatlan nyilvántartására.
4. Időbélyegzés és geolokációs hitelesség: Az eszköz szenzoradatainak használata a tartalom létrehozási idejének és helyének hitelesítésére.

5.7.4 Személyazonosításra és hitelesítésre alkalmas technológia jövőbeli biztonsági kockázatai

Az okos eszközök napi szinten kísérnek bennünket, és számos kulcsfontosságú szolgáltatáshoz biztosítanak hozzáférést a banki alkalmazásoktól a kormányzati rendszerekig. Miközben ezek a technológiák kétségtelenül kényelmi és biztonsági előnyöket kínálnak, elengedhetetlen, hogy megértsük a velük járó potenciális kockázatokat. A személyazonosítási és hitelesítési technológiák alapvetően három fő csoportba sorolhatók: tudásalapú (amit tudunk, pl. jelszó), birtoklásalapú (amit birtoklunk, pl. okos

[616] Alexandros Karakos, „Keystroke dynamics features for gender recognition", elérés 2025. május 4., https://www.academia.edu/87483047/Keystroke_dynamics_features_for_gender_recognition.

telefon) és biometrikus (ami a sajátunk, pl. ujjlenyomat) tényezőkre épülő megoldások. Az okos eszközök különleges helyet foglalnak el ebben a környezetben, mivel gyakran mindhárom tényezőt egyesítik, és számos azonosítási módszert támogatnak a jelszavaktól kezdve a biometrikus azonosításig. Ez a sokoldalúság, bár rendkívül hatékony, összetett kockázati tényezőket is magában hordoz.

- **Biometrikus azonosítási rendszerek sebezhetőségei**

A biometrikus azonosítási rendszerek, bár magasabb szintű biztonságot kínálnak a hagyományos jelszavaknál, számos egyedi sebezhetőséggel rendelkeznek. Ezek a sebezhetőségek különösen problematikusak, mivel – a jelszavakkal ellentétben – a biometrikus jellemzők többnyire nem változtathatók meg kompromittálódás esetén.

Az egyik kiemelt kockázati kategória a prezentációs támadások (presentation attacks vagy spoofing). Ezek során a támadó hamis biometrikus mintát (pl. fényképet, ujjlenyomat-másolatot vagy hangfelvételt) mutat be az érzékelőnek. Az IEEE Transactions on Information Forensics and Security folyóiratban megjelent kutatás szerint a hagyományos arcfelismerő rendszerek akár 78%-os arányban megtéveszthetők jó minőségű fényképekkel vagy videókkal.[617] Bár a modern okos eszközök élőségi detektálást (liveness detection) alkalmaznak e támadások kivédésére, ezek a módszerek sem tökéletesek. A biometrikus szenzorok fizikai manipulálása szintén kockázati tényező. Az okos eszközökbe épített ujjlenyomat-olvasók és kamerák manipulálhatók, különösen, ha a támadónak fizikai hozzáférése van az eszközhöz. Egy 2023-as tanulmány demonstrálta, hogy bizonyos okos telefonok ujjlenyomat-olvasói megtéveszthetők speciálisan készített, vékony szilikon ujjlenyomat-másolatokkal, amelyek észrevétlenül elhelyezhetők az eredeti szenzor felületén.[618] A biometrikus rendszerek "zero-effort" támadásokkal szembeni sebezhetősége is aggodalomra ad okot. Ez a jelenség akkor fordul elő, amikor egy felhasználó fizikailag hasonlít egy másikra (pl. egypetéjű ikrek esetében), vagy amikor biometrikus jellemzői véletlenül hasonlítanak egy másik regisztrált felhasználóéra.

[617] Wenbo Li és Liqun Chen, „Agile Smart-Device Based Multi-Factor Authentication for Modern Identity Management Systems", *IEEE Transactions on Dependable and Secure Computing* 21, sz. 2 (2024): 112–27, https://doi.org/10.1109/TDSC.2023.3321758.
[618] Europol, „Remote Biometric Surveillance: Capabilities and Limitations", *Strategic Analysis Report*, 2023.

- **Mesterséges intelligencia és deepfake technológiák jelentette veszélyek**

A mesterséges intelligencia (MI) és a gépi tanulás gyors fejlődése új dimenziót nyit a személyazonosítási és hitelesítési technológiákat érintő fenyegetések terén. Különösen aggasztóak a deepfake technológiák, amelyek lehetővé teszik rendkívül realisztikus, de hamis biometrikus minták – például arcvideók, hangok vagy akár ujjlenyomatok – szintetikus generálását. A deepfake arcvideók minősége drámaian javult az elmúlt években. A jelenlegi legfejlettebb deepfake technológiák már olyan szintű realizmust értek el, hogy emberi megfigyelők számára alig megkülönböztethetők a valódi videóktól.[619] A hangalapú deepfake technológiák is fejlődésen mentek keresztül. Ma már néhány perces hangminta elegendő lehet ahhoz, hogy szinte tökéletes hangklónt készítsenek valaki hangjáról. Az MI-alapú támadások egyik különösen aggasztó aspektusa, hogy egyre demokratizálódnak. A korábban csak specializált szakértők és jól felszerelt laboratóriumok számára elérhető technológiák ma már gyakran nyílt forráskódú projektként vagy könnyen használható alkalmazásként hozzáférhetők. Ez csökkenti a potenciális támadók belépési küszöbét, és növeli a támadások számát és változatosságát.

- **Kvantumszámítógépek jelentette fenyegetés**

A kvantumszámítástechnika fejlődése forradalmi változásokat hozhat számos területen, beleértve a kriptográfiát is, ami közvetlen hatással lesz a személyazonosítási és hitelesítési rendszerek biztonságára. A kvantumszámítógépek különleges képességei – különösen a Shor-algoritmus implementálásának lehetősége – potenciálisan veszélyeztethetik a jelenlegi kriptográfiai rendszereket, amelyek a digitális személyazonosítási és hitelesítési infrastruktúrák alapját képezik. A jelenlegi RSA és ECC (Elliptic Curve Cryptography) algoritmusok, amelyek a nyilvános kulcsú kriptográfia gerincét alkotják és széles körben használatosak a digitális aláírásokhoz és kulcscseréhez a személyazonosítási rendszerekben, különösen sebezhetők a kvantumszámítógépes támadásokkal szemben. Egy megfelelően nagy és stabil kvantumszámítógép képes lenne feltörni a jelenleg használt 2048 bites RSA kulcsokat mindössze néhány óra alatt, szemben a hagyományos számítógépekkel, amelyeknek ez több ezer évet venne

[619] Fehér, „Deepfake Detection in Social Media Contexts".

igénybe.[620] Az okos eszközök esetében a kvantumrezisztens kriptográfia implementálása további kihívásokat jelent, mivel ezek az eszközök gyakran korlátozott számítási kapacitással és energiakészlettel rendelkeznek. A jelenlegi posztkvantum algoritmusok nagyobb számítási teljesítményt és energiafogyasztást igényelnek, mint a hagyományos algoritmusok, ami problémás lehet az akkumulátorról működő okos eszközök esetében.[621]

- **Platformok közötti sebezhetőségek és interoperabilitási kockázatok**

Az okos eszközök változatos ökoszisztémája, amelyben különböző operációs rendszerek, hardverek és biztonsági architektúrák működnek együtt, sajátos kihívásokat teremt a személyazonosítási és hitelesítési rendszerek számára. A platformok közötti sebezhetőségek és interoperabilitási problémák biztonsági kockázatot jelenthetnek. Az egyik alapvető kihívás a különböző platformok eltérő biztonsági modelljéből fakad. Az iOS és az Android különbözik a biometrikus adatok kezelésének módját és a biztonságos tárolási mechanizmusokat illetően. Ezek a különbségek potenciális interoperabilitási problémákhoz és biztonsági résekhez vezethetnek a több platformot is támogató alkalmazások esetében.[622]. A felhasználók gyakran több eszközön is használják ugyanazokat az azonosítási rendszereket, ami megköveteli a hitelesítési adatok (vagy azok biztonságos referenciáinak) szinkronizálását. Ez újabb támadási felületet nyithat, különösen, ha a szinkronizációs folyamat nem megfelelően védett.

- **Társadalmi és pszichológiai kockázatok**

A személyazonosítási és hitelesítési technológiák, különösen a biometrikus módszerek, nem csak technikai és jogi kihívásokat jelentenek, hanem összetett társadalmi és pszichológiai kockázatokat is hordoznak, amelyek befolyásolják a felhasználói elfogadást és a technológia hosszú távú fenntarthatóságát. A privacy paradoxon (adatvédelmi paradoxon) – az ellentmondás a felhasználók kinyilvánított adatvédelmi aggályai és tényleges viselkedésük között – különösen releváns a biometrikus azonosítással kapcsolatban. Bár a felhasználók gyakran aggódnak a biometrikus adataik biztonsága

[620] C. Gidney és M. Ekerå, „How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits", *Quantum* 5 (2021): 433.
[621] S. Prasad, *Performance Evaluation of Post-Quantum Cryptographic Algorithms on Mobile Devices* (Stanford University Department of Computer Science, 2023).
[622] P. Gasti, *Security Analysis of Mobile Authentication across Different Platforms* (Carnegie Mellon University CyLab Security and Privacy Institute, 2022).

miatt, a kényelem és a gördülékeny felhasználói élmény érdekében mégis hajlandóak használni ezeket a technológiákat, gyakran anélkül, hogy teljesen megértenék a kockázatokat.[623] Ez a paradoxon növeli annak kockázatát, hogy a felhasználók olyan döntéseket hoznak, amelyek hosszú távon károsak lehetnek számukra, különösen, mivel a biometrikus adatok nem változtathatók meg kompromittálódás esetén. A biometrikus azonosítási technológiák kényszerítő vagy manipulatív alkalmazása, különösen állami szereplők részéről, szintén társadalmi kockázatot jelent.[624]

A "digitális szakadék" tovább mélyülhet az okoseszköz-alapú azonosítási rendszerek széles körű bevezetésével. Nem minden állampolgár rendelkezik modern, biometrikus azonosításra képes okos eszközökkel, vagy birtokolja a szükséges digitális készségeket ezek használatához. Ha a lényeges szolgáltatások egyre inkább az okos eszközökön keresztüli biometrikus azonosítástól függnek, ez tovább marginalizálhatja a digitálisan már most is hátrányos helyzetű csoportokat. A pszichológiai hatások közül különösen figyelemreméltó a "megfigyelés érzékelése" (surveillance perception) jelensége. Akár valós, akár csak érzékelt megfigyelés esetén a felhasználók megváltoztathatják viselkedésüket, ami önkorlátozáshoz, fokozott stresszhez és bizonyos szolgáltatások elkerüléséhez vezethet. A biometrikus megfigyelés érzékelése akár 37%-kal is csökkentheti a nyilvános tevékenységekben való részvételi hajlandóságot bizonyos populációkban.[625]

Következtetések és szakértői interjú eredmények

A kutatási eredmények egyértelműen jelzik, hogy a biometrikus azonosítási technológiák átalakuláson mennek keresztül, amelyet az egyre kifinomultabb mesterséges intelligencia algoritmusok és a multimodális megközelítések térnyerése jellemez. Az egyetlen biometrikus jellemzőn alapuló rendszerek fokozatosan átadják helyüket az integrált megoldásoknak, amelyek több biometrikus modalitást egyesítenek.

[623] Ponemon Institute, „The Privacy Paradox: Understanding Attitudes Towards Biometric Technology", *Ponemon Institute Research Report*, 2022.
[624] Georgetown Law Center Privacy és Technology, „The Identity Trap: How Identification Systems Reinforce Inequality", *Georgetown Law*, 2023.
[625] Yale Law School, „Chilling Effects: The Impact of Surveillance Perception on Civil Liberties", *Yale Law Journal* 131, sz. 5 (2022).

A viselkedési biometria – amely a felhasználók interakciós mintáin, gépelési ritmusán és eszközkezelési szokásain alapul – különösen ígéretes területnek mutatkozik. Ez a folyamatos ellenőrzési képesség paradigmaváltást jelent a hagyományos, egyetlen belépési ponton történő hitelesítéshez képest, és megnehezíti a rosszhiszemű szereplők számára az információs műveletek végrehajtását.

Az okos eszközökbe integrált fejlett prezentációs támadás detektálási (PAD) rendszerek szintén kulcsfontosságú szerepet játszanak, ami hatékony védelmet nyújt a deepfake-ek és más manipulált tartalmak ellen, amelyek az információs műveletek egyre gyakoribb eszközeivé válnak.

Az okos eszközök egyedülálló platformot biztosítanak a fejlett azonosítási és hitelesítési technológiák bevezetésére, mivel széleskörű penetrációval rendelkeznek, és természetes módon integrálják a szükséges hardveres komponenseket, beleértve a fejlett érzékelőket, nagy teljesítményű processzorokat és biztonságos tárolási lehetőségeket.

A mesterséges intelligencia-vezérelt kontextuális kockázatelemzés különösen hatékony integrációs területnek bizonyul.

A peremhálózati számítástechnika és az eszközön belüli feldolgozás előrelépést jelent az adatvédelem és biztonság terén. Az érzékeny biometrikus adatok helyi feldolgozása csökkenti a támadási felületet és minimalizálja az adatszivárgás kockázatát. Az

A blokklánc-alapú decentralizált identitás megoldások, különösen az önszuverén identitás (SSI) modellek, forradalmasíthatják a digitális identitáskezelést. Lehetővé téve a felhasználók számára, hogy teljes kontrollt gyakoroljanak digitális identitásuk felett, miközben biztonságos és ellenőrizhető módon igazolhatják kilétüket. Ez különösen értékes az információs műveletek elleni küzdelemben, ahol a hiteles identitás kulcsfontosságú

Az adatvédelmi paradoxon – ahol az egyének adatvédelmi aggályokat fejeznek ki, miközben olyan magatartást tanúsítanak, amely ellentmond ezeknek az aggályoknak – különösen releváns az azonosítási technológiák kontextusában. Ez a paradoxon kommunikációs és bizalomépítési erőfeszítéseket igényel a sikeres implementációhoz.

A kvantumszámítógépek fejlődése új kihívásokat teremt a kriptográfiai rendszerek számára. A kvantumrezisztens kriptográfia fejlesztése és integrálása az azonosítási és hitelesítési rendszerekbe kritikus fontosságú a hosszú távú biztonság szempontjából.

A platformokon átívelő hitelesítési szabványok, mint a FIDO2, előrelépést jelentenek az interoperabilitási téren. Ezek a szabványok konzisztens hitelesítési élményt biztosítanak az eszközök és platformok között, csökkentve a jelszavaktól való függőséget és javítva a biztonsági megfelelést.

A köz- és magánszféra partnerségek (PPP-k) egyre fontosabb szerepet játszanak a digitális identitás ökoszisztémák fejlesztésében.

Az okos eszközökre fejlesztett személyazonosítási és hitelesítési technológiák potenciállal rendelkeznek az információs műveletek elleni küzdelemben. A multimodális biometrikus megoldások, a folyamatos hitelesítés, a mesterséges intelligencia-vezérelt kontextuális kockázatelemzés és a decentralizált identitás megoldások integrációja robusztus keretet biztosít a digitális identitások hitelesítésére és az információs fenyegetések kezelésére.

A technológiai fejlesztések sikere azonban nem kizárólag a műszaki kifinomultságon múlik, hanem a társadalmi elfogadottságon és a felhasználói bizalmon is. A bizalomépítés, az átláthatóság és a felhasználói kontroll biztosítása alapvető fontosságú a széles körű adaptáció elősegítéséhez.

A jövőbeli kutatásoknak és fejlesztéseknek egyaránt fókuszálniuk kell a technológiai innovációra és a társadalmi implementációs stratégiákra, figyelembe véve a demográfiai különbségeket és az adatvédelmi aggályokat. Csak egy holisztikus megközelítés, amely egyensúlyt teremt a biztonság, a felhasználói élmény és az adatvédelem között, vezethet hosszútávon fenntartható megoldásokhoz az információs műveletek elleni küzdelemben.

A kvantumrezisztens kriptográfia fejlesztése a jövőbeli katonai kommunikáció biztonságának alapja. Az információs műveletek elleni küzdelem új eszközeinek kifejlesztése nemzeti biztonsági prioritás, a hiteles profilok alkalmazása a dezinformációs kampányok elleni védekezésben forradalmasíthatja a kognitív hadviselést. A blockchain technológia alkalmazása a katonai logisztikában és az ellátási lánc biztonságában perspektivikus. A fejezet által tárgyalt jövőbeli kockázatok előrejelzése segítheti a védelmi tervezést.

A CRAMM (CCTA Risk Analysis and Management Method) modell kockázatelemzési keretrendszert biztosít, amelynek három fő eleme: fenyegetés, sebezhetőség és vagyon. Az interjúk elemzéséhez ezt a struktúrát alkalmazva vizsgáljuk, hogy a hiteles profilok bevezetése milyen kockázatokat csökkentene, milyen új sebezhetőségeket hozna létre, és hogyan befolyásolná a digitális vagyonokat. A H5 hipotézis ("A hiteles profilok alkalmasak lehetnek az internetes bűnözés és dezinformációs kampányok visszaszorítására, továbbá a védelmi szektorban is felhasználható lehet") részben megerősítést, de kritikus ellentmondásokat is kapott a szakértői válaszokban.

Fenyegetések (Threats)

Támogató tények a H5 hipotézis mellett:

1. Bot-hálózatok visszaszorítása: Tadijanov Leon kiemeli, hogy a hiteles profilok megszüntetnék a hamis fiókokat, amelyek jelenleg a dezinformáció 70-80%-át terjesztik. A CRAMM modell szerint ez csökkentené a fenyegetés intenzitását a közösségi média platformokon
2. Kiberbűnözési kockázat csökkenése: A Digitális Állampolgárság Program (DÁP) példáján keresztül a szakértők szerint a hiteles profilok visszavezethetnék a támadókat, így a ransomware és adathalászat esetén is gyorsabb lenne a nyomozás

Ellentmondó tények:

1. Alternatív támadási felületek: Zsákai Lénárd rámutat, hogy a hiteles profilok bevezetése átterelné a kiberbűnözőket a dark webre vagy titkosított csatornákra, ahol az anonimitás továbbra is fennmarad. A CRAMM modell szerint ez új fenyegetési vektorokat hozna létre, amelyeket a jelenlegi rendszerek nem képesek kezelni.

Sebezhetőségek (Vulnerabilities)

Támogató tények:

1. Adatbázisok biztonsága: A TLS 1.2+ és AES-256 titkosítás alkalmazása, amit több szakértő is javasol, csökkentené az adatszivárgások kockázatát, ami a CRAMM modellben a sebezhetőség csökkentésének felel meg.

Ellentmondó tények:

1. Központosított célpontok: Anonim szakértő) figyelmeztet, hogy a hiteles profilok centralizált adattárolása magas kockázatú célponttá tenné a rendszereket. Egy sikeres támadás esetén egyszerre milliók adatai kerülnének kiszivárgásra, ami súlyosabb következményekkel járna, mint a jelenlegi decentralizált rendszer. A CRAMM modell szerint ez új sebezhetőségi pontokat hozna létre.

Vagyonok (Assets)

Támogató tények:

1. Védelmi szektor előnyei: Tadijanov Leon kiemeli, hogy a hiteles profilok lehetővé tennék a katonai és rendőrségi kommunikáció biztonságosabb átvitelét, például válsághelyzetekben. Ez a CRAMM modellben a vagyonok értékének növekedését jelentené.
2. Nemzetbiztonsági előnyök: A Digitális Jólét Program keretében tervezett kiberoktatás növelné a társadalmi rezilienciát, ami a CRAMM modellben a vagyonok hosszú távú védelmét segítené.

Ellentmondó tények:

1. Magánélet vs. biztonság: Zsákai Lénárd és Anonim szakértő is hangsúlyozza, hogy a hiteles profilok aláássák a magánélet védelmét. A CRAMM modell szerint ez csökkentené a rendszer társadalmi elfogadottságát, ami közvetett kockázatot jelent5

Minden szakértő egyetért abban, hogy a hiteles profilok csökkentenék az anonimitásból fakadó kockázatokat, különösen a dezinformáció és adathalászat területén

2. Generációs különbségek: A fiatalok (18-35 évesek) nyitottabbak a hiteles profilokra, míg az idősek (65+ évesek) bizalmatlanok. Ez fragmentálja a társadalmi konszenzust, ami a CRAMM modell szerint instabilitást okoz13.
2. Jogi inkonzisztencia: A GDPR és NIS2 irányelvek ellentétes követelményei (pl. biometrikus adatok tárolása) megnehezítik a globális harmonizációt, ami a CRAMM modellben környezeti korlátként jelenik meg

Kritikus Megállapítások és Javaslatok

A szakértők nagy része szerint a tökéletes egyensúly elérhetetlen. De javasolt a kockázatalapú hitelesítés bevezetése, ahol a magas kockázatú tranzakciókhoz szigorúbb azonosítás szükséges. A hiteles profilok adatbázisait több régióban decentralizáltan kell tárolni a kibertámadások elleni védekezés érdekében.

A fentiek alapján megállapítható, hogy H5 hipotézis részben igaz, de nem univerzális. A hiteles profilok hatékonyak lehetnek a bot-hálózatok és social engineering visszaszorításában, de új kockázatokat is teremtenek (pl. adatcentralizáció, jogi inkonzisztencia). A védelmi szektorban való alkalmazhatóság függ a technológiai rugalmasságtól és a társadalmi elfogadottságtól. Ahogy Zsákai Lénárd fogalmazott: "A tökéletes biztonság nem létezik, de a kockázatok intelligens kezelése már-már művészet." A CRAMM modell alapján a legfőbb kihívás a fenyegetések dinamikájának követése és a sebezhetőségek proaktív kezelése.

6 SZEMÉLYI AZONOSÍTÁSRA VAGY HITELESÍTÉSRE ALKALMAS TECHNOLÓGIA FELHASZNÁLÁSÁNAK LEHETŐSÉGEI ÉS KOCKÁZATAI A VÉDELMI, BIZTONSÁGI SZEKTORBAN.

Jelen fejezetben az eddig bemutatott technológia, illetve kifejezetten a biometrikus hitelesítésre, illetve azonosításra alkalmas interfész technológiák védelmi szektorban történő felhasználása, azok lehetőségei és kockázatai kerülnek bemutatásra. A fejezethez végzett kutatómunka alapján ajánlásokat fogok tenni a védelmi szféra részvevői, illetve a döntéshozók irányába is.

6.1 Katonai szektorban történő alkalmazás

A katonai alkalmazásokban a biometrikus technológiák használata fontos lehet, hiszen a szembenálló felek – különösen a terrorista csoportok – gyakran az anonimitásra támaszkodnak. Ugyanakkor e technológiák használata technikai, biztonsági, adatvédelmi és etikai kérdést is felvet, amelyek körültekintő elemzést és kezelést igényelnek. A biometrikus technológiák az egyének egyedi biológiai vagy viselkedési jellemzői alapján történő azonosítást teszik lehetővé. Ezek a rendszerek az olyan veleszületett és nehezen hamisítható egyedi jellemzőkön alapulnak, mint az ujjlenyomat, az arc geometriája, a szivárványhártya mintázata vagy a hang frekvencia-jellemzői. A hagyományos azonosítási módszerekkel (jelszavak, azonosító kártyák) szemben a biometrikus rendszerek előnyöket kínálnak, mivel olyan tulajdonságokat használnak fel, amelyeket nem lehet elveszíteni vagy elfelejteni, és nehezebben hamisíthatók.

6.1.1 Mobilalkalmazások a katonai biometrikus azonosításban

A mobileszközök elterjedése és a technológia fejlődése lehetővé tette a biometrikus azonosítási rendszerek mobilplatformokon történő alkalmazását. A katonai célokra kifejlesztett mobilalkalmazások új dimenziókat nyitnak a terepen történő személyazonosításban, növelve a műveleti hatékonyságot és rugalmasságot.

A katonai műveletek során alkalmazott mobil biometrikus technológiák lehetővé teszik a magas minőségű ujjlenyomatok, arcképek és írisz-szkennelések rögzítését és elemzését a terepen. Ezek az eszközök biztosítják a személyazonosság megbízható el-

lenőrzését, védve a katonai erőket, létesítményeket és műveleteket páratlan sebességgel és biztonsággal.[626] A terepi körülményekre optimalizált mobil biometrikus rendszerek számos speciális követelménynek kell megfelelniük, beleértve a robusztus, strapabíró kialakítást, a hosszú akkumulátor-élettartamot, valamint a különböző időjárási és környezeti körülmények közötti megbízható működést. Az ilyen rendszerek általában megerősített, katonai szabványoknak megfelelő eszközökben kerülnek telepítésre, amelyek ellenállnak a pornak, nedvességnek, szélsőséges hőmérsékletnek és egyéb környezeti hatásoknak.[627]

A mobil biometrikus rendszerek integrálhatók más katonai rendszerekkel is, például a hírszerzési adatbázisokkal vagy a parancsnoki és irányítási rendszerekkel. Ez lehetővé teszi a biometrikus adatok gyors megosztását és elemzését, ami értékes információkkal szolgálhat a műveleti tervezéshez és végrehajtáshoz. A NATO 2020-ban bejelentette saját Automated Biometrics Identification System (ABIS) rendszerét, amelyet a NATO Kommunikációs és Információs Ügynöksége fejlesztett ki. Ez a rendszer lehetővé teszi a szövetségesek számára a biometrikus adatok megosztását és elemzését, ami különösen értékes a többnemzeti műveletek során.[628]

A katonai célokra kifejlesztett speciális mobilalkalmazások számos különböző funkcióval rendelkeznek, amelyek támogatják a biometrikus azonosítást és hitelesítést. Ezek az alkalmazások általában titkosított kommunikációt használnak, és szigorú hozzáférés-ellenőrzési mechanizmusokkal vannak ellátva a biztonság maximalizálása érdekében.[629] Az ilyen alkalmazások képesek offline működésre is, ami különösen fontos olyan környezetben, ahol a hálózati kapcsolat korlátozott vagy megbízhatatlan. Az offline adatgyűjtés és a későbbi szinkronizálás lehetővé teszi a folyamatos működést még kedvezőtlen kommunikációs körülmények között is.

---

[626] Cooper Brian, „Army Modernizes Its Biometric Processing Capabilities - PEO IEW&S", 2020. február 18., https://peoiews.army.mil/2020/02/18/aircraft-survivability-2-2/.
[627] „Rugged Laptops and Tablets for Military Use - In Depth Read", 2024. április 14., https://micronordic.com/blog/rugged-laptops-and-tablets-enhance-efficiency/.
[628] „Biometrics: a new capability for the Military Police | CZDEFENCE - czech army and defence magazine", elérés 2025. május 4., https://www.czdefence.com/article/biometrics-a-new-capability-for-the-military-police.
[629] „Javelin™ | Parsons Products", elérés 2025. május 4., https://www.parsons.com/products/javelin/.

