

A mesterséges intelligencia szerepe a bűnmegelőzésben

The Role of Artificial Intelligence in Crime Prevention

DOI: [HTTPS://DOI.ORG/10.53793/RV.2026.3.5](https://doi.org/10.53793/RV.2026.3.5)

Absztrakt

A mesterséges intelligencia (MI) egyre meghatározóbb szerepet tölt be a bűnmegelőzésben, különösen az arcfelismerés, a megfigyelési rendszerek és a prediktív algoritmusok révén. E technológiák hozzájárulhatnak a rendészeti hatékonyság növeléséhez és a proaktív fellépéshez. Ugyanakkor jelentős kockázatokat hordoznak az alapvető jogok, különösen a magánszféra és az adatvédelem szempontjából. A tanulmány célja a mesterséges intelligencia bűnmegelőzésben betöltött szerepének elemzése, a nemzetközi gyakorlatok bemutatása és az Európai Unió szabályozási keretének – különösen az MI-rendeletnek – értékelése (2024). A vizsgálat rámutat arra, hogy az MI alkalmazása csak megfelelő jogi garanciák, átláthatóság és emberi kontroll mellett tekinthető elfogadhatónak.

KULCSSZAVAK: MESTERSÉGES INTELLIGENCIA, BŰNMEGELŐZÉS, PREDIKTÍV RENDÉSZET, ARCFELISMERÉS, RENDÉSZETI TECHNOLÓGIÁK

Abstract

Artificial intelligence (ai) is playing an increasingly significant role in crime prevention, particularly through the use of facial recognition, surveillance systems, and predictive algorithms. These technologies can contribute to improving the efficiency of law enforcement and enabling more proactive interventions. At the same time, they raise serious concerns regarding fundamental rights, especially in relation to privacy and data protection. The aim of this study is to analyse the role of artificial intelligence in crime prevention, present relevant international practices, and evaluate the regulatory framework of the European Union, with particular emphasis on the ai act (2024). The analysis demonstrates that the use of ai can only be considered acceptable if it is accompanied by adequate legal safeguards, transparency, and effective human oversight.

KEYWORDS: ARTIFICIAL INTELLIGENCE, CRIME PREVENTION, PREDICTIVE POLICING, FACIAL RECOGNITION, LAW ENFORCEMENT TECHNOLOGIES

Bevezetés

Az elmúlt évtizedben a mesterséges intelligencia alkalmazása a bűnmegelőzés és a rendészeti tevékenység területén világszerte egyre nagyobb jelentőségre tett szert. Az olyan technológiai megoldások, mint az arcfelismerő rendszerek, az intelligens térfigyelő kamerák, valamint a prediktív elemzéseken alapuló algoritmusok új lehetőségeket teremtenek a közbiztonság erősítése és a rendőrségi munka hatékonyságának növelése érdekében. Számos ország és nagyváros kísérletezik jelenleg is olyan MI-alapú eszközökkel, amelyek révén a bűncselekmények megelőzése célzottabbá, gyorsabbá és szervezettebbé válhat.

Egyes nemzetközi kutatások arra is rámutatnak (Braga–Turchan–Papachristos 2019; Welsh–Farrington 2009), hogy az úgynevezett „okos” biztonságtechnológiai megoldások – például a valós idejű térinformatikai rendszerek, a tömeges megfigyelési platformok vagy a lövésérzékelő hálózatok – alkalmazása bizonyos városi környezetekben akár jelentős mértékben is hozzájárulhat a bűnözés visszaszorításához. Mindez ugyanakkor nem kizárólag technológiai, hanem komoly társadalmi, jogi és etikai kérdéseket is felvet. A mesterséges intelligencia rendészeti célú felhasználása szükségszerűen érinti a demokratikus jogállamiság alapvető értékeit. Különösen hangsúlyos szerepet

¹ Budapest Környéki Törvényszék, bírósági fogalmazó; Károli Gáspár Református Egyetem, Állam- és Jogtudományi Doktori Iskola, hallgató; BM gyakoronoki program 2025 résztvevője

kapnak ebben az összefüggésben a személyiségi jogok, az adatvédelem, a magánélet tiszteletben tartása, valamint a gyülekezési és véleménynyilvánítási szabadság védelme. E jogok érvényesülése olyan korlátokat és garanciákat teremt, amelyek nélkül az MI-alapú rendszerek alkalmazása könnyen visszaélésekhez vagy aránytalan állami beavatkozásokhoz vezethetne. E kihívásokra reagálva az Európai Unió 2024-ben elfogadta a mesterséges intelligenciára vonatkozó átfogó szabályozását (AI Act), amelynek célja, hogy egységes keretrendszert biztosítson az MI fejlesztéséhez és alkalmazásához. A rendelet egyszerre törekszik az innováció ösztönzésére és a technológiával járó kockázatok mérséklésére, különös figyelmet fordítva a magas kockázatú rendszerek – így a rendészeti célú felhasználások – szabályozására.

