

36. Országos Tudományos Diákköri Konferencia

Had- és Rendészettudományi Szekció

Budapest, 2023. április 18-20

Nemzeti Közszolgálati Egyetem

Rendészettudományi Kar

Arcfelismerő rendszerek fejlődése és alkalmazhatósága

Jelige: *Big Brother*

Pályamunka lezárásának időpontja: *2022. szeptember*

2022.

BEVEZETÉS	3
1. BIOMETRIAI AZONOSÍTÁS	5
2. BIOMETRIKUS ADATKEZELÉS JOGI SZABÁLYOZÁSA	7
2.1 EURÓPAI JOGSZABÁLYI KERETEK.....	7
2.2 ADATTOVÁBBÍTÁS HARMADIK ORSZÁGOKBA	8
2.3 SZÜKSÉGESSÉG ÉS ARÁNYOSSÁG ELVE	9
2.4 MAGYAR RENDELKEZÉSEK	9
3. ARCDETEKTÁLÁS.....	11
3.1 ARCÉRZÉKELÉS/ARCDETEKTÁLÁS	11
3.2 ARCFELISMERÉS ADATKÉSZLETE	13
4. ARCFELISMERÉS	14
4.1 GEOMETRIAI.....	14
4.2 EDGE MAPPING	15
4.3 LINE EDGE MAPPING	15
4.4 HÁROMDIMENZIÓS ARCFELISMERÉS	16
4.5 MESTERSÉGES INTELLIGENCIA	17
5. ARCFELISMERÉS MASZK HASZNÁLATA IDEJÉN	19
5.1 A TESZT KÖRÜLMÉNYEI	19
5.2 EREDMÉNYEK.....	20
6. MÁR LÉTEZŐ, KÜLFÖLDI ARCFELISMERŐ RENDSZEREK	22
6.1 KÍNA.....	22
6.2 INDIA	24
6.3 EGYESÜLT KIRÁLYSÁG.....	26
7. HAZAI „ARCFELISMERŐ RENDSZEREK”	29
7.1 SIÓFOK	29
7.2 SZITAKÖTŐ PROJEKT.....	30
7.3 TOVÁBBI MAGYAR VONATKOZÁS	31
8. INTERJÚ	32
9. KUTATÁSOM	35
EREDMÉNYEK:.....	36
KONKLÚZIÓ.....	41
10. ÖSSZEGZÉS	42
JEGYZÉKEK.....	44
ÁBRAJEGYZÉK.....	44
TÁBLÁZATJEGYZÉK	44
DIAGRAMJEGYZÉK.....	44
FELHASZNÁLT IRODALOM	45

Bevezetés

A folyamatosan fejlődő digitalizáció meghatározó szereplőjévé vált a mindennapjainknak. A természetes személyek és a gazdaság résztvevőinek adatait manapság gyakran digitális formában hozzák létre. Ezeknek az adatoknak a hozzáféréséhez különböző jogosultságok tartozhatnak, a megfelelő jogosultságoknak az ellenőrzésére valamilyen személyazonosítás szükséges, az illetéktelen hozzáférés elkerülése érdekében. Ezt hívják lényegében hozzáférés szabályozásnak. Az információtechnológiai fejlődés miatt egyre nagyobb mértékben keletkezett igény a megbízhatóbb, kisebb kockázatú és kényelmesebb személyazonosítási módszerekre. Ez nagyban eredményezte a biometrikus azonosítás elterjedését. A másik tényező, amely elősegítette ennek a technológiának az elterjedését, az a különböző szenzorok tömegcikké válása és a gyártók között is megjelenő piaci verseny.

Az arcazonosítás a digitalizáció előtti időkre is visszavezethető. Gondoljunk bele, hogy a vadnyugaton is a XIX. században megjelentek a „wanted” feliratú arcképek a körözött személyekről. Már akkor próbálták az embereket egyedi tulajdonságok alapján azonosítani. Magyarországon, 1887-ben bevezették, hogy a bünyügyi nyilvántartást fényképekkel egészítik ki. Az 1896-os világkiállításra preventív céllal, 2000 példányban juttattak el fényképfelvételeket zsebtolvajokról a rendőrkapitányságokra. 2010-ben a rendőrség kísérletet tett egy automatizált arcképelemző rendszer bevezetésére, de áttörő sikert a 2013. évi LXXXVIII. törvény ért el az arcképprofil nyilvántartási rendszer létrehozásával, melynek értelmében a körözést lefolytató szerv jogosult arcképelemző tevékenységet folytatni. Manapság a rendészeti célú felhasználás mellett a polgári célú felhasználás egyre elterjedtebbé válik az érintésmentes azonosításnak köszönhetően, mely kényelmi és egészségügyi szempontból is előnyös. A biometrikus azonosítás lehetővé teszi a tudásalapú (kód) és a birtok alapú (kártya) azonosítás mellett a tulajdonságalapú azonosítást. Ez azt jelenti, hogy nehéz ellopni vagy megszemélyesíteni, nem lehet úgy eltulajdonítani, mint egy kódot vagy kártyát, így ez a technológia alternatívát, vagy kombinált azonosítást is lehetővé tesz. Az innovációkra a jogszabályalkotóknak gyors reagálásra van szükségük, hogy lépést tudjanak tartani a mai trendekkel. A jogszabályoknak egyszerre kell megfelelniük a jelen technológiáinak, az érintettek személyiségi jogainak, és a társadalom elvárásainak.

Jelen tanulmányom körbejárja az arcfelismeréssel kapcsolatos elméleti és gyakorlati kérdéseket. Ennek eredményessége elősegítése céljából végeztem egy kutatást, melynek hipotézisei a következők:

Hipotéziseim:

H1: Akik biztonság tudatosnak vallják magukat, nagyobb arányban használnak biometrikus azonosítást.

H2: Akik hallottak már a kínai megfigyelési rendszerről, azok közül kevesebben választanák a kínai fejlesztésű arcfelismerő szoftvert, mint akik még nem hallottak róla.

1. Biometriai azonosítás

Mit is jelent az a kifejezés, hogy biometria? A biometria a görög eredetű „bios” vagyis, mint élet és „metrein” mint megmér szavakból erednek. Ebben a kontextusban az ember fizikai jellemzőinek megmérését jelenti.

Az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete (továbbiakban: GDPR) 4/14. cikke szerint biometrikus adatnak minősül „egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat”. A biometrikus adatokat többnyire három csoportba sorolhatjuk: biológiai, morfológiai és viselkedési biometrikus adatok. A biológiai biometrikus tulajdonságokat genetikai és molekuláris szinten értelmezzük. Ezek magukban foglalhatnak olyan jellemzőket, mint a DNS vagy a vér, amelyeket a testnedvek mintájával lehet értékelni. A morfológiai biometrikus adatok a test szerkezetét foglalják magukban. Olyan fizikai tulajdonságok, mint például a szem, az ujjnyomat vagy az arc, ezeknek a testrészeknek a formái feltérképezhetőek biztonsági szkennerek használata során is. A viselkedési biometrikus adatok minden egyes személy egyedi mintáin alapulnak. Az, ahogyan sétál, beszél, vagy akár gépel a billentyűzeten, jelezheti személyazonosságát.

A biometriai azonosítás az a technológia, mely az ember egyedi, hamisíthatatlan paramétereit veszi figyelembe. Az adatok az érintett személyéhez szorosan köthetők, ezért a tudás, illetve a birtoklás alapú azonosításhoz képest jelentősen bizalmasabb. A biometrikus technológia egyre népszerűbb módja a személyazonosság ellenőrzéséhez. A biometrikus adatok más hitelesítésekkel kombinálva a legerősebb ismert biztonságot nyújtja. [1]

Biometrikus adatok jellegüknél fogva lehetővé teszik egy személy azonosítását és hitelesítését, a felismerhető és ellenőrizhető, egyedi adatok alapján. Azonosítás során arra keresi a választ, hogy: „Ön kicsoda?”, míg hitelesítés során arról kell meggyőződnie a szoftvernek, hogy: „Ön valóban xy?”¹

Az azonosítás két fő szakaszra osztható: először a szoftver begyűjti az arc adatait és egy sablonná alakítja át (ezt hívjuk regisztrációs folyamatnak), utána következik az arc azonosítása, ahol a sablont egy, vagy több másik sablonnal hasonlítja össze. Ilyenkor, a biometrikus szoftver „arc-lenyomatot” hoz létre a mért jellemzők, például a szemek közötti távolság és a homlok és

¹ Fontos tudni, hogy a rendszer nem tudja teljes mértékben eldönteni, hogy az a személy valóban az-e aki. Ezért inkább százalékban határozza meg az egyezést és ez tükrözi a döntésbe vetett bizalmat. Az egyezés elutasítottasága vagy elfogadása attól függ, hogy a kapott eredmény küszöbérték fölé vagy alá esik.

az áll közötti távolság alapján, amelyet azután össze lehet hasonlítani más arclenyomatokkal, például egy azonosító dokumentumban vagy adatbázisban található képekkel az egyén azonosításához. A cél annak megállapítása, hogy egy személy (egy sablon) egyezik-e egy fényképpel (egy másik sablon), vagy annak megerősítése, hogy az illető az, akinek vallja magát. Ilyen az engedélyezés/hitelesítés, például egy arc párosítása egy igazolványképpel a repülőtéren vagy annak megállapítása, hogy az illető az-e, akinek hiszik. [2].

2. Biometrikus adatkezelés jogi szabályozása

2.1 *Európai jogszabályi keretek*

A gyors technikai fejlődés és globalizáció új kihívások elé állította az adatvédelmet. Ezáltal szükség volt egy új, szilárd és következetes jogszabályra, mely magába foglalja, hogy a természetes személyek maguk rendelkezessenek adataik felett. Az arcfelismerő rendszerek terjedése magával vonzotta a technika megosztottságát a társadalom szemében. Tisztában kell lennünk az arcfelismerő rendszerek kockázataival, főleg a későbbiekben taglalt, mesterséges intelligencia (továbbiakban: MI) adta lehetőségeivel. Mivel egy személy arca az egyik leglátványosabb arcvonása, könnyen lehetővé teszi az azonosítást, ráadásul az arcfelismerési adatok a többi biometrikus adattól eltérően fizikai behatás nélkül, sőt az egyén ismerete nélkül is gyűjthetők.

A GDPR viszont keretet szab az adatgyűjtésnek és a felhasználásnak. Adatkezelésnek minősül jogszabály szerint a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, terjesztés, nyilvánosságra hozatal, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ide értve az ujjnyomatot). Vagyis, minden olyan személyes adattal kapcsolatos tevékenység mely kiterjed a személyes adatok kezelésére. Ilyenkor felvetődik az a kérdés, hogy akkor a GDPR (51) preambulumbekkezdése különbséget tesz az egyszerű „fényképek” és a biometrikus „arcképek” jogi természete között. Csak akkor számít biometrikus adatkezelésnek, ha egy személy egyedi azonosítását, vagy annak hitelesítését speciális eszközökkel hajtják végre. Vagyis, ha egy személy arcképét lefényképezzük, az nem számít biometrikus adatkezelésnek, de ha valamilyen algoritmust használunk az azonosításra, akkor már igen.

A személyes adatokkal kapcsolatos adatok feldolgozása GDPR hatálya alá tartoznak, ezért meg kell felelnie az 5. cikk elveinek, valamint a III. fejezet szerint az érintettek alapvető jogait garantálnia kell. A GDPR szigorú követelményeket fogalmaz meg az adatkezelőkre és az adatfeldolgozók számára, az előírások be nem tartása komoly szankciókat vonhatnak maguk után, akár 20 millió eurós közigazgatási bírság is kiszabható [3]. Az adatkezelés csak megfelelő jogalap fennállása esetén lehetséges. A 40. preambulumban alapján az adatkezelő köteles megnevezni a 6. cikk (1) bekezdéséből legalább egy jogalapot.

Viszont a biometrikus adatok különleges személyes adatnak minősülnek, amelynek kezelése alapvetően tilos. Csak és kizárólag abban az esetben jogszerű a biometrikus adatkezelés, ha a 6. cikk (2) bekezdésében foglaltaknak megfelel. Ilyen például, ha: más természetes személy létfontosságú érdekeinek védelméhez szükséges; az érintett egyértelműen hozzájárult; jelentős közérdek miatt szükséges. Viszont, kivételt képeznek a bűnüldözési irányelvek², melynek érdekében elő kell segíteni az Unión belül az illetékes hatóságok között a személyes adatok szabad áramlását a bűncselekmények megelőzése, nyomozása, felderítése céljából. Ez az Unió irányelv a személyes adatok automatizált feldolgozását, valamint a személyes adatok bármely más módon történő feldolgozását is tartalmazza.

2.2 Adattovábbítás harmadik országokba

A használt módszertől és adatforrástól függően arcfelismerő rendszerek alkalmazása az Európai Gazdasági Térségen kívülre történő adattovábbítással is járhat, ennek érdekében az Európai Bíróság nagyon fontos döntéseket hozott, az úgynevezett Schrems II ítéletet. A GDPR rendelet alapján a harmadik országba továbbított adat adatkezelőjének gondoskodnia kell a megfelelő védelmi színtről. A védelem megfelelő szintjének hiányára hivatkozott az Európai Bíróság, vagyis az Egyesült Államokban az adatvédelem szintje nem volt egyenértékű az Unió joggal, és érvénytelennek nyilvánította az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló (2016/1250) határozatát [2]. A Bíróság úgy ítélte meg, hogy az Egyesült Államok belső szabályozásának követelményei lehetővé teszik az Egyesült Államok hatóságai számára az Unióból az Egyesült Államokba továbbított személyes adatokhoz a nemzetbiztonsági célból való hozzáférést. Ez nagymértékben korlátozhatja a személyes adatok védelmét és nem biztosít az érintett személyek számára az amerikai hatóságokkal szemben érvényesíthető jogokat [4].

2021. decemberében az Osztrák Adatvédelmi Hatóság (DSB) azt véleményezte, hogy a Google Analytics, melynek adatait az Egyesült Államokban tárolják, és nem felel meg a GDPR V. fejezetének [5]. Úgy tűnik, hogy a nemzeti adatvédelmi hatóságok és az Európai Adatvédelmi Testület (EDPB) fel akarják számolni az ilyesfajta adattovábbítást. Ezek a szabályok nehézséget okozhatnak az arcfelismerő szolgáltatásokat használó EU-n kívül adatokat tároló vállalkozásoknak. Jelenleg nagyon szigorú követelmények vannak érvényben a harmadik országba való adattovábbításnak. A GDPR 46. cikke szerint megfelelő garanciáknak kell

² Az Európai Parlament és Tanács [\(EU\) 2016/680](#) Irányelve

érvényesülnie az adat továbbításához, feldolgozásához, vagy ennek hiányában a 49. cikkben meghatározott különleges helyzetekben alkalmazandó megoldások egyikének.