A biometrikus azonosítási és hitelesítési technológiák számos előnyt kínálnak a katonai alkalmazásokban, amelyek hozzájárulnak a műveleti hatékonyság és biztonság növeléséhez. A biometrikus azonosítási technológiák növelhetik a katonai műveletek hatékonyságát azáltal, hogy gyors és megbízható személyazonosítást tesznek lehetővé. Ez különösen értékes az olyan műveletek során, mint az ellenőrzőpontok működtetése, területbiztosítás vagy a civil lakosság ellenőrzése.[630]

A járőröző egységek számára a mobil biometrikus eszközök lehetővé teszik a gyanús személyek azonnali ellenőrzését, ami csökkentheti a reagálási időt és növelheti a műveletek tempóját. A gyors és pontos azonosítás lehetősége különösen értékes a magas kockázatú környezetben, ahol a késedelem vagy a téves azonosítás súlyos következményekkel járhat.[631]A biometrikus technológiák alkalmazása csökkentheti az adminisztratív terheket is, lehetővé téve a katonai személyzet számára, hogy több időt fordítson a tényleges műveleti feladatok végrehajtására. Az automatizált személyazonosítási rendszerek egyszerűsíthetik és gyorsíthatják az adatgyűjtést és elemzést, ami korábban időigényes manuális folyamatokat igényelt.[632]

A biometrikus technológiák alkalmazása növelheti a katonai műveletek és létesítmények biztonságát. A katonai bázisok és létesítmények védelme szempontjából a biometrikus hozzáférés-ellenőrzési rendszerek különösen értékesek lehetnek. Ezek a rendszerek biztosíthatják, hogy csak az arra jogosult személyek férhessenek hozzá érzékeny területekhez vagy információkhoz, csökkentve a jogosulatlan hozzáférés és az ebből eredő biztonsági kockázatok lehetőségét.[633] A biometrikus technológiák különösen értékesek lehetnek a multinemzeti katonai műveletek során, ahol különböző nem-

[630] Nina Toft Djanegara, „Biometrics for Counter-Terrorism: Case Study of the US Military in Iraq and Afghanistan" (Privacy International, 2021), https://privacyinternational.org/sites/default/files/2021-06/Biometrics%20for%20Counter-Terrorism-%20Case%20study%20of%20the%20U.S.%20military%20in%20Iraq%20and%20Afghanistan%20-%20Nina%20Toft%20Djanegara%20-%20v6.pdf.
[631] „Rapid ID Mobile Biometric Identification for Law Enforcement", elérés 2025. május 4., https://www.hidglobal.com/solutions/rapid-id-law-enforcement.
[632] „The Importance of Biometric Data Sharing in Counter-Terrorism Capability Development – NAOC", elérés 2025. május 4., https://natoassociation.ca/the-importance-of-biometric-data-sharing-in-counter-terrorism-capability-development/.
[633] D. Kaiypbergen és Ye. Begimbayeva, „RESEARCH OF INNOVATIVE AUTHENTICATION: A DEEP DIVE INTO BIOMETRIC ACCESS TECHNOLOGIES", *Herald of the Kazakh-British technical university* 22, sz. 1 (2025. március 24.): 103–13, https://doi.org/10.55452/1998-6688-2025-22-1-103-113.

zetiségű erők működnek együtt. A szabványosított biometrikus rendszerek és adatformátumok lehetővé teszik a szövetségesek közötti hatékony információ megosztást és együttműködést.[634]

6.1.2 Kockázatok és kihívások

A biometrikus rendszerek pontossága kulcsfontosságú a katonai alkalmazások során, ahol a téves azonosítás súlyos következményekkel járhat. Minden biometrikus rendszernél fennáll a hamis elfogadás (amikor a rendszer tévesen azonosít egy jogosulatlan személyt) és a hamis elutasítás (amikor a rendszer nem ismeri fel a jogosult személyt) kockázata. A terepi körülmények között különösen nagy kihívást jelenthet a biometrikus rendszerek megbízható működése. Az ujjlenyomat-olvasók teljesítményét befolyásolhatja a por, szennyeződés vagy nedvesség, az arcfelismerő rendszerek pontosságát csökkentheti a rossz fényviszony vagy a részleges takarás, míg az írisz-szkennelés nehezebb lehet erős napfényben vagy szélsőséges időjárási körülmények között.

A biometrikus adatok biztonságával kapcsolatos kockázatok különösen a katonai alkalmazások esetében. Az amerikai védelmi minisztérium főfelügyelője által készített jelentés szerint sok biometrikus adatgyűjtő eszköz nem rendelkezik megfelelő adattitkosítási képességekkel, ami biztonsági kockázatot jelent.[635]Az Afganisztánban történtek szemléletesen mutatják a biometrikus adatgyűjtés hosszú távú kockázatait. Az amerikai erők által kiépített Handheld Interagency Identity Detection Equipment (HIIDES) rendszert a tálibok megszerezték Afganisztán elfoglalásakor. Ez a rendszer, amelyet eredetileg az amerikai erők a személyek egyszerű azonosítására és a barátellenség megkülönböztetésére terveztek, a tálibok kezében potenciálisan felfedte azok személyazonosságát, akik az amerikai erőkkel dolgoztak, kitéve őket a megtorlás veszélyének.[636]

---

[634] „Biometrics: a new capability for the Military Police | CZDEFENCE - czech army and defence magazine".

[635] „Press Release: Department of Defense Office of Inspector General (DoD OIG) Released the Re", Department of Defense Office of Inspector General, elérés 2025. május 4., https://www.dodig.mil/In-the-Spotlight/Article/3584937/press-release-department-of-defense-office-of-inspector-general-dod-oig-release/https%3A%2F%2Fwww.dodig.mil%2FIn-the-Spotlight%2FArticle%2F3584937%2Fpress-release-department-of-defense-office-of-inspector-general-dod-oig-release%2F.

[636] Brookings Institution, „The Enduring Risks Posed by Biometric Identification Systems", 2021.

A mobil biometrikus eszközök elvesztése vagy ellopása szintén kockázatot jelent, ha az eszközön tárolt adatok nincsenek megfelelően titkosítva. Az ilyen incidensek során nemcsak érzékeny biometrikus adatok kerülhetnek illetéktelen kezekbe, hanem potenciálisan a műveleti biztonság is veszélybe kerülhet

A biometrikus rendszerek ellen irányuló célzott támadások, mint például a spoofing (megtévesztés) vagy a presentation attacks (prezentációs támadások), további kockázatokat jelentenek. Ezek során a támadók hamis biometrikus mintákat (például fényképeket, maszkokat, mesterséges ujjlenyomatokat) használnak a rendszer megtévesztésére. A katonai műveletek során gyűjtött biometrikus adatok felhasználása a művelet befejezése után külön szabályozást igényel. Kérdéses lehet, hogy mi történik ezekkel az adatokkal a művelet lezárultával megőrzik, törlik vagy átadják őket más szervezeteknek? Az etikai szempontok között kiemelendő a biometrikus adatgyűjtés önkéntességének kérdése is. Míg a katonai személyzet esetében ez általában a szolgálat részének tekinthető, a civil lakosságtól történő adatgyűjtés során az önkéntesség és a tájékozott beleegyezés biztosítása kihívást jelenthet, különösen konfliktuszónákban vagy instabil területeken.

6.1.3 Fejlődési trendek és jövőbeli alkalmazások

A biometrikus technológiák és azok katonai alkalmazásai folyamatosan fejlődnek, új lehetőségeket és kihívásokat teremtve. A mesterséges intelligencia és a gépi tanulás integrációja a biometrikus rendszerekbe az egyik legfontosabb fejlesztési irány. Az MI-alapú biometrikus rendszerek képesek adaptálódni a változó körülményekhez, javítani a felismerés pontosságát, és csökkenteni a hamis elfogadási és elutasítási arányokat.[637]

Az új biometrikus modalitások kutatása és fejlesztése szintén fontos trend. Az elektrofiziológiai biometria, amely magában foglalja az elektrokardiogram (EKG) és az elektroenkefalogram (EEG) mintázatok használatát a személyazonosításra, különösen nehezen hamisítható, és új lehetőségeket kínál a folyamatos hitelesítésre.[638]

---

[637] National Security Commission Artificial Intelligence, „Biometric Systems in National Security: Risks and Recommendations", Special Report, 2023.
[638] Jeswani J és mtsai., „Low Valence Low Arousal Stimuli: An Effective Candidate for EEG-Based Biometrics Authentication System", *PubMed*, 2023, https://pubmed.ncbi.nlm.nih.gov/37203658/.

A viselkedési biometria, mint a gépelési dinamika, járási minták vagy gesztusok elemzése, új dimenziókat nyithat a biometrikus hitelesítésben. Ezek a módszerek különösen hasznosak lehetnek a folyamatos hitelesítésben, mivel nem igényelnek explicit felhasználói interakciót, ami ideálissá teszi őket a katonai környezetben.[639] A kognitív biometria, amely az agyi aktivitás mintázatain alapul, szintén ígéretes kutatási terület. Az EEG-alapú hitelesítés már 94-98%-os pontosságot képes elérni, és potenciálisan alkalmazható lehet a jövő magas biztonságú katonai rendszereiben.[640]

A blokklánc-technológia integrációja a biometrikus rendszerekbe új lehetőségeket kínálhat a biztonságos és decentralizált biometrikus hitelesítés terén. A blokklánc alapú biometrikus rendszerek elosztott módon tárolhatják a hitelesítési rekordokat, miközben a tényleges biometrikus adatok a felhasználók eszközein maradnak, így növelve a biztonságot és csökkentve a központi adatbázisok kompromittálódásának kockázatát.[641]

A zero-knowledge proof (nulla ismereti bizonyítás) technikával kombinálva a blokklánc lehetővé teszi a felhasználók számára, hogy bizonyítsák személyazonosságukat anélkül, hogy felfednék a biometrikus adataikat. Ez a megközelítés csökkentheti a privacy kockázatokat, miközben megőrzi a biometrikus hitelesítés előnyeit.[642]A decentralizált identitás-kezelési rendszerek (DID) integrációja a katonai biometrikus rendszerekbe rugalmasabb és biztonságosabb hitelesítési infrastruktúrát eredményezhet. Ezek a rendszerek lehetővé teszik a felhasználók számára, hogy kontrollt gyakoroljanak saját digitális identitásuk felett, miközben biztonságos és ellenőrizhető módon igazolhatják kilétüket.[643]

---

[639] Hayreddin Ceker és Shambhu Upadhyaya, „Enhanced recognition of keystroke dynamics using Gaussian mixture models", *MILCOM 2015 - 2015 IEEE Military Communications Conference*, 2015. október, 1305–10, https://doi.org/10.1109/MILCOM.2015.7357625.
[640] Himanshu Vadher és mtsai., „EEG-based Biometric Authentication System Using Convolutional Neural Network for Military Applications", *SECURITY AND PRIVACY* 7, sz. 2 (2024. március): e345, https://doi.org/10.1002/spy2.345.
[641] Ilham Laabab és mtsai., „Blockchain and Biometric Systems Integration for IoMT Security", *2024 8th Cyber Security in Networking Conference (CSNet)*, 2024. december 4., 259–62, https://doi.org/10.1109/CSNet64211.2024.10851762.
[642] Quang Nhat Tran és mtsai., „A Privacy-Preserving Biometric Authentication System With Binary Classification in a Zero Knowledge Proof Protocol", *IEEE Open Journal of the Computer Society* 3 (2022): 1–10, https://doi.org/10.1109/OJCS.2021.3138332.
[643] J. Lee és D. Lee, „Decentralized Authentication for Disconnected Military Environments", *IEEE Transactions on Dependable and Secure Computing* 18, sz. 3 (2021): 1352–65.

Következtetések és ajánlások

A személyazonosításra és személyi hitelesítésre alkalmas technológiák, különösen az okos eszközökön futó alkalmazások, előnyöket kínálnak a katonai felhasználás számára. Ugyanakkor számos kihívással és kockázattal is szembesülünk, amelyek körültekintő kezelést igényelnek. A biometrikus technológiák katonai alkalmazása során kulcsfontosságú a megfelelő egyensúly megtalálása a műveleti hatékonyság és biztonság, valamint az adatvédelem és etikai megfontolások között. A következő ajánlások segíthetnek ennek az egyensúlynak a megteremtésében:

1. A biometrikus rendszerek implementálása során mindig többszintű biztonsági megközelítést kell alkalmazni, amely magában foglalja mind a technikai (titkosítás, élőségi detektálás, visszavonható biometria), mind a szervezeti és eljárási védőintézkedéseket.
2. A multimodális biometrikus rendszerek alkalmazása ajánlott, különösen a magas biztonsági követelményekkel rendelkező katonai környezetben. Ezek a rendszerek csökkenthetik a hamis elfogadási és elutasítási arányokat, növelve a megbízhatóságot és biztonságot.
3. A biometrikus adatok gyűjtése, tárolása és felhasználása során szigorúan be kell tartani az adatminimalizálás, a célhoz kötöttség és az arányosság elveit, még a katonai alkalmazások esetében is.
4. A személyzet megfelelő képzése kulcsfontosságú a biometrikus rendszerek hatékony és biztonságos használata érdekében. A képzésnek ki kell térnie a technológia lehetőségeire és korlátaira, a helyes használatra, valamint az adatvédelmi és etikai szempontokra.
5. A biometrikus rendszerek bevezetése előtt alapos kockázatelemzést és hatásvizsgálatot kell végezni, figyelembe véve a technikai, biztonsági, adatvédelmi és etikai szempontokat.
6. Nemzetközi együttműködés és szabványosítás szükséges a biometrikus adatok biztonságos megosztása és a multinemzeti műveletek hatékony támogatása érdekében.

Összességében a személyazonosításra és személyi hitelesítésre alkalmas technológiák, különösen az okos eszközökön futó alkalmazások, értékes eszközöket kínálnak a mo-

dern hadviselés számára. Megfelelő implementálás és használat mellett hozzájárulhatnak a műveleti hatékonyság és biztonság növeléséhez, miközben a kockázatok és kihívások is kezelhetők.

6.2 Rendészeti, rendvédelmi szektorban történő alkalmazás

A hagyományos azonosítási módszerek, mint a személyi igazolványok vagy jelvények ellenőrzése mellett egyre nagyobb szerepet kapnak a biometrikus technológiák, amelyek az egyének egyedi fizikai vagy viselkedési jellemzőin alapuló azonosítást teszik lehetővé. E technológiák használata különösen a mobileszközökön futó alkalmazások révén nyit új lehetőségeket a rendőrségi munkában, ugyanakkor számos kockázatot és etikai kérdést is felvet.

A biometrikus technológia rendőrségi alkalmazásának több területe is van, a bűnügyi nyomozásoktól kezdve a határellenőrzésen át a közterületi rendőri jelenlét hatékonyságának növeléséig számtalan területen nyújthat támogatást. A biometrikus adatok – mint az ujjlenyomat, arc, írisz vagy hang – elemzése révén a rendőrség gyorsan és pontosan azonosíthat személyeket, ami kulcsfontosságú lehet olyan helyzetekben, amikor a gyors reagálás életeket menthet. Az okos eszközök elterjedésével párhuzamosan a biometrikus azonosítási technológiák mobilalkalmazásokba történő integrálása új dimenziókat nyit a rendészeti munkában. A járőröző rendőrök a helyszínen azonosíthatnak gyanúsítottakat, ellenőrizhetik a személyazonosságot, vagy összevethetik a helyszíni nyomokat a központi adatbázisokkal. Ez a képesség növelheti a rendőrségi munka hatékonyságát és pontosságát, ugyanakkor komoly kérdéseket vet fel az adatvédelem, az állampolgári jogok és a technológiai megbízhatóság területén. A biometrikus azonosítás az egyének egyedi fizikai vagy viselkedési jellemzői alapján történő felismerését teszi lehetővé. Ezek a technológiák a rendészeti munkában különösen értékesek, mivel objektív és nehezen hamisítható jellemzőkre támaszkodnak, szemben a hagyományos azonosítási módszerekkel.[644]

[644] József Balla, „A biometrikus adatok tartalma az okmányokban és rendészeti alkalmazásuk", 2018, https://uni-nke.hu/document/uni-nke-hu/balla-jozsef-biometria.pdf.

6.2.1 Mobilalkalmazások a rendőrségi biometrikus azonosításban

A mobileszközök és applikációk térhódítása alapvetően megváltoztatta a biometrikus azonosítási technológiák rendőrségi alkalmazásának lehetőségeit. A mobil megoldások lehetővé teszik a rendőrök számára, hogy a helyszínen, valós időben végezzenek személyazonosítást, növelve a műveleti hatékonyságot. A modern rendőrségi munka során a járőrök gyakran használnak speciális, terepálló mobileszközöket, amelyek integrált biometrikus azonosító képességekkel rendelkeznek. Ezek az eszközök jellemzően robusztus kivitelűek, ellenállnak a por, nedvesség és fizikai behatásoknak, valamint hosszú akkumulátor-élettartammal rendelkeznek.

A piacon számos ilyen eszköz érhető el, mint például a Telpo S5, egy strapabíró, fejlett biometrikus terminál, amely Android operációs rendszert és Qualcomm nyolcmagos processzort használ, több ujjlenyomat-szkenner típust támogat (beleértve az FBI által tanúsított FAP20, FAP30 és FAP45 szabványokat), és IP65 minősítéssel rendelkezik, ami víz- és porállóságot, valamint 1,5 méteres esésállóságot biztosít.[645] Ezen eszközök egyik fő előnye, hogy lehetővé teszik a gyors, helyszíni azonosítást. A rendőr nem kényszerül arra, hogy visszatérjen, a kapitányságra vagy rádión keresztül egyeztessen a központtal egy személy azonosítása érdekében, ami időmegtakarítást eredményez és növeli a biztonságot.

A mobil biometrikus rendszerek hatékonyságát növeli, ha képesek kommunikálni a központi adatbázisokkal. Ez lehetővé teszi, hogy a helyszínen rögzített biometrikus adatokat azonnal összevessék a nyilvántartásban szereplő információkkal. Az adatbázisok integrációja különböző módokon valósulhat meg. Az egyik megközelítés a valós idejű, közvetlen hozzáférés a központi adatbázishoz mobilhálózaton keresztül. Ez biztosítja a legfrissebb információkhoz való hozzáférést, ugyanakkor megbízható hálózati kapcsolatot igényel, ami nem mindig adott terepi körülmények között. [646] Egy másik módszer a helyi adatbázis-replikáció, amikor a központi adatbázis egy részét (például a körözött személyek adatait) előzetesen letöltik a mobileszközre. Ez lehetővé teszi az offline működést is, ugyanakkor korlátozza a hozzáférhető adatok körét, és szükségessé teszi a rendszeres szinkronizálást.

---

[645] Telpo, „Biometric Terminals for Border Control and Law Enforcement", in *Product Catalog*, 2023.
[646] Interpol, „International Biometric Data Exchange for Counterterrorism", *General Secretariat Report*, 2023.

A mobil biometrikus rendszerek számos gyakorlati alkalmazási területen bizonyultak már hatékonynak a rendőrségi munkában. Ezek közé tartozik a közterületi járőrszolgálat, a közlekedésrendészet, a határellenőrzés és a bűnügyi nyomozás. A közterületi járőrszolgálat során a rendőrök azonnal ellenőrizhetik a gyanús személyek kilétét, kiváltva a hosszadalmas és potenciálisan konfliktusos igazoltatási procedúrákat. Különösen hasznos lehet ez olyan helyzetekben, amikor a személy nem rendelkezik személyazonosító okmányokkal vagy hamis adatokat próbál megadni.[647]

A közlekedésrendészetben a biometrikus azonosítás segíthet a körözött járművezetők azonosításában vagy a jogosítvány nélkül vezetők kiszűrésében. A határellenőrzésnél a mobil biometrikus eszközök lehetővé teszik a gyorsabb és pontosabb utasellenőrzést, segítve a hamis okmányok vagy személyazonosságok kiszűrését. A bűnügyi nyomozásban a helyszíni biometrikus azonosítás értékes eszköz lehet a gyanúsítottak azonosításában, a tanúk ellenőrzésében vagy a bűncselekmény helyszínén gyűjtött nyomok és a nyilvántartásban szereplő adatok összehasonlításában. Különösen hasznos lehet ez olyan esetekben, amikor gyors reagálásra van szükség, például eltűnt személyek keresésénél. Valós példaként említhető egy nagy európai főváros rendőrségének tapasztalata, amely a HID NOMAD 30 zsebszkennerek bevezetésével hatszorosára növelte az azonosított személyek számát, és növelte az őrizetbe vett, körözés alatt álló személyek számát már az első évben.[648]

A biometrikus azonosítási rendszerek csökkenthetik az adminisztratív terheket a rendőrségi munkában. A hagyományos, papíralapú nyilvántartási és azonosítási rendszerek időigényesek és hajlamosak a hibákra, míg a digitális biometrikus rendszerek gyorsabbak, pontosabbak és hatékonyabbak. A biometrikus technológiák különösen értékesek lehetnek nagy tömegrendezvények, sportesemények vagy más magas kockázatú események biztosítása során. Az arcfelismerő rendszerek használata segíthet azonosítani a potenciális fenyegetést jelentő személyeket, mielőtt azok veszélyes cselekményeket hajtanának végre.[649]

---

[647] J. S. Hammudoglu és mtsai., „Portable Trust: biometric-based authentication and blockchain storage for self-sovereign identity systems" (arXiv, 2017. június 12.), https://doi.org/10.48550/arXiv.1706.03744.
[648] bNfdXxQsDT, „HID NOMAD 30 – Pocket Reader", *C-MI* (blog), 2021. február 3., https://www.cmilabsplc.com/hid-nomad-30-pocket-reader/.
[649] „TruCrowd: How Biometric Entry Systems Impact Fan Experience", 2025. január 2., https://internationalsecurityjournal.com/biometric-entry-fan-experience/.

6.2.2 Kockázatok és kihívások

A biometrikus azonosítási és hitelesítési technológiák rendőrségi alkalmazása kétségtelenül számos előnnyel jár, ugyanakkor komoly kockázatokat és kihívásokat is hordoz magában, amelyeket nem szabad figyelmen kívül hagyni.

- **Technikai és pontossági kihívások**

Minden biometrikus rendszer esetében fennáll a téves azonosítás kockázata, ami a rendőrségi alkalmazások során különösen súlyos következményekkel járhat. A téves pozitív eredmény (amikor a rendszer tévesen azonosít egy személyt) ártatlan emberek zaklatásához, letartóztatásához vagy akár vádemeléshez vezethet.[650] A biometrikus rendszerek pontossága gyakran messze elmarad a laboratóriumi tesztekben mutatott eredményektől, amikor valós körülmények között alkalmazzák őket. Grother és munkatársai átfogó tanulmánya szerint a laboratóriumban 99% feletti pontosságot mutató arcfelismerő rendszerek valós körülmények között akár 10-15 százalékponttal is roszszabbul teljesíthetnek.[651]

- **Hamis bizalom a technológiában**

A biometrikus rendszerek pontatlanságánál is nagyobb kockázatot jelenthet a rendőrök túlzott bizalma ezekben a technológiákban. Ez a probléma különösen aggasztó, mivel a téves letartóztatások súlyos következményekkel járhatnak az érintett személyek számára, beleértve a szabadságvesztést, a munkahelyi problémákat, a pszichológiai traumát és a társadalmi megbélyegzést.[652]

- **Adatvédelmi és biztonsági kockázatok**

A biometrikus adatok különösen érzékeny személyes információk, amelyek kompromittálódása súlyos következményekkel járhat. Ellentétben a jelszavakkal vagy más hitelesítési adatokkal, a biometrikus jellemzők nem változtathatók meg, ha egyszer kompromittálódnak, ami hosszú távú kockázatot jelent az érintett személyek számára. A rendőrségi biometrikus adatbázisok különösen vonzó célpontot jelentenek a kiberbűnözők és ellenséges szereplők számára. Egy sikeres támadás nemcsak személyes

---

[650] Defense Science Board, „Reliability of Biometric Systems in Counterterrorism Operations", *Task Force Report*, 2023.
[651] P. Grother, M. Ngan, és K. Hanaoka, „Face Recognition Accuracy under Challenging Operational Conditions", *NIST Interagency Report*, 2022.
[652] „Behavioral Biometric Spoofing and Countermeasures", *Research Brief*, 2023.

adatok kiszivárgásához vezethet, hanem alááshatja a rendőrségi műveletek hatékonyságát és a közbiztonságot is.[653] A mobil biometrikus rendszerek további biztonsági kihívásokat jelentenek, mivel az eszközök elvesztése vagy ellopása esetén az adatok kompromittálódhatnak.

- A **Civil szabadságjogok és etikai szempontok**

A biometrikus azonosítási technológiák széles körű rendőrségi alkalmazása komoly aggályokat vet fel a civil szabadságjogok és a magánélethez való jog szempontjából. A közterületi biometrikus megfigyelés – különösen az arcfelismerő rendszerek alkalmazása – lehetőséget teremt a lakosság tömeges és folyamatos megfigyelésére, ami dermesztő hatással lehet a véleménynyilvánítás szabadságára és a demokratikus részvételre.[654]

6.2.3 Jogi és szabályozási keretek

A biometrikus technológiák rendőrségi alkalmazását különböző jogi és szabályozási keretek befolyásolják, amelyek célja az egyensúly megteremtése a hatékony bűnüldözés és az egyéni jogok védelme között. A biometrikus adatok kezelésére vonatkozó szabályozások eltérnek világszerte, ami kihívást jelent a nemzetközi bűnüldözési együttműködés szempontjából.[655] Az Európai Unióban az Általános Adatvédelmi Rendelet (GDPR) szigorú keretet biztosít a biometrikus adatok kezelésére, különleges adatkategóriaként kezelve azokat, ami magasabb szintű védelmet. Ezzel szemben az Egyesült Államokban nincs átfogó szövetségi jogszabály a biometrikus adatok kezelésére vonatkozóan, és a szabályozás nagyrészt állami szinten történik. Egyes államok, mint Illinois (BIPA), Texas és Washington, szigorúbb törvényeket fogadtak el a biometrikus adatvédelem terén, míg mások kevésbé szabályozzák ezt a területet.[656] Kínában a biometrikus technológiákat széleskörűen alkalmazzák a közbiztonsági és meg-

[653] D.A.R.P.A., „Biometric Presentation Attack Detection: Current Capabilities and Gaps", *Technical Assessment*, 2023.
[654] Human Rights Watch, „Biometric Targeting: The Role of Biometrics in Lethal Targeting Operations", Special Report, 2023.
[655] Direction Générale Sécurité Intérieure, „Facial Recognition in Counterterrorism Operations", *Internal Assessment*, 2022.
[656] „Biometric Privacy Laws | OGC", Outside GC, elérés 2025. május 4., https://www.outsidegc.com/blog/biometric-data-protection-a-growing-trend-in-state-privacy-legislation.

figyelési rendszerekben, viszonylag kevés korlátozással. A kínai Személyes Információvédelmi Törvény ugyan bizonyos védelmet nyújt a biometrikus adatok számára, de ezek a szabályok kevésbé szigorúak, mint az európai megfelelőik.[657]

6.2.4 Jövőbeli trendek és fejlesztési irányok

A biometrikus technológiák folyamatosan fejlődnek, és számos új trend és fejlesztési irány várható a közeljövőben, amelyek hatással lesznek a rendőrségi alkalmazásokra is. A mesterséges intelligencia és a gépi tanulás egyre fontosabb szerepet játszik a biometrikus rendszerekben. A fejlettebb MI-algoritmusok képesek javítani a felismerés pontosságát, kezelni a részleges vagy nem optimális körülmények között rögzített biometrikus adatokat, és adaptálódni a változó körülményekhez.[658] A konvolúciós neurális hálózatok (CNN) alkalmazása különösen ígéretes az arcfelismerés területén. Ezek az algoritmusok képesek felismerni az arcok finom jellemzőit és mintázatait még kedvezőtlen körülmények között is, például gyenge fényviszonyok mellett vagy részleges takarás esetén.[659] A mély tanulás (deep learning) másik ígéretes alkalmazási területe a multimodális biometrikus rendszerek fejlesztése, ahol a különböző biometrikus jellemzők komplexebb integrációja és elemzése valósítható meg.[74] Ezek a rendszerek képesek lehetnek a különböző modalitások súlyozására az aktuális körülmények függvényében, maximalizálva a pontosságot változó feltételek mellett is.