Jelen tanulmány célja, hogy átfogó képet adjon a mesterséges intelligencia bűnmegelőzésben betöltött szerepéről, annak lehetőségeiről és korlátairól. A kutatás bemutatja az alkalmazott technológiák működési sajátosságait, elemzi a kapcsolódó jogi és etikai keretrendszert – kiemelten az Európai Unió MI-rendeletét (AI Act 2024) –, valamint összehasonlító vizsgálatot végez a nemzetközi rendészeti gyakorlatok alapján, különös tekintettel az Egyesült Királyság, Franciaország, az Amerikai Egyesült Államok és Kína példáira. A tanulmány emellett feldolgozza az Országos Rendőr-főkapitányságon végzett empirikus kutatás eredményeit, ideértve az adatgyűjtés és a szakértői interjúk tapasztalatait is. Ezekre építve olyan szabályozási és eljárási modell kerül bemutatásra, amely alkalmas lehet arra, hogy kiegyensúlyozott módon szolgálja a közbiztonság erősítését, miközben megőrzi az alapvető jogok érvényesülésének garanciáit.

MI-technológiák a bűnmegelőzés szolgálatában: arcfelismerés, intelligens megfigyelés és prediktív algoritmusok működése

Arcfelismerő rendszerek működése és alkalmazása

Az arcfelismerő rendszerek napjainkban a mesterséges intelligencia bűnmegelőzési célú alkalmazásainak egyik legdinamikusabban fejlődő területét jelentik. Ezek a technológiák digitális fényképek vagy videofelvételek elemzésével képesek személyek azonosítására az arcuk egyedi jellemzői alapján.

Működésük alapját jellemzően mélytanuláson alapuló neurális hálózatok képezik, amelyeket rendkívül nagy mennyiségű arcképadat felhasználásával tanítanak be.

A felismerési folyamat első lépéseként a rendszer azonosítja az emberi arcokat a kamerák által rögzített képeken, majd részletesen elemzi azok jellegzetes pontjait, például a szemek közötti távolságot, az orr formáját, az arccsontok elhelyezkedését vagy az áll vonalát. Ezekből az adatokból egy sajátos, matematikai alapú leírást hoz létre, az úgynevezett arclenyomatot, amely az adott személy digitális „azonosítójaként” szolgál. Ezt az arclenyomatot a rendszer összeveti a rendelkezésére álló adatbázisban tárolt mintákkal, és az egyezések mértéke alapján dönti el, hogy az adott személy beazonosítható-e. Amennyiben az egyezés megfelelő szintet ér el, a szoftver képes a személy azonosítására vagy legalábbis nagy valószínűséggel történő felismerésére. Az elmúlt években az arcfelismerő technológiák pontossága jelentős mértékben javult, elsősorban a fejlettebb algoritmusok és a növekvő számítási kapacitás következtében. Napjainkban egyes rendszerek már gyengébb minőségű, kedvezőtlen fényviszonyok mellett készült felvételeken is megbízható eredményeket produkálnak, sőt bizonyos teszteredmények szerint akár az egyetű ikek megkülönböztetésére is alkalmasak lehetnek.

A rendészeti gyakorlatban az arcfelismerést többféle módon hasznosítják: utólagos azonosításra (pl. bűnügyi kamerafelvételeken szereplő gyanúsítottak beazonosítására), valós idejű megfigyelésre (tömegrendezvényeken vagy repülőtereken körözött személyek kiszűrésére) és igazolvány-ellenőrzés automatizálására is alkalmazzák. Az egyik legismertebb példát az Amerikai Egyesült Államokból a Clearview AI rendszere szolgáltatja, amely az interneten nyilvánosan elérhető fotók milliárdjainak lementésével épített fel egy hatalmas arcképadatbázist. Ezt a rendszert több amerikai bűnüldöző szerv is igénybe vette – például a 2021. január 6-i Capitolium elleni zavargás során sikeresen azonosítottak és előállítottak több elkövetőt az algoritmus segítségével. Ugyanakkor az ilyen gyakorlat – az interneten fellelhető képek engedély nélküli tömeges lementése biometrikus adatbázisok építéséhez – az Európai Unióban (EU) már tiltott, mivel súlyosan sérti a magánszférát.

Összességében az arcfelismerő technológia hatékony eszköz lehet a bűnüldözésben (például körözött bűnözők elfogásában), de működésének elve – az állampolgárok arcvonásainak folyamatos összevetése rendőrségi nyilvántartásokkal – komoly adatvédelmi és szabadságjogi kérdéseket is felvet, amelyek a tanulmány későbbi részeiben bemutatásra kerülnek.