2.3 Szükségesség és arányosság elve

Szükségesség elve szerint a személyes adatok feldolgozásának első kérdése az, hogy az feltétlenül szükséges-e. Ha nem, vagy van rá más mód, akkor az megkérdőjelezi annak szükségességét. Csak is objektív bizonyítékkal lehet ezt igazolni és ez a lépés megelőzi az arányosság kérdését.

Az arányosság megköveteli, hogy a jogkorlátozás hátrányai ne kerekedjenek felül a jog korlátozásából származó előnyeinek. A személyes adatok kezelése során ügyelni kell, hogy csak olyan személyes adatot dolgozzanak fel, amely az adatkezeléshez szükséges és releváns.

2.4 Magyar rendelkezések

Az Alkotmánybíróság máig ható elvi élel rögzítette határozatában, hogy „a meghatározott cél nélküli, előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés- és tárolás alkotmányellenes”, rögzítve ezzel a készletező adatgyűjtés máig tartó tilalmát.³ Az Országgyűlés az emberek információs önrendelkezésének érdekében és a magánszférájuk megtartása érdekében megszavazta a 2011. évi CXII. törvényt. Valamint hivatkozik, hogy a magánélethez és a személyes adatok védelméhez fűződő jog alkotmányos alapérték. Magyarország Alaptörvényének VI. cikke kimondja, hogy a magánélethez és a személyes adatok védelméhez fűződő jog alkotmányos alapérték.

Rendészeti tekintetben a növekvő adatgyűjtési igény következtében szükség volt új nemzeti jogszabálykeretre. Ennek érdekében hozták létre a 2009. évi XLVII. törvényt a bünyügyi nyilvántartásról, amely rendelkezik a biometrikus azonosításról, adatgyűjtési módszerekről és annak eljárási rendjéről. 2019-ben a rendőrségi törvény módosításakor az Országgyűlés elfogadta a 2019. évi CXVI. - egyes eljárások egyszerűsítése és elektronizálása érdekében szükséges törvénymódosítást. Amely azzal egészült ki például, ha az igazoltatott személy a rendőrnek nem tudja hitelt érdemlően bizonyítani személyazonosságát, úgy a rendőrnek joga

³ 15/1991. (IV. 13.) AB határozat

van, hogy fényképfelvételt készítsen a személyről és azt arcképelemző rendszerrel azonosítsa az arcképelemző rendszerről szóló törvényben meghatározottak szerint.⁴

1. táblázat: Jogszabályi keret időrendi változása

Kihirdetés ideje	Jogszabály neve
2009. VI. 19.	2009. évi XLVII. törvény a bünygyi nyilvántartási rendszerről
2011. VII. 26.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
2013. VI. 20.	2013. évi LXXXVIII. törvény a körözési nyilvántartási rendszerről és a személyek, dolgok felkutatásáról és azonosításáról
2015. XI. 27.	2015. évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről
2016. IV. 27.	AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE
2018. XI. 28.	AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/1860 RENDELETE AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/1861 RENDELETE AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/1862 RENDELETE
2019. XII. 18.	2019. évi CXVI. törvény egyes eljárások egyszerűsítése és elektronizálása érdekében szükséges törvénymódosítás

Forrás: Újhegyi Péter-Kun Tamás: Biztonságtudományi szemle 2020. II. évf. 3. szám. 14.

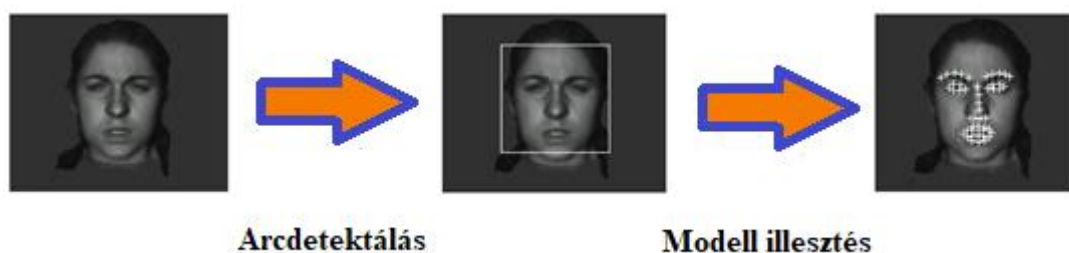
⁴ 1994. évi XXXIV. törvény a Rendőrségről 4.§ (4a) bekezdés

3. Arcdetektálás

A biztonságérzet csökkenése az egész világban tapasztalható és ezzel párhuzamosan nőtt az igény a felhasználók egyedi azonosítására. Erre az arcfelismerő technológia tökéletes megoldást nyújthat. Ezek a rendszerek sem tökéletesek, de a rohamos fejlődésnek hála egyre kisebb hibaarányú eredményeket kínálnak és magasabb biztonsági követelményeknek felelnek meg. Ezt jelzi az is, hogy már számos területen alkalmaznak arcfelismerő rendszereket, a teljesség igénye nélkül: bűnmegelőzés, kiberbiztonság, hozzáférés szabályozás (beléptető rendszerek, okostelefon feloldás), mobil fizetés, reptér, közösségi média és Google Fotók címkézése. Olyan területeken előnyös alkalmazni ahol az a fő cél, hogy az azonosítás érintésmentes és érzékelhetetlen legyen.

3.1 Arcérzékelés/arcdetektálás

Az arcfelismerést megelőzi az arcérzékelés, vagy arcdetektálás (1. ábra), amelynek feladata a beérkező kép/videóadatokon felismerni az arcokat [6]. Egy emberi arcnak a detektálása nem okoz nagy gondot egy ember számára, hiszen tudatában van azoknak az információknak, hogy mik jellemzőek egy arcra (szem, orr, száj stb.). Azonban egy számítógép esetében már nem olyan egyszerű feladat. Számos befolyásoló tényező létezik, amelyek nehezítik egy arc megtalálását a képen (bőrszín, arc mérete, elhelyezkedése, pozíciója stb.). Az elmúlt évtizedekben számos különféle kutatás és fejlesztés zajlott az arcok detektálásával kapcsolatban. Mindegyikben az a közös pont, hogy az arc speciális jellemzőit veszik figyelembe.



1. ábra: Az arcfelismerés lépései

Saját szerkesztés

Az arcérzékelés több, különböző módon is megvalósulhat:

1. Jellemző alapú módszer: az ilyen rendszerek lényege, hogy megkeresik az arc jellemző vonásait (szem, orr, száj), majd megvizsgálja, hogy megfelel-e egy arc geometriájának.
2. Mintaillesztés: ez a technika azon alapszik, hogy egy előre elkészített arcmintát keresünk a képen. A mintának nagyon reprezentatívnak kell lennie, ugyanis a különböző népcsoportok arcvonásai eltérhetnek egymástól. Ugyanis a téves azonosítások kellemetlenséget okozhatnak. Előfordult, hogy az algoritmus elfogultsága következtében afroamerikai, ázsiai arcokat 10-100 szoros tévedéssel azonosította [7].
3. Bőrszín alapú szegmentálás: lényege, hogy az algoritmus pixelre lebontva osztályozza a színeket és hasonlítja össze, hogy mennyire hasonlítanak az emberi arc színéhez. Előnye, hogy nem befolyásolja a fej pozíciója, hátránya, hogy megvilágításra érzékeny. Itt a gyártók jellemzően át szoktak térni más színtérbe és nem RGB-t⁵ alkalmaznak.
4. Mesterséges intelligencia alapú: Az arcfelismerés mesterséges intelligencia alapú algoritmusokat és gépi tanulást (machine learning) használ az emberi arcok észlelésére. Az algoritmus általában az emberi szem megkeresésével kezdi, majd ezt követi a szemöldök, az orr, a száj, az orrlyukak. Az összes arcvonás rögzítése után a nagy adatkészletekkel végzett ellenőrzések megerősítik, hogy egy emberi arcról van szó. A mesterséges intelligencia arcdetektálásra használt gyakori technikái közül a legtöbb a jellemző alapú, a megjelenés alapú, és a sablonillesztés alapú [8]. A mesterséges intelligencia segítségével a szoftver statisztikai elemzéseket hajt végre és a korábban kinyert képeket összehasonlítja a korábban tárolt arcminákkal vagy jellemzőkkel, és az eredményeket korrelálja⁶ az arc észleléséhez.

⁵ RGB= Red (piros), Green (zöld) és Blue (kék) kezdőbetűiből állnak. A videótechnikában az egyik leggyakrabban használt színtér. Ennek a három színnek a kombinációjából különféle színeket lehet létrehozni.

⁶ Korrelál= Felhasznál

3.2 *Arcfelismerés adatkészlete*

Az arcfelismerés leggyakoribb alkalmazásai közé két feladat tartozik. Az első feladat, amely során ellenőrizni kell, hogy, az arc ugyanazon személyhez tartozik-e. Ez „egy az egyhez” (1:1) egyeztetésként ismert, és gyakran használják ellenőrzési munkákhoz, például okostelefon feloldásához vagy útleveél ellenőrzéséhez. A második meghatározza, hogy a fényképen szereplő személynek van-e egyezése az adatbázisban, „egy-a-többhöz” (1:N) elemzésnek nevezik [9]. Ilyen, ha egy rablást elkövető ismeretlen személyről készült térfigyelőkamera felvételt hasonlítunk össze az adatbázisban lévő személyekkel.

4. Arcfelismerés

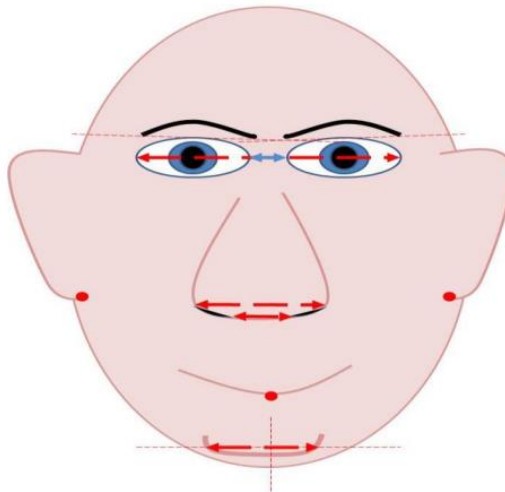
Ez az a lépés a folyamatban, ahol az észlelt arcot az egyedi jellemzők alapján egy személyhez kapcsoljuk. Az informatika fejlődése magával vonzotta, hogy különböző arcfelismerő technikák jöjjenek létre.

4.1 Geometriai

Az arc különböző részleteinek – szem, orr, száj, egymáshoz viszonyított elhelyezkedését és méreteit elemzi [6].

Fontos paraméterek [10]:

- a) a jobb és bal szem két szélső pontja
- b) a jobb és bal orrcimpa két szélső pontja
- c) a száj középpontja (stabilabb, mint a két szélső pontja)
- d) az áll jobb és bal pontjának vízszintes pozíciója
- e) az áll közepének függőleges pozíciója
- f) szemöldökök vízszintes pozíciója
- g) fülcimpák alsó pontja

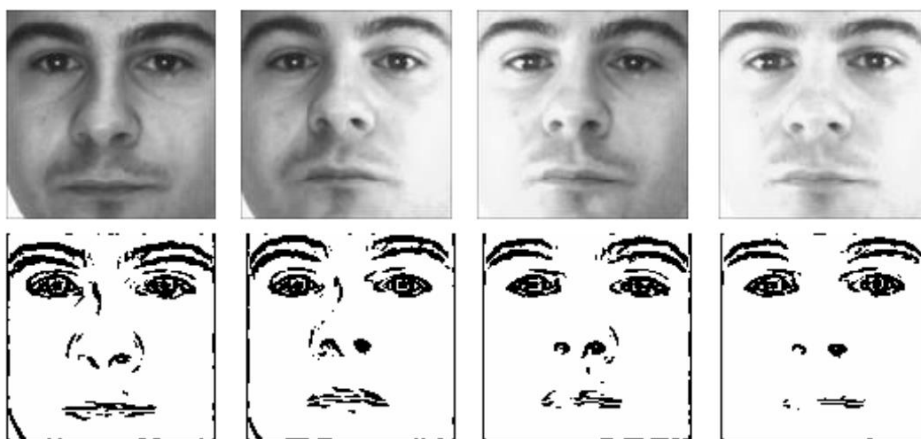


2. ábra: A geometriai arcfelismerés leglényegesebb paraméterei

Forrás: Földesi Krisztina: A biometrikus azonosítási eljárások alkalmazhatósági scenáriói a rendőri munkában. (2016).

4.2 Edge mapping

A szoftver egy élkeresést hajt végre az arcon és összeveti az adatbázisban lévő különböző képekkel, amelyek tartalmazzák az éleket. Hátránya az, hogy sok adatot tárol és ezáltal nagyobb tárhelykapacitás szükséges, ráadásul a fényváltozásokra érzékeny (3. ábra). A kísérleti eredmények azt mutatják, hogy 92,73% - 95,62% közötti arcfelismerési arány érhető el a megvilágítás függvényében [11]. A technológia előrehaladtával nem vált túl elterjedtté, jelenleg ezt a féle arcdetektálást nem használják a mai modern arcfelismerő rendszerek.

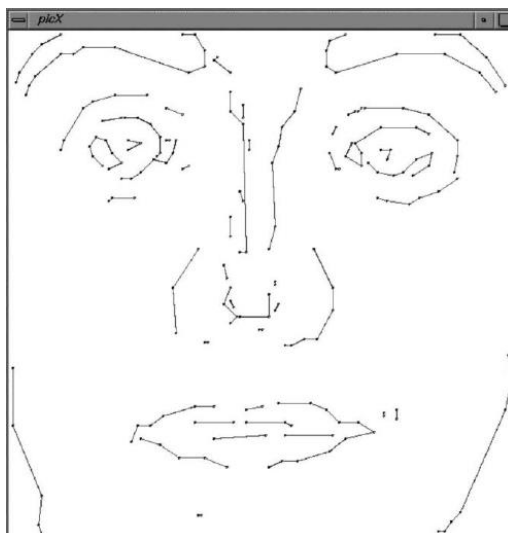


3. ábra-A fényviszonyok nagyban befolyásolják az élek keresését.