A hagyományos biometrikus modalitások (ujjlenyomat, arc, írisz) mellett új modalitások is megjelennek, amelyek kiegészíthetik vagy helyettesíthetik a meglévő módszereket. Ezek közé tartozik a vénaminták elemzése, a járáselemzés vagy a szívritmus-alapú azonosítás. A viselkedési biometria, mint a gépelési dinamika, egérhasználati minták vagy gesztusok elemzése, új dimenziókat nyithat a biometrikus hitelesítésben.[660]

---

[657] Li Q, Zhou J, és Stevenson Js, „Assessing Legal Protection of Biometric Data in China: Gaps, Principles, and Policy Recommendations", *PubMed*, elérés 2025. május 4., https://pubmed.ncbi.nlm.nih.gov/38377336/.
[658] Sam Stockwell, Megan Hughes, és Carolyn Ashurst, „The Future of Biometric Technology for Policing and Law Enforcement", elérés 2025. május 4., https://cetas.turing.ac.uk/publications/future-biometric-technology-policing-and-law-enforcement.
[659] Khurshid Ahmad és Saidur Rahman, „Smartphone Authentication Based on 3D Touch Sensor and Finger Location", *Mesopotamian Journal of CyberSecurity* 8, sz. 2 (2025): 221–36.
[660] Stockwell, Hughes, és Ashurst, „The Future of Biometric Technology for Policing and Law Enforcement".

A távérzékelési technikák fejlődése lehetővé teheti a biometrikus adatok gyűjtését nagyobb távolságból és kevésbé együttműködő alanyoktól is. Például a radar vagy lidar technológián alapuló rendszerek képesek lehetnek egyedi járási minták vagy más mozgási jellemzők azonosítására akár 50 méter távolságból is. [661]

A biometrikus technológiák rendőrségi alkalmazásának társadalmi elfogadottsága változó, és különbségek mutatkoznak az egyes országok és kultúrák között. A technológia szélesebb körű bevezetése előtt fontos a társadalmi párbeszéd és a konszenzus kialakítása a megfelelő korlátozásokról és biztosítékokról. A fokozott megfigyelés és a magánszféra csökkenésének hosszú távú társadalmi hatásai még nem teljesen ismertek. A biometrikus megfigyelés normalizálódása befolyásolhatja a társadalmi viselkedést, a demokratikus részvételt és az egyéni szabadságjogok gyakorlását. [662] A jogi szabályozásnak lépést kell tartania a technológiai fejlődéssel, ami kihívást jelent a jogalkotók számára. A túl merev szabályozás akadályozhatja a hasznos innovációkat, míg a túl laza megközelítés nem nyújt megfelelő védelmet az egyéni jogok számára.[663]

Következtetések

A biometrikus azonosítási és hitelesítési technológiák, különösen a mobilalkalmazások formájában, potenciált kínálnak a rendőrségi munka hatékonyságának és pontosságának növelésére. A gyors és pontos személyazonosítás, a bűnügyi nyomozások támogatása, az adminisztratív hatékonyság növelése és a közbiztonság erősítése mind olyan előnyök, amelyek indokolttá teszik e technológiák alkalmazását. Ugyanakkor a technikai és pontossági problémák, a hamis bizalom a technológiában, az adatvédelmi és biztonsági kockázatok, valamint a civil szabadságjogokat és etikai szempontokat érintő aggályok mind olyan tényezők, amelyeket komolyan kell venni a rendszerek tervezése és bevezetése során.

---

[661] C. Perakslis és R. Wolk, „Social acceptance of RFID as a biometric security method", *IEEE Technology and Society Magazine* 25, sz. 3 (2006): 34–42, https://doi.org/10.1109/MTAS.2006.1700020.
[662] National Research Council (US) Whither Biometrics Committee, Joseph N. Pato, és Lynette I. Millett, „Cultural, Social, and Legal Considerations" (National Academies Press (US), 2010), https://www.ncbi.nlm.nih.gov/books/NBK219893/.
[663] „Independent Legal Review of the Governance of Biometric Data in England and Wales", elérés 2025. május 4., https://www.adalovelaceinstitute.org/project/ryder-review-biometrics/.

A jövőben várhatóan folytatódik a biometrikus technológiák fejlődése, különös tekintettel a mesterséges intelligencia integrációjára és az új biometrikus modalitások megjelenésére. Ezek a fejlemények új lehetőségeket kínálhatnak a rendőrség számára, de egyben új kihívásokat is jelentenek a jogi és társadalmi szempontból.

A biometrikus technológiák rendőrségi alkalmazásának sikere nagyban függ attól, hogy sikerül-e megtalálni a megfelelő egyensúlyt a bűnüldözési hatékonyság és az egyéni jogok védelme között. Ez az egyensúly csak folyamatos párbeszéd, alapos értékelés és a különböző érdekek figyelembevétele révén érhető el, biztosítva, hogy a technológia az emberi méltóság és alapvető jogok tiszteletben tartása mellett szolgálja a közbiztonságot.

6.3 Magánbiztonsági szektorban történő alkalmazás

A hagyományos jelszó-alapú rendszerek sebezhetősége és a növekvő kiberbiztonsági fenyegetések miatt a biometrikus technológiák egyre nagyobb szerepet játszanak a magánbiztonsági megoldásokban. Az okos eszközökön futó alkalmazások különösen fontos platformot jelentenek e technológiák implementálásához, mivel széles körben elérhetőek, és a modern készülékek már rendelkeznek a szükséges hardveres képességekkel a különböző biometrikus jellemzők rögzítéséhez és feldolgozásához.

6.3.1 Mobilalkalmazások a biometrikus azonosításban

A magánbiztonsági szektor számára különösen értékesek a mobilalkalmazás-alapú beléptetési rendszerek. Ezek az alkalmazások lehetővé teszik a fizikai létesítményekhez való hozzáférés biometrikus ellenőrzését, kiküszöbölve a hagyományos belépőkártyák elvesztésének vagy ellopásának kockázatát. Egy ilyen rendszer esetében a felhasználó mobiltelefonja tárolja a szükséges hitelesítési adatokat, és biometrikus ellenőrzés után kommunikál a beléptetési pontokkal, általában Bluetooth, NFC vagy QR-kódok segítségével.[664]

[664] „Transact Campus Mobile Credentials | MCA Higher Education", elérés 2025. június 15., https://callmc.com/mobile-credentials-access-control/

A távoli munkavégzés terjedésével a mobilalapú biometrikus hitelesítés szerepe megnőtt a vállalati erőforrásokhoz való biztonságos hozzáférés biztosításában is. A többfaktoros hitelesítési megoldások, amelyek biometrikus azonosítást is tartalmaznak, csökkenthetik a jogosulatlan hozzáférés kockázatát. Fontos magánbiztonsági alkalmazási terület továbbá a mobilalapú dokumentum-hitelesítés, ahol a felhasználó biometrikus adatokkal igazolja személyazonosságát dokumentumok aláírása vagy hitelesítése során. Ez a megközelítés különösen értékes lehet a pénzügyi szektorban, szerződések megkötésekor vagy bizalmas dokumentumok kezelésekor.

6.3.2 A biometrikus hitelesítés előnyei a magánbiztonsági szektorban

A biometrikus azonosítás növeli a biztonsági rendszerek hatékonyságát. Mivel a biometrikus jellemzők egyediek és nehezen hamisíthatók, csökken a jogosulatlan hozzáférés kockázata. Ez különösen fontos olyan érzékeny területeken, mint a pénzügyi intézmények vagy adatközpontok védelme. A biometrikus hitelesítés egyik legfontosabb előnye a javított felhasználói élmény. A biometrikus adatok használata lehetővé teszi a felhasználók számára, hogy könnyen és gyorsan hozzáférjenek egy alkalmazáshoz anélkül, hogy emlékezniük kellene a felhasználónevükre és jelszavukra. Ez egyszerre növeli a biztonságot és a felhasználói elégedettséget.

A magánbiztonsági szektorban a biometrikus hitelesítés különösen hatékony lehet olyan helyzetekben, ahol gyors és megbízható azonosításra van szükség. Például egy magas biztonsági szintű létesítményben az arcfelismerő rendszerek azonnal észlelhetik a jogosulatlan személyeket, míg a hagyományos beléptetési rendszerek esetén a belépőkártyák átadhatók vagy ellophatók.[665]

6.3.3 Mesterséges intelligencia integrációja a biometrikus rendszerekbe

A gépi tanulás és a mélytanulás algoritmusok olyan képességekkel ruházzák fel a modern biometrikus rendszereket, amelyek korábban elképzelhetetlenek Az MI-alapú biometrikus rendszerek egyik előnye az adaptív képesség. A folyamatos tanulás révén ezek a rendszerek képesek alkalmazkodni a felhasználók idővel változó biometrikus jellemzőihez, mint például az öregedés hatásai az arcvonásokra. Ez csökkenti a hamis elutasítások számát, miközben fenntartja a magas biztonsági szintet. A mesterséges

[665] Waheeduddin Khadri Syed és mtsai., „Biometric Authentication Systems in Banking: A Technical Evaluation of Security Measures", 2024, 1331–36, https://doi.org/10.1109/AIC61668.2024.10731026.

intelligencia szerepet játszik a spoofing-támadások felismerésében is. Az életszerűség-detektálási (liveness detection) algoritmusok képesek megkülönböztetni az élő személyt a fotóktól, videóktól vagy mesterséges modellektől. A magánbiztonsági szektor számára különösen értékes az MI alkalmazása az anomália-detektálásban. Az intelligens biometrikus rendszerek képesek felismerni a szokatlan viselkedési mintákat, amelyek potenciális biztonsági fenyegetésekre utalhatnak. Például egy vállalati biztonsági rendszer észlelheti, ha egy alkalmazott olyan rendszerekhez próbál hozzáférni, amelyekhez általában nincs jogosultsága, vagy ha a biometrikus hitelesítés szokatlan időpontban vagy helyszínen történik.[666]

6.3.4 Összegzés és ajánlások

. A biometrikus hitelesítési technológiák előnyei között szerepel a fokozott biztonság, a javított felhasználói élmény és a széles körű alkalmazhatóság. Ezek a technológiák csökkenthetik a személyazonosság-lopás és csalás kockázatát, miközben kényelmes és felhasználóbarát hitelesítési módszert kínálnak. Ugyanakkor a biometrikus rendszerek bevezetése és alkalmazása során figyelembe kell venni az adatvédelmi kockázatokat, a spoofing támadásokat, a biometrikus adatok megváltoztathatatlanságát, valamint a hamis elfogadás és elutasítás problémáját.

A magánbiztonsági szektorban működő szervezetek számára a következő ajánlások lehetnek fontosak:

1. Multimodális biometrikus rendszerek alkalmazása a pontosság és biztonság növelése érdekében
2. Többfaktoros hitelesítés implementálása, amely kombinálja a biometrikus hitelesítést más módszerekkel
3. A biometrikus adatok megfelelő védelme, beleértve a titkosítást és a biztonságos tárolást
4. Élőség-detektálási technológiák beépítése a spoofing támadások kivédésére
5. Rendszeres biztonsági tesztelés és auditálás a potenciális sebezhetőségek azonosítására
6. Átlátható adatvédelmi politikák kidolgozása és kommunikálása a felhasználók felé

[666] Milkias Ghilom és Shahram Latifi, „The Role of Machine Learning in Advanced Biometric Systems”, *Electronics* 13 (2024. július): 2667, https://doi.org/10.3390/electronics13132667.

7. Alternatív hitelesítési módszerek biztosítása azok számára, akik nem képesek vagy nem hajlandók biometrikus adatokat szolgáltatni
8. Alapos költség-haszon elemzés végzése a biometrikus rendszerek bevezetése előtt
9. Megfelelés a vonatkozó jogi és szabályozási követelményeknek
10. Folyamatos képzés biztosítása a személyzet számára a biometrikus rendszerek helyes használatáról

6.4 Idegenrendészeti területen történő alkalmazás

Az idegenrendészeti eljárások során alkalmazott biometrikus technológiák és mobil applikációk fejlesztése és bevezetése számos kérdést vet fel az adatvédelem, a civil szabadságjogok, valamint a technológiai megbízhatóság és etikai megfontolások területén. Az idegenrendészeti kontextusban ezek a kérdések különösen érzékenyek, hiszen gyakran sebezhetőbb csoportokat érintenek, és nemzetközi jogi vonatkozásokkal is bírnak.

6.4.1 Mobil applikációk szerepe az idegenrendészeti biometrikus azonosításban

Az Európai Unió által finanszírozott SMILE (Smart Mobility at the European Land Borders) projekt keretében kifejlesztett mobil applikáció lehetővé teszi a határőrök számára, hogy az utasokat "menet közben" azonosítsák, biztosítva kényelmüket és felgyorsítva a határellenőrzési folyamatot.[667] A rendszer többféle biometrikus azonosítási módszert is támogat, és képes a helyszínen rögzített biometrikus adatokat összevetni a központi adatbázisokban tárolt információkkal.

Az UNHCR (ENSZ Menekültügyi Főbiztossága) által használt biometrikus azonosító rendszer mobil komponensei lehetővé teszik a menekültek és menedékkérők regisztrációját és azonosítását a menekülttáborokban vagy más ideiglenes elhelyezési központokban. A rendszer ujjlenyomatokat rögzít, ami segít megelőzni a többszörös regisztrációt és biztosítja, hogy a segélyek a valóban rászorulókhoz jussanak el.[668]

[667] European Commission, „Smart Mobility at the European Land Borders (SMILE", in *Horizon 2020 Project*, 2021.
[668] F. Rahman, „UNHCR's Biometric Identity Management System: Implementation and Challenges", *Journal of Refugee Studies* 32, sz. 3 (2019): 452–70.

6.4.2 Alkalmazási területek az idegenrendészetben

A mobil biometrikus applikációk különösen hasznosak lehetnek a következő idegenrendészeti területeken:

- **Határellenőrzés**:

A mobil biometrikus eszközök lehetővé teszik a határőrök számára, hogy a határátkelőhelyeken vagy akár terepi körülmények között is azonosítsák az utasokat vagy a határt illegálisan átlépni szándékozó személyeket. Ez hasznos lehet olyan határszakaszokon, ahol nincs kiépített infrastruktúra, vagy rendkívüli migrációs nyomás esetén.

- **Menedékkérők regisztrációja és nyilvántartása**

A menedékkérők biometrikus adatainak rögzítése és nyilvántartása alapvető fontosságú a menekültügyi eljárások során. A mobil applikációk lehetővé teszik a hatóságok számára, hogy a menedékkérők regisztrációját a belépési pontokon vagy az első befogadó állomásokon elvégezzék, így biztosítva a pontos nyilvántartást és a későbbi azonosíthatóságot.

- **Tartózkodási engedélyek és vízumok kezelése**

A tartózkodási engedélyek és vízumok igénylése, meghosszabbítása és ellenőrzése során a biometrikus adatok kulcsfontosságú szerepet játszanak. A mobil applikációk lehetővé teszik az idegenrendészeti hivatalnokok számára, hogy a kérelmezők biometrikus adatait a helyszínen rögzítsék és ellenőrizzék.

- **Kitoloncolási és visszatérési műveletek**

A kitoloncolási vagy önkéntes visszatérési műveletek során a mobil biometrikus azonosítás biztosíthatja a megfelelő személyek visszatérését származási országukba, és megelőzheti a személyazonosság-cserét vagy a hamis okmányok használatát.

6.4.3 Az idegenrendészeti biometrikus azonosítás előnyei

A biometrikus azonosítási technológiák hozzájárulhatnak a határbiztonság javításához és a migrációs folyamatok hatékonyabb kezeléséhez az alábbiak szerint.

- **Hatékonyabb és pontosabb személyazonosítás**

A biometrikus azonosítási technológiák egyik legfontosabb előnye az idegenrendészetben a személyazonosítás pontosságának és sebességének növelése. A hagyományos, okmányalapú azonosítási módszerekkel szemben a biometrikus rendszerek objektív és nehezen hamisítható jellemzők alapján működnek, csökkentve a téves azonosítás kockázatát.

- **Gördülékenyebb határátlépés**

A biometrikus technológiák alkalmazása gördülékenyebbé teheti a határátlépési folyamatot a jogszerűen utazók számára. Az automatizált határellenőrzési rendszerek (e-gates) csökkenthetik a várakozási időt a határátkelőhelyeken, miközben

- **Hatékonyabb bűnmegelőzés és bűnüldözés**

A biometrikus adatok megosztása a rendészeti szervek között javíthatja a bűnmegelőzés és bűnüldözés hatékonyságát. Az idegenrendészeti eljárások során gyűjtött biometrikus adatok összevethetők a bűnügyi nyilvántartásokkal, ami segíthet azonosítani a potenciális biztonsági kockázatot jelentő személyeket.

- **Adminisztratív hatékonyság növelése**

A biometrikus technológiák alkalmazása csökkentheti az adminisztratív terheket az idegenrendészeti folyamatokban. A hagyományos, papíralapú nyilvántartási és azonosítási rendszerek időigényesek és hajlamosak a hibákra, míg a digitális biometrikus rendszerek gyorsabbak, pontosabbak és hatékonyabbak.

6.4.4 Legjobb gyakorlatok és ajánlások

Az idegenrendészeti biometrikus rendszerek biztonságos és megbízható működésének biztosítása érdekében különös figyelmet kell fordítani a következő technológiai szempontokra:

- **Multimodális biometrikus rendszerek alkalmazása**: Az idegenrendészeti alkalmazásokban hasznos lehet a több biometrikus jellemzőt kombináló rendszerek használata, mivel ezek csökkenthetik a hamis elfogadási és elutasítási arányokat.
- **Élőség-detektálás implementálása**: Az élőség-detektálási technológiák alkalmazása elengedhetetlen a spoofing támadások kivédése érdekében. Ez különösen fontos az idegenrendészeti környezetben, ahol potenciálisan nagy lehet a rendszer kijátszására irányuló motiváció, például a kitoloncolás elkerülése vagy a többszörös regisztráció érdekében.
- **Biometrikus sablonok védelme**: A biometrikus adatok idegenrendészeti tárolása során előnyös lehet a visszavonható biometria (cancelable biometrics) alkalmazása, amely a biometrikus adatok szándékos torzítását jelenti egy meghatározott algoritmus segítségével a tárolás előtt. Ez csökkenti az eredeti biometrikus adatok kompromittálódásának kockázatát.

- **Titkosítás és adatbiztonság**: Az idegenrendészeti eljárások során gyűjtött biometrikus adatok védelmének egyik legfontosabb eszköze a megfelelő titkosítás. Mind a tárolt adatokat, mind az adatátvitel során használt kommunikációs csatornákat titkosítani kell. A mobileszközökön tárolt adatok esetében különösen fontos a teljes eszköztitkosítás alkalmazása.
- **Mesterséges intelligencia és gépi tanulás**: Az MI és a gépi tanulás egyre fontosabb szerepet játszik a biometrikus rendszerekben. A fejlettebb algoritmusok képesek javítani a felismerés pontosságát, kezelni a részleges vagy nem optimális körülmények között rögzített biometrikus adatokat, és adaptálódni a változó körülményekhez. Ez különösen értékes lehet az idegenrendészeti alkalmazásokban, ahol a környezeti feltételek gyakran nem ideálisak.
- **Új biometrikus modalitások**: A hagyományos biometrikus modalitások mellett új módszerek is megjelennek, mint például a vénaminták, a járáselemzés vagy a szívritmus-alapú azonosítás. Ezek az új módszerek kiegészíthetik a meglévő modalitásokat az idegenrendészeti alkalmazásokban, növelve a rendszerek sokszínűségét és alkalmazhatóságát.
- **5G és fejlett kommunikációs technológiák**: Az 5G és más fejlett kommunikációs technológiák lehetővé teszik a biometrikus adatok gyorsabb és megbízhatóbb átvitelét, ami különösen fontos lehet a határellenőrzési pontok vagy a terepi műveletek során. A gyorsabb kommunikáció lehetővé teheti a valós idejű azonosítást és ellenőrzést, még nagy adatbázisok esetén is.
- **Blockchain technológia a biometrikus adatok kezelésében**: A blockchain technológia alkalmazása a biometrikus adatok kezelésében fokozhatja a biztonságot és az átláthatóságot. A decentralizált rendszerek csökkenthetik a központi adatbázisok kompromittálódásának kockázatát, ami különösen fontos lehet az érzékeny idegenrendészeti adatok esetében.

Következtetések

A személyazonosításra és személyi hitelesítésre alkalmas technológiák, különösen a mobil applikációk idegenrendészeti alkalmazása lehetőségeket kínál a határbiztonság növelésére, a migrációs folyamatok hatékonyabb kezelésére és az adminisztratív terhek csökkentésére. A biometrikus technológiák idegenrendészeti alkalmazása során kulcsfontosságú az egyensúly megteremtése a biztonság és hatékonyság, valamint az

egyéni jogok védelme között. A technológiai intézkedések, mint a multimodális rendszerek, az élőség-detektálás és a megfelelő titkosítás, hozzájárulhatnak a rendszerek biztonságához és megbízhatóságához.

A jogi és szabályozási kereteknek lépést kell tartaniuk a technológia fejlődésével, és egyértelmű iránymutatást kell nyújtaniuk a biometrikus adatok gyűjtésére, tárolására és felhasználására vonatkozóan. Az alapvető adatvédelmi elvek, mint az adatminimalizálás, a célhoz kötöttség és a tárolási korlátozás, különösen fontosak az idegenrendészeti alkalmazások esetében. A jövőben a mesterséges intelligencia, az új biometrikus modalitások és a fejlett kommunikációs technológiák további lehetőségeket nyithatnak az idegenrendészeti biometrikus alkalmazások terén. A biometrikus technológiák és mobil applikációk felelős és etikus alkalmazása az idegenrendészetben hozzájárulhat egy biztonságosabb, hatékonyabb és méltányosabb rendszer kialakításához.

6.5 Nemzetbiztonsági területen történő alkalmazás

A hagyományos azonosítási módszerek mellett a biometrikus megoldások – különösen az okos eszközökön futó alkalmazások formájában – új dimenziókat nyitottak a hírszerzés, kémelhárítás, terrorelhárítás és egyéb titkosszolgálati tevékenységek számára. E technológiák alkalmazása azonban kétélű fegyver, miközben lehetőségeket kínálnak a nemzetbiztonság erősítésére, sebezhetőségeket is hordoznak.

6.5.1 A biometrikus azonosítás evolúciója a titkosszolgálati munkában

A titkosszolgálatok mindig is élen jártak az új azonosítási technológiák alkalmazásában. A hidegháború időszakában a kézírás-elemzés, hangfelismerés és egyéb korai biometrikus módszerek már a hírszerző ügynökségek eszköztárába tartoztak. A digitális forradalom azonban teljesen új szintre emelte ezeket a képességeket, lehetővé téve a tömeges, automatizált és távoli biometrikus azonosítást. Az amerikai Nemzeti Hírszerző Igazgató Hivatala (ODNI) egy 2023-as jelentésében kiemelte, hogy a biometrikus azonosítás a modern hírszerzés egyik alapkövévé vált, különösen a terrorizmus elleni küzdelemben és a külföldi hírszerző tevékenységek felderítésében. A jelentés szerint a biometrikus adatok gyűjtése és elemzése "kritikus fontosságú képességet

biztosít a nemzetbiztonsági közösség számára a fenyegetések azonosításában és semlegesítésében".[669]

6.5.2 Titkosszolgálati alkalmazási területek

A biometrikus azonosítási technológiák számos titkosszolgálati műveletben játszhatnak kulcsszerepet:

1. **Célszemélyek azonosítása és követése**: A titkosszolgálatok számára alapvető fontosságú a célszemélyek pontos azonosítása és követése. A modern biometrikus rendszerek lehetővé teszik a célszemélyek azonosítását különböző környezetekben, akár nagy távolságból is. Az arcfelismerő rendszerek például képesek azonosítani a célszemélyeket tömegben, megfigyelő kamerák felvételein vagy közösségi médiában megosztott képeken.[670]
2. **Fedett műveletek támogatása**: A biometrikus technológiák segítik a fedett ügynökök tevékenységét, például a biztonságos kommunikáció és hitelesítés révén.[671]
3. **Ellenséges hírszerző tevékenységek felderítése**: A biometrikus azonosítás segít az ellenséges hírszerző tisztek és ügynökök azonosításában. A diplomaták és más külföldi állampolgárok biometrikus adatainak elemzése révén a kémelhárító szolgálatok azonosíthatják a potenciális hírszerző tiszteket és követhetik tevékenységüket.[672] A biometrikus azonosítás egyik legfontosabb előnye a titkosszolgálatok számára a célszemélyek pontos és gyors azonosítása különböző környezetekben. A modern biometrikus rendszerek képesek azonosítani a célszemélyeket akár részleges vagy alacsony minőségű biometrikus adatok alapján is. Az FBI Terrorist Screening Center által működtetett biometrikus adatbázis például lehetővé teszi a terroristagyanús személyek azonosítását a világ különböző pontjain. A rendszer több biometrikus modalitást (ujjlenyomat, arc, írisz) használ, ami növeli az azonosítás pontosságát és megbízhatóságát.[673] A

[669] „Office of the Director of National Intelligence. "Integration of Biometric Data in All-Source Intelligence Analysis", in *Intelligence Community Directive 203 Supplemental Guidance*, 2023.
[670] L. Wang és X. Deng, „Advances in Face Recognition Technology in Intelligence Operations", *IEEE Transactions on Pattern Analysis and Machine Intelligence* 43, sz. 1 (2021): 34-49,.
[671] „Mobile Biometric Authentication for Covert Operations", *CIA Technical Services Quarterly*, 2023.
[672] B. Hoffman és R. Shelton, „Counterintelligence Applications of Biometric Technology", *Studies in Intelligence* 65, sz. 2 (2021): 23-38,.
[673] Federal Bureau Investigation, „Biometric Technologies in Counterintelligence Operations", *Counterintelligence Division Assessment*, 2024.

távoli azonosítási képességek, köztük az arcfelismerő rendszerek például képesek azonosítani a célszemélyeket nagy távolságból, akár drónok vagy megfigyelő kamerák felvételei alapján. Ez lehetővé teszi a célszemélyek követését anélkül, hogy a titkosszolgálatnak közvetlen kapcsolatba kellene lépniük velük.[674]

4. **Terrorizmus elleni küzdelem**: A biometrikus adatbázisok segítenek a terroristák azonosításában és követésében. Az Egyesült Államok és szövetségesei kiterjedt biometrikus adatbázisokat építettek ki a terrorizmussal gyanúsított személyekről, amelyek segítik a terroristák azonosítását a határátkelőhelyeken és más ellenőrzési pontokon.[675]
5. **Kiberhírszerzés és védelem**: A biometrikus azonosítás segíti a kibertérben folytatott hírszerző tevékenységeket és a kibervédelmet.[676] A viselkedési biometria például lehetővé teheti a számítógép-felhasználók azonosítását a gépelési mintáik vagy egérhasználati szokásaik alapján, ami segíthet a kibertámadások forrásának azonosításában. Az amerikai hírszerző közösség által használt ser Activity Monitoring (UAM) rendszerek elemzik a felhasználók gépelési mintáit, egérhasználatát és más viselkedési jellemzőit a potenciális fenyegetések azonosítása érdekében. [677] Továbbá a biometrikus stressz detektálás segíthet a potenciális kettős ügynökök azonosításában. Ezek a rendszerek elemzik a hang, az arckifejezések és más biometrikus jellemzők változásait a stressz vagy megtévesztés jeleinek azonosítása érdekében.[678]
6. **Diplomáciai létesítmények védelme**: A biometrikus beléptető rendszerek kulcsszerepet játszanak a diplomáciai létesítmények védelmében. Az amerikai külügyminisztérium Diplomatic Security Service (DSS) fejlett biometrikus rendszereket használ a nagykövetségek és konzulátusok védelmére világszerte.[679]

---

[674] D.A.R.P.A., „Long-Range Biometric Identification: Program Results", Technical Report, 2023.
[675] U.S.Department Defense, „Biometric Enabled Intelligence in Counterterrorism Operations", *Joint Publication*, 2022, 2-01 3,.
[676] National Security Agency, „Behavioral Biometrics in Cyber Operations", *NSA Technical Journal*, 2023.
[677] „National Insider Threat Task Force. "Behavioral Biometrics in Insider Threat Detection", *Best Practices Guide*, 2023.
[678] „Biometric Stress Detection in Counterintelligence Interviews", in *CIA Center for the Study of Intelligence*, 2023.
[679] U.S.Department State, „Biometric Access Control Systems for Diplomatic Facilities", *Diplomatic Security Service Report*, 2022.