Megfigyeléstechnikai eszközök nyilvános rendezvényeken

A nyilvános események – tüntetések, sportesemények, fesztiválok – biztosítása során hagyományosan is nagy szerepe van a megfigyelésnek (pl. térfigyelő kamerák, rendőrségi megfigyelőtorony, helikopteres/drónos felderítés). Az MI megjelenésével ezek az eszközök „intelligens” képességekkel bővültek.

Egy 2025-ös budapesti Pride-felvonulás példája jól szemlélteti, hogy az MI-alapú megfigyelési technológiák képesek nagy tömegek viselkedésének elemzésére, valamint potenciálisan veszélyes vagy rendellenes helyzetek korai felismerésére.² Ugyanakkor az ilyen rendszerek alkalmazása érzékeny alapjogi kérdéseket vet fel, mivel a résztvevők megfigyelés-tudata visszatartó hatással lehet az alkotmányos jogok, különösen a békés gyülekezés szabadságának gyakorlására. Napjaink legkorszerűbb térfigyelő kamerái nem pusztán rögzítik a történéseket, hanem valós időben elemzik is a képet. Különböző szenzorokkal vannak felszerelve (pl. hőkamerák, mozgásérzékelők), és MI-algoritmusok segítik őket abban, hogy előre meghatározott eseményeket vagy rendellenességeket automatikusan észleljenek. Ilyen *rendellenes* esemény lehet például, ha valaki átmászik egy elzárt terület kerítésén, egy tiltott zónába behatol, vagy éppen egy csomagot/gyanús tárgyat felügyelet nélkül hagynak a tömegben.

A 2024-es párizsi olimpia kapcsán Franciaország be is vezetett egy kísérleti jellegű „algoritmikus videómegfigyelést”: 485 kamera üzemelt MI-szoftverekkel a játékok idején, amelyek képesek voltak detektálni többek között a hirtelen tömegmozgásokat, a földre került személyt vagy az elhagyott csomagokat. Az ilyen technológia felbecsülhetetlen értékű lehet egy terrorcselekmény megelőzésében – hasonló rendszer, időben figyelmeztethetett volna például a 2016-os nizzai merényletre, amikor egy teherautó a tömegbe hajtott. A valós idejű mesterséges intelligencia így gyakorlatilag *virtuális megfigyelőként* működik: a nap 24 órájában szemmel tartja a kameraképeket, és azonnal riasztja az operátorokat, ha valami gyanúsát észlel.

Ezen felül a nyilvános rendezvényeken egyre gyakoribb a drónok alkalmazása is – ma már léteznek olyan drónalapú megfigyelőrendszerek, amelyek AI segítségével autonóm módon tudnak tömeget monitorozni vagy például egy menekülő gyanúsítottat követni.

A rendőrök felszerelésében is megjelentek az MI-t támogató eszközök: bizonyos testkamerák valós idejű videóelemzést kínálnak (pl. automatikusan megjelölik a fontos eseményeket a felvételen), ami megkönnyíti az utólagos visszanezést.

Fontos megjegyezni, hogy Franciaországban – noha a kameraképek algoritmikus elemzését engedélyezték az olimpiára – a törvény kifejezetten *tiltotta* a biometrikus azonosítást (France 2023), így az arcfelismerést nem vezették be a rendezvényeken. Ez azt mutatja, hogy a technológia kínálta lehetőségeket még a leginnovatívabb gyakorlatokban is igyekeznek bizonyos korlátok között tartani a személyes adatok védelme érdekében.

Összességében a nyilvános eseményeken bevetett MI-alapú megfigyeléstechnika hatékony eszköz lehet a rendőrség kezében: segíthet a tömegkezelésben, a veszélyes szituációk korai felismerésében és a gyors reagálásban. Ugyanakkor ezen eszközök használata kapcsán azonnal felmerül az arányosság és a jogszerűség kérdése – mely a 2. fejezetben részletes bemutatásra kerül.

Prediktív algoritmusok és a bűnözés előrejelzése

A prediktív algoritmusok alkalmazása – amelyet a szakirodalom gyakran „prediktív rendszertként” említ – arra irányul, hogy a korábbi bűnügyi adatok, statisztikák és tendenciák elemzése alapján előre jelezze, hol és mikor nőhet meg a bűncselekmények előfordulásának kockázata, valamint, hogy kik válhatnak potenciális elkövetővé vagy áldozattá. Ebben az összefüggésben a mesterséges intelligencia elsődleges feladata a nagyméretű, összetett adathalmazokban rejlő összefüggések és mintázatok azonosítása, amelyek feldolgozása emberi elemzők számára már rendkívül időigényes vagy gyakorlatilag kivitelezhetetlen lenne.

A prediktív rendszert alkalmazási gyakorlatában alapvetően három fő megközelítés különíthető el:

- Az első a helyalapú (place-based) modellek csoportja, amelyek a korábbi bűncselekmények térbeli és időbeli eloszlását elemezve jelölik ki azokat a területeket, ahol fokozott kockázattal lehet számolni.