Forrás: Wei Wang: 1st International Conference on Bioinformatics and Biomedical Engineering (2007)

4.3 Line edge mapping

A line edge mapping az edge mapping továbbfejlesztése. Ami annyiban jelent különbséget, hogy ez a megoldás, csak a vonalszakaszok végpontjait rögzíti a görbéken, és ez tovább csökkenti a tárolási igényt. A szoftver ehhez a két végpont közötti távolságot veszi figyelembe. A vonalszakasz távolságát Hausdorff távolságnak hívjuk. Az arcok hatékony kódolása nagyon fontos szempont az arcfelismerő rendszerben. Plusz előnye, hogy kevésbé érzékeny a megvilágítás változásaira.



4. ábra: Edge line mapping felület illusztrációja, jól láthatóak a végpontok.

Forrás: Varga Miklós: Azonosítás Arcfelismeréssel (2016).

4.4 Háromdimenziós arcfelismerés

Az arcazonosítási technológia új iránya a 3D szenzorokkal végez adatgyűjtést, ami további információkat képes begyűjteni az arc sajátosságairól a bőr textúrájának és hőterképének analizálásával [12]. A detektált arcból egy háromdimenziós modellt képeznek. A 3D arcfelismerés hatékonyabban tudja végrehajtani az arcfelismerést, mint a 2D arcfelismerés, mert a 2D arcfelismerő rendszereket olyan tényezők korlátozhatják, mint például: a fényintenzitás, fejpozíció, smink vagy képek elmosódásával kapcsolatos problémák. A 3D technológia a Microsoft által kifejlesztett Kinect technológiával vált igazán elterjedté.⁷ Ez a technológia azon alapszik, hogy többféle kamerát helyezünk egy eszközbe, amelyek egyszerre különböző feladatot látnak el. Az eszköznek rendelkeznie kell egy infravörös fényt kibocsájtó modullal (továbbiakban: infravörös projektorral), amely szabad szemmel nem látható fénytartományú infravörös fényt bocsájt ki. Az általa kibocsájtott fénynek a visszaverődését egy infravörös kamera begyűjti és rögzíti, ez a mélységet hivatott meghatározni. A második kamera egy RGB kamera, amely a színek megjelenítését teszi lehetővé [13]. A Kinect technológiát 2017-ben vezette be az Apple az iPhone X okostelefonján (5. ábra). Az iPhone X 30 000 infravörös pontot vetít ki a felhasználó arcára (DOT projektor), hogy domborlenyomatot hozzon létre. Ez a technológia az okostelefonok legfejlettebb biztonsági eszköze, 0,0001%-os hibaarányával. Ez volt az első okostelefon, amely 3D arcfelismerő technológiával rendelkezett.

⁷ Az Xbox 360 játékkonzolhoz lehetett külön megvásárolni 2010-től.



5. ábra: Az iPhone X lényegében egy Kinect. Megtalálhatóak rajtuk ugyanazon jellemzők.

Forrás: TechRadar

4.5 Mesterséges intelligencia

A mesterséges intelligencia és a gépi tanulás (machine learning) lehetővé teszi az öntanulás folyamatát. De tisztáznunk kell mit is jelent a mesterséges intelligencia és a gépi tanulás.

A gépi tanulás a mesterséges intelligencia részhalmazának tekintendő. A szoftver egy emberi gondolkodást kísérel meg, és feladatokat hajt végre egyedül algoritmusok segítségével. Ezeknek az algoritmusoknak az emberi logikára való betanításának egyik módja a neurális hálózat. Ez olyan algoritmusok sorozata, amelyek az emberi agy modellje alapján készültek [14].

Az agy viszont lassan tanul, inkább ismétlődő ingerek kellene és gyakran lényegesen sok időt vesz igénybe, hogy teljesen megértsen egy nagyon összetett problémát. A mesterséges neurális hálózatok számítógépek programozásával készülnek, és úgy viselkednek, mintha milliárd párhuzamosan működő, erősen összekapcsolt agysejtekből készítették volna őket. A mesterséges neurális hálózat az emberi agytól leginkább pontosságában és gyorsaságában különbözik [15].

Mély tanulás a gépi tanulás egy speciális formája, amely szintúgy neurális hálózatokkal működik. A mély tanulás képes pontosságot mérni, döntést hozni, és az adatokat az emberi agyhoz hasonlóan osztályozza. Arcfelismerés terén, a legelterjedtebb körben használt funkciója a kategorizálás. Ebbe bele tartozik a kormeghatározás, nemek meghatározása és az érzelmek megállapítása is. Nagy előnye, hogy rendkívül alacsony a faji vagy nemi elfogultsága, a több millió arcra kiterjedő adatkészletnek, modellképzésnek köszönhetően.

Minden személy arca számos adatpontra van felosztva; ezek lehetnek a szemek távolsága, az arccsont magassága, a szem és a száj távolsága stb. A mesterséges intelligencia arcfelismerése ezeken az adatpontokon veszi figyelembe az eltéréseket.

Működésének alapvető módja az, hogy egy címkézett funkciókészlettel kezdjük. Lényegében olyan fotókkal kezd, amelyek már kézzel illesztett összefüggéseket mutatnak az érintettekkel. Például, mikor én elkezdem egyesével párosítani a személyeket az arcképükhöz a rendszerbe. Egy kezdeti, manuális korrelációnak kell lennie egy személy arca és identitásuk között, ugyanis lesznek kezdetben hibák. És amint ez a folyamat elkezdődik, egyre könnyebb lesz az arcok azonosítása.

A mesterséges intelligencia arcfelismerést nem csak a biztonságtechnikában, vagy a rendészetben használják. Polgári felhasználásban a Google Fotók címkéző funkciója is ezt használja, ahol, ha feltöltünk magunkról egy képet, és társítjuk hozzá a nevünket, akkor az összes többi képen amin szerepelünk, ahhoz hozzárendeli a nevünket.

5. Arcfelismerés maszk használata idején

Számos olyan körülmény van, amikor az arcokat valami eltakarhatja, ilyen például világjárvány esetén az arcmaszk. Maszkhasználat esetén az arcdetektálás a szemközti és a felette lévő részekre korlátozódik. Ilyenkor felvetődik az a kérdés, hogy biztosan tudja azonosítani az arcot miközben maszkot viselek? Hiszen a „fél” arcot kitakarja. A másik ilyen felvetés az az, hogyha mégis tudja valamilyen módon azonosítani, nem nő meg a hibalehetőségek aránya? A kérdések jogosak, ennek járt utána az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete (továbbiakban: NIST) [16]. Arra voltak kíváncsiak, hogy a COVID előtti algoritmusok milyen hibaarányal képesek felismerni a személyeket⁸ maszkkal-és maszk nélkül. A kutatás során 1:1 arányú eredményeit dokumentálta 93 féle gyártótól származó algoritmussal.

5.1 A teszt körülményei

A teszt során csak utólag, digitálisan helyezték fel a maszkokat. Ennek több oka is van. Az egyik, hogy az idő és az erőforrások szűkössége miatt nem gyűjtöttek fényképeket maszkot viselő alanyokról. Másodszor, mivel sok kamera expozícióvezérléssel működik, ezáltal lehetséges, hogy a sötét maszk kevesebb fényt ver vissza, és a kamera növeli az érzékelő erősítését a szemközti régió túlexponálását okozva. Hasonlóképpen egy fehér maszk alulexponáláshoz vezethet. Harmadszor, előfordulhat, hogy egyes fényképezőgépek, amelyek arcérzékelőt tartalmaznak, nem tudnak megfelelően fókuszálni. Mivel a valós maszkok különböznek egymástól, a csapat kilenc digitális maszkváltozatot dolgozott ki, amelyek alakban, színben és orrfedésben is különböztek. Alak tekintetében volt széles és kerek. A digitális maszkok fekete vagy világoskék színűek voltak (2. táblázat), ami megközelítőleg ugyanolyan színű, mint a kék sebészeti maszk. Orrfedésben alacsony, közepes és magas orrfedésű változatok voltak.

⁸ Ezeket az algoritmusokat két nagy, az Egyesült Államok kormányzatában gyűjtött fényképadatkészlettel használták. Egyik a bevándorlást kérelmezők adatbázisa, másik a határátkelő személyeknek az adatbázisa. Ez összesen 6,2 millió fényképet jelentett 1 millió személyről.

2. táblázat: Példák a tanulmányban használt digitálisan létrehozott arcmaszkokra.



Forrás: NIST

5.2 Eredmények

Mielőtt elmélyednénk a maszkhasználat okozta hibaarányokban, tisztáznunk kell, hogyan osztályozzuk a hibalehetőségeket. A téves arcfelismeréseket két fő csoportra osztjuk: hamis pozitív és hamis negatív. Hamis pozitív esetén a szoftver úgy érzékelte, hogy két különböző személy képe ugyanazt a személyt ábrázolja. Ezt úgy kell elképzelni, például a Liszt Ferenc Nemzetközi repülőtéren található automatizált határellenőrzés (ABC kapu) során, az úti okmányon lévő arckép és az élőképen rögzített személy arcképe a valóságban eltér, de a szoftver egyezést mutat. Hamis negatív során a rendszer úgy észleli, hogy a két képen lévő arcok két különböző személyhez tartoznak. Például egy telefon esetében nem engedélyezi a feloldást, miközben a személy jogosult lenne rá. Azért szükséges különbséget tennünk a téves jelzések között, mert mindegyik más súlyú következményekkel járhat.

A teszt során a maszkolás nélküli képek használatával a legpontosabb algoritmusok az esetek 0,3%-ában nem tudtak hitelesíteni egy személyt. Emellett 100 000 csalóból legfeljebb 1-et fogadott el hamisan (azaz FNMR= 0:003, FMR= 0:00001).⁹ Viszont a maszkolt képek esetében még ezeknek a legjobb algoritmusoknak a meghibásodási arányát is körülbelül 5%-ra növelték (FNMR = 0,05), míg néhány algoritmus kirívó módon az esetek 20-50%-ában is hibázott.

⁹ FNMR=False-non match rate (Hamis negatív)
FMR= False match rate (Hamis pozitív)

Minden algoritmus növelte a hamis pozitív egyezés arányát a mérések során, amelyek maszkkal együtt lettek tesztelve.

Viszont a maszkok nem hatnak kedvezőtlenül a hamis pozitív egyezésre, így ilyen szempontból nincsenek biztonsági kockázatai.

Az eredmények tekintetében még a maszkok színe közt is volt különbség. A legtöbb algoritmus nagyobb hibával rendelkezik a fekete és fehér maszkokban, mint a világoskék maszkokban. Valószínűleg azért, mert a világos maszkokban az emberek bőre elsötétedik a maszk által visszavert fény miatt, a sötét maszkok pedig elnyelik a fényt és a bőr színe lesz túl világos. A legjobb eredményt a széles, alacsony magasságú világoskék maszk érte el.

Az is előfordul, hogy maszk hatására a szoftver még az arcot sem érzékeli. Ilyenkor az algoritmusok nem észlelik azt az arcot, vagy azt állapítják meg, hogy az arc nem rendelkezik elegendő információval.

6. Már létező, külföldi arcfelismerő rendszerek

A világ számos országában alkalmaznak arcfelismerő rendszereket, legyen szó rendészeti felhasználásról vagy magánbiztonsági területen való alkalmazásról. Viszont vannak ezen a téren kiemelkedő országok, ahol komolyan gondolják a személyek nyomon követését és mindennapi életük megfigyelését.

6.1 Kína

A nagy népességnövekedéssel járó problémákat valamilyen módon ki kell küszöbölni és megoldásokat találni a technológia segítségével a fenntartható, élhető nagyvárosok érdekében. Ez vezetett el minket a smart city, vagyis az okos városok ötletéhez. A világ fejlett államai elkezdtek fejleszteni nagyvárosaik okosítását. Ez az újítás magával vonzotta a mesterséges intelligencián alapuló rendszerek hálózatba kötését.

A smart city technológiák esetében az előnyök mellett kockázatok is jelentkeznek. Ilyen például a településeken üzemelő okos kamerák általi nagy mennyiségű információgyűjtés (Big data) a lakosság életmódjáról, mobilitásáról, viselkedési mintáiról, amit az arcfelismerő és mesterséges intelligencia- technológiák tesznek lehetővé.

Mint köztudott, Kínában nagy szerepet játszik az emberek mindennapjaiban az állandó megfigyelés. A világon körülbelül 1 milliárd zártláncú videómegfigyelő rendszer (továbbiakban: CCTV) működik, ennek 54%-a mind Kínában található. Ami azt jelenti, hogy 2021-ben ez 540 millió kamerának felel meg [17]. A kínai megfigyelőrendszer a Skynet nevet kapta, ennek jelentős része képes arcot felismerni.

A mesterséges intelligencia, arcfelismerés és a Big data technológiáknak köszönhetően Kína kidolgozta az úgynevezett társadalmi kreditrendszert, amely a kínai állampolgárok magatartásának, viselkedésének és adatainak gyűjtése révén a rendszer jutalmazza, illetve bünteti az embereket [18].

Az arcfelismerés a kínai oktatás intézményein belül is jelen van. A pekingi Normal Egyetem kampuszán már évek óta arcfelismeréssel és kártya használatával lehet bejutni, amit nemcsak a diákok azonosítására használnak, de a viselkedési szokásaikat is elemzik. Kína több középiskolájában pedig a teremben tanuló diákokat figyelik meg arcfelismerő kamerákkal, melyek képesek az emberi arckifejezéseket értékelni, boldog, dühös, féltő, zavart vagy ideges kategóriába sorolva őket. A rendszer rögzíti a tanulók olyan tevékenységeit is, mint például az írás, az olvasás, a kézfelemelés és az álmoság [19]. Így, ha egy diák tekintete sokáig

elkalandozik, csukva van a szeme vagy ásítózik, azt a rendszer észleli. A tapasztalati visszajelzések alapján a tanulmányi teljesítmény javult, persze, hiszen ki merne nem az előadásra figyelni, ha közben tudja, hogy több kamera folyamatosan figyeli és értékeli. A rendszer viszont nem rögzíti a képeket és nem tölt fel adatokat a felhőbe, csak a belső rendszer számára készít statisztikákat. 2020-ban a COVID-19 arra ösztönözte a kínai iskolákat, kollégiumokat, hogy növeljék az arcfelismerés használatát hőmérsékletmérő funkcióval kombinálva [20]. Ez a be- és kiléptetéshez megfelelő megoldást nyújt, ugyanis kártyás beléptető használata nem feltétlen tudja kiküszöbölni azt a helyzetet, hogy kívülálló ne lépjenek be az intézménybe, vagy esetleg a lázas betegek. Szerintem másik hasznos funkciója, hogy a szülők megkaphatják gyermekük iskolába lépésének vagy távozásának időpontját, valamint a helyszínen készült fényképeket.