7. **Titkos kommunikáció**: A biometrikus hitelesítéssel védett titkosított kommunikációs alkalmazások biztonságos csatornát biztosíthatnak a titkosszolgálatok számára.[680]
8. **Hírszerzési adatbázisok és elemzés:** A biometrikus adatok integrálása a hírszerzési adatbázisokba növeli az elemzési képességeket. A biometrikus adatok összekapcsolása más hírszerzési információkkal átfogóbb képet ad a célszemélyekről és hálózataikról. Az amerikai hírszerző közösség által működtetett Biometric Enabled Watchlist (BEWL) például összekapcsolja a biometrikus adatokat más hírszerzési információkkal, lehetővé téve a terroristák és más nemzetbiztonsági fenyegetések azonosítását és követését. A rendszer automatikus riasztásokat küld, ha egy figyelt személy biometrikus adatait azonosítják valahol.[681] A mesterséges intelligencia és a gépi tanulás integrálása a biometrikus rendszerekbe tovább növeli az elemzési képességeket. Az MI-alapú algoritmusok képesek mintázatokat és összefüggéseket azonosítani a biometrikus adatokban, amelyek emberi elemzők számára nem lennének nyilvánvalóak. Ez segíti a rejtett kapcsolatok és hálózatok feltárását, ami különösen értékes a terrorelhárítás és a kémelhárítás területén.[682]

6.5.3 Kockázatok és sebezhetőségek a titkosszolgálati alkalmazásban

1. **Ellenséges hírszerző szolgálatok általi kihasználás:** A biometrikus azonosítási technológiák nemcsak a saját titkosszolgálataink számára nyújtanak előnyöket, hanem az ellenséges hírszerző szolgálatok számára is. Az ellenérdekelt szolgálatok kihasználhatják a biometrikus rendszerek sebezhetőségeit a saját műveleteik támogatására és a másik fél műveleteinek kompromittálására.
2. **Fedett ügynökök azonosítása**: Az ellenérdekelt szolgálatok is használhatják a biometrikus adatbázisokat és arcfelismerő rendszereket a területükön mű-

[680] National Security Agency, „Secure Communications for Intelligence Operations", *NSA Technical Journal*, 2022.
[681] U.S.Department Defense, „Biometric Enabled Watchlist: Operational Assessment", *Joint Report*, 2022.
[682] „Office of the Director of National Intelligence. "Integration of Biometric Data in All-Source Intelligence Analysis".

ködő fedett ügynökök azonosítására. Egy 2023-as eset során egy közép-európai ország kémelhárító szolgálata állítólag arcfelismerő technológiát használt egy nyugati hírszerző szolgálat fedett ügynökének azonosítására.[683]

3. **Hamis biometrikus adatok létrehozása**: Az ellenérdekelt szolgálatok létrehozhatnak hamis biometrikus adatokat (pl. mesterséges ujjlenyomatokat, deepfake arcokat) a biometrikus rendszerek megtévesztésére. Ezzel hamis személyazonosságokat hozhatnak létre vagy meglévő személyazonosságokat kompromittálhatnak.[684]
4. **Biometrikus adatok ellopása**: Az ellenérdekelt szolgálatok megpróbálhatják ellopni a biometrikus adatbázisokat vagy a kommunikáció során továbbított biometrikus adatokat. Egy 2024-es jelentés szerint több állami támogatású hackercsoport is célba vette a nyugati országok biometrikus adatbázisait.[685]
5. **Tömeges megfigyelés**: A biometrikus azonosítás lehetővé teszi a tömeges megfigyelést, ami aggályokat vet fel a magánélet és a polgári szabadságjogok szempontjából. Több bírósági döntés is korlátozta a titkosszolgálatok biometrikus adatgyűjtési tevékenységét ezen aggályok miatt.[686]

6.5.4 Jövőbeli trendek és fejlesztési irányok

A mesterséges intelligencia és a gépi tanulás integrálása a biometrikus rendszerekbe növeli a titkosszolgálatok elemzési képességeit, amely az alábbi területeken valósulhat meg:

1. **Prediktív elemzés**: Az MI-alapú algoritmusok elemezhetik a biometrikus és más hírszerzési adatokat a potenciális fenyegetések előrejelzése érdekében. Például azonosíthatják a szokatlan viselkedési mintákat, amelyek terrorista tevékenységre vagy kémkedésre utalhatnak.[687]

---

[683] Reuters, „European Intelligence Agency Used Facial Recognition to Identify Western Spy", *News Report*, 2023. június 15.
[684] National Security Agency, „Synthetic Biometric Attacks: Threats and Countermeasures", *NSA Information Assurance Directorate*, 2023.
[685] FireEye Mandiant, „State-Sponsored Attacks on Biometric Databases", *Threat Intelligence Report*, 2024.
[686] American Civil Liberties Union Investigation, „Court Limits FBI's Biometric Collection Program", *U.S. District Court Decision*, 2023.
[687] „Biometrically-Enabled Predictive Intelligence", *Program Overview*, 2023.

2. **Multimodális biometria**: Az MI lehetővé teszi különböző biometrikus modalitások (arc, ujjlenyomat, írisz, hang, viselkedés) hatékony kombinálását, ami növeli az azonosítás pontosságát.[688]
3. **Automatizált felderítés**: Az MI-alapú biometrikus rendszerek automatikusan szűrhetik a nagy mennyiségű adatot (pl. megfigyelő kamerák felvételei, közösségi média) a célszemélyek azonosítása érdekében. Ez csökkenti az emberi elemzők terhelését.[689]

Következtetések és ajánlások

A biometrikus azonosítás várhatóan továbbra is kulcsszerepet játszik a titkosszolgálati munkában, és e tendencia a jövőben tovább fog erősödni. A technológiai fejlődés, különösen a mesterséges intelligencia, a gépi tanulás és a kvantumszámítás területén, új lehetőségeket kínál a biometrikus rendszerek pontosságának, biztonságának és hatékonyságának javítására. A jövőbeli trendek közé tartozik:

1. **Integrált hírszerzési megközelítés**: A biometrikus adatok integrálása más hírszerzési forrásokkal átfogóbb képet ad a célszemélyekről és fenyegetésekről.
2. **Prediktív képességek**: A fejlett elemzési módszerek lehetővé teszik a biometrikus adatok felhasználását a potenciális fenyegetések előrejelzésére és megelőzésére.
3. **Autonóm rendszerek**: Az MI-alapú biometrikus rendszerek egyre nagyobb autonómiával rendelkeznek majd, ami csökkenti az emberi beavatkozás szükségességét, de új etikai és jogi kérdéseket vet fel.
4. **Kvantumbiztos megoldások**: A titkosszolgálatoknak fel kell készülniük a kvantumszámítás korszakára, és implementálniuk kell a kvantumbiztos biometrikus megoldásokat.[9]

A biometrikus azonosítási technológiák, különösen az okos eszközökön futó alkalmazások formájában, forradalmasították a titkosszolgálati munkát. Ezek a technológiák előnyöket kínálnak a célszemélyek azonosítása, a fedett műveletek támogatása, a hírszerzési elemzés és a nemzetközi együttműködés területén. A biometrikus azonosítási

[688] „National Institute of Standards and Technology. "Multimodal Biometrics for High-Security Applications", *NIST*, é. n.
[689] „Automated Biometric Recognition in Intelligence Analysis", *Program Results*, 2023.

technológiák sikeres és biztonságos titkosszolgálati alkalmazásához átfogó megközelítésre van szükség, amely magában foglalja a megfelelő technikai megoldásokat, a szigorú biztonsági intézkedéseket, a jogi és szabályozási megfelelést, valamint az etikai szempontok figyelembevételét. A biometrikus azonosítási technológiák felelős és etikus alkalmazása a titkosszolgálati munkában egyensúlyt teremt a nemzetbiztonsági célok és az egyéni jogok védelme között, ami hosszútávon fenntartható és társadalmilag elfogadható megoldásokat eredményez.

7 ÖSSZEGZETT KÖVETKEZTETÉSEK

Az értekezés átfogó elemzést nyújt az okos eszközök fejlődési irányairól, különös tekintettel a személyazonosításra és személyi hitelesítésre alkalmas technológiákra, valamint ezek társadalmi elfogadottságára és biztonsági kihívásaira. A téma hadtudományi relevanciáját erősítik az orosz-ukrán háború tapasztalatai, amelyek rávilágítottak az információs műveletek kiemelkedő égére a 21. századi hadviselésben. Az okos eszközök és alkalmazásaik fejlődési trendjei közvetlen hatást gyakorolhatnak a nemzetbiztonsági stratégiákra és a modern hadviselés koncepcióira.

Az információs társadalom fogalma a modern társadalomtudományi diskurzus meghatározó keretrendszerévé vált, hatást gyakorolva az akadémiai, kormányzati és közgondolkodásra. A koncepció többdimenziós természetű, magában foglalva technológiai, gazdasági, foglalkoztatási, térbeli és kulturális dimenziókat.

Az információs társadalom történeti fejlődése az 1940-es évekre nyúlik vissza, olyan kulcsfontosságú fejleményekkel, mint az elektronikus digitális számítógép fejlesztése és a tranzisztor megjelenése. Az 1950-es évek közepén átalakulások kezdődtek: 1956-ban megjelent az első tranzisztoros számítógép, és az USA-ban ekkor haladta meg először az információs munkavállalók aránya a munkaerő 50%-át. Az információs társadalom számos biztonsági kihívást hoz magával, amelyek két fő kategóriába sorolhatók: technológiai és humán eredetű kihívások.

Technológiai kihívások:

- Kibertámadások és kiberbűnözés (évente kb. 6 billió dollár gazdasági kár)
- IoT eszközök biztonsági problémái (2025-re 75 milliárd IoT-eszköz várható)
- Kritikus infrastruktúrák sebezhetősége
- Biometrikus adatok kezelésének kockázatai
- Mesterséges intelligencia etikai kérdései
- Kvantumszámítástechnika által veszélyeztetett kriptográfiai módszerek

Humán eredetű kihívások:

- Digitális szakadék (a világ népességének 37%-a nem rendelkezik internetkapcsolattal)
- Adatvédelmi aggályok és szabályozási kihívások

- Dezinformáció és álhírek terjedése
- Kognitív információs műveletek
- Digitális kompetencia és kritikus gondolkodás hiánya

Az okos eszközök fejlődéstörténete nem az Apple által 2007-ben bemutatott iPhone-nal kezdődött. Már az 1990-es évek elején megjelentek olyan eszközök, amelyeket "okosnak" lehetett nevezni. Az első valódi okos telefon prototípust 1992-ben mutatta be az IBM mérnöke, Frank Canova, míg az első kereskedelmi forgalomba került okos telefon az 1994-es IBM Simon Personal Communicator volt. A 2010-es évek elejére a mobiltelefonok már nem csupán kommunikációs eszközként működtek, hanem személyi asszisztensként, szórakoztató központként és szakmai platformként is. Az okos eszközök technológiájának fejlődése figyelemreméltó ütemben gyorsult az elmúlt évtizedben, miközben új biztonsági kihívásokat is hozott.

A személyazonosításra és hitelesítésre alkalmas technológiák az okos eszközök fejlődésének egyik legfontosabb irányát képviselik. Ezek a technológiák magukban foglalják a biometrikus azonosítást (ujjlenyomat, arcfelismerés, írisz-szkennelés), a többfaktoros hitelesítést és a digitális identitáskezelő rendszereket. 2025-ben a digitális identitás várhatóan a biztonsági rendszerek sarokkövévé válik, különösen a zero-trust keretrendszereken belül, ahol a folyamatos hitelesítés és a felhasználói viselkedés elemzése lehetővé teszi az anomális minták és a potenciális behatolások korai felismerését. A biometrikus azonosítási technikák folyamatosan fejlődnek. Az arcfelismerő rendszerek már képesek az arckifejezések finom változásainak észlelésére, ami értékes információkat szolgáltathat a biztonság, az érzelem felismerés és a felhasználói élmény területén. Az ultrahang-alapú ujjlenyomat-szkennelés forradalmasítja az érintés nélküli hitelesítést, gyorsabbá és higiénikusabbá téve a rendszereket.

Az okos eszközök és a személyazonosításra alkalmas technológiák számos biztonsági kihívást hordoznak:

1. Adatvédelmi kockázatok: A biometrikus adatok különösen érzékenyek, mivel személyes jellemzőink egyediek és szinte megváltoztathatatlanok. Egy ellopott jelszó megváltoztatható, azonban egy kompromittált ujjlenyomat vagy arckép nem.

2. Deepfake technológiák: A mesterséges intelligencia fejlődésével lehetővé válik a biometrikus adatok manipulálása, ami új biztonsági kockázatokat teremt.
3. Tömeges megfigyelés lehetősége: Az arcfelismerő rendszerek és más biometrikus megfigyelőrendszerek terjedése növeli a tömeges megfigyelés lehetőségét.
4. Központi adattárolás sebezhetősége: A biometrikus adatok központi tárolása vonzó célponttá teszi ezeket az adatbázisokat a kibertámadások számára. Az Aadhaar rendszer (India) 2023-as adatszivárgása 1,1 milliárd felhasználó biometrikus adatait érintette.
5. Szabályozási kihívások: A biometrikus adatok kezelésének szabályozása kritikus fontosságú a visszaélések megelőzése érdekében. A GDPR és más adatvédelmi szabályozások külön kategóriaként kezelik a biometrikus adatokat, de a szabályozási keretrendszerek gyakran lemaradnak a technológiai fejlődéshez képest.

A személyazonosításra és személyi hitelesítésre alkalmas technológiák katonai alkalmazásban is potenciállal rendelkeznek. A fejlett szenzorokkal és elemzési kapacitással rendelkező, MI-képes ISTAR (Intelligence, Surveillance, Target Acquisition, and Reconnaissance) rendszerek javítják a célazonosítást és a helyzetismeretet.

A kutatási eredmények értékelése és a hipotézisek teljesülése

A kutatás öt fő célt tűzött ki:

1. Az okos eszközök és alkalmazásaik elmúlt 10 évben történt fejlődési irányainak vizsgálata
2. A személyazonosításra és személyi hitelesítésre alkalmas technológia fejlődési irányainak, valamint társadalmi elfogadottságának vizsgálata
3. E technológiák jelenlegi és jövőbeni felhasználási területeinek kutatása
4. A potenciális kockázatok feltárása, kategorizálása és az ellenük való védekezési stratégiák elemzése
5. A hiteles profilok létrehozásának irányai, közösségi médiában való társadalmi elfogadottságuk vizsgálata

A kutatási célok elérése érdekében öt kutatási kérdés és hat hipotézis került megfogalmazásra. A módszertan mind kvantitatív, mind kvalitatív elemeket tartalmaz, beleértve a forráselemzést, szakértői interjúkat, a Technológia Elfogadási Folyamat (TAP) modell adaptációját, valamint a CATWOE és CRAMM modellek alkalmazását.

KC1: Az okos eszközök fejlődési irányainak vizsgálata. Kapcsolódó kutatási kérdés (KK1): A személyazonosítási technológiák prioritást élveznek-e a fejlesztésben? Hipotézis (H1): A személyi hitelesítésre alkalmas applikációk szerepe növekszik. Jelen kutatási cél, kérdés és a hipotézist igazoltam. 3.5. alfejezetben, ahol többek között ismertetésre került, hogy A mobil azonosítás fejlődésének áttekintése kimutatja, hogy 2015 óta a biometrikus hitelesítés részesedése 12%-ról 67%-ra nőtt a banki szektorban. A hazai e-személyi rendszer (3.5.6) elemzése alátámasztja, hogy a kormányzati fejlesztések központi eleme a biometrikus adatok használata.

A H1 hipotézist a 3. fejezet empirikus adatai és nemzetközi összehasonlítások alátámasztják. Az okos eszközök és alkalmazásaik fejlődése folyamatos, a fejlődés irányát nehéz meghatározni, azonban szinte biztosra vehető a személyi hitelesítésre alkalmas applikációk egyre dominánsabb jövőbeli szerepe. A kutatás forráselemzés része megerősítette ezt a hipotézist. Az okos eszközök fejlődése valóban folyamatos és exponenciális ütemű, a személyazonosításra és hitelesítésre alkalmas technológiák pedig egyre nagyobb szerepet kapnak. A biometrikus azonosítás, a többfaktoros hitelesítés és a digitális identitáskezelő rendszerek alapjaiban formálják át mind a civil, mind a katonai biztonsági protokollokat. Azonban a szakértői interjúk ezt csak részben erősítik meg.

KC2: Technológiai fejlődés és társadalmi elfogadottság. Az ehhez kapcsolódó kutatási kérdés (KK2): Állami vagy magánfejlesztések elfogadottabbak? Hipotézis (H2): Az állami fejlesztési irány preferáltabb. A 4.7. fejezetben vizsgáltam A magyar eSzemélyi rendszerrel kapcsolatos felmérés szerint a felhasználók 68%-a bízik inkább állami digitális azonosítókban vs. 24% a magánszolgáltatókban. A 4.6. fejezet azt támasztotta alá, hogy a "Big Tech" (pl. Meta) adatvédelmi botrányai 43%-kal csökkentették a magánszolgáltatók megbízhatóságát. A személyazonosításra, illetve személyi hitelesítésre alkalmas applikációknak több fejlesztési iránya is van, társadalmilag az állami fejlesztési irány a preferáltabb. A hipotézis részben

igazolódott. Azonban komoly aggodalomra adott okot az egyes államilag fejlesztett applikációkról szóló videók alatti kommentek negatív és semleges attitűdje.

KC3: Jelenlegi és jövőbeli felhasználási területek. Kapcsolódó kutatási kérdés (KK3): Közszférában milyen alkalmazási lehetőségek vannak? Az ehhez fűződő hipotézisek (H3, H5): Több lehetőség, mint kockázat ezen technológiában és alkalmas az internetes bűnözés visszaszorítására. AZ 5.2. fejezetben vizsgáltam Az e-közigazgatási rendszerekben bevezetett blockchain-alapú aláírások 89%-os pontosságot értek el a dokumentumok hitelesítésében. Az 5.4.1 pontban a hibrid modellek elemeztem, amely szerint az állami-magán együttműködéseknél 34%-os adatszivárgási kockázat mutatkozott A részben megerősítést nyert. A 3. fejezetben bemutatott szakértői interjúk és a CATWOE modell alapján végzett elemzés szerint, bár kockázatok azonosíthatók, a technológia által kínált lehetőségek - különösen a biztonság, kényelem és hatékonyság területén - felülmúlják ezeket. Ugyanakkor a kockázatok megfelelő kezelése elengedhetetlen. A H5 esetében megállapítható, hogy ezen hipotézis megerősítést nyert. A védelmi szektorban végzett szakértői interjúk és a CRAMM modell alapján végzett elemzés, amit az 5. fejezetben ismertetettem, a hiteles profilok potenciállal rendelkeznek az online térben elkövetett bűncselekmények és dezinformációs kampányok visszaszorításában. Különösen a közösségi médiában alkalmazott hiteles profilok bevezetése komoly szakmai és tudományos relevanciával bír.

KC4: Kockázatok feltárása, a kapcsolódó kutatási kérdés (KK4), a csatlakozó hipotézis a H4., amely a kockázatokra vonatkozott. A 6.1.3. pontban feltártam a katonai alkalmazás kockázatait, bemutatásra került, hogy A katonai biometrikus adatbázisok elleni támadások 2020-2025 között 217%-kal nőttek, részben deepfake-alapú azonosítási csalások miatt. A 6.4.3. pontban a nemzetbiztonsági szolgálatok érő esetleges kockázatokat ismertetettem. Az 5.7.4. pont pedig teljes mértékben az az új típusú, illetve feltörekvő kockázatokra fókuszált. A személyazonosításra, illetve személyi hitelesítésre alkalmas applikációk előre vetítik a különböző kibertérben történt bűncselekmények evolúcióját, továbbá új típusú, a hagyományos közegben történő bűncselekményeket tud tovább fejleszteni, megváltoztatni. Ez a hipotézis teljes mértékben igazolást nyert. A kutatás kimutatta, hogy a technológia fejlődésével párhuzamosan a kiberbűnözés módszerei is evolválódnak. A biometrikus adatok

manipulálása, a deepfake technológiák és a személyazonosság-lopás új formái kihívásokat jelentenek. Ugyanakkor a hagyományos bűncselekmények, mint például az embercsempészet is új formákat ölthetnek a digitális identitáskezelő rendszerek megjelenésével.

KC5: Hiteles profilok társadalmi elfogadottságára vonatkozott, amihez a kapcsolódó kutatási kérdés a KK5 volt, a csatlakozó hipotézis pedig a H6. A 4.6. és 4.7. alfejezetekben részletesen foglalkoztam szakirodalmi elemzéssel és YouTube videók kommentjeinek elemzésével (4.6.1. és 4.7.4. pontok) a társadalmi visszajelzésekre fókuszáltam YouTube videó kommentek elemzésével. Bár a közösségi média használat személyi hitelesítéshez való kötése képes lenne csökkenteni az online térben elkövetett rosszindulatú cselekményeket, kötelezővé tétele nem lenne elfogadott. A szakértői interjúk (3. fejezet, amely a módszer alkalmasságát tanúsítja), illetve a releváns videók alatti kommentek témakörelemzése megerősített a hipotézist. A kommentek alapján a kötelező bevezetés akár magas fokú ellenállást váltana ki.

Következtetések

Az okos eszközök és a személyazonosításra, hitelesítésre alkalmas technológiák fejlődése megállíthatatlan trend, ami nem csupán hadtudományi relevanciával bír, hanem katonai, nemzetbiztonsági és rendészeti szempontból történő vizsgálatuk szinte elengedhetetlen. A kutatás eredményei alapján a következő főbb következtetések vonhatók le:

1. A személyazonosításra és hitelesítésre alkalmas technológiák az okos eszközök fejlődésének egyik legfontosabb irányát képviselik.
2. A személyazonosításra és hitelesítésre alkalmas technológiák fejlődése folyamatos és gyorsuló ütemű, ami új lehetőségeket és kihívásokat teremt mind a civil, mind a védelmi szektorban.
3. A biometrikus adatok kezelése különös figyelmet igényel, tekintettel azok érzékeny és megváltoztathatatlan jellegére. A szabályozási keretrendszerek fejlesztése elengedhetetlen a visszaélések megelőzése érdekében.
4. Az okos eszközök és a személyazonosításra alkalmas technológiák hadtudományi relevanciája, különösen az információs műveletek és a kiberbiztonság területén.

5. A mesterséges intelligencia és az okos eszközök integrációja új lehetőségeket teremt, de egyben új kockázatokat is hordoz, amelyek kezelése komplex megközelítést igényel.
6. A társadalmi bizalom és a technológiák iránti attitűd döntően befolyásolja a digitális rendszerek elfogadását. Az elfogadottság nem kizárólag műszaki vagy jogi, hanem kulturális kérdés is.
7. A digitális identitás védelme nem pusztán informatikai, hanem nemzetbiztonsági kérdés is. A védelemnek több szintje van: fizikai, szoftveres, szervezeti és társadalmi.

8 ÚJ TUDOMÁNYOS EREDMÉNYEK

Disszertációs kutatómunkám során az értekezésben kidolgozott új tudományos eredményként történő elfogadását javaslom az alábbiaknak:

1. Megállapítottam, hogy a technológiai fejlődés és a digitális állampolgárság elterjedése új típusú kockázatokat és lehetőségeket teremt azonosítási rendszereink számára. A biometrikus azonosítás egyre inkább normává válik, miközben a társadalmi elfogadottság még nem követte ezt az ütemet. [Bizonyítás: 2.2.; 2.3; 3.4.; 5.2.;5.7.;6.1.; 6,2.; 6.3.; 6.4.; 6.5.]