² A Budapest Pride több tízezres részvétellel zajló nyilvános felvonulás, amelynek biztosítása a rendőrség részéről komplex közrendvédelmi feladatot jelent. Az ilyen események tipikusan alkalmasak a modern megfigyeléstechnikai és adatfeldolgozó eszközök – így az MI-alapú rendszerek – potenciális alkalmazási lehetőségeinek vizsgálatára.

- A második irányzatot a személyalapú (person-based) elemzések jelentik, amelyek egyénekhez kapcsolódó kockázati tényezőket – például bűnügyi előéletet vagy korábbi áldozattá válást – vizsgálnak annak érdekében, hogy megbecsüljék a későbbi bűnelkövetés valószínűségét.
- A harmadik megközelítés a hálózati vagy csoportalapú elemzés, amely a bűnözői csoportok, bandák és informális kapcsolati rendszerek feltérképezésére épül, és ezek alapján próbálja előre jelezni a konfliktusok vagy erőszakos események kialakulását.

E rendszerek működésének alapvető feltétele a nagymennyiségű történeti adat rendelkezésre állása. Ide tartoznak többek között a bűnügyi statisztikák, a korábbi esetek részletes leírásai, a tér- és időbeli információk, valamint esetenként a társadalmi és gazdasági mutatók is. Az algoritmusok ezen adatok feldolgozásával képesek visszatérő mintázatokat felismerni. Például, hogy bizonyos városrészekben hétvégenként gyakoribbak az autólopások, vagy egy adott személy kapcsolati hálójában több, erőszakos cselekményekhez köthető szereplő is megjelenik. Az így létrejövő előrejelzések lehetőséget adnak a rendőrség számára arra, hogy proaktív módon lépjen fel. Ennek keretében megerősítheti a járőrszolgálatot a veszélyeztetett területeken, fokozott figyelmet fordíthat bizonyos visszaesőként értékelt személyekre, illetve célzott megelőző programokat indíthat a kockázatnak kitett fiatalok körében.

A prediktív rendszert támogatói elsősorban az alkalmazás lehetséges előnyeit hangsúlyozzák. Kiemelik mindenekelőtt a bűnmegelőzés hatékonyságának növekedését, mivel a rendészeti szervek a hagyományosan reaktív fellépés helyett egyre inkább megelőző jelleggel avatkozhatnak be. Ennek eredményeként bizonyos bűncselekménytípusok száma mérséklődhet, ha a potenciális elkövetők azt tapasztalják, hogy a rendőrségi jelenlét már a kritikus időszakokban is biztosított. Másrészt az erőforrások hatékonyabb beosztását: a prediktív modellek segíthetnek optimalizálni a járőrözési útvonalakat, azonosítani a „többletmunkát” igénylő területeket, és bizonyítékok hiányában is ráirányíthatják a figyelmet lappangó problémákra. Nem véletlen, hogy számos szoftvercég kínál már kifejezetten rendőrségi célú prediktív elemző eszközöket. Van olyan rendszer, amely a terrorcselekmények megelőzésére fókuszál: integrálja a térfigyelő kamerák képeit, a rendszámfelismerő adatokat és más intelligenciaforrásokat, hogy valós idejű *fenyegetettségi térképet* készítsen. Más eszközök konkrét taktikai javaslatokat is felállítanak, például, hogy adott körülmények között hogyan érdemes megerősíteni a rendőri jelenlétet.

Fontos ugyanakkor látni, hogy a prediktív algoritmusok alkalmazása csak kevés helyen van teljes mértékben integrálva a mindennapi rendőri munkába. Egy 2019-es felmérés szerint (Deloitte) a városok mindössze 8%-a használja kiterjedten a *data-driven* (adatvezérelt) rendészet eszközeit – vagyis a technológia még gyerekcipőben jár, és gyakran kísérleti jellegű projektek formájában van jelen.