A gyereket már kiskoruktól fogva szigorral nevelik, mi sem bizonyítja ezt jobban, hogy már jogszabályban határozzák meg mennyit játszhatnak. A játékfüggőség nagy problémát okoz az országban és ez a tanulmányi eredményeken is meglátszik. Lépniük kellett és egy 2019-es törvény értelmében hétköznaponként 90 percet, hétvégeente 180 percet lehet játszani. Kezdetben ezt a fiókhoz kötött életkor alapján határozták meg, viszont túl sok visszaélés történt. Ezért a kormeghatározás arcfelismerő technológiával történik. Kína legbefolyásosabb technológiai vállalata a Tencent Holdings Ltd. biztosítja majd azt az arcfelismerő rendszert, mely kifejezetten a játékosok életkorát hivatott ellenőrizni [21]. Ezen az ellenőrzésen mindenki köteles bejelentkezéskor átesni. Ha a rendszer azt találja, hogy egy 18. életévét be nem töltött személy próbálkozik, úgy automatikusan érvényes lesz rá a jogszabályi időkeret.

Ezt a kínai totális megfigyelést, nyilván, úgy is fel lehet fogni, hogy akinek nincs rejtegetnivalója annak nincs mitől tartani, viszont az emberek egy része kényelmetlenül érzi magát, ha kamerák szegeződnek rá és tudja, hogy éppen megfigyelik. Éppen ezért a „Nyugat” aggodalmát fejezte ki, hogy ezek a rendszerek a nemzetbiztonságra és az emberi jogokra veszélyt jelentenek.

Viszont Kínában az arcfelismerés technológiáját nem csak megfigyelésre használják, mint ahogyan a rendőrség, vagy az állam teszi. A pénzügyi szektorban az arcfelismeréssel való fizetés nagy népszerűségnek örvend. A felhasználóknak először regisztrálniuk kell arcukat, és fel kell tölteniük a bankkártya adatait egy mobilalkalmazásba. Ezután a fizetéseket úgy hajthatják végre, hogy az üzletekben a pénztárnál elhelyezett kamerák elé helyezik az arcukat. Az arcfelismeréssel történő fizetés széles körű elterjedése Kínában 2017 körül történt, mikor az

okostelefon-gyártók egymás után bevezették az arcfelismerő funkciót.¹⁰ 2021-ben több mint 495 millió kínai ember fizetett arc-szkenneléssel, ez nagyjából az ország lakosságának egyharmada. Az idei évben várhatóan meghaladja a 760 milliót [22]. Hátránya viszont az, hogy időnként lassú, akár 10-15 másodpercig is eltarthat a folyamat, ellenben a kártyás vagy az NFC alapú fizetéssel, ami ennek a töredéke. 2022-ben egy teszt során két személynél az Alipay megerősítésként kérte a fiókhhoz tartozó telefonszám utolsó 4 számjegyének beütését, mert nem tudta egyértelműen beazonosítani [23]. Ennek oka az lehetett, hogy a rögzített arc elmosódott, így elvesztette egyik nagy előnyét, az érintésmentességet. Valamint, a felhasználók másik legnagyobb aggodalma ezzel az azonosítással kapcsolatban, az a biztonság. Attól tartanak, hogy az arcfelismerő technológia hibája jogosulatlan terhelésekhez vezet.

Véleményem szerint minden olyan új termék aggodalomra adhat okot, ami az embereknek a meglévő szokásainak megváltoztatásáról szól, főleg ha az egy olyan érzékeny terület, mint a pénzügyek. Azonban a gyors fejlődésnek és a mesterséges intelligenciának köszönhetően egyre megbízhatóbb rendszereket alkotnak és ezáltal még többen fogják használni a jövőben.

6.2 India

Kínához hasonlóan Indiában is létrehoztak egy teljes lakosságra kiterjedő biometrikus azonosítási rendszert. 2010-ben az Indiai Egyedi Azonosító Hatóság (UIDAI) elindította az Aadhaar programot, egy nemzeti azonosítási rendszert, amelynek célja, hogy India minden lakosának egyedi identitást és digitális platformot biztosítson a hitelesítéshez. Mivel India továbbra is a nagy gazdasági és népességi növekedés útján halad, ennek a nemzeti azonosító rendszernek az a célja, hogy összegyűjtse és kezelje a teljes lakosság nevét, címét és biometrikus adatait egy olyan társadalom létrehozása érdekében, amelyben minden egyes ember egyenlő hozzáférést kaphat az oktatáshoz, az egészségügyi ellátáshoz, a szociális jóléthez, a banki szolgáltatásokhoz és más köz- és pénzügyi szolgáltatásokhoz. Nagy figyelmet fordítottak az esetleges visszaélések kiküszöbölésére, például az ellen, hogy egy személy kétszer regisztrálja be magát két különböző néven. Ezt a rendszert nem csak arc, hanem ujjnyomat és írisz azonosítással is kiegészítették [24].

¹⁰ 2017-ben az Apple az akkori csúcskategóriás iPhone X okostelefonján teljes mértékben lecserélte az addig használt saját fejlesztésű ujjnyomatolvasóját (Touch ID) a 3D arcfelismerési technológiára (Face ID). Az Apple azóta sem használ a csúcskategóriás telefonjain kijelzőbe integrált ujjnyomat olvasót.

Miután egy személy regisztrál a rendszerbe, kap egy egyéni 12 jegyű azonosító számot, vagyis "Aadhaar"-t. Több mint 1,3 milliárd regisztrálással az Aadhaar program a világ egyik legnagyobb nemzeti azonosítási rendszere, naponta 1 millió regisztrálást képes befogadni. Ezt a rendszert a Japán székhelyű NEC Corporation multinacionális vállalat fejlesztette ki. Ez a vállalat többször is bebizonyította, hogy a biometrikus azonosításban világszerte vezető szerepet töltenek be. Az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete (NIST) által végzett gyártói tesztek során a NEC többször is a világ legpontosabb arcfelismerő technológiája lett az első helyen [25]. Az Aadhaar rendszerben az arcfelismerést a nyugdíjadatok hitelesítésére, digitális élettanúsítványok benyújtására is használják, a nyugdíjasoknak ehhez csak egy applikációt kell letölteniük és otthonról intézhetik az ügyeiket. 2022. januárjára közel 20 millió nyugdíjast hitelesítettek ezzel az arcfelismerő technológiával. Valamint a Covid 19 vírus második hulláma idején az oltóközpontoknál a személyek azonosítására kísérleti jelleggel arcfelismerést használtak, hogy érintésmentes legyen a folyamat. Ezt jogvédő egyesületek támadták, miszerint a kormány felhasználná valamilyen megkülönböztetésre, továbbá kizárná az oltás lehetőségéből azt a 100 millió állampolgárt, aki még nem regisztrált az Aadhaar rendszerbe [26]. Azonban van egy egyértelműen pozitív példa az indiai rendszer használatára. Újdelhiben a rendőrség próba jelleggel használt arcfelismerő rendszereket eltűnt gyermekek felkutatására. A négynapos tesztüzem során 45.000 gyermekotthonban lévő gyerek arcát szkennelték be és 2930 eltűnt gyerek személyazonosságát sikerült megállapítani. Indiában ugyanis nagy problémát okoz a gyermekkereskedelem és az olcsónak számító gyermekmunka. Pontos adatok nincsenek, de feltehetőleg 500.000 gyerek tűnik el évente Indiában [27].

2020 márciusában a rendőrség arcfelismerő technológia segítségével azonosított 1100 rendbontót Delhiben. [28]. A nyilvános helyekre kitett CCTV kamerák felvételeit arcfelismerő szoftver segítségével hasonlították össze a saját adatbázisaikkal. Az indiai rendőrség azt állítja, hogy a CCTV kamerák rendészeti felhasználása miatt jelentősen visszaesett a bűnözés, és nőtt az elítélések aránya. Bár jogvédő aktivisták szerint ez nem tudható be ennek egyértelműen.

Idén áprilisban India elnöke, Ram Nath Kovind aláírta az új büntetőeljárás törvényt, melynek értelmében még azok is kötelesek lesznek megadni a biometriai paramétereit, (mint például: arc, tenyérnyomat vagy kézírás) akiket gyanúsítottként kezelnek és még semmiféle ítélet nem született. Ez a törvény feljogosítja arra az államot, hogy hozzáférhessen minden biometrikus adathoz vagy információhoz bírói engedély nélkül.

Kína után a második helyen, Indiában a van a legtöbb CCTV kamera a világon. Lakosságárányosan, 10 ezer főre vetítve pedig a negyedik helyen áll. Városok tekintetében, a

terület méretéhez viszonyítva Delhiben van a legtöbb kamera, ami négyzetkilométerenként 705 darabot jelent. Így, ebben a kategóriában megelőzi Shanghait és Londont is [29].

Hyderabadban, India negyedik legnépesebb városában körülbelül 450 ezer kamera van kihelyezve, így a világ 16. legmegfigyeltőbb városa. A Covid 19 járvány tombolása közben a Hyderabad rendőrség elkezdte CCTV kameráit arra használni, hogy mesterséges intelligencia segítségével nyomon kövessék azokat az embereket, akik nem viseltek arcmaszkot nyilvános helyen, majd pénzbírságot szabnak ki rájuk. Néhány hónappal később, több indiai város is bejelentette, hogy frissítik okoskameráikat, hogy észre vegyék a szájmazsk nélküli polgárokat, és azonnal bírságot szabjanak ki rájuk. Ezek az intelligens kamerák a város megfigyelő és irányító központjához kapcsolódnak [30].

Szerintem, India még messze van a Kínában zajló megfigyelések mértékétől, azonban az a tendencia, ami az utóbbi években zajlik, mind a jogalkotásban mind az indiai technológiai fejlettségben, okot ad arra, hogy itt is kialakuljon egy hasonló, állandó megfigyelés alatt tartott társadalom.

6.3 Egyesült Királyság

Példaként érdemes felhozni még az Egyesült Királyságot is, azon belül Londont. London a kilencedik város a világban, ahol a legtöbb az egy főre jutó CCTV kamerák száma. [31] Számokban kifejezve ez azt jelenti, hogy minden 10. lakosra jut egy kamera. A kamerák számának növekvő tendenciája visszavezethető a 2005. júliusi londoni metrómerényletekre, amelyek során 52 ember meghalt és további 700-an megsérültek, a robbantókat a londoni Metropolitan Rendőrség CCTV felvételeinek elemzése alapján azonosították [32]. Hasonlóképpen, a Boston maratoni robbantókat, akik három embert megöltek és több száz embert megsebesítettek, kormányzati és magánkamerák által rögzített CCTV-képek segítségével találták meg és fogták el. A robbantók a videón a viselkedésük miatt tűntek ki. Amíg a tömeg menekült a helyszínről, Ők lézengtek, vagy lazán elsétáltak. Ez is bizonyítja, hogy Anglia nemzetközi szinten is kiemelkedik a megfigyelés terén, fejlett nyugati, európai államként is.

Igény keletkezett a gyanús személyek, bűnelkövetők azonosítására bűnmegelőzés céljából. Ennek érdekében 2016 augusztusában a londoni rendőrség teszt jelleggel bevetett élő, videoalapú arcfelismerő rendszereket.¹¹ Az élő arcfelismerő technológia (LFR) lehetővé teszi

¹¹ 2016 augusztus 28-29. között használták először a Notting Hill-i fesztiválon.

a videóképek valós idejű biometrikus feldolgozását. Ezeket a feldolgozott adatokat továbbítja egy adatbázisba, ahol összevetik a már meglévő sablonokkal és egyezés esetén riasztást generál. Ez egy előre meghatározott számú adatbázis, amely a Bevándorlási és Menekültügyi Hivatal biometrikus rendszeradatait és a Rendőrségi Nemzeti Adatbázis adatait tartalmazza. Baroness Williams államminiszter úgy fogalmazott: „Ez az adatbázis egy testre szabott „figyelőlista”, amely tartalmazhat bizonyos rendezvények részvételtől eltiltott személyeket, ismert bűnözőket, illetve körözött személyeket” [33]. Ha a szoftver egyezést talál, akkor az a riasztás befut a Metropolitan Rendőrség vezérlőszobájába, vagy magába a furgonba (6. ábra), ahol a kezelők figyelemmel követik az eseményeket és azonnal megjelenik az élőkép. Ez azért szükséges, hogy a párosított képet a bent lévő személyek vizuálisan is összevessék a beavatkozás megkezdése előtt. A teszttelepítések során a kamerarendszereket a hagyományos utcai térfigyelő kamerákhoz hasonlóan fix helyeken, vagy egy mobil arcfelismerő furgonon helyezték el. A megfigyelt helyszín teljes lefedettsége érdekében jellemzően két kamerát telepítettek [34]. A Metropolitan Rendőrség 2016 és 2019 között összesen 10 tesztbevetést hajtott végre, kipróbálva az élő arcfelismerő technológiát a rendészeti műveletek során. Ezen idő alatt a tesztelés eredményei segítenek tájékoztatni a rendőrséget arról, hogy miként használják, fejlesszék az arcfelismerő technológiát a londoniak biztonsága érdekében. A teszttelepítések előrehaladtával számos fokozatos fejlesztés történt.



6. ábra: A megfigyeléshez használt furgon és a kamerái által rögzített kép.

Forrás: Western Mail

Jelenleg is alkalmaznak London közterületein élő arcfelismerést. 2022. január 28-án a rendőrség LFR furgonokat helyezett ki London egyik forgalmas területén, az Oxford Circus környékén, 9756 személyt tartalmazó figyelőlistával. A korábbi tapasztalatokhoz képest a hibaarány 0,08%-ról lement 0,008%-ra. A szoftver 12 120 arcot vizsgált meg, abból 11 személyre érkezett riasztás és 1 volt közülük a hamis (7. ábra). A 10 ember közül 4-et letartóztattak [35].