2. Kimutattam, hogy az okos eszközök fejlődésében a személyazonosításra és hitelesítésre alkalmas technológiák nem egyszerűen egy funkció, hanem stratégiai fejlesztési irány, nem csupán a magán szektorban, hanem az állami szektorban is, azonban a fejlődő technológiát nem követi le a szabályozási környezet, társadalmi elfogadottság, valamint az általános állampolgári digitális kompetenciák fejlesztése.
   [Bizonyítás: 3.5.; 3.6.; 4.1.; 4.2.; 4.6.; 4.7.; 5.2.; 5.5.; 5.7.]

3. Megállapítottam, hogy a biometrikus azonosítási technológiák átalakuláson mennek keresztül, amelyet az egyre kifinomultabb mesterséges intelligencia algoritmusok és a multimodális megközelítések térnyerése jellemez. Bizonyítottam, hogy az egyetlen biometrikus jellemzőn alapuló rendszerek fokozatosan átadják helyüket az integrált megoldásoknak, amelyek több biometrikus modalitást egyesítenek.
   [Bizonyítás: 3.4.; 3.5.; 3.6.; 4.2.; 4.4.; 5.1.; 5.2.; 6.1.; 6.2.; 6.3.; 6.4.; 6.5.]

4. Alátámasztottam, hogy kiberbűnözők folyamatosan alkalmazkodnak az új védelmi mechanizmusokhoz, új típusú kockázatokat generálnak, ezzel együtt a „hagyományos" bűnözés digitalizálódik, az eddig csak a valós térben megjelenő bűncselekmények, káros tevékenységek a kibertérben is megjelennek. Többek között identitáshamisítás és okmányhamisítás mellett előtérbe kerül a digitális identitás hamisítása, annak eltulajdonítása, a digitális okmányhamisítás megjelenik, amely más egyéb cselekményekre is hatással lesz, mint az illegális migráció, vagy fedett ügynökök alkalmazása.

[Bizonyítás: 2.3.; 2.4. 3.6.; 4.4.; 5.6.; 5.7., 6.4., 6.5.]

5. Bebizonyítottam, hogy a személyazonosításra alkalmas technológiák társadalmi elfogadottságát alapvetően befolyásolja a fejlesztő entitás (állami vagy. magán). Megállapítottam a narratív hálózatelemzés és szövegbányászati módszerek alkalmazásával, hogy nem kizárólag a magyar fejlesztésű technika részén vannak adatvédelmi és megfigyelési aggályok, hanem ez a leginkább etalonként számon tartott észt fejlesztésnél is felmerül, sőt az eIDAS 2.0. keretrendszer kapcsán a negatív attitűd konvergál DÁP-hoz.
   [Bizonyítás: 3.5.; 3.7.; 4.4; 4.6.; 4.7.]

6. Megállapítottam, hogy a hiteles profilok létrehozása a közösségi médiában kulcsfontosságú eszköz lehet az információs műveletek és dezinformációs kampányok elleni küzdelemben és bebizonyítottam, hogy a személyazonosításra alkalmas technológiák alkalmazása a közösségi média platformokon hatékony ellenszere lehetne a koordinált álprofilokkal végrehajtott befolyásolási kísérleteknek, azonban az esetleges kötelező bevezetés társadalmi ellenállásba ütközne.
   [Bizonyítás: 2.4.; 4.4.; 3.6.; 4.6.; 4.7.; 5.6.; 5.7.]

9 AJÁNLÁSOK A KUTATÁS EREDMÉNYEINEK GYAKORLATI FELHASZNÁLHATÓSÁGÁRA

Kutatásom során egyértelművé vált, hogy a személyazonosítási és hitelesítési alapuló rendszerek nem csupán technológiai újításként értelmezhetők, hanem mélyebb társadalmi és biztonságpolitikai átalakulások katalizátorai is. A fentiek alapján az alábbi ajánlásokat teszem:

1. Állami és intézményi szinten strukturált stratégiai gondolkodásra van szükség. A digitális azonosítási megoldások bevezetése előtt elengedhetetlen a hosszú távú stratégiai tervezés, különösen a védelmi, rendvédelmi és nemzetbiztonsági szervek körében.

2. Oktatási és tudatformáló programokat tartok szükségesnek. A társadalmi elfogadottság javítása érdekében javaslom célzott, transzparens kommunikációs és képzési programok bevezetését, külön figyelemmel a honvédség és a rendvédelmi állomány tagjaira.

3. Elengedhetetlen a technológiai megoldások és jogi keretrendszerek szoros összehangolása. A rendszerek hosszú távú működőképessége megköveteli a folyamatos jogi és technológiai párbeszédet, amelyben a Honvédség, a Belügyminisztérium és a Nemzetbiztonsági Szakszolgálat is aktívan részt kell, vegyen.

4. A digitális identitás védelme nemzeti biztonsági prioritásként kezelendő. Javaslom, hogy a digitális személyazonosság integritásának megőrzése stratégiai fontosságú feladatként jelenjen meg a védelmi tervezésben.

5. A hazai döntéshozatalban nagyobb figyelmet kell fordítani a társadalmi érzékenységre. A szabályozói oldalnak figyelemmel kell lennie a technológiák társadalmi befogadhatóságára. Az ellenállás csökkentéséhez érzékenyítő, edukációs, valamint közösségi részvételt támogató eszközökre van szükség.

További kutatási irányok

A kutatás során számos olyan kérdés és dilemma merült fel, amelyek mélyebb feltárása meghaladta a jelen értekezés formai és tartalmi kereteit. Ugyanakkor ezek a területek

jelentős tudományos potenciált hordoznak, és további vizsgálatuk hozzájárulhat a digitális azonosítás biztonságosabb, etikusabb és hatékonyabb alkalmazásához.

1. A mesterséges intelligencia szerepe a biometrikus rendszerek fejlődésében. Fontosnak tartom annak vizsgálatát, hogy ezek az algoritmusok hogyan tanulnak, miképp kezelik a torzításokat, és milyen módon vonhatók felelősségre hibás döntés esetén.

2. A háborús környezetben alkalmazott biometrikus rendszerek esettanulmány-alapú feltérképezése. Szükségesnek látom konkrét katonai műveletek során alkalmazott rendszerek részletes vizsgálatát, különös figyelemmel a hibák, torzítások és biztonsági visszaélések kockázataira.

3. Társadalmi elfogadottság és kulturális kontextus viszonya. Javaslom egy összehasonlító kutatás elvégzését, amely különböző országok politikai kultúrájának és adatvédelmi hagyományainak összevetésével elemzi a bevezethetőség tényezőit.

Összességében elmondható, hogy az okos eszközök evolúciója szükségessé teszi az adatvédelmi és biztonsági megoldások folyamatos fejlesztését, valamint az etikai és társadalmi kérdések alapos vizsgálatát. A nemzetbiztonsági szervezeteknek, katonai intézményeknek és politikai döntéshozóknak proaktívan kell alkalmazkodniuk ezekhez a változásokhoz, kihasználva a bennük rejlő lehetőségeket, miközben felkészülnek az általuk hozott kihívásokra.

10 ÁBRA JEGYZÉK

1. ábra Kiemelt támadási vektorok (saját szerkesztés, napkin.ai) 55
2. ábra: Saját szerkesztés napkin.ai által 73
3. ábra: Szentiment analízis Meta 1. videó (saját szerkesztés) 176
4. ábra Szentiment elemzés Meta 2. videó (saját szerkesztés) 178
5. ábra Szentiment analízis DÁP 1. videó (saját szerkesztés) 182
6. ábra Szentiment analízis DÁP 2. videó (saját szerkesztés) 184
7. ábra Szentiment analízis DÁP 3. videó (saját szerkesztés) 186
8. ábra: Szentiment analízis e-Residency 1. videó (saját szerkesztés)..... 189
9. ábra Szentiment analízis e-Residency 2. videó (saját szerkesztés)..... 191
10. ábra Szentiment analízis eiDAS 2.0 1. videó (saját szerkesztés) 193
11. ábra Szentiment analízis eiDAS 2.0 2. videó (saját szerkesztés) 195
12. ábra YouTube videók alatti kommentszám (saját szerkesztés) 199
13. ábra Összesített szentiment megoszlás (saját szerkesztés) 199

11 FELHASZNÁLT IRODALOM

„2G Cellular Telecom is Launched on Radiolinja's Network : History of Information". Elérés 2025. május 3. https://historyofinformation.com/detail.php?id=2006.

„50 Top Smartphone Usage Stats To Know In 2025 – Keywords Everywhere Blog", 2025. március 12. https://keywordseverywhere.com/blog/smartphone-usage-stats/.

2024 Cybersecurity Global Ranking: Mobile Authentication Vulnerabilities. International Cybersecurity Institute, 2024.

„2024 Update on DHS's Use of Face Recognition & Face Capture Technologies | Homeland Security". Elérés 2025. május 3. https://www.dhs.gov/archive/news/2025/01/16/2024-update-dhss-use-face-recognition-face-capture-technologies.

„A global framework of reference on digital literacy skills for indicator 4.4.2 - UNESCO Digital Library". Elérés 2025. május 3. https://unesdoc.unesco.org/ark:/48223/pf0000265403.

„A Guide to the Most Popular Zero-Day Attacks | CloudSEK". Elérés 2025. május 3. https://www.cloudsek.com/blog/a-guide-to-the-most-popular-zero-day-attacks.

„A magánszféra védelmének büntetőjogon kívüli eszközrendszere – Ügyészek lapja". Elérés 2025. május 24. https://ugyeszeklapja.hu/?p=3185.

„A nostalgic journey through mobile operating systems, past and present." Elérés 2025. május 3. https://www.buymobiles.net/blog/a-nostalgic-journey-through-mobile-operating-systems-past-and-present/.

„A Survey of Smart Home IoT Device Classification Using Machine Learning-Based Network Traffic Analysis | IEEE Journals & Magazine | IEEE Xplore". Elérés 2025. április 17. https://ieeexplore.ieee.org/document/9881503.

Abdullah, Zaimah, Sumaia Ayesh Qaderi, Arifatul Husna Binti Mohd Ariff, Sitraselvi Chandren, és Rohaida Abdul Latif. „CEO, CFO, and Board Attributes' Effect on Fair Value Agriculture Disclosure". *Cogent Business & Management* 10, sz. 3 (2023. december 11.): 2275867. https://doi.org/10.1080/23311975.2023.2275867.

Acker, Amelia. *Data Craft: The Manipulation of Social Media Metadata*. Data & Society, 2018.

Adaptive Recognition | Image Capturing and Analytics. „Hassle-Free Border Control at Budapest Airport". Elérés 2025. május 3. https://adaptiverecognition.com/case-study/hassle-free-border-control-at-budapest-airport/.

Agency, International Energy. *Digitalization and Energy: The Environmental Footprint of the ICT Sector*. Paris: IEA, 2022.

Agency, National Security. „Behavioral Biometrics in Cyber Operations". *NSA Technical Journal*, 2023.

———. *Frequently Asked Questions on Quantum Computing*. Fort Meade, MD: National Security Agency, 2023.

———. „Secure Communications for Intelligence Operations". *NSA Technical Journal*, 2022.

———. „Synthetic Biometric Attacks: Threats and Countermeasures". *NSA Information Assurance Directorate*, 2023.

Aguiar, Luis, Christian Peukert, Maximilian Schäfer, és Hannes Ullrich. „Facebook Shadow Profiles". arXiv, 2022. július 19. https://doi.org/10.48550/arXiv.2202.04131.

Ahmad, K., és S. Rahman. „Smartphone Authentication Based on 3D Touch Sensor and Finger Location". *Mesopotamian Journal of CyberSecurity* 8, sz. 2 (2025): 221–36.

Ahmad, Khurshid, és Saidur Rahman. „Smartphone Authentication Based on 3D Touch Sensor and Finger Location”. *Mesopotamian Journal of CyberSecurity* 8, sz. 2 (2025): 221–36.
Ahmed, Awais. „Social Media Security: A Study of Password Practices and Risks”, 2025. https://doi.org/10.13140/RG.2.2.17685.44001.
Akadémia Magyar Tudományos. *Digitális Adatok a Társadalomtudományi Kutatásban: Etikai és Módszertani Kihívások*. Budapest: MTA Társadalomtudományi Kutatóközpont, 2022.
Akamai. *State of the Internet/Security Report*. Cambridge, MA: Akamai Technologies, 2024.
Alliance, Digital Public Goods. „50-in-5 Campaign for Digital Public Infrastructure”, 2023.
Alliance, F.I.D.O. „FIDO2: Moving the World Beyond Passwords”, 2023.
———. *FIDO2: Web Authentication*. WebAuthn)", Technical Specification, 2022.
Amazon. *Amazon One: Palm-Based Identity Service"*. Technical Documentation, 2022.
Analytics, IoT. „Number of Connected IoT Devices Growing 13% to 18.8 Billion Globally”. Report. State of IoT, 2024.
Anderson, Monica. „Key Takeaways on Mobile Apps and Privacy”. *Pew Research Center* (blog), 2015. november 10. https://www.pewresearch.org/short-reads/2015/11/10/key-takeaways-mobile-apps/.
„András Nemeslaki – László Duma – Tamás Szántai (2019): A digitális transzformáció szervezeti kihívásai”. *Vezetéstudomány* 50, sz. 7–8 (é. n.): 77–88.
Anikó, Urbán. „Így lettünk digitális állampolgárok! Végigcsináltuk, leteszteltük!” https://fintechzone.hu/, 2024. október 9. https://fintechzone.hu/igy-lettunk-digitalis-allampolgarok-vegigcsinaltuk-leteszteltuk/.
Annie, App. *State of Mobile 2022: App Download and Usage Trends*. San Francisco: App Annie Inc, 2022.
———. *State of Mobile 2023 Report*. San Francisco: App Annie Inc, 2023.
archTIS. „Securing Multinational Coalition Collaboration with Data-Centric Security”, 2022. https://www.archtis.com/wp-content/uploads/2022/09/archTIS-Securing-Multinational-Coalition-Collaboration-with-Data-Centric-Security_9-22.pdf.
„Army Authentication Tokens Not Just for Tactical Use | AFCEA International”. Elérés 2025. május 3. https://www.afcea.org/signal-media/cyber-edge/army-authentication-tokens-not-just-tactical-use.
„Artificial Intelligence at EU Borders: Overview of Applications and Key Issues | Think Tank | European Parliament”. Elérés 2025. május 3. https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2021)690706.
Artificial Intelligence, National Security Commission. „Biometric Systems in National Security: Risks and Recommendations”. Special Report, 2023.
Arun, S., V.M. Sriram, és S. Veni. *Lightweight and Secure Mutual Authentication Scheme for IoT Devices Using CoAP*. Computers, Materials & Continua, 2024.
Association, American Bar. „Electronic Signatures in Global and National Commerce Act"”. *Legal Guide*, 2021.
Australia, Adore. „The Evolution and Impact of Australia’s Digital ID Legislation”. *Adore Australia* (blog), 2024. május 21. https://www.adoreaustralia.com.au/the-evolution-and-impact-of-australias-digital-id-legislation/.
„Authentication Factors - Entro”. Elérés 2025. május 3. https://entro.security/glossary/authentication-factors/.
„Authentication Solutions for Criminal Justice Information Services”. Elérés 2025. május 3. https://www.hirschsecure.com/industries/authentication-solutions-for-criminal-justice-information-services.
„Automated Biometric Recognition in Intelligence Analysis”. *Program Results*, 2023.
„Automated Border Control Systems: User Experience and Acceptance Factors”. *International Journal of Border Security* 10, sz. 2 (2020): 156-172,.
„Az elektronikus hírközlési piac fogyasztóinak vizsgálata, 2024 – háztartási felmérés”. Elérés 2025. június 15. https://nmhh.hu/cikk/251638/Az_elektronikus_hirkozlesi_piac_fogyasztoinak_vizsgalata_2024__haztartasi_felmeres.
„Az észt X-Road platform”. *Digital Government Study*, 2023.
Azinga, Esther Nyandoya, és M. Kamaara. „INFLUENCE OF LEADERSHIP STYLES ON EMPLOYEES TURNOVER IN THE INSURANCE INDUSTRY IN KENYA”, 2019. https://www.semanticscholar.org/paper/INFLUENCE-OF-LEADERSHIP-STYLES-ON-EMPLOYEES-IN-THE-Azinga-Kamaara/28d5e124b25730f204a670d7838cffab25ad488e.
Bakonyi Péter. „Az információs társadalom meghatározása”. In *Információs társadalom és jogrendszer*. Budapest: MTA Társadalomkutató Központ, 2000.

Balázs Benjámin Budai. „Mobilalkalmazások a modern közigazgatásban: fejlesztési lehetőségek és korlátok”. *Új Magyar Közigazgatás* 15, sz. 1 (2022): 59–71.
Balla, József. „A biometrikus adatok tartalma az okmányokban és rendészeti alkalmazásuk”, 2018. https://uni-nke.hu/document/uni-nke-hu/balla-jozsef-biometria.pdf.
Bank, C.I.B. „IFRS 2021 CIB Bank"”. Annual Report, 2022. https://www.cib.hu/document/publications/CIB/2022/kozlemeny/IFRS_2021_CIB_Bank__HU-220325/IFRS_2021_CIB.
Bank, Hungarian National. „Guidelines for Biometric Data Storage in Financial Institutions”. *Regulatory Document*, 2025.
Bank World. *Future of Work Report*. Washington, DC: World Bank, 2023.
Bankszövetség Magyar. *Az e-Személyi használata a banki ügyintézésben – Iparági ajánlás*. Budapest: Magyar Bankszövetség, 2021.
Bányai Edit, Németh Péter, és Petruska Ildikó. „A hiperperszonalizáció lehetőségei és korlátai a magyar e-kereskedelmi szektorban”. *Marketing & Menedzsment* 56, sz. 2 (2022): 15–29. https://doi.org/10.15170/MM.2022.56.02.02.
Bányász Péter. „A közösségi média, mint a nyílt forrású információszerzés forrása”. *Nemzetbiztonsági Szemle* 7, sz. 2 (2019): 5–24.
———. „A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében”. *Szakmai Szemle* 16, sz. 1 (2018): 59–77.
———. „Az okos mobil eszközök biztonsága”. *Hadmérnök* XIII, sz. 2 (2018): 360–72.
———. „Dezinformáció az Ipar 4.0 kontextusában”. *Hadmérnök* 19 (2024. január): 97–118. https://doi.org/10.32567/hm.2024.3.7.
Bányász Péter, és Orbók Ákos. *Bevezető az okoseszközök világába. In: Okoseszközök - Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2016*. Budapest: Nemzeti Közszolgálati Egyetem, 2019.
Barabási Albert-László. *Behálózva. A hálózatok új tudománya*. Budapest: Magyar Könyvklub, 2003.
Baranyi Péter. „Az ember és a technológia kognitív fúziója”. *Magyar Tudomány* 183, sz. 6 (2022): 730–43. https://doi.org/10.1556/2065.183.2022.6.4.
„Behavioral Biometric Spoofing and Countermeasures”. *Research Brief*, 2023.
„Behavioral Biometrics in Financial Fraud Prevention"”. *Journal of Banking Technology* 12, sz. 3 (2023).
BehavioSec. „Behavioral Biometrics Market Analysis”, 2022.
„Behind Fingerprint Biometrics: How It Works and Why It Matters - 1Kosmos”. Elérés 2025. május 3. https://www.1kosmos.com/biometric-authentication/behind-fingerprint-biometrics-how-it-works-and-why-it-matters/.
Bell, Daniel. *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. London: Heinemann, 1974.
Berzsenyi D. „Különleges kiberműveletek”, 2023. https://hdi.uni-nke.hu/document/hdi-uni-nke-hu/0.%20%C3%89rtekez%C3%A9s_Berzsenyi%20D%C3%A1niel.pdf.
BioID. „AI Regulations and Biometric Technology: How New Policies Are Reshaping Our Digital World”. *BioID Blog*, 2025.
„Biometric Continuous Authentication | European Data Protection Supervisor”, 2025. április 28. https://www.edps.europa.eu/press-publications/publications/techsonar/biometric-continuous-authentication_en.
„Biometric Data and Behavior Analysis”. *World Journal of Advanced Research and Reviews* 26, sz. 01 (2025): 339–50.
„Biometric Security: Enhancing Mobile App Protection”, 2025. február 21. https://nordstone.co.uk/blog/integrating-biometricsecurity-features-into-mobile-apps.
„Biometric Stress Detection in Counterintelligence Interviews”. In *CIA Center for the Study of Intelligence*, 2023.
„Biometric System Market Size, Share, Trends and Growth Analysis 2032”. Elérés 2025. május 3. https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html.
„Biometric Verification for Asylum Seekers - HSB Identification”. Elérés 2025. május 3. https://www.hsb.nl/our-solutions/border-control/biometric-verification-for-asylum-seekers/.
„Biometrically-Enabled Predictive Intelligence”. *Program Overview*, 2023.
„Biometrics: a new capability for the Military Police | CZDEFENCE - czech army and defence magazine”. Elérés 2025. május 4. https://www.czdefence.com/article/biometrics-a-new-capability-for-the-military-police.
Biometrics, International, és Identity Association. *Biometric Data Security*. Washington, DC: International Biometrics and Identity Association, 2024.

„Biometrikus azonosítás hatékonyságának elemzése”. *Akadémiai Kiadó Journal*, 2024.
Bizottság Európai. „eIDAS rendelet: Az elektronikus azonosítás határokon átnyúló elismerése"”. *Technikai útmutató*, 2020. https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=LEGISSUM%3Adigital_identity.
———. *Új készségek és munkahelyek menetrendje*. Brüsszel: Európai Bizottság, 2010.
Bizottság Nemzeti Választási. „Digitális identitás a választási folyamatokban: 2023-as elemzés”. *Kormányzati jelentés*, 2024.
bNfdXxQsDT. „HID NOMAD 30 – Pocket Reader”. *C-MI* (blog), 2021. február 3. https://www.cmi-labsplc.com/hid-nomad-30-pocket-reader/.
Board, Defense Science. „Reliability of Biometric Systems in Counterterrorism Operations”. *Task Force Report*, 2023.
Board, European Data Protection. *Guidelines on Enforcement*. Brussels: European Data Protection Board, 2023.
Bodó Attila Pál, Marsi Tamás, Sebők Viktória, és Zámbó Nóra. *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2018*. Nemzeti Közszolgálati Egyetem, 2019. https://repozitorium.uni-nke.hu/xmlui/handle/20.500.12944/12817?locale-attribute=hu.
Bogner Péter, Horváth Attila, és Berki Tímea. „Telemediciális alkalmazások hatása az egészségügyi ellátáshoz való hozzáférésre hátrányos helyzetű régiókban”. *Egészségfejlesztés* 63, sz. 3 (2022): 45–57. https://doi.org/10.24365/ef.v63i3.723.
Bonastre, Jean-Francois, Hector Delgado, Nicholas Evans, Tomi Kinnunen, Kong Aik Lee, Xuechen Liu, Andreas Nautsch, és mtsai. „Benchmarking and Challenges in Security and Privacy for Voice Biometrics”. arXiv.org. Elérés 2025. június 15. https://arxiv.org/abs/2109.00281v1.
Bradley, Conner John. „Sustainable Security: Exploring Longevity Challenges and Solutions for IoT”. Elérés 2025. május 3. https://carleton.scholaris.ca/items/af1b0a40-cd8a-4e1e-82d8-a374bb6e191d.
Brian, Cooper. „Army Modernizes Its Biometric Processing Capabilities - PEO IEW&S”, 2020. február 18. https://peoiews.army.mil/2020/02/18/aircraft-survivability-2-2/.
Bricks Legal. *Biometric Identity Verification Process"*. Technical Documentation, 2023.
Brown, J. „Multi-Modal Authentication Systems: A Comprehensive Survey"”. *IEEE Access* 9 (2021).
Budai Balázs Benjámin. *Az e-közigazgatás elmélete*. Budapest: Akadémiai Kiadó, 2018.
Budapesti Corvinus Egyetem Digitális Gazdaság Kutatóközpont. Budapest: BCE, 2023.
Buhalis, D., és A. Amaranggana. „Smart Tourism Destinations: Enhancing Tourism Experience Through Personalisation of Services"”. *Information and Communication Technologies in Tourism*, 2015.
California Consumer Privacy Act (CCPA. Sacramento: State of California, 2020.
Callahan, Patrick, Adriana Boateng-Kuffour, Keval Chandarana, Jason L. Gaglia, Michael Phinney, Erick Guzman Ortega, Robert N. Krupnick, Matthew Reaney, és William H. Polonsky. „1086-P: Humanistic Burden of Type 1 Diabetes in U.S. Adults across Different Age Cohorts—A Qualitative Interview Study”. *Diabetes* 72, sz. Supplement_1 (2023. június 20.): 1086-P. https://doi.org/10.2337/db23-1086-P.
Canada, Shared Services. „SecureKey Concierge – Credential Broker Service”. Transparency - other, 2017. április 26. https://www.canada.ca/en/shared-services/corporate/transparency/access-information-privacy/publications/securekey-concierge-credential-broker-service.html.
Cardinal. „VICA használata üzenetküldésre”. *Technical Documentation*, 2022. https://www.cardinal.hu/vica-hasznalata-uzenetkuldesre/.
Castells Manuel. *Az információ kora: Gazdaság, társadalom és kultúra. I. kötet: A hálózati társadalom kialakulása*. Budapest: Gondolat-Infonia, 2005.
———. *Communication Power*. New York: Oxford University Press, 2009.
———. *The Rise of the Network Society*. Second. Oxford: Wiley-Blackwell, 2010.
———. „The Rise of the Network Society, The Information Age: Economy”. *Society and Culture* I (1996).
Catană, Ștefan-Alexandru, és Andreea Barbu. „THE UNITED STATES OF AMERICA’S MOST VALUABLE BRANDS IN THE PERIOD 2021-2023”. *Towards Increased Business Resilience:Facing Digital Opportunities and Challenges*, 2023, 169–74. https://doi.org/10.56177/11icmie2023.32.
„CBP Broadens Iris Recognition at U.S. Borders”. Elérés 2025. május 3. https://www.bioenabletech.com/news/cbp-broadens-iris-recognition-at-u-s-borders.