Az eddigi tapasztalatok vegyesek. Több amerikai nagyváros kedvező eredményekről számolt be (Thomson Reuters Legal 2025): New York rendőrsége 2016-ban hozott létre egy „Stratégiai Megelőzési és Reagálási Egységet”, amely prediktív módszerekkel azonosította a magas kockázatú személyeket, miközben szociális munkásokat is bevetettek náluk konfliktusmegelőzésre – két év alatt az érintett területeken 5,1%-kal csökkent a gyilkosságok száma. Hasonlóképpen, Chicago 2017-ben kísérletezett azzal, hogy a prediktív modell által kijelölt magas kockázatú környékeken fokozott járőrözést és közösségi támogatást nyújtott; az első évben 23%-os csökkenést jelentettek a gyilkossági rátában. Ezek biztató adatok, de önmagukban nem perdöntőek. Utóbb kiderült ugyanis, hogy a prediktív rendszerek sok esetben *nem váltják be a reményeket*. Egy New York-i Egyetem által vizsgált 13 városban például azt találták, hogy a prediktív algoritmusok valójában felerősítették a már meglévő diszkriminatív mintákat a rendőri munkában. A bűnüldözés adatai köztudottan torzíthatnak – ha egyes (például etnikai vagy szociális szempontból hátrányos) csoportokat a múltban gyakrabban ellenőriztek és vontak eljárás alá, akkor a keletkezett adathalmaz is azt fogja mutatni, hogy *ott több a bűnözés*. Az MI pedig kritika nélkül tanul ezekből az adatokból, így könnyen *önbeteljesítő jóslatként* hat: újra és újra ugyanazokra a környékekre irányítja a rendőrséget, ahol aztán több szabálysértést derítenek fel, megerősítve a modell eredeti feltételezését. Egy oknyomozó elemzés (Sankin–Mattu 2023) Plainfield városában (New Jersey állam) kimutatta, hogy a szoftver előrejelzései szinte soha nem estek egybe a valós bejelentett bűncselekményekkel – 100 „előrejelzésből” kevesebb mint 1 teljesült be érdemben. Ráadásul több nagyváros visszalépett a használatuktól: Los Angeles és Chicago is leállította korábban nagy reményekkel indított prediktív programjait, mivel hosszabb távon nem hoztak kézzelfogható eredményt.

A prediktív algoritmusok esetleges pontatlansága mellett súlyos bírálat éri ezeket etikai szempontból is. Sok kritikus szerint az ilyen rendszerek esszenciálisan *büntetőjogilag releváns következményt fűznek olyan eseményekhez, amelyek még meg sem történtek*.

Felmerül a kérdés: vajon összeegyeztethető-e az ártatlanság vélelmével, ha valakit csak azért von kiemelt rendőri figyelem alá a rendszer, mert a statisztika szerint „magas kockázatúnak” minősül? Továbbá az állampolgárok magánszférájának védelme is kihívás: a prediktív rendszerek rengeteg személyes adatot használnak és kombinálnak, ami adatvédelmi aggályokat vet fel. Ideális esetben ezeket az adatokat anonimizálni kellene és szigorúan biztonságosan tárolni, de a gyakorlatban nem mindig világos, ki fér hozzá és mire használja az így keletkezett információkat.

Összességében a prediktív algoritmusok nagy ígéretet hordoznak a bűnmegelőzésben, de alkalmazásuk rendkívüli körültekintést igényel. Ahogy a fentiek mutatják, fontos a tudományosan megalapozott értékelés: valóban hatékonyak-e, és ha igen, milyen áron. A következő fejezetben ezzel összefüggésben olvasható, milyen jogi és etikai korlátokat kell szabni az MI ilyen jellegű alkalmazásának ahhoz, hogy a demokratikus jogállamiság elvei ne sérüljenek.

Jogi és etikai keretek: az MI felelős és biztonságos alkalmazása a jogállamiság és az alapvető jogok tükrében

Az MI-rendszerek bűnmegelőzési alkalmazása kapcsán a legnagyobb kihívás azoknak a jogi és etikai kereteknek a megalkotása, amelyek biztosítják a technológia felelős használatát. E keretek célja kettős: egyrészt lehetővé kell tenni, hogy a rendvédelmi szervek kihasználhassák az MI nyújtotta előnyöket a közbiztonság erősítésében, másrészt garantálni kell, hogy az alkalmazás során ne sérüljenek a polgárok alapvető jogai, és a hatóságok működése továbbra is a demokratikus jogállamiság normái között maradjon.

Adatvédelem és a magánszféra védelme

Az egyik legfontosabb jogi-etikai aspektus az állampolgárok személyes adatainak védelme. Az arcfelismerés és más biometrikus azonosító rendszerek használata során érzékeny személyes adatokat kezelnek (az emberi arc képmása, mozgása, viselkedésmintái). Európában a szigorú adatvédelmi szabályok – különösen a GDPR (General Data Protection Regulation – Általános Adatvédelmi rendelet) (Az Európai Parlament és a Tanács (EU) 2016/679 rendelete 2016) és a bűnüldözési célú adatkezelésre vonatkozó irányelv (Az Európai Parlament és a Tanács (EU) 2016/680 irányelve 2016) – előírják, hogy a hatóságok csak megfelelő jogalappal, szükséges és arányos mértékben, célhoz kötötten kezelhetik ezeket az adatokat. A *szükségesség és arányosság elve* azt követeli meg, hogy az MI-eszközök alkalmazása ténylegesen indokolt legyen a közbiztonság

érdekében, és ne járjon az érintettek jogainak túlzott korlátozásával. Például, ha egy tüntetésen minden résztvevőt arcfelismerő kamerákkal azonosítanak, az felveti a *tömeges megfigyelés* problémáját, ami összeegyeztethetetlen lehet a személyes adatok védelmének európai standardjaival. Az ilyen gyakorlatot az Európai Unió Alapjogi Chartájának 7. és 8. cikke (2012) – a magánélet és a személyes adatok védelméhez való jog – garantálja, valamint a magyar Alaptörvény VI. cikke (2011) is hasonló alapjogi védelmet biztosít.