Deployment	Date (DD/MM/YY)	Purpose Reference	Watchlist Size	Total Alerts	False Alert / Confirmed False Alerts	False Alert / Confirmed False Alert Engagements	True Alerts ¹	True Alert Engagements	Arrests / Disposals	Faces seen (Estimate)	False Alert Rate
Stratford	11/02/20	1, 2	5816	0	0	0	0	0	0	4600	0.00%
Oxford Circus (technical fault stopped deployment)	21/02/20	1, 2	7316	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Oxford Circus	27/02/20	1, 2	7292	8	7	5	1	1	1	8600	0.08%
Oxford Circus	28/01/22	1, 2	9756	11	1	1	10	7	4	12120	0.008%
Leicester Square	10/03/22	1, 2	6793	0	0	0	0	0	0	10740	0.00%
Oxford Circus	07/07/22	1, 2, 3	6699	4	0	0	4	3	3	34286	0.00%
Oxford Circus	14/07/22	1, 2, 3	6713	3	1	1	2	2	1	34360	0.003%
Oxford Circus	16/07/22	1, 2, 3	6747	1	1	1	0	0	0	36420	0.003%
Piccadilly Circus	28/07/22	1, 2, 3	6858	1	0	0	1	0	0	16440	0.00%

7. ábra: A rendőrség hivatalos jelentése az arcfelismerő rendszerek telepítéséről.

Forrás: Metropolitan Police

7. Hazai „arcfelismerő rendszerek”

7.1 Siófok

Siófok polgármestere Lengyel Róbert 2021-ben jelentette be Facebook oldalán, hogy a Petőfi sétányon arcfelismerésre is alkalmas kamerát fognak telepíteni. Siófok Önkormányzatának 2021.06.10-i közleményében is megjelent, hogy a Petőfi sétány területén 39 új, mesterséges intelligenciával ellátott kamera került telepítésre. Ezek a kamerák arcdetektálásra képesek, ami azt jelenti, hogy egy adott emberre jellemző vonásokat rögzítve továbbítja az adatokat a rendszerben lévő egyéb kamerák részére, és így a feltételezett elkövető személyt nyomon lehet követni. A képeket a rendőrségen kialakított operatív szobában csak a rendőrség és a városőrség munkatársai láthatják és a felvételeket 30 nap múlva törlik a hatályos jogszabályoknak megfelelően [36]. A város honlapján elérhető adatvédelmi tájékoztató szerint a kamerarendszer zárt, egyéb adatbázissal nincs összekötve, a felvételeken szereplők személyazonossága nem megállapítható.

A Siófokon tervezett, Dahua Technology által gyártott rendszer az elérhető információk alapján csak arcdetektálást végezne, azaz a tömegben az operátor által "kiszúrt" személy automatizált nyomon követését tenné lehetővé, így az ember által végzett megfigyelést támogatná valós időben.

A Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: NAIH) a sajtóhírekből arról értesült, hogy Siófok Város Önkormányzata arcfelismerésre képes mesterséges intelligenciával bővített, 39 kamerából álló kamerarendszert kíván kiépíteni a Petőfi sétányon a közterület megfigyelése érdekében. Mivel az arcfelismerésre képes rendszerek működtetése számos adatvédelmi aggályt vet fel, a Hatóság az Infotv. 51/A § (1) bekezdése alapján NAIH-5481/2021. számon vizsgálatot indított. A NAIH a Siófoki Önkormányzati Hivatal, a Siófoki Rendőrkapitányság, és a Techno-Tel Távközlési és Informatikai, Kivitelező és Szolgáltató Kft. vonatkozásában Siófok közigazgatási területén arcfelismerésre képes kamerákat is magában foglaló közterületi rendszer működtetése tárgyában hivatalból indított adatvédelmi hatósági eljárást.

Megállapították, hogy a Siófoki Önkormányzat és a Siófoki Rendőrkapitányság megsértette az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban Infotv) 25/B § (1) bekezdés 25/F § (1) bekezdés d pontját, a 25/F § (4) bekezdését és a 25/I § (3) bekezdés c, és e pontját. A Techno-Tel Távközlési és

Informatikai, Kivitelező és Szolgáltató Kft megsértette az Infotv 25/D § (3) bekezdés a pontját és e jogsértés miatt 500.000 forint adatvédelmi bírság megfizetésére kötelezte.

7.2 Szitakötő projekt

Felmerült, hogy a Belügyminisztérium kiépít egy figyelőrendszert, melyet „Szitakötő projekt”-nek neveztek. A miniszterelnök és a belügyminiszter támogatásával hardvereket és szoftvereket szereznének be, amelynek célja, hogy a hatóságok percek alatt kideríthetik egy személyről, autóról, hogy benne van-e az országos rendszer egyik kamerájának látóterében, vagy, hogy hol járt korábban. Csak a NAIH bírálatából tudható, mekkora költséggel számolnak: a projektben 35 ezer kamera képeit gyűjtenék folyamatosan a Kormányzati Adatközpontban, és a 25 ezer terabájtnyi megfigyelési adat folyamatos kezelése 50 milliárd forint elköltését jelentené [37]. A lap belügyi forrásokra hivatkozva azt írta, csak a megfelelő minőségű kamerák beszerzési költsége megközelítheti a 40 milliárd forintot, és ehhez jön még a Magyarországon eddig nem látott kapacitású adattároló rendszer és a speciális, nagyon drága szoftverek.

Kormánypárti sajtók szerint a projekt ötlete azért született meg, mert a meglévő térfigyelő kamerák nem tudták lekövetni a Teréz körúti robbantás elkövetőjét. Bár az elmúlt évtizedekben jelentős anyagi forrást használtak fel az önkormányzatoknál a térfigyelő hálózatok fejlesztésére, a kamerák nagy része elavult és sokszor értékelhetetlen képeket készítenek.

Az új rendszer a korábban elterjedt típusoknál sokkal nagyobb felbontású, legalább 16 megapixeles kamerákat használ, mert csak ezzel a képminőséggel működhetnek nagy biztonsággal a rendszám- és az arcfelismerő programok. A rendszerbe a terv szerint a közútfenntartók, az önkormányzatok, a közlekedési vállalatok és a pénzügyintézetek utakon, állomásokon, köztereken, intézményekben kihelyezett kamerái lennének bekötve.

A projektben először összekapcsolnák a működőképes budapesti rendszereket. A BKK és a főváros rendészeti igazgatósága (FÖRI) kamerahálózata és irányító központja olyan, hogy nagyobb ráfordítás nélkül megfelel a Belügyminisztérium technikai követelményeinek. Ezután előbb a fővárost, majd a megyei jogú városokat, végül az ország többi települését szerelnék fel kamerákkal.

Jelenleg nincs hír arról, hogy hol tart a projekt, feltehetőleg szünetel. Valószínűleg az időközben berobbanó Covid járvány következtében.

7.3 *További magyar vonatkozás*

Karunk szakmai hetének során lehetőségünk nyílt betekinteni az újonnan épült Szépművészeti Múzeumba. Az itt töltött látogatásunk alkalmával előadást tartott nekünk a terület biztonsági vezetője és a biztonságtechnikus is. Utóbbi mesélt nekünk arról, hogy az objektumba a beléptetést már biometrikus azonosítóval is ellátták, ezek az ujjnyomat és a tenyérlenyomat. Kamerarendszer tekintetében olyan analitikát alkalmaznak, amely jelzést ad az elhagyott csomagok, illetve a céltalan, gyanús mozgásra. Kérdeztem az előadás során, hogy alkalmaznak-e arcfelismerő rendszereket. Azt a választ kaptam, hogy jelenleg nem, de a jövőben még tervben lehet. A kamerarendszerük alkalmas ennek alkalmazására, csak még nincs élesítve.

Bankbiztonsági esetre is van példa. Magyarországon az egyik bank, nevezetesen a CIB Bank 2022 nyaratól hirdette meg azt az akcióját, ahol egy szelfi készítéssel lehet számlát nyitni. A szelfi képét összehasonlítják az igazolvány képével, és máris alkalmas arra, hogy személyes banki jelenlét nélkül számlát nyithassunk [38]. Ez a dolog viszont nem új hazánkban, a Revolut már előző évben is alkalmazta ezt a megoldást.

8. Interjú

A dolgozatom elősegítése céljából felkerestem egy szakembert azzal kapcsolatban, hogy annak sikerességéhez hozzájáruljon egy interjú keretein belül.

Juhász Tamás a Műszaki Egyetem elvégzése után már közel 14 éve dolgozik a Criterion ZRT-nél. Az alapoktól, terepi kivitelezéstől kezdte, úgy, mint a kábelhúzás, terepmunka, kamerák feltelepítése. Később műszaki rajzoló, tervező, és jelenleg projektvezetőként dolgozik. Ezáltal a teljes folyamatot részletesen megismerhette.

Munkája során az elmúlt négy évben kezdett el foglalkozni az arcfelismerő és biometrikus azonosítási rendszerekkel. Ez a tervezéstől a megvalósulásig mindent magában foglal.

Elmondása szerint jelenleg a biztonságtechnikában az arcfelismerést leginkább beléptetésre és hozzáférés korlátozásra használják. Ezzel automatizálni szeretnék a beléptetést, amivel lehetséges kiváltani a humán erőforrást. Egy egyszeri beruházás sokkal könnyebben megy, mint a hosszú távú humán erőforrás alkalmazása. Viszont, az emberi erőforrást nem lehet mindig automatizációval kiváltani, szükség lesz a jövőben is az emberek bevonására a folyamatokba.

Munkája során az egyik nehézség amibe ütközik, az ügyfelek tájékozottsága. Sokan azt hiszik, hogy bűnözők kiszűrésére is alkalmas lesz az ő rendszerük. Valójában, csak egy szűkebb adatbázisból dolgozik a polgári felhasználásra szánt rendszer.

A másik nehézség, azok a jogszabályi előírások. A GDPR miatt nagy fenntartással kezelik ezeket a rendszereket. Sokan megijednek a GDPR-tól és annak következményeitől, mert nincsenek teljesen tisztában annak előírásaival. A jogszabály előírásai valóban szigorú követelményeket fogalmaznak, de az évek során enyhítettek a szabályozáson. A GDPR azt írja elő, hogyan lehet megoldani, ha belső szabályozást hozol létre. A vállalatoknak, cégeknek meg kell tudni indokolni, hogy miért használja az arcfelismerő rendszert, és egy belső szabályzatot kell létrehozni, amelyben szerepelnie kell, hogy mi célból jött létre, ki az adatkezelő, és ki a felhasználó. A cégek általában megbíznak egy adatvédelmi tisztviselőt (DPO), aki segít megírni a belső szabályzatot, tanácsot ad a személyes adatok feldolgozására. Az adatvédelem valóban nagyon érzékeny téma. Ezért is megbízható személyekkel, cégekkel érdemes együtt dolgozni. A kamerarendszerek során is ez érvényes. Tamás a munkája során is megbízható cégek termékeivel dolgozik, úgy mint a Svéd gyártású Axis Communications, aki magas színvonalú termékeket gyárt. Amit használ videómenedzsment szoftver a Dán székhelyű Milestone Systems-től származik, mindezek mellett az arcfelismeréshez egy analitikai szoftver is

szükséges, ehhez a Herta Security szoftverét használja. Ezek a vállalatok mind piacvezető pozíciót töltenek be.

Az IP kamera gyártás terén nagy a piaci verseny. A kínai gyártók nagy szeletet vesznek ki a piacból. Elmondása szerint, egyre több kamera jelenik meg a piacon, melyeknek az áruk olcsóbb, viszont sokszor ez a kamerák képminőségére, illetve a fényviszonyok gyors változására (fénykompenzáció) való reagálására negatívan hathat. Nem beszélve arról, hogy a jó IP kamerák és arcfelismerő rendszereknek az alapja az a megfelelő IT hálózat. Véleményünk egyezett abban, hogy általában jobban megéri az egyszeri, drágább, de megbízható rendszerek kiépítése, mert mögöttük van teljesítmény és hatékonyság. Illetve ezek mögött van valamilyen ügyfélszolgálat, elérhetőség, ellenben az olcsóbban kifejlesztett kamerák, szoftverek mellé sokszor csak egy PDF-fájlt mellékelnek. Viszont tudni kell, hogy ezeknek a rendszereknek a magas árazása nem feltétlen egyenesen arányos a minőséggel. Hiszen ha valami sok kézen megy keresztül az szintén drága lehet, mert mindenki ráteszi a hasznát.

Az interjú során szó esett arról, hogy elterjedhet-e Magyarországon az arcfelismeréssel való fizetés. Ezt a kérdést lehet vizsgálni anyagi, technológiai és az emberek megítélésének szempontja alapján. A technológia már létezik rá, ennek határt igazából az anyagi és a piaci igény szab. Az elkövetkezendő 3-5 éven belül nagyon kevés esély van rá és sok változásra van szükség. Mi, Magyarországon sokkal kevésbé vagyunk nyitottak az ilyen újdonságokra, mint például a Nyugat-Európában vagy a Kínában élő emberek. Ezt a tanulmányom is alátámasztja. Szó esett köztünk arról, hogy az arcfelismerő rendszerek használatát betilthatják-e az EU-n belül. Tamás úgy látja, hogy az elkövetkezendő néhány évben nem valószínű, hogy betiltják. Ezeknek a rendszereknek a kutatása és fejlesztése jelentős anyagi ráfordítást igényelt. Az elképzelhető, hogy az arcfelismerő rendszerek nem fognak akkora teret hódítani a lakosság körében, mint esetleg a biztonságtechnika, a hadiipar és a rendészet területén.

Beszélgetésünk során a vírushelyzet okozta változásokról is meg kellett kérdezzem. A COVID járvány, mint ahogy sok más területet, ezt sem kerülhette el. Ahogyan a dolgozatom témája is említi a maszkhordás új kihívások elé állította a gyártókat. Tamás elmondása szerint a gyártók hamar lereagálták az új piaci igényeket és nagyon gyorsan átálltak ennek megfelelően. Igaz a maszkviselés következtében lecsökkent csak a szemre, szemek közti távolságra, szemgödrökre és a felette lévő részre az érzékelési terület, de így is több millió ponton hajtják végre az azonosítást és nagyon megbízható eredményeket érnek el. Igény keletkezett még az egymástól való távolság (social distancing) ellenőrzésére is, a kamerarendszerek segítségével. Erre az igényre is azonnal tudtak reagálni, ezáltal könnyedén be tudták tartatni a távolságtartást.