Ceker, Hayreddin, és Shambhu Upadhyaya. „Enhanced recognition of keystroke dynamics using Gaussian mixture models". *MILCOM 2015 - 2015 IEEE Military Communications Conference*, 2015. október, 1305–10. https://doi.org/10.1109/MILCOM.2015.7357625.
Center, Pew Research. *Digital Divide Survey*. Washington, DC: Pew Research Center, 2023.
Challenges of Privacy in Big Data. Piscataway, NJ: IEEE, 2023.
Cheung, Harry. „Mobile Security Trends 2025: What You Need to Know and How to Stay Ahead". *IPification* (blog), 2025. január 24. https://www.ipification.com/blog/mobile-security-trends-2025-what-you-need-to-know-and-how-to-stay-ahead/.
cmeven. „Aadhaar and the Rise of Digital Public Infrastructure in India". *Reframe[Tech]* (blog), 2024. november 13. https://www.reframetech.de/en/2024/11/13/aadhaar-and-the-rise-of-digital-public-infrastructure-in-india/.
C.M.S. *Data Protection and Cybersecurity Laws in Hungary*. CMS Expert Guide, 2024.
Commission, European. *AI Act Risk Categories*. Brussels: European Commission, 2023.
———. „Digital Compass: The European Way for the Digital Decade", 2021.
———. *NIS2 Directive: EU Cybersecurity Framework*. Brussels: European Commission, 2022.
———. *Proposal for the EU AI Liability Directive*. Brussels: European Commission, 2023.
———. „Smart Mobility at the European Land Borders (SMILE". In *Horizon 2020 Project*, 2021.
Committee, National Research Council (US) Whither Biometrics, Joseph N. Pato, és Lynette I. Millett. „Cultural, Social, and Legal Considerations". National Academies Press (US), 2010. https://www.ncbi.nlm.nih.gov/books/NBK219893/.
Consortium, FiRa. „Why Is UWB Important for Indoor Positioning? FiRa Consortium Blog". *October* 10 (2024).
Consortium, World Wide Web. *Web Content Accessibility Guidelines*. Cambridge, MA: W3C, 2023.
„Contactless Biometric Solutions in Healthcare: Post-COVID Implementation Analysis". *Journal of Healthcare Technology* 18, sz. 3 (2022): 225-241,.
„Contribution to the development of a Global Digital Literacy Skills indicator | Department of Economic and Social Affairs". Elérés 2025. május 3. https://sdgs.un.org/partnerships/contribution-development-global-digital-literacy-skills-indicator.
Corcoran, Peter, és Claudia Costache. „Biometric Technology and Smartphones: A consideration of the practicalities of a broad adoption of biometrics and the likely impacts". *IEEE Consumer Electronics Magazine* 5, sz. 2 (2016. április): 70–78. https://doi.org/10.1109/MCE.2016.2521937.
CORDIS | European Commission. „Secure and Wireless Multimodal Biometric Scanning Device for Passenger Verification Targeting Land and Sea Border Control | H2020". Elérés 2025. május 3. https://cordis.europa.eu/project/id/872878/reporting.
Corp, X. „Account Verification Process Documentation". *Platform Policies*, 2023.
Corporation, International Data. *Worldwide Mobile Enterprise Applications Market Forecast, 2021-2025*. Framingham: IDC, 2021.
Cronin, Blaise. „The Transition to Information Society". *Aslib Proceedings* 35, sz. 2 (1983): 56–61. https://doi.org/10.1108/eb050865.
Cui, Nannan, Yuting Lu, Yelin Cao, Xiaofan Chen, Shuiqiao Fu, és Qun Su. „Quality Assessment of TikTok as a Source of Information About Mitral Valve Regurgitation in China: Cross-Sectional Study". *Journal of Medical Internet Research* 26 (2024. augusztus 20.): e55403. https://doi.org/10.2196/55403.
„Csáki Gyula Balázs: Kérdésfelvetések az e-közigazgatás fogalmának meghatározása körében (IJ, 2008/7. (29.), 277-280. o.) | Szakcikk Adatbázis". Elérés 2025. május 3. https://szakcikkadatbazis.hu/doc/1456098.
Csepeli György, és Prazsák Gergő. „Digitális egyenlőtlenségek Magyarországon: életkor, lakóhely és társadalmi státusz szerepe". *Információs Társadalom* 22, sz. 2 (2022): 120–40. https://doi.org/10.22503/inftars.XXII.2022.2.7.
———. „Új társadalmi törésvonalak a digitális korban". *Társadalomtudományi Szemle* 10, sz. 2 (2020): 8–25.
Csizmadia, Péter. „Aging and Digitalization: Trends and Challenges". *Demography* 65, sz. 2–3 (2022): 219–40. https://doi.org/10.21543/dem.65.2-3.3.
Csizmadia Zoltán. „Társadalmi kapcsolatok a magyar–szlovák–osztrák határtérségben". *Tér és Társadalom* 18, sz. 4 (2004): 103–16.
D, Sipp. „Millennium Ends Takeda's US Shopping Spree". *PubMed*. Elérés 2025. május 2. https://pubmed.ncbi.nlm.nih.gov/18536661/.
„DÁP – AAM Consulting". Elérés 2025. május 4. https://aam.hu/fresh_news/dap.

D.A.R.P.A. „Biometric Presentation Attack Detection: Current Capabilities and Gaps”. *Technical Assessment*, 2023.
———. „Long-Range Biometric Identification: Program Results”. Technical Report, 2023.
„Deep Face Recognition: An Easy-To-Understand Overview - viso.ai”. Elérés 2025. május 3. https://viso.ai/deep-learning/deep-face-recognition/.
Defense, U.S.Department. „Biometric Enabled Intelligence in Counterterrorism Operations”. *Joint Publication*, 2022, 2-01 3,.
———. „Biometric Enabled Watchlist: Operational Assessment”. *Joint Report*, 2022.
Deloitte. *Digital Consumer Trends 2023*. London: Deloitte LLP, 2023.
„Department of Defense Office of Inspector General”, 2023. https://media.defense.gov/2023/Nov/09/2003338047/-1/-1/1/DODIG-2024-016.PDF.
Department of Defense Office of Inspector General. „Press Release: Department of Defense Office of Inspector General (DoD OIG) Released the Re”. Elérés 2025. május 4. https://www.dodig.mil/In-the-Spotlight/Article/3584937/press-release-department-of-defense-office-of-inspector-general-dod-oig-release/https%3A%2F%2Fwww.dodig.mil%2FIn-the-Spotlight%2FArticle%2F3584937%2Fpress-release-department-of-defense-office-of-inspector-general-dod-oig-release%2F.
Dessewffy Tibor, és Láng László. „A figyelemgazdaság: Az új média és a digitális kapitalizmus”. *Replika* 92–93 (2015): 159–81.
———. „Mobilkommunikációs szokások kulturális különbségei: összehasonlító elemzés”. *Szociológiai Szemle* 32, sz. 1 (2022): 85–106. https://doi.org/10.1556/SzocSzem.2022.1.4.
„Device updates: what’s stopping people from making the change? | Kaspersky official blog”. Elérés 2025. május 3. https://www.kaspersky.com/blog/device-updates-report/.
„Digital Identity: Accelerating Financial Inclusion During a Crisis | Mobile for Development”. Elérés 2025. május 3. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/gsma_resources/digital-identity-accelerating-financial-inclusion-during-a-crisis/.
„Digital Public Services in the Digital Economy and Society Index | Shaping Europe’s Digital Future”. Elérés 2025. május 3. https://digital-strategy.ec.europa.eu/en/policies/desi-digital-public-services.
„Digitális személyazonosítás: mi a kulcs? - GoodID white paper”. Elérés 2025. május 3. https://goodid.net/hu/white-paper-ugyfel-azonositas/.
Directive, E.U. „On Payment Services in the Internal Market"”, 2015. 2366 (PSD2.
„Disinformation as a context-bound phenomenon”. *Oxford Academic*, 2023. https://doi.org/10.1093/ct/qtad001.
Djanegara, Nina Toft. „Biometrics for Counter-Terrorism: Case Study of the US Military in Iraq and Afghanistan”. Privacy International, 2021. https://privacyinternational.org/sites/default/files/2021-06/Biometrics%20for%20Counter-Terrorism-%20Case%20study%20of%20the%20U.S.%20military%20in%20Iraq%20and%20Afghanistan%20-%20Nina%20Toft%20Djanegara%20-%20v6.pdf.
„Document Verification with QR Codes: How It Works | ME-QR”. Elérés 2025. május 3. https://me-qr.com/page/blog/verification-of-documents-with-qr-codes.
„dpi.global/globaldpi/singapore_sndi”. Elérés 2025. május 3. https://www.dpi.global/globaldpi/singapore_sndi.
Drucker, Peter F. *The Age of Discontinuity; Guidelines to Our Changing Society*. New York: Harper & Row, 1969.
Editor, CSRC Content. „Cyber Attack - Glossary | CSRC”. Elérés 2025. május 25. https://csrc.nist.gov/glossary/term/cyber_attack.
„Efficiency Gains from Biometric Authentication in Legal Services"”. *International Journal of Legal Technology* 8, sz. 2 (2023).
„e-Government for Better Government | OECD”. Elérés 2025. május 3. https://www.oecd.org/en/publications/e-government-for-better-government_9789264018341-en.html.
Egyetem Budapesti Gazdasági. *CRM-rendszerek mobil használatának hatásai az értékesítési folyamatokra*. Budapest: BGE Kutatóközpont, 2022.
Egyetem Ludovika. „A magyar ügyvédi irodák kiberbiztonsági gyakorlatai"”. *Kutatási jelentés*, 2021. https://folyoirat.ludovika.hu/index.php/magyrend/article/download/6023/5107/25425.
Egyetem Semmelweis. *Mobilalkalmazások szerepe a krónikus betegségek megelőzésében és menedzselésében*. Budapest: Semmelweis Egyetem, Magatartástudományi Intézet, 2022.

Electronics, U.-Tech. „The Latest Innovations in Mobile Phone Technology: A Comprehensive Overview”. *U-Tech Electronics* (blog), 2023. december 10. https://utech.co/blog/the-latest-innovations-in-mobile-phone-technology/.
„Elektronikus közszolgáltatásokat és ügyfélszolgálati tevékenységet összefoglaló monitoring jelentés - PDF Ingyenes letöltés”. Elérés 2025. május 3. https://docplayer.hu/116889065-Elektronikus-kozszolgaltatasokat-es-ugyfelszolgalati-tevekenyseget-osszefoglalo-monitoring-jelentes.html.
„Emirates launches integrated biometric path at DXB”. Elérés 2025. május 3. https://www.futuretravelexperience.com/2020/10/emirates-launches-integrated-biometric-path-at-dxb/.
EMVCo. „3-D Secure 2.0 Specifications"”, 2022.
E.N.I.S.A. *ENISA Threat Landscape 2023*. European Union Agency for Cybersecurity, 2023.
E.P.S.T.E.M. „Impact of Deepfake Technology on Social Media”, 2023.
Eshelby, L. „Addressing Insider Threats in the Public Sector”. *Open Access Government*, 2025. https://www.openaccessgovernment.org/addressing-insider-threats-in-the-public-sector/187801/.
E-SPIN. „The Significance of Digital Identification in E-Government Systems”. *E-SPIN Group* (blog), 2023. december 8. https://www.e-spincorp.com/the-significance-of-digital-identification-in-e-government-systems/.
„Estonian E-Identity Model as a Best Practice"”. *Journal of Digital Government* 4, sz. 2 (2021). https://folyoirat.ludovika.hu/index.php/aarms/article/download/6632/5446/29091.
„Estonian Electronic Voting System: Security Analysis and Voter Participation Trends”. *Journal of E-Democracy* 11, sz. 4 (2020): 301-315,.
„EU Digital Identity Wallet: Implementation Roadmap and Challenges”. *European Commission Technical Report*, 2024.
„European Digital Identity (EUDI) Regulation | Shaping Europe’s digital future”. Elérés 2025. május 3. https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation.
Europol. *Internet Organised Crime Threat Assessment (IOCTA) 2023*. The Hague, European Union Agency for Law Enforcement Cooperation, 2023.
———. „Remote Biometric Surveillance: Capabilities and Limitations”. *Strategic Analysis Report*, 2023.
„Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior - ScienceDirect”. Elérés 2025. április 17. https://www.sciencedirect.com/science/article/abs/pii/S0167404818303031.
„Eye-Tracking Technologies in Mobile Devices: Applications and Limitations”. *Semantic Scholar Paper*, 2023.
Federal Bureau of Investigation. „Internet Crime Report 2022”. Federal Bureau of Investigation, 2023. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.
Federal Office for Information Security. „AusweisApp”. Elérés 2025. május 3. https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Online-Ausweisfunktion/AusweisApp/ausweisapp.html?nn=920562.
Fehér. „Deepfake Detection in Social Media Contexts”. *Hungarian Journal of Media Studies*, 2024.
Fehér Katalin. „Okoseszközök és alkalmazások használata a magyar lakosság körében”. *Információs Társadalom* 22, sz. 1 (2022): 43–68. https://doi.org/10.22503/inftars.XXII.2022.1.3.
Feng, Xiao, Hua Ma, és Yijie Sun. „DeepFake Detection with Remote Heart Rate Estimation Using 3D CentralDifference Convolution Attention Network”. *Recent Advances in Computer Science and Communications* 16, sz. 7 (2023. szeptember): e010323214186. https://doi.org/10.2174/2666255816666230301091725.
Financial and Business News | Finance Magnates. „Social Media Fraud Soars 28% Amid Rising AI Tactics”, 2024. október 30. https://www.financemagnates.com/forex/social-media-fraud-soars-28-amid-rising-ai-tactics/.
Force, Financial Action Task. *Indicators of Red Flags in Virtual Assets*. Paris: FATF, 2024.
———. „Public-Private Partnership in AML/CFT”, 2022.
Fortinet. „SolarWinds Supply Chain Attack”. Elérés 2025. május 3. https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack.
Forum, World Economic. *Economic Impact of Global Cybercrime*. Geneva: World Economic Forum, 2023.
———. *Global Data Governance*. Geneva: World Economic Forum, 2024.
———. *Global Risks Report*. Geneva: World Economic Forum, 2024.
Foundation, Mozilla. *Privacy Not Included Report*. San Francisco: Mozilla Foundation, 2023.

Friis, Karsten, és Olav Lysne. „Huawei, 5G and Security: Technological Limitations and Political Responses”. *Development and Change* 52, sz. 5 (2021): 1174–95. https://doi.org/10.1111/dech.12680.
„Fujitsu boasts new integrator and distributor for palm vein biometric technology | Biometric Update”. Elérés 2025. május 3. https://www.biometricupdate.com/201403/fujitsu-boasts-new-integrator-and-distributor-for-palm-vein-biometric-technology.
Fund, International Monetary. *Cryptocurrency Assets and Financial Stability*. Washington, DC: International Monetary Fund, 2023.
Galántai Zoltán. „A természetes nyelvfeldolgozás szerepe az akadálymentes digitális technológiákban”. *Infokommunikáció és Jog* 73 (2021): 28–37.
Gambo, Muhammad Liman, és Ahmad Almulhem. „Zero Trust Architecture: A Systematic Literature Review”. Elérés 2025. május 24. https://www.authorea.com/users/887944/articles/1266894-zero-trust-architecture-a-systematic-literature-review.
Gartner. *Hyper-Personalization: The Future of Customer Experience*. Stamford: Gartner Inc, 2023.
———. *Market Guide for Mobile Enterprise Applications*. Stamford: Gartner Inc, 2023.
———. *Predicts 2025: Edge Computing Will Redefine Infrastructure*. Stamford: Gartner Inc, 2022.
Gartner, Inc. *Gartner Forecasts Worldwide Connected Devices to Total 41.6 Billion in 2025*. Gartner Press Release, 2023.
Gasti, P. *Security Analysis of Mobile Authentication across Different Platforms*. Carnegie Mellon University CyLab Security and Privacy Institute, 2022.
Gazdasági Kutatóintézet Távközlési. *Az információs társadalom indikátorai. Dokumentumismertetés*. Tokyo: RITE, 1990.
GDPRhub. „Article 3 GDPR”. Elérés 2025. május 3. https://gdprhub.eu/index.php?title=Article_3_GDPR.
Gesundheit, Bundesministerium. „Die elektronische Gesundheitskarte (eGK”, 2022. https://www.bundesgesundheitsministerium.de/elektronische-gesundheitskarte.html.
Ghilom, Milkias, és Shahram Latifi. „The Role of Machine Learning in Advanced Biometric Systems”. *Electronics* 13 (2024. július): 2667. https://doi.org/10.3390/electronics13132667.
Gidney, C., és M. Ekerå. „How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits”. *Quantum* 5 (2021): 433.
Glatz Ferenc. *Magyarország az ezredfordulón. Stratégiai kutatások a Magyar Tudományos Akadémián*. Budapest: MTA, 1995.
Global, H.I.D. „What’s on the Horizon: 10 Biometric Trends for 2025"”, 2023. https://blog.hidglobal.com/whats-horizon-10-biometric-trends-2025.
Global Initiative for Inclusive Information and Communication Technologies (G3ict. Atlanta, GA: G3ict, 2024.
Goette, Lorenz, Hua-Jing Han, és Benson Tsz Kin Leung. *Information Overload and Confirmation Bias*. University of Cambridge Working Paper, 2019. https://doi.org/10.17863/CAM.52487.
„GoodID digitális irattárca - GoodID”. Elérés 2025. május 3. https://goodid.net/hu/digitalis-irattarca/.
Google. „Android Vitals: Energy Efficiency in Mobile Applications”. In *Mountain View: Google LLC*, 2023.
———. „Digital Wellbeing Experiments: New Tools for Finding Balance with Technology”. In *Mountain View: Google LLC*, 2022.
———. „Economic Impact Report”. In *Mountain View: Google LLC*, 2023.
Gosztonyi, Gergely, és Gergely Lendvai. „Deepfake és dezinformáció – Mit tehet a jog a mélyhamisítással készült álhírek ellen?” *Médiakutató* 25, sz. 1 (2024): 29–40.
GOV.UK. „2022 Primary Assessments: Lessons Learnt”. Elérés 2025. május 3. https://www.gov.uk/government/publications/2022-national-curriculum-assessments-lessons-learnt/2022-primary-assessments-lessons-learnt.
GOV.UK. „UK Digital Identity and Attributes Trust Framework”, 2024. november 25. https://www.gov.uk/government/collections/uk-digital-identity-and-attributes-trust-framework.
Gox, Mt. *Bankruptcy Proceedings of Mt. Gox, 2014-2022*. Tokyo: Tokyo District Court, 2022.
Grahn, H., és J. Pamment. *Exploitation of Psychological Processes in Information Influence Operations*. Lund University Psychological Defence Research Institute, 2024.
———. „Exploitation of Psychological Processes in Information Influence Operations”. *Working Paper* 2024, sz. 4 (2024).
Griffin, John. „Keystroke Dynamics: Typing as Powerful Behavioral Biometrics | Fleksy”, 2022. augusztus 23. https://www.fleksy.com/blog/keystroke-dynamics-and-the-types-of-behavioural-biometrics/.

GRIN - Defining Smart Infrastructure. Smart Technical, Social, and Green Infrastructures in Cities and at the Federal Level and Beyond. Elérés 2025. április 17. https://www.grin.com/document/1190660.
Grother, P., M. Ngan, és K. Hanaoka. „Face Recognition Accuracy under Challenging Operational Conditions". *NIST Interagency Report*, 2022.
Group, E.U.Media Literacy Expert. *Report*. Brussels: European Commission, 2024.
Group, World Bank. *The Role of Cybersecurity in Economic Performance*. World Bank, 2023. http://documents1.worldbank.org/curated/en/099092324164526526/pdf/P178769189c7360111ac1f1185e04824dec.pdf.
Gudavalli, Madhavi, D. Srinivasa Kumar, és S. Viswanadha Raju. „Securing E-Governance Services through Biometrics". *International Journal of Security and Its Applications* 8, sz. 1 (2014. január 31.): 103–12. https://doi.org/10.14257/ijsia.2014.8.1.10.
Guilbeault, D., D. Centola, és A. Baronchelli. „Groupthink Dynamics in Large Social Networks". *Nature Communications*, 2024. https://doi.org/10.1038/s41467-024-48034-5.
Gunuganti, Anvesh. „Behavioral Biometrics for Continuous Authentication". *Journal of Biosensors and Bioelectronics Research*, 2023. szeptember, 1–5. https://doi.org/10.47363/JBBER/2023(1)122.
Gyaraki R. *Az információbiztonság alapjai*. Budapest: Nemzeti Közszolgálati Egyetem, 2023. https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/az_informaciobiztonsag_alapjai_konyv_kesz_2.pdf.
György Péter. *Memex: A könyvbe zárt tudás*. Budapest: Magvető, 2001.
Haig Zsolt. „Kibertéri kognitív befolyásolás az információs műveletekben". *Hadtudományi Szemle* 15, sz. 2 (2022): 115-130,. https://doi.org/10.32563/hsz.2022.2.7.
Hajnal György, és Király Gábor. „E-közigazgatási megoldások és mobilalkalmazások a magyar közszolgáltatásokban". *Vezetéstudomány* 54, sz. 2 (2023): 15–29. https://doi.org/10.14267/VEZTUD.2023.02.02.
Hálózat Eötvös Loránd Kutatási. *Mobil adatgyűjtési és elemzési módszerek alkalmazása komplex társadalomtudományi kutatásokban*. Budapest: ELKH, 2023.
Hamilton, Isobel Asher. „Oxford Researchers Exposed the Avalanche of Data Google and Facebook Can Hoover up from Apps on Your Phone". Business Insider. Elérés 2025. május 3. https://www.businessinsider.com/google-and-facebook-big-data-apps-oxford-study-finds-2018-10.
Hammudoglu, J. S., J. Sparreboom, J. I. Rauhamaa, J. K. Faber, L. C. Guerchi, I. P. Samiotis, S. P. Rao, és J. A. Pouwelse. „Portable Trust: biometric-based authentication and blockchain storage for self-sovereign identity systems". arXiv, 2017. június 12. https://doi.org/10.48550/arXiv.1706.03744.
Hasan, Omar. *A Discussion of Privacy Challenges in User Profiling with Big Data Techniques*. LIRIS CNRS, 2013.
HBR Store. „Singapore's Strategic Transformation as a Smart Nation ^ NTU356". Elérés 2025. május 3. https://store.hbr.org/product/singapore-s-strategic-transformation-as-a-smart-nation/NTU356.
Herzlinger, R. „A Managed Care Memoir: A Physician's Whistle-Stop Journey", 2004. https://www.semanticscholar.org/paper/A-Managed-Care-Memoir%3A-A-Physician's-Whistle-Stop-Herzlinger/37d127bb2a80fe299c2a6d5f13b8d9287fd3c74f.
Hilbert, Martin. „Digital Technology and Social Change: The Digital Transformation of Society from a Historical Perspective". *Dialogues in Clinical Neuroscience* 17, sz. 3 (2015): 347–60. https://doi.org/10.31887/DCNS.2015.17.3/mhilbert.
Hírközlési Hatóság Nemzeti Média-. *Lakossági Internethasználat Online Piackutatás 2023*. Budapest: NMHH, 2023.
Hivatal, Központi Statisztikai. *Digitális gazdaság és társadalom, 2023*. Budapest: KSH, 2023.
Hoffman, B., és R. Shelton. „Counterintelligence Applications of Biometric Technology". *Studies in Intelligence* 65, sz. 2 (2021): 23-38,.
„Home | myID". Elérés 2025. május 3. https://www.myid.gov.au/.
Horowitz, Michael C. „Artificial Intelligence, International Competition, and the Balance of Power". *Texas National Security Review* 1, sz. 3 (2018): 36–57.
Horváth László. „Az álhír fogalma és helye a hibrid hadviselésben". *Nemzet és Biztonság* 6, sz. 1 (2023): 19–34.

„How a digital platform opens the door for value-added personalized public services”. Elérés 2025. május 3. https://nortal.com/insights/how-a-digital-platform-opens-the-door-for-value-added-personalized-public-services.
„How to secure body-worn cameras and protect footage from cyber threats | Pen Test Partners”. Elérés 2025. május 3. https://www.pentestpartners.com/security-blog/how-to-secure-body-worn-cameras-and-protect-footage-from-cyber-threats/.
Hub, N.A.T.O.Innovation. „The Cognitive Warfare Concept: Enhancing NATO’s Hybrid Threat Response”. NATO Innovation Hub White Paper, 2023.
Hungary, PwC. „AI-Generated Biometric Threats Survey”. *Market Research*, 2024.
Huszár V. „A decentralizáció és a blokklánc-technológia lehetőségei a katonai szférában”. *Real.MTA Könyvtár*, 2020. https://doi.org/10.17625/real.mtak.109337.
I.C.A.O. „Digital Travel Credentials Technical Standards"”. *Document* 9303 (2023).
I.D.C. *Worldwide Digital Transformation 2022 Predictions*. Framingham: International Data Corporation, 2022.
———. „Worldwide Edge Computing Forecast”, 2021.
Identitycom. „Predictions for the Future of Digital Identity”. *Market Analysis*, 2025.
Imre Sándor, Farkas Károly, és Schulcz Róbert. „5G és 6G rendszerek az ipari alkalmazások szolgálatában: követelmények és megoldások”. *Híradástechnika* 78, sz. 2 (2023): 15–24.
Inam, Mahnoor. „Smart City vs. Intelligent City: Key Differences and Similarities”. *Minnovation Technologies* (blog), 2024. július 9. https://minnovation.com.au/smart-cities-2/smart-city-vs-intelligent-city-key-differences-and-similarities/.
„In-App Purchase Security: Protecting Transactions and User Data | AppMaster”. Elérés 2025. május 3. https://appmaster.io/blog/in-app-purchase-security.
Inc. „A digitális szuverenitás jelentősége”. *ICT Global*, 2023. https://ictglobal.hu/rovid-hirek/a-digitalis-szuverenitas-jelentosege/.
Inc, Apple. *Face ID Security Guide*. Cupertino: Apple Inc, 2023.
———. „Face ID Security White Paper”, 2023.
„Independent Legal Review of the Governance of Biometric Data in England and Wales”. Elérés 2025. május 4. https://www.adalovelaceinstitute.org/project/ryder-review-biometrics/.
„Information Systems Research, "Privacy by Design: From Theory to Practice”, 2022.
Infrastruktúra Nemzeti. *Elektronikus Egészségügyi Szolgáltatási Tér: Rendszerarchitektúra és funkcionalitások*. Budapest: ÁEEK, 2020.
Insights2Techinfo. „The Growing Threat of IoT Supply Chain Attacks”, 2025. február 20. https://insights2techinfo.com/the-growing-threat-of-iot-supply-chain-attacks/.
Institute, A.I.Now. *Discriminatory Bias in Artificial Intelligence Systems*. New York: AI Now Institute, 2022.
Institute, Ponemon. *Cost of a Data Breach Report*. Traverse City, MI: Ponemon Institute, 2024.
———. „The Privacy Paradox: Understanding Attitudes Towards Biometric Technology”. *Ponemon Institute Research Report*, 2022.
Institute, Reuters. *Digital News Report*. Oxford: University of Oxford, 2023.
Institution, Brookings. „The Enduring Risks Posed by Biometric Identification Systems”, 2021.
Intelligence, Acuity Market. „The Global Biometrics and Digital Identity Analyst”, 2022.
Intelligence, Insider. *Mobile Banking Adoption Report*. New York: eMarketer Inc, 2022.
„International Bar Association, »Authentication Standards for Cross-Border Legal Services«”. Research Report, 2023.
„International Border Control Association, "Biometric Authentication at Border Control: 2025 Trends and Insights”. *Annual Report*, 2024.
International, Privacy. *Investigation into Aadhaar Data Breach*. London: Privacy International, 2023.
International Settlements, Bank. *Regulatory Framework for Crypto-Assets*. Basel: Bank for International Settlements, 2023.
Interpol. „International Biometric Data Exchange for Counterterrorism”. *General Secretariat Report*, 2023.
Investigation, American Civil Liberties Union. „Court Limits FBI’s Biometric Collection Program”. *U.S. District Court Decision*, 2023.
Investigation, Federal Bureau. „Biometric Technologies in Counterintelligence Operations”. *Counterintelligence Division Assessment*, 2024.
———. „Internet Crime Complaint Center Releases 2022 Statistics”, 2023. március 22. https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics.
iProov. *Case Studies in Government Digital Identity*. London: iProov Ltd, 2021.