A valós idejű biometrikus megfigyelés – amikor a hatóságok élőben, automatizáltan azonosítják az embereket közterületen – különösen érzékeny területnek számít. Ahogy a Társaság a Szabadságjogokért egyik elemzése rámutat (2025), az ilyen *RBI-rendszerek* (valós idejű távoli biometrikus azonosító rendszerek) „súlyosan sértik az emberek magánszféráját, elriasztva őket alapvető jogaik – például a gyülekezéshez való jog – gyakorlásától”.

A megfigyelés pusztán tudata is úgynevezett *dermesztő hatást* (chilling effect) válthat ki: sokan éppen a megfigyeléstől való félelmükben mondanak le arról, hogy éljenek a jogaikkal. Ezt a jogalkotónak mindenképp figyelembe kell vennie, és olyan garanciákat kell beépíteni, amelyek minimalizálják e hatást. Ilyen garancia lehet például, hogy a hatóságok *csak konkrét gyanú vagy veszély esetén* vehetnek be azonosító technológiákat, és nem folytathatnak általános, indokolatlan profilalkotást a lakosságról.

A gyülekezési szabadság és a véleménynyilvánítás védelme

Külön kiemelendő a gyülekezési jog, hiszen éppen a nyilvános rendezvények (tüntetések, felvonulások) azok az alkalmak, amikor a rendőrség az MI-alapú megfigyelést próbálhatja alkalmazni. Az alapvető jogállami követelmény az, hogy a békés gyülekezéshez való jogot csak rendkívül indokolt esetben – például közbiztonsági vagy nemzetbiztonsági okból – és a szükséges mértékben lehessen korlátozni. Amint azt a következő fejezetben is látni fogjuk, az EU új MI-rendelete (AI Act 2024) kifejezetten tiltja, hogy pusztán a gyülekezésen való részvétel miatt automatizált arcfelismeréssel vegyék nyilvántartásba vagy szankcionálják az embereket. Ha a polgárok attól tartanak, hogy egy tüntetésen „feketelistára” kerülhetnek MI segítségével, az a demokratikus diskurzust, a szabad véleménynyilvánítást is csorbítja. Ezért etikai szempontból alapkövetelmény, hogy az MI alkalmazása ne irányulhasson politikai vélemények vagy törvényes tiltakozások megfigyelésére.

A történelmi tapasztalatok (akár a diktatúrák titkosrendőrségeinek gyakorlata, akár a mai orwelli megfigyelőállamok példái) azt mutatják, hogy a tömeges biometrikus megfigyelés könnyen a hatalommal való visszaélés eszközévé válhat. Nem véletlen, hogy az Európai Parlament a jogszabályalkotás során határozottan állást foglalt a demokratikus alapjogok védelme mellett, és ragaszkodott ahhoz, hogy a nyílt területen történő AI-megfigyelés csak a *legsúlyosabb körben* lehessen megengedett.

Összhangban ezzel, a magyar Alaptörvény VIII. cikk (1) bekezdése is kimondja a békés gyülekezés jogát, amelynek gyakorlását a hatóságok kötelesek biztosítani – nem pedig eltántorítani a technológia fenyegető árnyékával (Magyarország Alaptörvénye 2011).

Felelősség, átláthatóság és emberi kontroll

Az MI alkalmazásának etikai követelményei közül kiemelkedik a *felelősségre vonhatóság* (accountability) elve. Bármilyen döntést is támasszon alá egy algoritmus, végső soron egy emberi rendőri vezetőnek kell vállalnia a felelősséget érte. Nem fordulhat elő, hogy „a gép hibájára” hivatkozva hárítsák el a felelősséget túlkapások vagy tévedések esetén. Ennek megfelelően nélkülözhetetlen az *emberi kontroll* fenntartása: az MI csupán döntéstámogató eszköz lehet, a végső döntéseket mindig embereknek kell meghozniuk. Az Európa Tanács és az EU több ajánlása, szakértői csoportja hangsúlyozza a „human-in-the-loop” (ember a döntési láncban) megközelítést, mely szerint az automatizált rendszerek nem működhetnek teljesen önállóan a rendszetben.

A *transzparencia* szintén kulcskérdés. Az MI algoritmusok gyakran *fekete dobozként* működnek, nehéz megérteni belső logikájukat. Pedig elengedhetetlen, hogy legalább az ellenőrző hatóságok számára világos legyen: milyen adatok alapján, milyen modell szerint ad javaslatot a rendszer. Ha például egy prediktív algoritmus bizonyos városrészeket jelöl „veszélyesként”, tudni kell, hogy mely adatok vezettek erre a konklúzióra – különben nem lehet felmérni, hogy nincs-e benne elfogult torzítás.