Kérdeztem Tamást arról, hogy egy esetleges hibás azonosítás okozott-e valakinek anyagi kárt, megkülönböztetést. Előbbinél a hamis pozitív és hamis negatív közti különbségre reflektáltam. Ilyen konkrét esetről még nincs tudomása. Az analitikát a fejlesztők úgy írják meg, hogy inkább több embert engedjen be, mint egy jogosult személyt ne. Az ügyfelek számára is kisebb hiba és jobban elfogadják. Mivel 100%-os biztonság nem létezik, ezért szükség van kompromisszumokra. Persze igyekeznek a gyártók 99,9%-os aránnyal csak a jogosult személyeket beengedni. Az, hogy anyagi kár ért volna valakit az arcfelismerő rendszer hibája miatt, olyanról még nem hallott. Valószínűleg azért, mert Magyarországon nincsen olyan anyagi érdek, mint például az arcfelismeréssel való fizetés. Ezáltal nem látnak napvilágot olyan hírek, hogy megkárosított volna ez a rendszer valakit. Persze, mindig vannak kivételek. Megkülönböztetésre viszont van példa. Erre az algoritmus túlzott elfogultsága adhat okot, ezekről több tanulmány is született, mint ahogy korábban említettem a dolgozatomban. Ezt a kijelentést Tamás is megerősítette, miszerint az Európában élőknek többnyire kontrasztosabb a bőrszínük, a színesbőrűeknek viszont nem, és ezáltal kevésbé felismerhetőek a szoftvernek. Kezdetben az elfogultság az ázsiaiakat is érintette a túlzott elfogultság, mert nehezen állapította meg az arckarakterek eltérését, ám mára ez eltűnt.

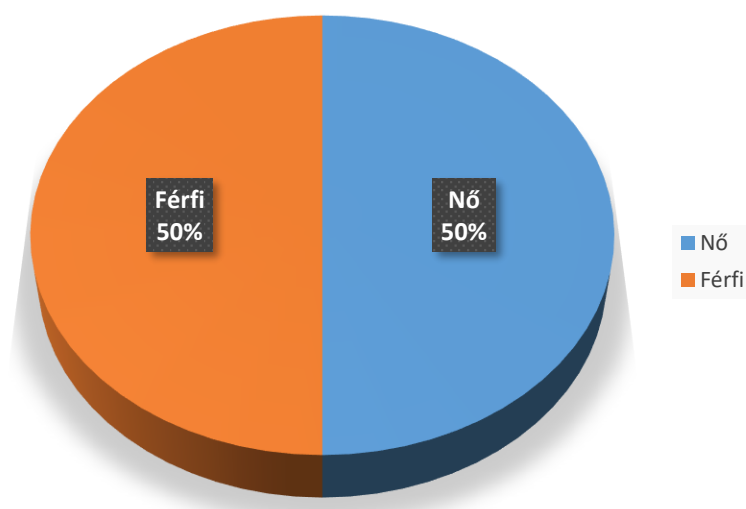
Az interjú vége felé megkérdeztem arról, hogy az arcfelismerő rendszereknek a rendészeti felhasználásban valóban van-e preventív jellegű bűnmegelőzési hatása, vagy inkább a bűncselekményben résztvevők utólagos azonosítására szolgál. Véleményünk egyezik abban, hogy a kamerák jelenlétének mindenképpen van preventív bűnmegelőző hatása, hiszen ezzel a célzattal is helyezik ki, gondoljunk például csak az álkamerákra.

Nyilván, az állami szektorban, reptereken, határátkelő helyeken az arcfelismerő rendszereket elsősorban bűnmegelőzési céllal használhatják, de már ennek is van preventív jellegű hatása. A felhasználási területtől is függ, de általában az utólagos analitikát részesítik előnyben, viszont ugyanúgy jelen lehet a real time alapú is. Az azonosítás és a prevenció is egyformán fontos, egyik a másikból következik.

9. Kutatásom

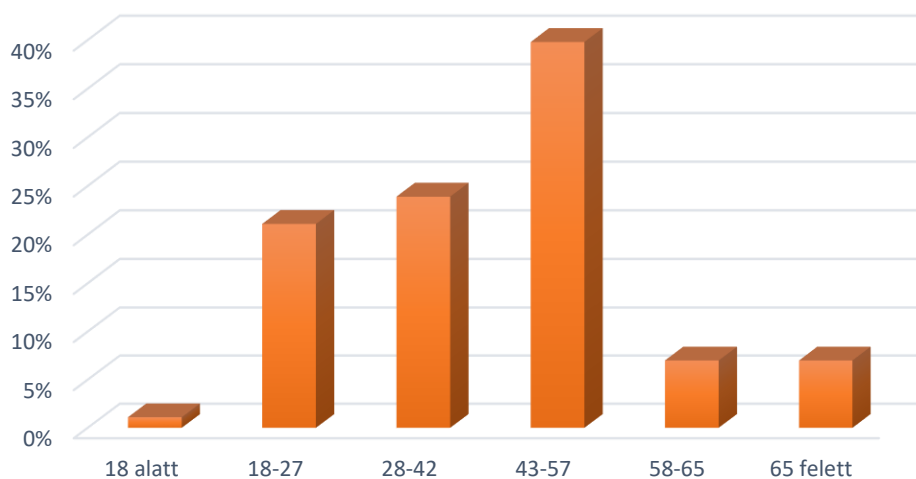
Vajon, a magyar társadalom is akar a megfigyelt társadalmak közé tartozni? Kutatásom célja, hogy felmérjem a lakosság véleményét a társadalmi megfigyelésről és magáról az arcfelismerő rendszerek használatáról. egy kérdőív segítségével. Ehhez a Google Forms űrlapkitöltő weblapját használtam. Kérdőívemet összesen 284-en töltötték ki (n=284), meglepő módon pont 50-50% volt a férfiak és a nők megoszlása (**Hiba! A hivatkozási forrás nem található.**). Az életkorcsoportokat a generációk szerint állapítottam meg. A legtöbb kitöltés a 43-57 évig terjedő korcsoportban volt (n=113), a legkevesebb a 18 alattiak körében volt (n=3).

1. diagram: Nemek megoszlása



Forrás: saját szerkesztés

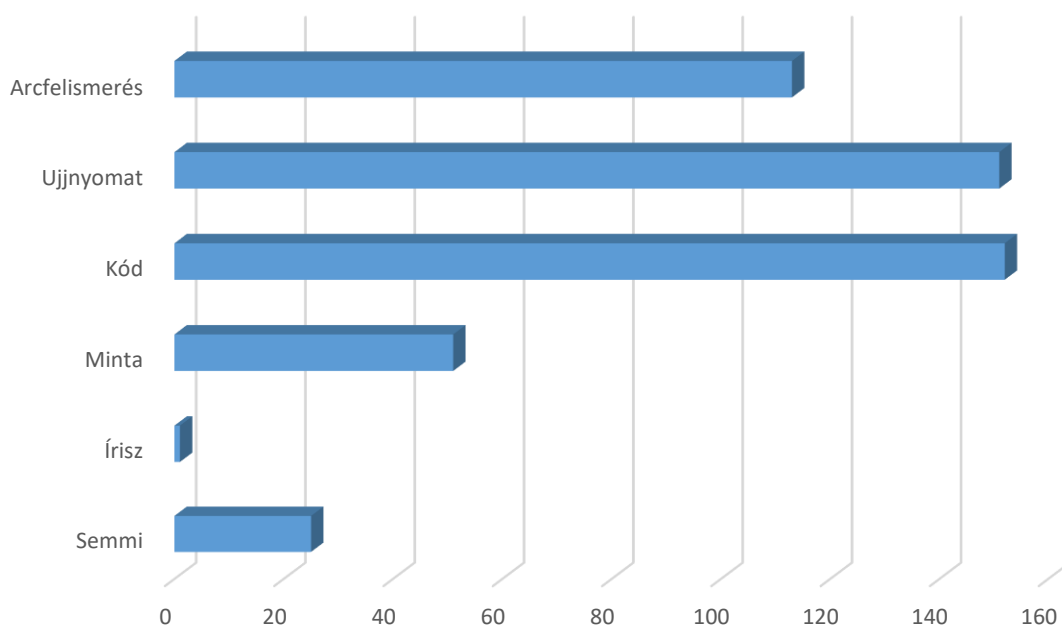
2. diagram: Életkorcsoport megoszlása



Forrás: saját szerkesztés

Eredmények:

3. diagram: Okostelefon feloldás módszerek megoszlása



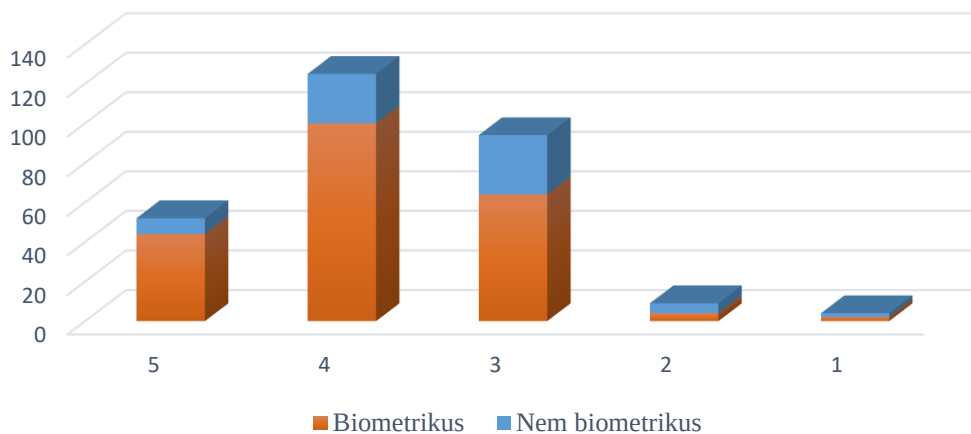
Forrás: saját készítés

Okostelefonjaink meghatározó szerepet töltenek be mindennapjaink során. Éppen ezért, sok fontos dolgot tárolunk eszközeinken és nem szeretnénk, hogy illetéktelen személyek véletlenül is hozzáférhessenek. Éppen ezért, kíváncsi voltam arra, hogy a kérdőívet kitöltők közül hányan bízzák rá az arcfelismerő technológiára az adataiknak a védelmét. A legtöbben kódot használnak telefonjuk feloldásához ($n=152$), majd ezt követi, az ujjnyomat ($n=151$). A 284 válaszból összesen 113 ember használ arcfelismerő technológiát a telefonján. Érdekességgépp megjegyezném, meglepő módon 25 ember nem használ semmiféle azonosítást a telefonján, pedig a mai világban szerintem nagyon fontos adataink védelme. A kérdőív következő kérdésében megvizsgáltam, hogy elsődleges vagy másodlagos funkciónak használják-e az arcaazonosítást.

Akik elsődlegesként használják az arcfelismerő funkciót ($n=56$), azoknak a száma több, mint akik csak másodlagos jelleggel, kiegészítésként használják ezt a funkciót ($n=53$). Közülük a legtöbben az ujjnyomatolvasás kiegészítéseként használják, mikor a szenzor éppen nem olvassa be az ujjnyomatukat.

A kérdőív megmutatja, hogy a biometrikus azonosítások közül az ujjnyomattal való azonosítás a legelterjedtebb a telefonok körében. Viszont, az arcfelismeréssel ki tudják egészíteni egymást, mert közülük 35% párhuzamosan használja az arcaazonosítást is.

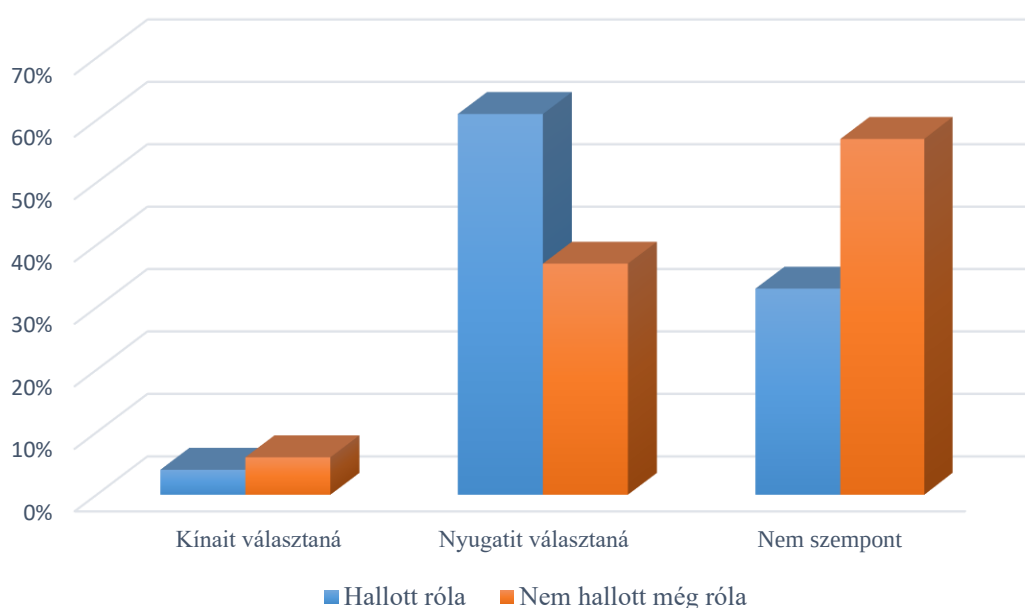
4. diagram: Összefüggés a biometrikus azonosítás és a biztonságtudatosság között



Forrás: saját szerkesztés

Arra a kérdésre, hogy vajon van-e összefüggés a mobiltelefon feloldásához használt, biometrikus azonosítás alkalmazása és a biztonságtudatosság között, a válasz az, hogy igen. Ahogy szemügyre vesszük a diagrammot, látjuk, hogy akik a legmagasabb, ötös biztonságtudatúnak vallották magukat, arányában közöttük van a legtöbb olyan személy, akik használnak valamilyen biometrikus azonosítást. Ez az arány folyamatosan csökken a biztonságtudatosság csökkenésével.

5. diagram: A kínai megfigyelési módszerekről tudomással rendelkező személyek és az arcfelismerő szoftverek származási országa közötti összefüggés



Forrás: saját készítés

„Akik hallottak már a kínai megfigyelési rendszerről, azok közül többen választanák a nyugati fejlesztésű arcfelismerő szoftvert, mint akik még nem.”