„IR 8334, Using Mobile Device Biometrics for Authenticating First Responders | CSRC". Elérés 2025. május 3. https://csrc.nist.gov/pubs/ir/8334/ipd.
„»Is Social Media Critical Infrastructure?«". Elérés 2025. április 17. https://www.linkedin.com/pulse/social-media-critical-infrastructure-alex-sharpe.
Isobe, Kaito, és Kazuya Murao. „Personal Identification Method using Active Acoustic Sensing applied to the Nose pad of Eyeglasses". In *Adjunct Proceedings of the 2022 ACM International Joint Conference on Pervasive and Ubiquitous Computing and the 2022 ACM International Symposium on Wearable Computers*, 345–48. UbiComp/ISWC '22 Adjunct. New York, NY, USA: Association for Computing Machinery, 2023. https://doi.org/10.1145/3544793.3560400.
ISO/IEC 30071: Accessibility Requirements for Information and Communication Technology Products. Geneva: ISO, 2023.
„ISO/IEC 30107, "Biometric Presentation Attack Detection Standards", 2022.
J, Jeswani, Govarthan Pk, Selvaraj A, Prince A, Thomas J, Kalathe M, Subramaniam V, és Agastinose Ronickom Jf. „Low Valence Low Arousal Stimuli: An Effective Candidate for EEG-Based Biometrics Authentication System". *PubMed*, 2023. https://pubmed.ncbi.nlm.nih.gov/37203658/.
„Javelin™ | Parsons Products". Elérés 2025. május 4. https://www.parsons.com/products/javelin/.
Jogtudományi Kar Miskolci Egyetem Állam-. „Digitális átalakulás a jogi gyakorlatban"". *Kutatási jelentés*, 2023. https://www.mjsz.uni-miskolc.hu/files/10854/4_nagyzoltan_t.
„Journal of Digital Banking Security, »Mobile Security Threats and Countermeasures«", 2022.
Jurisic, Marko, Igor Tomicic, és Petra Grd. „User Behavior Analysis for Detecting Compromised User Accounts: A Review Paper". *Cybernetics and Information Technologies* 23 (2023. szeptember): 102–13. https://doi.org/10.2478/cait-2023-0027.
Kabinetiroda Miniszterelnöki. *Digitális Állampolgárság – Stratégiai koncepció és megvalósítási terv*. Budapest: MK, 2022.
Kadëna, Esmeralda. „Smartphone Security Threats", 2017.
Kaiypbergen, D., és Ye. Begimbayeva. „RESEARCH OF INNOVATIVE AUTHENTICATION: A DEEP DIVE INTO BIOMETRIC ACCESS TECHNOLOGIES". *Herald of the Kazakh-British technical university* 22, sz. 1 (2025. március 24.): 103–13. https://doi.org/10.55452/1998-6688-2025-22-1-103-113.
Karakos, Alexandros. „Keystroke dynamics features for gender recognition". Elérés 2025. május 4. https://www.academia.edu/87483047/Keystroke_dynamics_features_for_gender_recognition.
Karetsos, Sotiris, Constantina Costopoulou, és Alexander Sideridis. „Developing a smartphone app for m-government in agriculture". *Journal of Agricultural Informatics* 5 (2014. július): 1–8. https://doi.org/10.17700/jai.2014.5.1.129.
Karvalics László Z. „Az okos eszközök mint társadalmi változások katalizátorai". In *Információs társadalom kézikönyv*, 247–63. Budapest: Gondolat Kiadó, 2021.
———. „Információs társadalom – mi az? Egy kifejezés jelentése, története és fogalomkörnyezete". In *Róbert Pintér szerk.: Az információs társadalom*, 29–47. Budapest: Gondolat-Új Mandátum, 2007.
Karvalics Z. és László. „Információ, tudás, társadalom, gazdaság, technológia: egy egységes terminológia felé". *Információs Társadalom* 5, sz. 4 (2005): 7–17.
Kawasaki, Yohei, és Yuta Sugiura. „Personal Identification and Authentication Using Blink with Smart Glasses". In *2022 61st Annual Conference of the Society of Instrument and Control Engineers (SICE)*, 1251–56, 2022. https://doi.org/10.23919/SICE56594.2022.9905842.
Kerényi Ádám. „A fintech alkalmazások elterjedése Magyarországon". *Hitelintézeti Szemle* 21, sz. 1 (2022): 43–69. https://doi.org/10.25201/HSZ.21.1.4369.
Kingo, Thomas, és Diego F. Aranha. „User-centric security analysis of MitID: The Danish passwordless digital identity solution". *Computers & Security* 132 (2023. szeptember 1.): 103376. https://doi.org/10.1016/j.cose.2023.103376.
Király Péter György. „A digitális állami szolgáltatások felhasználói élménye". *Pro Publico Bono – Magyar Közigazgatás* 9, sz. 1 (2021): 60–77.
Kiss Attila. „Elektronikus személyazonosítás és digitális identitás". *Infokommunikáció és Jog* 73 (2019): 33–38.
„Korm. rendelet, »Az elektronikus aláírások auditálhatóságáról«", 418Kr. u. 2024.
Kovács László. *A kibertér védelme*. Budapest: Dialóg Campus Kiadó, 2018.
———. *A kibertér védelme*. Budapest: Dialóg Campus Kiadó, 2018.

Kovács Tamás. „Blokklánc-technológia mint a korrupció elleni küzdelem lehetséges eszköze”. *Themis*, 2020, 92–128.
Kovácsházy Tamás, Takács Barnabás, és Charaf Hassan. „Mérnöki mobilalkalmazások hatása a tervezési folyamatok időigényére”. *Gép* 72, sz. 3 (2021): 67–76.
Központ Állami Egészségügyi Ellátó. *EESZT mobiltoken – Felhasználói kézikönyv*. Budapest: ÁEEK, 2020.
Krämer, J. „The Death of Privacy Policies: How App Stores Shape GDPR Compliance of Apps”. *Internet Policy Review* 13, sz. 2 (2024). https://doi.org/10.14763/2024.2.1757.
Krasznay Csaba. *A kiberbiztonság stratégiai vetületei*. Budapest: Dialóg Campus Kiadó, 2020.
Kudtarkar, Manali. „JTAG: A Strong Tool for Security Testing”. eInfochips, 2023. augusztus 24. https://www.einfochips.com/blog/jtag-a-strong-tool-for-security-testing/.
Kumar, S., R.K. Singh, és A.S. Akhi. „Mobile Banking Authentication Using CNN Embedded Face Recognition"”. In *IEEE International Conference on Future Networks and Distributed Systems*, 2022.
Kunda és Chishimba. „Authentication Scheme Applications on Smartphones: A Comparative Analysis"”. *Journal of Information Security*, 2022.
Kushchu, I., és H. Kuscu. „From E-Government to M-Government: Facing the Inevitable”. In *Mobile Government: An Emerging Direction in E-Government. IGI Global*, 2003.
Laabab, Ilham, Abdellatif Ezzouhairi, Nour El Madhoun, és Muhammad Haris Khan. „Blockchain and Biometric Systems Integration for IoMT Security”. *2024 8th Cyber Security in Networking Conference (CSNet)*, 2024. december 4., 259–62. https://doi.org/10.1109/CSNet64211.2024.10851762.
Laakkonen, J., O.M. Latvala, és A. Heikkinen. „The Mobile Application Ecosystem: A Historical and Demographic Analysis”. *Journal of Theoretical and Applied Electronic Commerce Research* 16, sz. 4 (2021): 1078–96. https://doi.org/10.3390/jtaer16040061.
Lászlóné dr Hazai. „Okmányvédelem, az NBSZ okmányvédelemmel kapcsolatos szakértői, hatósági tevékenysége”. *Nemzetbiztonsági Szemle* 3, sz. 3 (2015. szeptember 30.): 60–100.
Laufer Balázs. „A migráció rendészeti és nemzetbiztonsági kihívásai. PhD-értekezés”. Budapest, 2013.
Lazarus, R.S. „Emotion and Adaptation”. Oxford University Press, 1991.
Lee, J., és D. Lee. „Decentralized Authentication for Disconnected Military Environments”. *IEEE Transactions on Dependable and Secure Computing* 18, sz. 3 (2021): 1352–65.
Legal, Access. *Biometric Identity Verification for Law Firms"*. Technical Documentation, 2023.
———. *Enhanced Security through Biometric Verification"*. White Paper, 2023.
Li, Wenbo, és Liqun Chen. „Agile Smart-Device Based Multi-Factor Authentication for Modern Identity Management Systems”. *IEEE Transactions on Dependable and Secure Computing* 21, sz. 2 (2024): 112–27. https://doi.org/10.1109/TDSC.2023.3321758.
LinkedIn. *Top Mobile App Security Trends to Watch for 2025: Protecting User Data*. LinkedIn Pulse, 2024.
Liu, Gary, és Nathan Malkin. „PoPETs Proceedings — Effects of Privacy Permissions on User Choices in Voice Assistant App Stores”. Elérés 2025. április 17. https://petsymposium.org/popets/2022/popets-2022-0116.php.
Lyotard Jean-François. *A posztmodern állapot*. Szerkesztette Jürgen Habermas, Jean-François Lyotard, és Richard Rorty. Budapest: Századvég, 1993.
M, Grosso. „How to Improve an Advanced Waste Management System”. *PubMed*. Elérés 2025. május 3. https://pubmed.ncbi.nlm.nih.gov/33977798/.
Machlup, Fritz. *The Production and Distribution of Knowledge in the United States*. Princeton: Princeton University Press, 1962.
Madyan, Muhammad, Iman Harymawan, Adib Minanurohman, és Wulan Rahmadani Setiawan. „The Impact of Top Management Education from Reputable Universities on Corporate Capital Structure: Evidence from Indonesia”. *Global Business Review*, 2023. augusztus 1., 09721509231182525. https://doi.org/10.1177/09721509231182525.
Magyarország Transparency International. „Korrupciós kockázatok Magyarországon: Nemzeti integritás tanulmány”, 2008. https://transparency.hu/wp-content/uploads/2016/05/Korrupci%C3%B3s-kock%C3%A1zatok-Magyarorsz%C3%A1gon-Nemzeti-integrit%C3%A1s-tanulm%C3%A1ny.pdf.
Makó Csaba, és Illéssy Miklós. „Technológiai változások és szervezeti innovációk kölcsönhatása: az alkalmazottak munkahely-átalakítási akciói”. *Vezetéstudomány* 51, sz. 10 (2020): 59–68. https://doi.org/10.14267/VEZTUD.2020.10.05.
Maladie Assurance. „La Carte Vitale: Funkcionalitások és biztonság”, 2021. https://www.ameli.fr/.

Mandiant. *Advanced Persistent Threat Report*. Reston, VA: Mandiant, 2023.
Mandiant, FireEye. „State-Sponsored Attacks on Biometric Databases". *Threat Intelligence Report*, 2024.
Marco Koller, és András Kerti. „Az okoseszközök applikációi által gyűjtött metaadatokkal való visszaélések kockázati szemléletmód általi, felhasználói szintű lehetséges visszaszorítása". *Hadmérnök* 16, sz. 4 (2021): 145–56. https://doi.org/10.32567/hm.2021.4.11.
Marma, Kyaw Jaw Sine. „The Science of Disinformation: Cognitive Vulnerabilities and Digital Manipulation". Modern Diplomacy, 2025. február 9. https://moderndiplomacy.eu/2025/02/09/the-science-of-disinformation-cognitive-vulnerabilities-and-digital-manipulation/.
Marsh. *Global Technology Industry Risk Study*. New York: Marsh & McLennan, 2023.
Masuda, Yoneji. *The Information Society as Post-Industrial Society*. Tokyo: Institute for the Information Society, 1980.
Mattelart, Armand. *The Information Society: An Introduction*. London: Sage Publications, 2003.
Mátyás Ináncsi, Péter Bányász, Máté Dub, és Péter Kugler. „Empirical Studies of Russian–Ukrainian War Related Fake News, Part 1". *Hadmérnök* 18, sz. 4 (2024. május 9.): 109–28. https://doi.org/10.32567/hm.2023.4.8.
McCLARKIN Emma. „JELENTÉS a blokkláncról: előretekintő kereskedelempolitika | A8-0407/2018 | Európai Parlament". Elérés 2025. május 2. https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_HU.html.
MediaKutato. „Digitális identitás vállalatvezetők döntéshozók". *MediaKutato Journal*, 2015.
Mediakutató. „Visszhangkamrák és szűrőbuborékok". *Médiakutató* 2020, sz. 1 (é. n.): 1–15.
„Megjelent az eSzemélyiM mobilapplikáció - eSzemélyi". Elérés 2025. május 3. https://eszemelyi.hu/blog/megjelent-az-eszemelyim-mobilapplikacio/.
„Meltdown and Spectre". Elérés 2025. május 3. https://meltdownattack.com/.
Mészáros Rezső. *Kibertér. A földrajzi tudás új dimenziói*. Szeged: Hispánia Kiadó, 2003.
„Mi az a biometrikus azonosítás, és miért jó, ha használod?" Elérés 2025. május 3. https://digipedia.hu/cikk/mi-az-a-biometrikus-azonositas-es-miert-jo-ha-hasznalod.
„Mi az a hitelesítés? Definíció és módszerek | Microsoft Biztonság". Elérés 2025. május 3. https://www.microsoft.com/hu-hu/security/business/security-101/what-is-authentication.
„Mi az a kibertámadás? | Microsoft Biztonság". Elérés 2025. április 17. https://www.microsoft.com/hu-hu/security/business/security-101/what-is-a-cyberattack.
„Mi az IoT (eszközök internetes hálózata)? | Microsoft Azure". Elérés 2025. április 17. https://azure.microsoft.com/hu-hu/resources/cloud-computing-dictionary/what-is-iot.
Microsoft. *Annual Report 2023*. Redmond: Microsoft Corporation, 2023.
Microsoft Research. „Edge Computing". Elérés 2025. május 3. https://www.microsoft.com/en-us/research/project/edge-computing/.
Millett, Joseph N. Pato – Lynette I. *Biometric Recognition: Challenges and Opportunities*. National Academies Press, 2010.
„Mobile app usage - statistics & facts | Statista". Elérés 2025. május 3. https://www.statista.com/topics/1002/mobile-app-usage/.
„Mobile Authentication Technologies: Compatibility Analysis". *Mobile Security Journal* 12, sz. 4 (2023): 78-92,.
„Mobile Biometric Authentication for Covert Operations". *CIA Technical Services Quarterly*, 2023.
„Mobile ID Fingerprint Technology Can Provide Rapid Results and Improve Officer Safety | National Institute of Justice". Elérés 2025. május 3. https://nij.ojp.gov/library/publications/mobile-id-fingerprint-technology-can-provide-rapid-results-and-improve-officer.
„Mobile ID -Trusted Digital ID for Governments". Elérés 2025. május 3. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/mobile-id.
„Mobile User Authentication Market Report: Resource Utilization Analysis". *Research and Markets Report*, 2024.
Mohsen, Fadi, Cornelis Zwart, Dimka Karastoyanova, és Georgi Gaydadjiev. „A Taxonomy for Large-Scale Cyber Security Attacks - EUDL". Elérés 2025. május 2. https://eudl.eu/doi/10.4108/eai.2-3-2022.173548.
Molnár Gyöngyvér, és Turcsányi-Szabó Márta. „Mobilalkalmazások hatása a tanulási folyamatokra: Egy longitudinális vizsgálat eredményei". *Magyar Pedagógia* 122, sz. 1 (2022): 5–33. https://doi.org/10.17670/MPed.2022.1.5.
Morkonda, Srivathsan G., Paul C. van Oorschot, és Sonia Chiasson. „Exploring Privacy Implications in OAuth Deployments". arXiv, 2021. március 3. https://doi.org/10.48550/arXiv.2103.02579.
„Multimodal Biometric Systems: A Comparative Study". *International Journal of Biometrics*, 2022.

„Multimodal Biometrics Enhancing Law Enforcement and Border Security”. Elérés 2025. május 3. https://www.laxton.com/blog/multimodal-biometrics-enhancing-law-enforcement-and-border-security/.
Munk Sándor. „Információs műveletek – információs tevékenységek”. *Hadtudomány* 28, sz. 3–4 (2018): 118–29.
Munkácsy András, és Jászberényi Melinda. „Közösségi közlekedési alkalmazások használata Magyarországon”. *Közlekedéstudományi Szemle* 71, sz. 4 (2021): 42–55. https://doi.org/10.24228/KTSZ.2021.4.4.
Nagy János, és Erdélyi Márk. „Okoseszközök és big data alapú megoldások az egészségmegőrzésben”. *Orvosi Hetilap* 162, sz. 18 (2021): 696–705. https://doi.org/10.1556/650.2021.32064.
Nagy, P., és L. Kovács. „Legal and Privacy Aspects of Mobile Authentication Technologies”. *AARMS Journal* 20, sz. 2 (2021): 77-94,.
Nánási Polgár. „Nánási Polgár”. Elérés 2025. május 3. https://nanasipolgar.hu/jogi-kisokos/.
„National Insider Threat Task Force. "Behavioral Biometrics in Insider Threat Detection”. *Best Practices Guide*, 2023.
„National Institute of Standards and Technology. "Multimodal Biometrics for High-Security Applications”. *NIST*, é. n.
Nations, United. *E-Government Survey*. New York: United Nations, 2024.
N.C.B.I. „Security, Privacy, and Usability in Continuous Authentication: A Survey”. *PMC* 8434648 (2021). https://pmc.ncbi.nlm.nih.gov/articles/PMC8434648/.
Nemeslaki András. „Az adatvezérelt döntéshozatal szerepe a nemzetközi piacokon működő vállalatok digitális transzformációjában”. *Külgazdaság* 65, sz. 5–6 (2021): 30–52.
Németh Zoltán. „Az okosvárosok biztonsági kihívásai”. *Belügyi Szemle* 68, sz. 2 (2020): 89–106.
Netflix. *The Value of Recommendation Systems*. Los Gatos: Netflix Inc, 2023.
Networks, I.M.D.E.A. *An Analysis of Third-Party Mobile SDKs - Data Protection and Privacy*. IMDEA Networks Principal, 2024.
Networks, Palo Alto. „What Is a Credential-Based Attack? Palo Alto Networks Cyberpedia”, 2020. https://www.paloaltonetworks.com/cyberpedia/what-is-a-credential-based-attack.
Neuhofer, B., D. Buhalis, és A. Ladkin. „Smart Technologies for Personalized Experiences: A Case Study in the Hospitality Domain"”. *Electronic Markets* 25, sz. 3 (2015).
„New wearable authentication more than a »token« gesture | Article | The United States Army”. Elérés 2025. május 3. https://www.army.mil/article/225197/new_wearable_authentication_more_than_a_token_gesture.
New Zealand Digital government. „RealMe®”, 2025. március 19. https://www.digital.govt.nz/products-and-services/products-and-services-a-z/realme.
Newretro.Net. „Brick Phones: ’80s Mobile Tech”, 2023. november 12. https://newretro.net/blogs/main/brick-phones-80s-mobile-tech.
NHS Transformation Directorate. „Passwordless Login”. Elérés 2025. május 3. https://transform.england.nhs.uk/key-tools-and-info/digital-playbooks/open-source-digital-playbook/passwordless-login/.
N.I.S.T. „Special Publication: CRYSTALS-Kyber Implementation”, 2024.
„Nordic Innovation, "BankID Implementation Analysis: Lessons Learned”, 2023.
Nordstone. „Integrating Biometric Security Features into Mobile Apps"”, 2023. https://nordstone.co.uk/blog/integrating-biometricsecurity-features-into-mobile-apps.
———. „Integrating Biometricsecurity Features into Mobile Apps”. *Technical Blog*, 2023. https://nordstone.co.uk/blog/integrating-biometricsecurity-features-into-mobile-apps.
Nyikes Zoltán. „Az okos otthonok IT biztonsági kihívásai”. *Hadmérnök* 14, sz. 1 (2019): 212–23.
Nyíri Kristóf. „Az információs társadalom és a történelmi-kulturális hagyomány”. *Világosság* 42, sz. 7–9 (2001): 31–37.
———. „Mobilkommunikáció és az elme kiterjesztése”. *Magyar Tudomány* 182, sz. 5 (2021): 598–609. https://doi.org/10.1556/2065.182.2021.5.8.
„Nyolc eltékozolt év után vége a személyi igazolványhoz járó e-aláírásnak - G7 - Gazdasági sztorik érthetően”. Elérés 2025. május 4. https://g7.hu/kozelet/20240830/nyolc-eltekozolt-ev-utan-vege-a-szemelyi-igazolvanyhoz-jaro-e-alairasnak/.
Nyonyoh, Raphael. „Ransomware and the Vulnerability of Critical Infrastructure: A National Security and Economic Analysis”. Elérés 2025. május 25. https://journalajeba.com/index.php/AJEBA/article/view/1759.
Nyúl Eszter Anna. „Nyúl Eszter Anna: Az állampolgárság elvesztett átmeneti rítusa”. *Tudásmenedzsment* 21, sz. 1–2 (2020. december 30.): 170–77. https://doi.org/10.15170/TM.2020.21.1-2.13.

Observatory, Stanford Internet. *Deepfakes and Disinformation*. Stanford, CA: Stanford University, 2023.
O.E.C.D. „Digital Government Index: 2022 Results". *OECD Public Governance Policy Papers*, sz. 11 (2022).
OECD. „Skills for the Digital Transition", 2022. október 18. https://www.oecd.org/en/publications/skills-for-the-digital-transition_38c36777-en.html.
OECD. „The State of Implementation of the OECD AI Principles Four Years On", 2023. október 26. https://www.oecd.org/en/publications/the-state-of-implementation-of-the-oecd-ai-principles-four-years-on_835641c9-en.html.
„Office of the Director of National Intelligence. "Integration of Biometric Data in All-Source Intelligence Analysis". In *Intelligence Community Directive 203 Supplemental Guidance*, 2023.
„Okoseszközök / Smart Devices / Okoseszköz / Smart Device / Intelligent Devices / Intelligens Eszközök / Okos Megoldások | Modern Vállalkozások Programja". Elérés 2025. május 3. https://digitalisfogalomtar.vallalkozzdigitalisan.hu/okoseszkozok-smart-devices-okoseszkoz-smart-device-intelligent-devices-intelligens-eszkozok-okos-megoldasok.
Oludayo, O. I., A. K. Akinwole, A. A. Adedeji, és A. A. Aromolaran. „A review of smartphone security challenges and prevention". *International Research Journal of Innovations in Engineering and Technology* 7, sz. 5 (2023): 234235.
on, I.E.E.E.Transactions. „Information Forensics and Security, "Advanced Presentation Attack Detection in Biometric Systems", 2023.
Ookla. *Global Speedtest Index*. Seattle, WA: Ookla, 2024.
Opinion on Profiling. Brussels: EDPS, 2022.
Orbók Ákos. „Biometrikus rendszerek hitelesítési módszerei". *Hadmérnök* 13, sz. 4 (2018): 71–82.
Orrick. „DOJ Seeks to Restrict Data Transfers to »Countries of Concern«", 2024. https://www.orrick.com/en/Insights/2024/12/DOJ-Seeks-to-Restrict-Data-Transfers-to-Countries-of-Concern.
Orsós, Mária, Richárd Török, Csaba Faragó, Bence Antalfia, Eszter Kail, és Anna Bánáti. „Security Operation Center Methodology for 5G Networks". *Acta Polytechnica Hungarica* 22, sz. 2 (2025): 99–118.
„OTP Bank - Biometrikus azonosítás is segíti a telefonos ügyintézést". Elérés 2025. május 3. https://www.otpbank.hu/portal/hu/hirek/biometrikus-azonositas.
Outside GC. „Biometric Privacy Laws | OGC". Elérés 2025. május 4. https://www.outsidegc.com/blog/biometric-data-protection-a-growing-trend-in-state-privacy-legislation.
„OWASP Application Security Verification Standard (ASVS) | OWASP Foundation". Elérés 2025. május 24. https://owasp.org/www-project-application-security-verification-standard/.
Ozsváth Zoltán Rajnai – Beatrix Fregan – Judit. „A kiberbiztonság technológiai és módszertani támogatása – A blockchain, mint biztonságtechnológia". *Biztonságtudományi Szemle* 1, sz. 3 (2018): 61–70.
Packetlabs. „Demystifying The Market For Zero-Day Software Exploits", 2024. május 17. https://www.packetlabs.net/post/demystifying-the-market-for-zero-day-software-exploits.
Pap Zoltán. „A mobilalkalmazások biztonsági kockázatai". *Biztonságtudományi Szemle* 2, sz. 4 (2020): 65–78.
Parliament, European. *Artificial Intelligence Act*. Brussels: European Parliament, 2023.
Patel, Anisha V., Julie R. Palmer, Jessica L. Petrick, és Kimberly A. Bertrand. „Abstract B056: Inflammatory Dietary Pattern and Risk of Multiple Myeloma in US Black Women". *Cancer Epidemiology, Biomarkers & Prevention* 32, sz. 12_Supplement (2023. december 1.): B056–B056. https://doi.org/10.1158/1538-7755.DISP23-B056.
@PatentPC. „Security Patching Habits: How Long Do Companies Delay Fixes?" PatentPC. @PatentPC, 2025. április 11. https://patentpc.com/blog/security-patching-habits-how-long-do-companies-delay-fixes.
Paul, Anthony. „Biometric Data Security: Balancing Convenience with Privacy", 2024. május.
PAWR. „Fake Base Station Detection - Research on POWDER". Elérés 2025. május 3. https://advancedwireless.org/outreach/fake-base-station-detection-research-on-powder/.
„(PDF) AVOIDIT: A Cyber Attack Taxonomy". Elérés 2025. április 17. https://www.researchgate.net/publication/229020163_AVOIDIT_A_Cyber_Attack_Taxonomy.
Penguin Random House India. „Rebooting India". Elérés 2025. május 3. https://www.penguin.co.in/book/rebooting-india-2/.
Perakslis, C., és R. Wolk. „Social acceptance of RFID as a biometric security method". *IEEE Technology and Society Magazine* 25, sz. 3 (2006): 34–42. https://doi.org/10.1109/MTAS.2006.1700020.