Az átláthatósághoz tartozik továbbá a nyilvánosság tájékoztatása is: fontos, hogy a polgárok tudatában legyenek, hol és hogyan alkalmaz a rendőrség MI-t. Ennek érdekében több országban is biztosítják a nyilvánosság tájékoztatását: például az Egyesült Királyságban a rendőrség részletes adatvédelmi hatásvizsgálatokat (Data Protection Impact Assessment – DPIA) és működési irányelveket tesz közzé az élő arcfelismerő rendszerek alkalmazásáról, míg az Egyesült Államok egyes városaiban – így például New Yorkban –

nyilvános regiszterekben teszik közzé a hatóságok által használt megfigyelési technológiákat.

Algoritmikus torzítás és diszkrimináció elleni védelem

Etikai szempontból külön figyelmet érdemel az algoritmusokban rejlő esetleges *elfogultság*, azaz előítéletes torzítás. Mint az előzőekben említésre került, a prediktív rendszet terén konkrét kutatások igazolták, hogy a modellek a történelmi adatok elfogultságait újratermelhetik. Hasonló probléma merül fel az arcfelismerő rendszereknél is. Számos tanulmány kimutatta (Buolamwini–Gebru 2018), hogy egyes algoritmusok sokkal kevésbé pontosak például a nők vagy bizonyos etnikai kisebbségek arcainak felismerésében, mert a betanításukhoz használt adatkészletek túlnyomórészt fehér férfiak képeiből álltak. Egy hiba pedig súlyos következményekkel járhat – több olyan esetről tudni az USA-ban (Hill 2020; Garvie 2019), amikor ártatlan embereket tartóztattak le téves arcfelismerési találatok miatt. Az ilyen diszkriminatív hatások ellen a jogállami elvárás az, hogy *minden* technológia bevezetése előtt alapos hatásvizsgálat történjen. Amennyiben egy MI-rendszerről kiderül, hogy jelentős egyenlőtlenséget visz a rendőri intézkedésekbe, úgy annak használatát fel kell függeszteni vagy korrigálni kell. Ezt szolgálják az úgynevezett *algoritmikus auditok*, melyeket független szakértők végeznek a rendszerek ellenőrzésére. Jogi oldalról pedig az antidiszkriminációs normák alkalmazandók. Az egyenlő bánásmód követelményét biztosító jogszabályok ugyanúgy tiltják az algoritmikus alapon megvalósuló faji, nemi vagy egyéb diszkriminációt, mint a humán döntéshozók által tanúsított megkülönböztetést; ilyen például az Európai Unió Alapjogi Chartájának 21. cikke, valamint a magyar jogban az egyenlő bánásmódról szóló 2003. évi CXXV. törvény.

Demokratikus felügyelet és társadalmi párbeszéd

Végül, de nem utolsósorban, a jogállamiság megőrzéséhez elengedhetetlen a demokratikus kontroll a rendőrségi MI-alkalmazások felett. Ez több szinten értendő. Egyrészt intézményes felügyelet formájában – például a független adatvédelmi hatóságok (Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)) ellenőrzik, hogy a rendőrség betartja-e az adatvédelmi előírásokat az MI használata során, illetve a bíróságok is felülvizsgálhatják egyes intézkedések jogszerűségét.

Másrészt a jogalkotó feladata világos törvényi kereteket alkotni (ahogy erről a 3. fejezetben részletesebben szó lesz az EU-szintű szabályozás kapcsán), és a parlamenti nyilvánosság biztosíthatja, hogy a téma társadalmi vitája se maradjon el. A társadalmi párbeszéd kulcsfontosságú, hiszen a közbiztonság és a szabadságjogok közti egyensúly értékválasztás kérdése is. A polgárok bizalma a rendvédelemben csak akkor tartható fenn, ha tudják, hogy véleményüket meghallgatják és a hatóságok átláthatóan, indokolhatóan járnak el. Ennek jegyében több országban – így pl. az Egyesült Királyságban – létrejöttek etikai testületek, tanácsadó bizottságok, amelyek civil szakértőket is bevonva vizsgálják a rendőrségi MI-projektek hatásait és tesznek javaslatot a jó gyakorlatokra.

Összességében a jogi és etikai keretek kialakítása egyfajta *ütköző zóna* szerepét tölti be a technológia és a társadalom között. E keretrendszer célja nem a technológiai innováció akadályozása, hanem annak mederben tartása. Olyan szabályozási környezet kialakítására törekszik, amely egyszerre képes támogatni a hatékony rendészeti munkát és megőrizni az egyéni szabadságjogok érvényesülését. A következő fejezetben a konkrét európai szabályozást, a 2024-es EU MI-rendelet (AI Act 2024) kerül elemzésre, amely jelenleg az egyik legátfogóbb jogi keret ezen a téren.