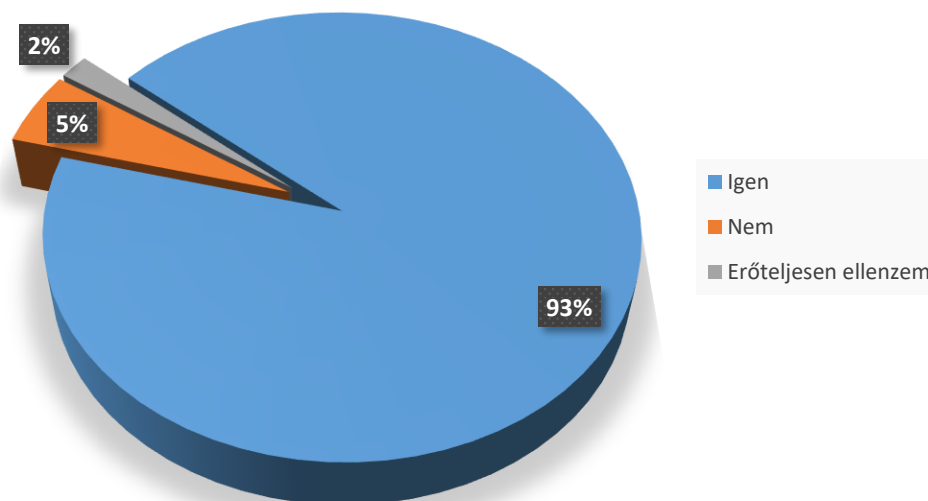
Először is, megvizsgáltam, ha az embereknek választaniuk kellene a nyugati, illetve a kínai fejlesztésű szoftver között, akkor az emberek 53,9%-a nyugatit választana, 40,8%-a szerint nem szempont, és csak 15% választaná a kínait.

A kitöltők közül összesen 70,1% hallott a Kínában zajló megfigyelésről (n=199), a maradék 29,9% (n=85) pedig nem. Ezeket az adatokat összevetettem egymással.

Jól látható (5. diagram), hogy ez hipotézis igaznak bizonyult. Ráadásul megfigyelhető, hogy akik még nem hallottak róla, azok közt nőtt az olyan személyek száma, akiknél ez már nem szempont, illetve kevesebben választották a nyugatit.

Azért voltam erre a feltevésre kíváncsi, hogy vajon befolyásolja-e az emberek megítélését, az, ha az arcfelismerő szoftver egy olyan országból származik, ahol ezt a társadalom totális megfigyelésére használják. A válasz az, hogy igen. Azokban az emberekben magasabb kockázati faktort jelent, akik ismerik ennek a negatívumait.

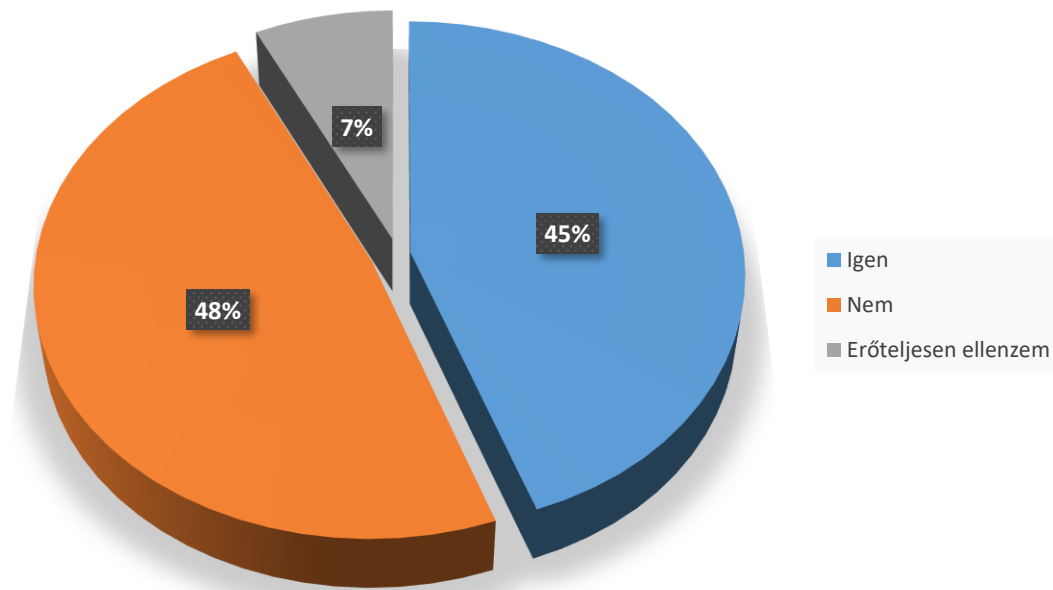
6. diagram: Térfigyelő kamerák támogatottsága



Forrás: saját készítés

A megkérdezett emberek túlnyomó többsége támogatja a térfigyelő kamerák jelenlétét az országban. Szerintem ennek oka az lehet, hogy a kamera jelenléte növeli az állampolgárokban a szubjektív biztonságérzetet, biztonságban érzik magukat. Az emberek tudatában már benne van, ha esetleg vagyoni kár, személyi sérülés vagy valamely cselekmény áldozatául esnek, akkor az utólag bizonyító erejű lehet.

7. diagram: Arcfelismerő rendszerek támogatottsága, a térfigyelő kamerákat támogatók körében

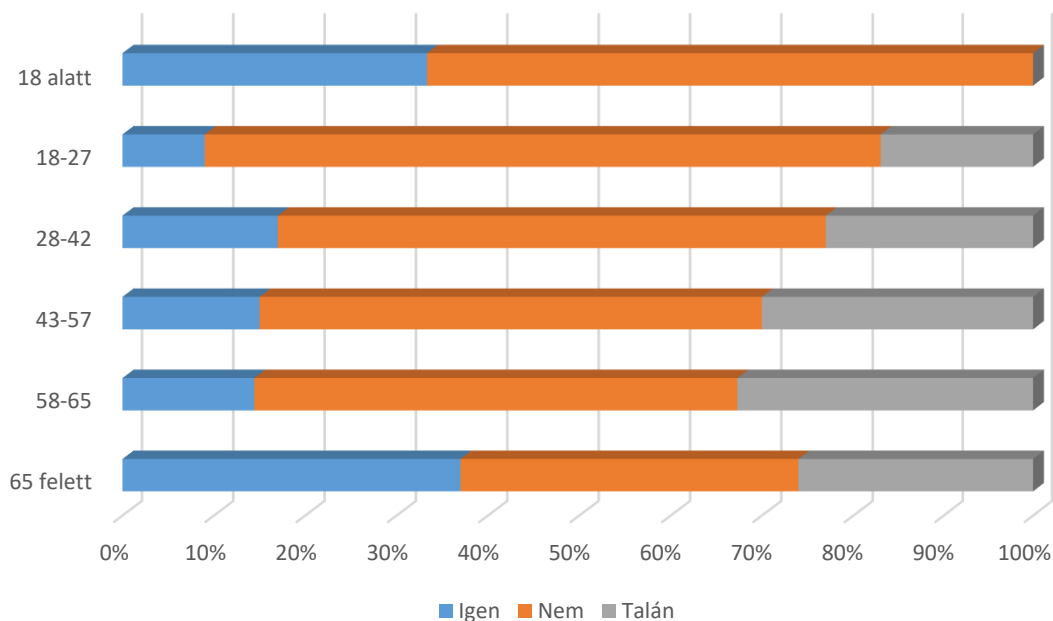


Forrás: saját készítés

Viszont, ha a kérdésben szerepel az, hogy alkalmazzanak-e arcfelismerő technológiát a térfigyelő kamerákon és adatokat gyűjtsenek személyekről, akkor szemmel láthatóan megváltoznak az eredmények. Jól látható, hogy szignifikáns eltérés következik be, mikor már személyes érintettség is társul a technológiához. Itt viszont felmerülhet az, hogy miért lett ekkora az elutasítottsága, még a térfigyelő kamerákat támogatók körében is, miközben azokat a kamerákat a többség támogatja, és ugyanúgy be lehet azonosítani személyeket. A különbség az, hogy ezzel a technológiával naplózni lehet az emberek mindennapi tevékenységeit, szokásait, és konkrét profilalkotást lehet létrehozni adatbázistól függően.

Azzal a kijelentéssel, hogy „Ha az állam arcfelismerő rendszereket alkalmazna közterületen, az az emberek mindennapi tevékenységük, szokásaik megfigyelésére is szolgálna.” a kitöltők 44%-a, vagyis a relatív többsége egyetértett, 37%-a szerint van realitása és csak 14,1% nem értett vele egyet. Szóval, szerintem ez azt bizonyítja, hogy túl nagyok az emberekben a kételyek ezekkel a rendszerekkel kapcsolatban és ott van az a kellemetlen tudat, hogy éppen adatokat gyűjtenek róluk és nem tudják pontosan, mire is használják fel.

8. diagram: Jelenléti ív arcfelismeréssel az életkorra vetítve

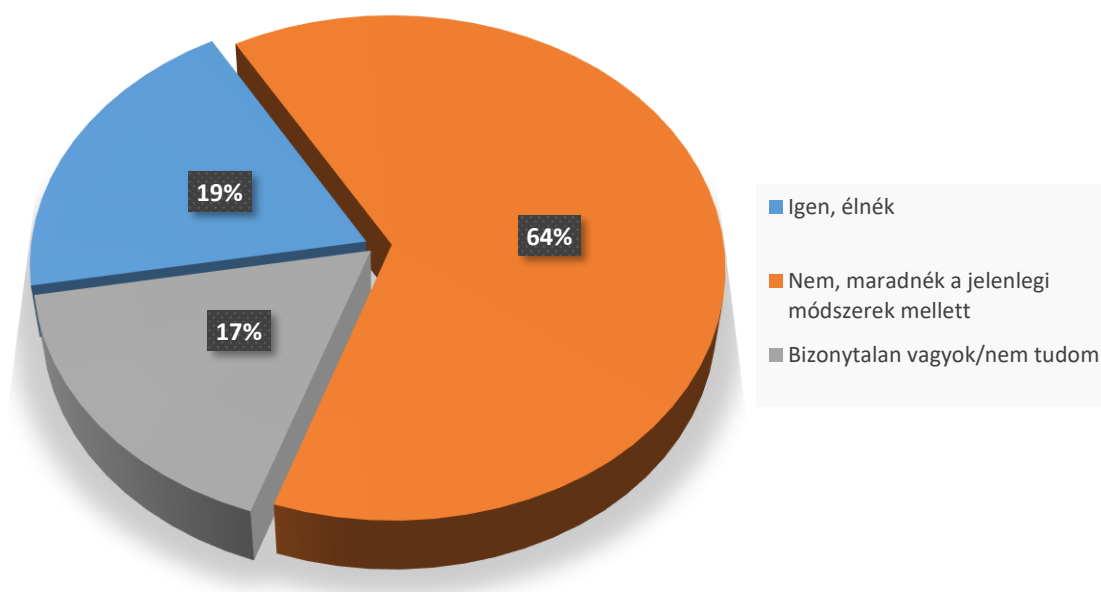


Forrás: saját készítés

Az órai jelenléti ív készítésének ötletét Bálint Krisztián tanulmánya adta, aki a kutatásában arról győződött meg, hogy a biztonsági kamerák képesek lehetnek a hallgatókról online jelenléti ívet készíteni [37].

Az általam felmért 18-27 éves korosztályban, akik vélhetően még iskolába, egyetemre járnak, azok között a legnagyobb az arcfelismeréssel történő órai jelenléti ív készítésének elutasítottsága. A 65 év feletti korosztályban volt az arcfelismerő órai jelenléti ív támogatottsága a legnagyobb. Vélhetően azért, mert az Ő személyes érintettségük a legkisebb a jelenlegi oktatás terén. Igaz, a 18 alattiak között volt a második legnagyobb a támogatottsága, viszont csak 3 kitöltő volt ebben a korosztályban, így véleményem szerint az nem tekinthető relevánsnak.

9. diagram: Arcfelismeréses fizetés lehetőségével élők száma.



Forrás: saját készítés

A Kínában már elterjedt arcfelismeréssel történő fizetés nagy teret hódított magának, viszont itt jól látható, hogy kevesen élnének vele. A kérdőívben szereplő „Önmagát az új technológiák alkalmazására nyitott embernek tartja?” kérdésben, összesen az emberek 80,1%-a (n=225) válaszolt igennel. Viszont meglepő módon, a Magyarországon, sőt még Európában is újnak számító arcképpel való fizetéssel a kitöltők 64%-a (n=180) nem élne. Itt egy jelentős ellentmondást érzek. Ennek oka az lehet, hogy alapvetően az emberek tényleg nyitottak az új technológiák iránt, viszont ha e mögött meghúzódik valamilyen anyagi háttér (jelen esetben a bankszámlán lévő pénz) akkor jobban megfontolják döntéseiket.

Konklúzió

Véleményem szerint, ahogy a kutatásomból is kiderült, a magyarországi társadalom még nem áll készen az arcfelismerő rendszerek teljeskörű bevezetésére. Ezalatt értem az arcfelismeréssel való fizetést az áruházakban, bűnmegelőzési célú arcfelismerő azonosítást a közterületeken, illetve a jelenléti ív készítést az oktatási intézményekben.

10. Összegzés

A kutatási téma feldolgozása során a következő eredményeket kaptam:

H1: A biztonságtudatosabb emberek a mobiltelefonjaikon inkább használnak biometrikus azonosítást, mint bármely más okostelefon adta lehetőséget.

H2: Akik hallottak már a Kínában zajló megfigyelési rendszerről, azok közül kevesebben választják a kínai szoftvert, ellenben azokkal, akik még nem hallottak róla és nem ismerik ennek a kockázatát, hátrányait.

Kutatásom során mind a két felvetésem beigazolódott. Az emberek egyre több adatot tárolnak mobiltelefonjaikon, egyre biztonságtudatosabbak és kihasználják a technológia adta biztonsági lehetőségeket. A biztonságtudatosabb személyek inkább használnak biometrikus azonosításokat, feltehetőleg hatékonyságuk, megbízhatóságuk és kényelmesebb használatuk miatt.

Másik hipotézisből érzékelhető, hogy a kérdőívet kitöltők jelentős része nem akarna egy megfigyelt társadalomban élni. Véleményem szerint a Magyarországon élő emberek döntő többsége is hasonlóképpen gondolná. Fontos megjegyezni, hogy a kérdőívem nem volt reprezentatív és nem tükrözi a teljes magyar társadalom véleményét.