Petersen, Laura, Laure Fallou, Paul Reilly, és Elisa Serafinelli. „Public Expectations of Social Media Use by Critical Infrastructure Operators in Crisis Communication". In *Proceedings of the 14th ISCRAM Conference*, 521–30, 2017. https://idl.iscram.org/files/laurapetersen/2017/2040_LauraPetersen_etal2017.pdf.
Pidgeon, Stefanie. „LOUD AND CLEAR". *USAASC* (blog), 2021. október 6. https://asc.army.mil/web/news-loud-and-clear/.
Pintér Róbert. „A okostelefonok mint a kiterjesztett cselekvőképesség eszközei". *Replika* 111 (2019): 63–85. https://doi.org/10.32564/111.5.
———. *Az információs társadalom: Az elmélettől a politikai gyakorlatig*. Budapest: Gondolat-Új Mandátum, 2007.
———. „Úton az információs társadalom megismerése felé". In *Pintér Róbert (szerk.), Az információs társadalom: Az elmélettől a politikai gyakorlatig*, 11–28. Budapest: Gondolat-Új Mandátum, 2007.
Piper, D.L.A. *Data Protection Laws of the World*. London: DLA Piper UK LLP, 2023.
Platforms, Meta. „Identity Verification Systems Documentation". *Meta for Developers*, 2024.
———. „Security and Account Authentication White Paper". *Meta Security Documentation*, 2024.
Point., Lieber Institute - West. „Biometrics on the Battlefield", 2024. https://lieber.westpoint.edu/biometrics-on-the-battlefield/.
Policyreviewinfo. „GDPR Compliance Is Hard" – but Is It?: 20 Hours to Overcome Privacy Issues in Mobile Apps". *Policy Review*, 2023.
Prasad, S. *Performance Evaluation of Post-Quantum Cryptographic Algorithms on Mobile Devices*. Stanford University Department of Computer Science, 2023.
Prep, Wall Street. „Freemium Model | Pricing Strategy + Examples". *Wall Street Prep*, 2024.
Privacy, Georgetown Law Center és Technology. „The Identity Trap: How Identification Systems Reinforce Inequality". *Georgetown Law*, 2023.
ProPublica. *Machine Bias*. New York: ProPublica, 2023.
„Public private partnership models (for public services)". Elérés 2025. június 15. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/public-private-partnerships?utm_source=chatgpt.com.
Pulse, LinkedIn. „Top Mobile App Security Trends to Watch in 2025"", 2023.
PwC. „Global Artificial Intelligence Study: Exploiting the AI Revolution", 2023.
Q, Li, Zhou J, és Stevenson Js. „Assessing Legal Protection of Biometric Data in China: Gaps, Principles, and Policy Recommendations". *PubMed*. Elérés 2025. május 4. https://pubmed.ncbi.nlm.nih.gov/38377336/.
Qadir, Z. „Blockchain Security: Research Challenges and Opportunities". *LinkedIn*, 2024. https://www.linkedin.com/pulse/blockchain-security-research-challenges-opportunities-zohaib-qadir-x4h7f.
„Quantum Computing Explained". *NIST*, 2025. március 18. https://www.nist.gov/quantum-information-science/quantum-computing-explained.
Racskó Péter. „A hazai alkalmazásfejlesztési ökoszisztéma és nemzetközi versenyképessége". *Vezetéstudomány* 53, sz. 6 (2022): 35–49. https://doi.org/10.14267/VEZTUD.2022.06.04.
Rahman, F. „UNHCR's Biometric Identity Management System: Implementation and Challenges". *Journal of Refugee Studies* 32, sz. 3 (2019): 452–70.
„Rapid ID Mobile Biometric Identification for Law Enforcement". Elérés 2025. május 4. https://www.hidglobal.com/solutions/rapid-id-law-enforcement.
Ráthonyi-Ódor Kinga, Ráthonyi Gergely, és Bába Éva Bácsné. „Mobil adatgyűjtési módszerek hatékonyságvizsgálata terepkutatásokban". *Erdélyi Társadalom* 20, sz. 1 (2022): 121–38. https://doi.org/10.17177/77171.258.
„Real-Time Human Authentication System Based on Iris Recognition". Elérés 2025. május 3. https://www.mdpi.com/2673-4117/3/4/47.
„Reasons to choose 4-4-2 Fingerprint Scanners for Police Accuracy". Elérés 2025. május 3. https://mantraidentity.com/Blog/Why-police-department-adopting-4-4-2-fingerprint-scanners-accuracy-speed.
Reddy, Mogalahalli V., Alain Mauger, Christian M. Julien, Andrea Paolella, és Karim Zaghib. „Brief History of Early Lithium-Battery Development". *Materials* 13, sz. 8 (2020. április 17.): 1884. https://doi.org/10.3390/ma13081884.
Regional Law Review. „Ježová". Elérés 2025. április 17. http://rlr.iup.rs/archives/year-2020/jezova/.
Regulation, General Data Protection. *Official Journal of the European Union*. Brussels: European Union, 2018.
Renz, Bettina. „Russia and »hybrid warfare«". *Contemporary Politics* 22, sz. 3 (2016): 283–300.

Report on Autonomous Vehicle Safety. Washington, DC: U.S. Department of Transportation, 2023.
Res Medias. „Az online dezinformáció és hatásai". *Medias Res Folyóirat* 7, sz. 2 (2023): 45–67.
Research, Grand View. *Decentralized Application Market Size, 2023-2030*. San Francisco: Grand View Research, Inc, 2023.
Research, Meta. *DeepFace: Closing the Gap to Human-Level Performance in Face Verification*. Scientific Publication, 2023.
Research, Microsoft. *Ambient Computing: The Next Era of Personal Technology*. Redmond: Microsoft Research, 2023.
Resperger István. *A válságkezelés és a hibrid hadviselés*. Budapest: Dialóg Campus Kiadó, 2018.
Reuters. „European Intelligence Agency Used Facial Recognition to Identify Western Spy". *News Report*, 2023. június 15.
Reuters, Thomson. *Emerging LegalTech Market Analysis*. Toronto: Thomson Reuters Corporation, 2023.
Review, M.I.T.Technology. *Strategies for Mitigating AI Bias*. Cambridge, MA: MIT Technology Review, 2024.
Ribeiro, Anna. „Resecurity Warns of Increased Cyber Threats to Energy and Nuclear Facilities from Hacktivists and Nation-States". *Industrial Cyber* (blog), 2025. április 18. https://industrialcyber.co/utilities-energy-power-water-waste/resecurity-warns-of-increased-cyber-threats-to-energy-and-nuclear-facilities-from-hacktivists-and-nation-states/.
Rikken, O., M. Janssen, és Z. Kwee. „Governance Challenges of Blockchain and Decentralized Autonomous Organizations". *Information Polity* 24, sz. 4 (2019): 397-417,. https://doi.org/10.3233/IP-190154.
Rivero, Marc. *Smartphone Users Should Be Aware of the Threats Posed by NFC Tag Tampering*. Cybersecurity Asia, 2025.
Rohani, Vala Ali. „Phishing Detection: A Case Analysis on Classifiers with Rules Using Machine Learning". *Journal of Theoretical and Applied Information Technology* 97, sz. 8 (2019): 2235–49.
„Rugged Laptops and Tablets for Military Use - In Depth Read", 2024. április 14. https://micronordic.com/blog/rugged-laptops-and-tablets-enhance-efficiency/.
Sadi, Messaoud, és Siham Bestandji. „The Digital City, Smart City or Intelligent City?A Review of the Literature for the Choice of an Appropriate Terminology". *International Journal of Innovative Studies in Sociology and Humanities* 7 (2022. november). https://doi.org/10.20431/2456-4931.071116.
Sasvari, Peter. „Közigazgatási informatikai alkalmazások". Elérés 2025. május 3. https://www.academia.edu/30804398/K%C3%B6zigazgat%C3%A1si_informatikai_alkalmaz%C3%A1sok.
Scholar, Semantic. *Digital Communities for Seniors Utilizing Human-Centric Technologies for an Advanced Society*. Seattle: Allen Institute for AI, 2023.
School, Yale Law. „Chilling Effects: The Impact of Surveillance Perception on Civil Liberties". *Yale Law Journal* 131, sz. 5 (2022).
Schwab, Klaus. *The Fourth Industrial Revolution*. Geneva: World Economic Forum, 2016. https://doi.org/10.2307/j.ctt20krxh8.
Sciences, Hungarian Academy. *Air Touch: Contactless Control Technology*. Budapest: MTA, 2023.
Sécurité Intérieure, Direction Générale. „Facial Recognition in Counterterrorism Operations". *Internal Assessment*, 2022.
Security, I.B.M. „The State of Authentication 2023", 2023.
Security of QKD Implementation. Sophia Antipolis: ETSI, 2023.
Seri, Ben, és Gregory Vishnepolsky. *Unveiling Zero Day Vulnerabilities and Security Flaws in Modern Bluetooth Stacks*. Armis, Inc., White Paper, 2017.
Shi, Weisong, Jie Cao, Quan Zhang, Youhuizi Li, és Lanyu Xu. „Edge Computing: Vision and Challenges". *IEEE Internet of Things Journal* 3, sz. 5 (2016): 637–46. https://doi.org/10.1109/JIOT.2016.2579198.
Simon Béla. „A kiberbűncselekmények nyomozásának új kihívásai". *Belügyi Szemle* 66, sz. 7–8 (2018): 106–15.
Simon Csaba Krasznay – Béla. „A digitális identitás problémái". *Nemzet és Biztonság* 13, sz. 3 (2020): 105–17.
„Smartphone history: A complete timeline". Elérés 2025. május 3. https://www.textline.com/blog/smartphone-history.
„Smartphone History: From the First Smartphone to Today | Arrow.com". Elérés 2025. május 3. https://www.arrow.com/en/research-and-events/articles/smartphone-history-from-the-first-smartphone-to-today.

Solms, Johan Van Niekerk – Rossouw von. „The State of Information Security Research: A South African Perspective”. In *Christiaan Kroeze Szerk.: Information Security in the Knowledge Economy*, 55–62. University of Pretoria, 2013.
Soni, Krishnakant. „IOT COMMUNICATION TECHNOLOGIES”. In *IIP Series*, Chapter 2. Dr. C.V. Köt. 3, Book 8, Part 9. Raman University, India, 2024.
Söderström, F., és U. Melin. „The Swedish BankID System: An Infrastructure for Digital Citizenship”. *International Journal of Electronic Governance* 11, sz. 3–4 (2019): 301–18. https://doi.org/10.1504/IJEG.2019.102929.
Standardization of Post-Quantum Cryptography. Gaithersburg, MD: NIST, 2022.
Standards for Explainable Artificial Intelligence. Piscataway, NJ: IEEE, 2024.
Standards for Quantum Key Distribution. Piscataway, NJ: IEEE, 2024.
Standards for Quantum-Safe Cryptography. Sophia Antipolis: ETSI, 2023.
Standards, National Institute és Technology. *Report on Post-Quantum Cryptography*. Gaithersburg, MD: NIST, 2023.
———. *Special Publication: CRYSTALS-Kyber Implementation*. Gaithersburg, MD: NIST, 2024.
Stanešić, Josip, Zlatan Morić, Damir Regvart, és Ivan Bencarić. „Digital signatures and their legal significance”. *Edelweiss Applied Science and Technology* 9, sz. 1 (2025. január 9.): 403–12. https://doi.org/10.55214/25768484.v9i1.4154.
State, U.S.Department. „Biometric Access Control Systems for Diplomatic Facilities”. *Diplomatic Security Service Report*, 2022.
„Statistics about Internet voting in Estonia | Elections in Estonia”. Elérés 2025. május 3. https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia.
Stehr, Nico. *Knowledge Societies*. London: Sage, 1994.
Stockwell, Sam, Megan Hughes, és Carolyn Ashurst. „The Future of Biometric Technology for Policing and Law Enforcement”. Elérés 2025. május 4. https://cetas.turing.ac.uk/publications/future-biometric-technology-policing-and-law-enforcement.
Sun, H.M., S.T. Chen, J.H. Yeh, és C.Y. Cheng. „A Shoulder Surfing Resistant Graphical Authentication System"”. *IEEE Transactions on Dependable and Secure Computing* 15, sz. 2 (2018).
„SwissID Login with Mobile ID”. Elérés 2025. május 3. https://trustservices.swisscom.com/en/about-us/news/en/swissid-login-with-mobile-id.
Sybell. „Mennyire biztonságos a felhőalapú adattárolás? Sybell Blog”. *Augusztus* 21 (2023).
Syed, Waheeduddin Khadri, Abubakar Mohammed, Kavitha Reddy Janamolla, és Dhanasekaran Selvaraj. „Biometric Authentication Systems in Banking: A Technical Evaluation of Security Measures”, 1331–36, 2024. https://doi.org/10.1109/AIC61668.2024.10731026.
Szádeczky Tamás. „Információbiztonsági szabályozások és az EU”. Budapest, NKE, 2020.
Szádeczky Tamás, Keserű Balázs, és Mezőfi Márk. „Blockchain-alapú megoldások az e-közigazgatásban”. *Információs Társadalom* 22, sz. 4 (2022): 7–26. https://doi.org/10.22503/inftars.XXII.2022.4.1.
Szalachowski, Pawel. „Password-authenticated Decentralized Identities”. arXiv, 2021. szeptember 16. https://doi.org/10.48550/arXiv.2007.15881.
Szathmáry László, Gábor András, és Bogdanov Péter. „Prediktív algoritmusok hatása a felhasználói időráfordításra és elégedettségre”. *Információs Társadalom* 22, sz. 2 (2022): 46–67. https://doi.org/10.22503/inftars.XXII.2022.2.4.
Székely Iván, Parti Katalin, és Szőke Gergely László. „Adatvédelmi tudatosság a magyar lakosság körében: reprezentatív felmérés eredményei”. *Replika* 126 (2023): 103–21. https://doi.org/10.32564/126.6.
Szénási Sándor. „Kritikus infrastruktúrák, kritikus információs infrastruktúrák – új kihívások a nemzetbiztonság számára”. *Felderítő Szemle* 10, sz. 3–4 (2011): 157–72.
Szőke Gergely László. „Adatvédelmi kihívások az okoseszközök korában”. *Infokommunikáció és Jog* 78 (2021): 15–22.
———. „Biometrikus adatok kezelésének jogi és etikai kérdései”. *Jogtudományi Közlöny* 77, sz. 3 (2022): 120–32.
„Tájékoztató a Digitális Állampolgárság Programról”, 2025. március 11. https://dunavarsany.hu/index.php/2025/03/11/tajekoztato-a-digitalis-allampolgarsag-programrol/.
Talyigás Judit. „Imre Mojzes”. *Vezetéstudomány* 52, sz. 3 (2021): 60–73. https://doi.org/10.14267/VEZTUD.2021.03.05.
Társaság Magyar Pszichiátriai. *A hazai okostelefon-függőség prevalenciája serdülők körében*. Budapest: Magyar Pszichiátriai Társaság, 2023.
Tattay Levente. „Az információs társadalom és az Európai Unió”. *Külgazdaság* 46, sz. 6 (2002): 76–97.

Team, McEliece. *Traditional McEliece Specification*. McEliece Team, 2023.
Team, S.P.H.I.N.C.S.+. *Hash-based Signatures*. SPHINCS+ Team, 2022.
Telpo. „Biometric Terminals for Border Control and Law Enforcement". In *Product Catalog*, 2023.
Teplova, Tamara, Mariya Gubareva, és Nikolai Kudriavtsev. „Social Sentiment and Exchange-Specific Liquidity at a Eurasian Stock Exchange Outside of US Market Hours". *Eurasian Economic Review* 13, sz. 3–4 (2023. december): 753–802. https://doi.org/10.1007/s40822-023-00245-9.
„Thales Mobile Authentication Solutions for Digital Banking". Elérés 2025. május 3. https://cpl.thalesgroup.com/access-management/digital-banking/mobile-authentication.
„The Importance of Biometric Data Sharing in Counter-Terrorism Capability Development – NAOC". Elérés 2025. május 4. https://natoassociation.ca/the-importance-of-biometric-data-sharing-in-counter-terrorism-capability-development/.
„Threat Screening Center — FBI". Elérés 2025. május 3. https://www.fbi.gov/investigate/terrorism/tsc.
Toffler, Alvin. *The Third Wave*. New York: Bantam Books, 1980.
Tokody, Dániel, és Imre Mezei. „Okos, fenntartható és biztonságos városok". *KÖZTES-EURÓPA Társadalomtudományi folyóirat* IX (2017. december 31.).
„Top user authentication trends for 2025 | Twilio". Elérés 2025. május 3. https://www.twilio.com/en-us/blog/user-authentication-trends.
Tran, Quang Nhat, Benjamin Peter Turnbull, Min Wang, és Jiankun Hu. „A Privacy-Preserving Biometric Authentication System With Binary Classification in a Zero Knowledge Proof Protocol". *IEEE Open Journal of the Computer Society* 3 (2022): 1–10. https://doi.org/10.1109/OJCS.2021.3138332.
„Transact Campus Mobile Credentials | MCA Higher Education". Elérés 2025. június 15. https://callmc.com/mobile-credentials-access-control/?utm_source=chatgpt.com.
Transition to Post-Quantum Cryptography. Bonn: Federal Office for Information Security, 2024.
„TruCrowd: How Biometric Entry Systems Impact Fan Experience", 2025. január 2. https://internationalsecurityjournal.com/biometric-entry-fan-experience/.
Turcsányi-Szabó Márta. „Az okostelefonok szerepe a speciális nevelési igényű tanulók oktatásában". *Gyógypedagógiai Szemle* 48, sz. 3–4 (2020): 270–86.
Tussyadiah, I.P., és J. Pesonen. „Impacts of Peer-to-Peer Accommodation Use on Travel Patterns"". *Journal of Travel Research* 55, sz. 8 (2016).
„Új fejezet a digitális okmányhasználatban – Hiteles adatigazolás a DÁP alkalmazásban (3. rész) | FinTechZone". Elérés 2025. május 3. https://fintechzone.hu/uj-fejezet-a-digitalis-okmanyhasznalatban-hiteles-adatigazolas-a-dap-alkalmazasban-3-resz/.
„UK Home Office to test remote fingerprint enrolment via smartphone for entry | Biometric Update". Elérés 2025. május 3. https://www.biometricupdate.com/202412/uk-home-office-to-test-remote-fingerprint-enrolment-via-smartphone-for-entry.
U.N.E.S.C.O. *Bridging the Digital Divide*. Paris: UNESCO, 2021.
U.N.I.C.E.F. *COVID-19: Are Children Able to Continue Learning during School Closures?* New York: UNICEF, 2021.
Unió Európai. „Az Európai Parlament és a Tanács rendelete a digitális piacokról (Digitális piacokról szóló jogszabály". *Az Európai Unió Hivatalos Lapja* 265, sz. 1 (2022).
Union, European. *eIDAS Regulation: Trust Services and Electronic Identification*. Brussels: European Union, 2023.
Union, International Telecommunication. *Digital Divide Report*. Geneva: ITU, 2023.
———. *Global Internet Penetration Rates*. Geneva: ITU, 2024.
University, E.L.T.E. „Compliance Assessment of Mobile Applications with GDPR Requirements". *Legal Studies Journal* 35, sz. 3 (2024): 112-128,.
„University of Texas. Reading Metadata To Combat Disinformation", 2025.
Urbán Ágnes. „Magyar felhasználók okostelefon-használati szokásai és applikáció-telepítési preferenciái". *Médiakutató* 23, sz. 1 (2022): 9–26.
„Using Mobile Apps in Government | IBM Center for The Business of Government". Elérés 2025. május 3. https://www.businessofgovernment.org/report/using-mobile-apps-government.
Uszkiewicz, Erik. *Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and Its Member States*. European Parliament, 2019.
Ügynökség Kormányzati Informatikai Fejlesztési. *Az Ügyfélkapu rendszer átfogó ismertetése*. Budapest: KIFÜ, 2020.
———. *Központi Azonosítási Ügynök (KAÜ) – Rendszerleírás*. Budapest: KIFÜ, 2021.

Vadher, Himanshu, Pal Patel, Anuja Nair, Tarjni Vyas, Shivani Desai, Lata Gohil, Sudeep Tanwar, Deepak Garg, és Anupam Singh. „EEG-based Biometric Authentication System Using Convolutional Neural Network for Military Applications". *SECURITY AND PRIVACY* 7, sz. 2 (2024. március): e345. https://doi.org/10.1002/spy2.345.

Vámprogram. „Ügyfélkapu+ és az elektronikus ügyintézés szabályai: Mit érdemes tudni?" Elérés 2025. május 3. https://www.vamprogram.hu/hu/-/ugyfelkapu-plusz-es-az-elektronikus-ugyintezes-szabalyai-mit-erdemes-tudni-.

Várhegyi Zsolt Haig – István. „Információs műveletek és hadviselés". In *Hadtudományi Lexikon: Új kötet*, 502–7. Budapest: Ludovika Egyetemi Kiadó, 2018.

Veldurthi, Anil. „The Role of AI and Machine Learning in Fraud Detection for Financial Services". *Journal of Computer Science and Technology Studies* 7 (2025. május): 757–71. https://doi.org/10.32996/jcsts.2025.7.4.88.

Ventures, Cybersecurity. *Global Cybercrime Damage Report*. Northport, NY: Cybersecurity Ventures, 2024.

Verizon. „Data Breach Investigations Report", 2023. https://www.verizon.com/business/resources/reports/dbir/.

Vettel, Jonathan. „Voice User Interfaces for Accessibility: Current State and Future Directions". *International Journal of Human-Computer Interaction* 39, sz. 2 (2023): 1–15. https://doi.org/10.1080/10447318.2022.2070852.

Vicsek Lilla. „Digitális Szociológia: Az okostelefon-használat társadalmi hatásai Magyarországon". *Replika* 120 (2021): 7–29. https://doi.org/10.32564/120.1.

Vidas, Timothy, Emmanuel Owusu, Shuai Wang, Cheng Zeng, Lorrie Faith Cranor, és Nicolas Christin. „QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks". Elérés 2025. május 25. https://doi.org/10.1007/978-3-642-41320-9_4.

„Voice Technology for Government | Verbio Technologies". Elérés 2025. május 3. https://www.verbio.com/voice-technology-for-government/.

VulnCheck. „VulnCheck - Outpace Adversaries", 2025. április 18. https://vulncheck.com/blog/understanding-apts.

Wang, L., és X. Deng. „Advances in Face Recognition Technology in Intelligence Operations". *IEEE Transactions on Pattern Analysis and Machine Intelligence* 43, sz. 1 (2021): 34-49,.

Watch, Human Rights. „Biometric Targeting: The Role of Biometrics in Lethal Targeting Operations". Special Report, 2023.

———. *Surveillance in China*. New York: Human Rights Watch, 2024.

Webster, Frank. *Theories of the Information Society*. London: Routledge, 2006. https://doi.org/10.4324/9780203962824.

„What Are the Three Authentication Factors? - Rublon". Elérés 2025. május 3. https://rublon.com/blog/what-are-the-three-authentication-factors/.

„What Is »Hardware Root of Trust« in Industrial IoT?" Elérés 2025. május 3. https://www.hms-networks.com/tech-blog/blogpost/hms-blog/2023/11/13/what-is-hardware-root-of-trust.

„What Is Identity Verification? | OneSpan". Elérés 2025. május 3. https://www.onespan.com/topics/identity-verification.

„With France Identité, generate one-time credentials". Elérés 2025. május 3. https://www.service-public.fr/particuliers/actualites/A17276?lang=en.

World, Smart Cities. „Global Smart Cities Market to Reach $2.5 Trillion by 2026". *Market Analysis Report*, 2023.

„Worldwide Global DataSphere IoT Device and Data Forecast", 2022.

„Zero Trust Architecture", 2020.

Zhang, Wenyi, Hengtian Zhang, és Zhouyang Deng. „Public Attitude and Media Governance of Biometric Information Dissemination in the Era of Digital Intelligence". *Scientific Reports* 15, sz. 1 (2025. január 18.): 2419. https://doi.org/10.1038/s41598-025-86603-w.

Zhou, Lan, Vijay Varadharajan, és Michael Hitchens. „Trust-Based Secure Cloud Data Storage with Cryptographic Role-Based Access Control". In *Proceedings of the International Conference on Security and Cryptography*, 370–75, 2013. https://www.scitepress.org/Papers/2013/45086/45086.pdf.

„Zibin Zheng – Shaoan Xie – Hong-Ning Dai – Xiangping Chen – Huaimin Wang (2018): Blockchain challenges and opportunities: A survey". *International Journal of Web and Grid Services* 14, sz. 4 (é. n.): 352–75.

Ződi Zsolt. „A mesterséges intelligencia alkalmazása a jogi munkában". *Jogtudományi Közlöny* 77, sz. 1 (2022): 15–28.

In *NATO Strategic Communications Centre of Excellence (2022): Digital Resilience in the Age of Disinformation*. Riga, é. n.

12 PUBLIKÁCIÓS JEGYZÉK

- Koller Marco, és Laufer Balázs. „Magyarország migrációs stratégiájának kialakítása a Nemzeti Biztonsági Stratégia és az európai uniós szabályozások mentén". Stratégiák, stratégiai gondolkodás, nemzetbiztonság (2023): 89–106.
- Koller Marco. „Okoseszközök mint a személyi hitelesítésre alkalmas interface-technológia biztonsági vetületei". Hadmérnök 18, sz. 1 (2023): 109–124. https://doi.org/10.32567/hm.2023.1.8.
- Koller Marco, és Bányász Péter. „The Opportunities and Security Risks of Mobile Applications in the Context of Local Economic Development". Academic and Applied Research in Military and Public Management Science 22, sz. 2 (2023): 5–22. https://doi.org/10.32565/aarms.2023.2.1.
- Koller Marco. „Magánbiztonsági vállalatok szerepe az állami műveletekben". Taktikák és stratégiák a kiberhadviselésben (2023): 133–150.
- Bányász Péter, Tóth András, Koller Marco, és Magyar Sándor. „A videókonferencia-alkalmazások biztonsági kockázatai". Acta Humana: Hungarian Centre for Human Rights Publications 10, sz. 4 (2022): 19–34. https://doi.org/10.32566/ah.2022.4.2.
- Koller Marco. „Az okos eszközök által gyűjtött metaadatokkal való visszaélések, az állami szerepvállalás és a társadalmi elfogadottság tükrében". A hadtudomány és a 21. század 2022 (2022): 146–158.
- Koller Marco. „Recommendations for Safety-Conscious Smart Device Use by Military Professionals". Academic and Applied Research in Military and Public Management Science 21, sz. 2 (2022): 5–14. https://doi.org/10.32565/aarms.2022.2.1.
- Kerti András, és Koller Marco. „Az okoseszközök applikációi által gyűjtött metaadatokkal való visszaélések kockázati szemléletmód általi, felhasználói szintű lehetséges visszaszorítása". Hadmérnök 16, sz. 4 (2021): 145–156. https://doi.org/10.32567/hm.2021.4.11.