Az arcfelismerő technológia egy korszerű digitális eszköz, amelyet széles körben használnak magán- és állami szervezetek. A korábban már sokat említett előnyei figyelemre méltóak, de az általa jelentett kihívásokat nem lehet figyelmen kívül hagyni, amelyre ez a dolgozat is rávilágít. Európában komoly kihívást jelent az általános adatvédelmi rendeletnek való megfelelés biztosítása. Kezdve az adatkezelés megfelelő jogalapjának felkutatásával és a biometrikus adatok feldolgozását lehetővé tevő megfelelő kivétel felismerésével. Figyelembe kell venni a biztonsági intézkedések végrehajtását és a harmadik országokba irányuló adattovábbítással járó kockázatokat is. Viszont, a polgárok szemével nézve, szerintem a legnagyobb kockázatot az állam által, közterületen kihelyezett arcfelismerő rendszerek hordozzák. Gondoljunk bele, hogy egy diktatórikus berendezkedésű államban milyen retorziókkal járhat, ha egy állami dolgozó véleményt nyilvánítana egy tüntetésen. Véleményem szerint a közterületen kiépített arcfelismerés és a gyülekezési jog kisebb-nagyobb mértékbeli korlátozása szorosan összefügghet egymással. Ugyanis ez az egyik alapjog, melyet jelentősen sérthet például egy országosan kiépített arcfelismerő rendszer. Így az embereket elriasztják a tüntetéseken való részvételtől, az nemcsak véleménynyilvánítási szabadságukkal ütközik, hanem a gyülekezési szabadságukba is komoly beavatkozást jelent. Főleg ha esetleg az az ország egy olyan mértékben kiépített kreditrendszert alkalmaz, mint Kína, ahol szankciók

érhetnek ezért. Erőszakos tüntetések során szerintem talán alkalmazható lenne, viszont a békés összejövetelek során történő használata eltántoríthatja az embereket a demonstrációtól. Az arcfelismerő technológiák alkalmazása olyan hatást válthat ki, amelyben az egyének tartózkodnak gyülekezési és egyesülési szabadságuk jogszerű gyakorlásától, mert félnek az ebből következő negatív következményektől. Így elbátortalanodhatnak attól, hogy bizonyos egyénnel vagy szervezetekkel találkozzanak, vagy bizonyos találkozókon vegyenek részt. Ennek a hatásnak egyértelmű következményei vannak a részvételi demokrácia hatékony működésére nézve is, és így közvetlenül beavatkozik a gyülekezési és egyesülési szabadságba. Ennél fogva az arcfelismerő technológia, közterületen való alkalmazása már felveti a kérdést, hogy a szükségességi és arányossági küszöböt eléri-e? Magyarországon nem látok rá esélyt, hogy az elkövetkezendő 3-4 éven belül létrehozzanak egy országosan kiépített arcfelismerő rendszert. A magyar társadalom szerintem még nem tart ott, hogy elfogadná ezeknek az eszközöknek a létjogosultságát, nem mellelleg jelentős anyagi ráfordítást igényelne.

Köszönetnyilvánítás

Szeretnék köszönetet nyilvánítani a konzulensemnek, aki segítette dolgozatom megírását, illetve szeretném megköszönni Juhász Tamásnak, hogy hozzájárult az interjú elkészítéséhez.

Jegyzékek

Ábrajegyzék

1. ábra: Az arcfelismerés lépései.....	11
2. ábra: A geometriai arcfelismerés leglényegesebb paraméterei	14
3. ábra-A fényviszonyok nagyban befolyásolják az élek keresését.	15
4. ábra: Edge line mapping felület illusztrációja, jól láthatóak a végpontok.	16
5. ábra: Az iPhone X lényegében egy Kinect. Megtalálhatóak rajtuk ugyanazon jellemzők. .	17
7. ábra: A megfigyeléshez használt furgon és a kamerái által rögzített kép.	27
8. ábra: A rendőrség hivatalos jelentése az arcfelismerő rendszerek telepítéséről.	28

Táblázatjegyzék

1. táblázat: Jogszabályi keret időrendi változása.....	10
2. táblázat: Példák a tanulmányban használt digitálisan létrehozott arcmaszkokra.	20

Diagramjegyzék

1. diagram: Nemek megoszlása.....	35
2. diagram: Életkorcsoport megoszlása.....	35
3. diagram: Okostelefon feloldás módszerek megoszlása.....	36
4. diagram: Összefüggés a biometrikus azonosítás és a biztonságtudatosság között.....	37
5. diagram: A kínai megfigyelési módszerekről tudomással rendelkező személyek és az arcfelismerő szoftverek származási országa közötti összefüggés	37
6. diagram: Térfigyelő kamerák támogatottsága.....	38
7. diagram: Arcfelismerő rendszerek támogatottsága, a térfigyelő kamerákat támogatók körében	39
8. diagram: Jelenléti ív arcfelismeréssel az életkorra vetítve	40
9. diagram: Arcfelismeréses fizetés lehetőségével élők száma.	41

Felhasznált irodalom

- [1] Kaspersky, „What is Biometrics? How is it used in security?,” Kaspersky, 7 október 2020. [Online]. Available: <https://www.kaspersky.com/resource-center/definitions/biometrics>. [Hozzáférés dátuma: 19 augusztus 2022].
- [2] V. L. Raposo, „(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation,” *Taylor&Francis Group*, p. 18, 2022.
- [3] d. D. Edina, „Egy éves az általános adatvédelmi rendelet (GDPR),” *Parlament infójegyzet*, %1. kötet10, p. 2, 2019.
- [4] A. Jelinek, „Gyakran feltett kérdések az Európai Unió Bíróságának a C- 311/18. sz. adatvédelmi biztos kontra Facebook Ireland Ltd és Maximillian Schrems ügyben hozott ítéletéről,” *Európai Adatvédelmi Testület*, p. 2, 2020.
- [5] NOYB, „Austrian DSB: Use of Google Analytics violates "Schrems II" decision by CJEU,” 13 január 2022. [Online]. Available: <https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal>. [Hozzáférés dátuma: 15 08 2022].
- [6] N. Attila és T. Gergely, „Arcfelismerő rendszerek alkalmazása,” *Belügyi Szemle*, %1. kötet67, p. 129, 2019.
- [7] P. Grother, M. Ngan és K. Hanaoka, Face Recognition Vendor Test (FRVT), National Institute of Standards and Technology, 2019, p. 5.
- [8] Suneratech, „What Is AI, ML & How They Are Applied to Facial Recognition Technology,” 22 október 2021. [Online]. Available: <https://www.suneratech.com/blog/ai-ml-and-how-they-are-applied-to-facial-recognition-technology/>. [Hozzáférés dátuma: 20 szeptember 2022].
- [9] National Institute of Standards and Technology, „NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software,” 19 december 2019. [Online]. Available: <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software> . [Hozzáférés dátuma: 15 augusztus 2022].
- [10] F. Krisztina, „A biometrikus azonosítási eljárások alkalmazhatósági szcenáriói a rendőri munkában,” p. 62, 2016.
- [11] W. Wang, „Face Recognition Based on Binary Edge Map and Support Vector Machine,” Semantic Solar, 6 július 2017. [Online]. Available: <https://www.semanticscholar.org/paper/Face-Recognition-Based-on-Binary-Edge-Map-and-Qiu-Wang/55fd4639c2126de5ad69d23b8a6e670a05911b9d>. [Hozzáférés dátuma: 20 szeptember 2022].
- [12] H. Irén, „Biometrikus azonosítás,” *Parlament infójegyzet*, %1. kötet27, p. 2, 2020.

- [13] I. Adjabi és A. Benzaoui, „Past, Present, and Future of Face Recognition: A Review,” MDPI, 16 június 2020. [Online]. Available: <https://www.mdpi.com/2079-9292/9/8/1188/htm>. [Hozzáférés dátuma: 10 szeptember 2022].
- [14] Azure, „Mi a gépi tanulás?,” Microsoft, 2022. [Online]. Available: <https://azure.microsoft.com/hu-hu/resources/cloud-computing-dictionary/what-is-machine-learning-platform/#benefits>. [Hozzáférés dátuma: 20 szeptember 2022].
- [15] S. G. – S. Gyula, Az okos város kameraképeinek elemzése, Budapest: Dialóg Campus, 2019.
- [16] M. Ngan, P. Grother és K. Hanaoka, „Ongoing Face Recognition Vendor Test (FRVT) Part 6A: Face recognition accuracy with masks using pre-COVID-19 algorithms,” július 2020. [Online]. Available: <https://doi.org/10.6028/NIST.IR.8311>. [Hozzáférés dátuma: 27 augusztus 2022].
- [17] Comparitech, „Surveillance camera statistics: which cities have the most CCTV cameras?,” 12 július 2022. [Online]. Available: <https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/>. [Hozzáférés dátuma: 12 augusztus 2022].
- [18] N. Milada, „A kínai „okosváros”-eszközök biztonsági kockázatai,” *Nemzet és Biztonság*, %1. kötet2, p. 27, 2021.
- [19] O. Akhahenda, „A school in China is monitoring students with facial-recognition technology that scans the classroom every 30 seconds,” Lifeboat, 21 október 2019. [Online]. Available: <https://lifeboat.com/blog/2019/10/a-school-in-china-is-monitoring-students-with-facial-recognition-technology-that-scans-the-classroom-every-30-seconds>. [Hozzáférés dátuma: 16 augusztus 2022].
- [20] J.-C. Hong, Y. Li, S.-Y. Kuo és X. An, „Supporting schools to use face recognition systems,” p. 3, 2022.
- [21] PCX, „Kína arcfelismeréssel szabályozza a gyerekek játékidejét,” 7 július 2021. [Online]. Available: <https://www.pcx.hu/a-tencent-vallalat-arcfelismerero-rendszerrel-szabalyozza-a-kinai-gyerekek-videojatekkal-eltoltott-idejet>. [Hozzáférés dátuma: 18 augusztus 2022].
- [22] iiMedia, „Kutatási jelentés az arcszkennelő fizetési technológia alkalmazásának társadalmi értékéről Kínában,” 21 november 2019. [Online]. Available: <https://www.iimedia.cn/c400/66866.html>. [Hozzáférés dátuma: 17 augusztus 2022].
- [23] L. Tang, „Revisiting Facial-Recognition Payment: Old Problems Still Linger,” NNGROUP, 20 március 2022. [Online]. Available: <https://www.nngroup.com/articles/facial-recognition-payment/>. [Hozzáférés dátuma: 16 augusztus 2022].
- [24] G. Gárdonyi, „Az állóképes arcképezonosítás Magyarországon,” *Belügyi szemle*, %1. kötet69, %1. szám7, p. 4, 2021.

- [25] NEC, „Biometric Identification for Over 1 Billion People,” Nippon Electric Company, 8 november 2018. [Online]. Available: <https://www.nec.com/en/case/uidai/index.html>. [Hozzáférés dátuma: 19 augusztus 2022].
- [26] National Library of Medicine, „India slated for using facial recognition in virus battle,” 25 május 2021. [Online]. Available: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8148534/>. [Hozzáférés dátuma: 20 augusztus 2022].
- [27] BBC, „A routine abduction - of a 13-year-old girl,” 4 március 2018. [Online]. Available: <https://www.bbc.com/news/stories-43262319>. [Hozzáférés dátuma: 20 augusztus 2022].
- [28] V. Singh, „1,100 rioters identified using facial recognition technology,” The Hindu, 12 március 2020. [Online]. Available: <https://www.thehindu.com/news/cities/Delhi/1100-rioters-identified-using-facial-recognition-technology-amit-shah/article31044548.ece>. [Hozzáférés dátuma: 20 augusztus 2022].
- [29] Forbes, „Delhi, Chennai among most surveilled in the world, ahead of Chinese cities,” 26 augusztus 2021. [Online]. Available: <https://www.forbesindia.com/article/news-by-numbers/delhi-chennai-among-most-surveilled-in-the-world-ahead-of-chinese-cities/69995/1>. [Hozzáférés dátuma: 21 augusztus 2022].
- [30] LiveMint, „The Hyderabad model of CCTV surveillance,” 10 november 2020. [Online]. Available: <https://www.livemint.com/news/india/the-hyderabad-model-of-cctv-surveillance-11604926158442.html>. [Hozzáférés dátuma: 21 augusztus 2022].
- [31] P. Bischoff, „Surveillance camera statistics: which cities have the most CCTV cameras?,” Comparitech, 11 július 2022. [Online]. Available: <https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/>. [Hozzáférés dátuma: 1 szeptember 2022].
- [32] R. Weaver, „The Constitutional Implications of Drones, Facial Recognition Technology and CCTV,” *Public Governance*, %1. kötet6, %1. szám2, p. 9, 2021.
- [33] „Baroness Williams levele,” 28 március 2018. [Online]. Available: <https://www.parliament.uk/globalassets/documents/commons-committees/science-technology/Correspondence/180328-Baroness-Williams-to-chair-Biometrics-Strategy-and-Forensic-Services.pdf>. [Hozzáférés dátuma: 5 szeptember 2022].
- [34] P. Fussey és D. D. Murray, Independent report on the London Metropolitan Police Service's trial of live facial recognition technology, Essex: University of Essex, 2019.
- [35] F. Hersey, „Live facial recognition resumes for London Met as law enforcement seeks wider use,” Biometric Update, 14 február 2022. [Online]. Available: <https://www.biometricupdate.com/202202/live-facial-recognition-resumes-for-london-met-as-law-enforcement-seeks-wider-use>. [Hozzáférés dátuma: 5 szeptember 2022].

- [36] P. László, „Arcfelismerő kamerák Siófokon?,” GDPR.blog, 14 június 2021. [Online]. Available: https://gdpr.blog.hu/2021/06/14/arcfelismero_kamerak_siofokon. [Hozzáférés dátuma: 5 szeptember 2022].
- [37] H. Márk, „A totális megfigyelés ellen senki sem tüntet, pedig jó úton haladunk felé,” 444, 24 április 2019. [Online]. Available: <https://444.hu/2019/04/24/a-totalis-megfigyeles-ellen-senki-sem-tuntet-pedig-jo-uton-haladunk-fele>. [Hozzáférés dátuma: 2 szeptember 2022].
- [38] CIB, „Mastercard Év Bankja pályázat 2021,” CIB, 2022. [Online]. Available: <https://www.cib.hu/Maganszemelyek/hirek/evbankja-2021.html>. [Hozzáférés dátuma: 15 szeptember 2022].
- [39] B. Krisztián, „Biztonsági kamerákon alapuló hallgatói jelenléti ívkészítő rendszer analitikai funkciói,” in *Doktoranduszok Országos Szövetsége Kiadó*, Budapest, 2021.