Az EU 2024-es MI-rendeletének elemzése és végrehajtási mechanizmusai

2024. nyarán az Európai Unió mérföldkőnek számító jogszabályt fogadott el a mesterséges intelligencia szabályozására. Az Európai Parlament és Tanács (EU) 2024/1689 rendelete – közismert nevén *AI Act* vagy MI-rendelet – az első átfogó próbálkozás a világon arra, hogy egy horizontális jogi keretben kezeljék az MI technológiák jelentette kihívásokat és kockázatokat. A rendelet célja kettős: egyrészt elősegíteni az MI innovatív, biztonságos és bizalomépítő használatát az EU egységes piacon, másrészt megóvni a polgárokat az MI bizonyos káros vagy alapjogsértő alkalmazásaitól. Mivel a rendelet közvetlenül alkalmazandó minden tagállamban, a magyar jogrendre is jelentős hatással bír. A tanulmány későbbi részében, az 5. fejezetben kerül bemutatásra, hogy ez a szabályozás miként illeszkedik a hazai jogi környezetbe.

Kockázati kategóriák és tiltott MI-alkalmazások

A rendelet újszerű, *kockázatalapú megközelítést* vezet be. Az MI-rendszereket négy fő kategóriába sorolja a lehetséges kockázataik alapján: tiltott (elfogadhatatlan

kockázatú), magas kockázatú, korlátozott kockázatú és minimális kockázatú csoportok.

Tiltott (elfogadhatatlan kockázatú) MI-rendszerek

Az elfogadhatatlan kockázatúnak minősített MI-alkalmazások használatát teljes mértékben betiltja a jogszabály, mivel ezek összeegyeztethetetlenek az EU értékeivel vagy súlyosan sértik az alapvető jogokat. Ide tartozik mindenképp az állami célú társadalmi pontozás (social scoring) kínai típusú gyakorlata, amikor is a polgárokat a megfigyelt viselkedésük alapján pontozzák és aszerint részesítik előnyben vagy hátrányban. Tiltott továbbá minden olyan MI-rendszer, amely sérülékeny csoportokat (például gyerekeket vagy fogyatékkal élőket) szándékosan manipulál, vagy bárkit tudat alatt befolyásol oly módon, hogy az fizikai vagy pszichológiai kárt okoz. Szintén tiltólistára került a *bűnözési kockázat előrejelzése egyének szintjén*. A rendelet 5. cikke értelmében tilos olyan MI használata, amely egy személy jövőbeni bűncselekmény-elkövetési valószínűségét próbálja megjósolni (gyakorlatilag a *prediktív profilalkotás* ezen formája tehát EU-szinten nem megengedett). Kiemelt figyelmet kaptak a biometrikus azonosítási technológiák: tilos lett a valós idejű, távoli biometrikus azonosítás közterületen, rendészeti célból – vagyis a rendőrség nem alkalmazhat például élő arcfelismerő kamerahálózatot a nyilvánosság számára nyitva álló helyeken, néhány kivételes esettől eltekintve. Ez utóbbi tilalom a jogalkotási viták egyik sarkalatos pontja volt, és a végső szöveg kompromisszumot tükröz: az 5. cikk (1)(d) és (1)(f)–(h) pontjai részletezik azokat a szűk körű kivételeket, amikor mégis alkalmazható a technológia (például eltűnt gyermekek felkutatása, bizonyos terrorcselekmények vagy életveszély elhárítása esetén), de ezekben az esetekben is *bírói engedély*hez és utólagos ellenőrzéshez kötik a használatot. A tiltott alkalmazások listáján szerepel még többek között az érzelemelemző MI munkahelyi vagy oktatási környezetben (nem lehet pl. mimikából vagy hangszínből következtetni a dolgozók érzelmeire), illetve a *visszaélészerű adatgyűjtés* olyan célból, mint arcképadatbázis építése – ahogy fent utaltunk rá, a Clearview AI-féle gyakorlattal az EU kifejezetten szembehelyezkedett. A tiltott kategóriák tehát lényegében a legaggályosabbnak ítélt felhasználásokat fedik le, ahol a potenciális alapjogsérelem nem elfogadható.

Magas kockázatú MI-rendszerek

Az *AI Act* második kategóriája a magas kockázatú MI-rendszereké. Ide sorolja a rendelet azokat az alkalmazásokat, amelyek ugyan hasznosak lehetnek, de

komoly veszélyt jelenthetnek az emberek biztonságára vagy jogaira, ha nem megfelelően tervezik és használják őket. A jogszabály 6. cikke és II. melléklete részletezi, mi minősül magas kockázatúnak – ezek közé tartozik számos közvetlenül a bűnmegelőzéshez kapcsolódó terület. Például: a rendőrségi és igazságügyi célú MI-rendszerek szinte mindegyike magas kockázatúnak számít. Külön említi a rendelet a *bűnüldözésben használt MI-t, amely hatással lehet az emberek alapvető jogaira* – ilyen lehet egy bizonyíték megbízhatóságát értékelő algoritmus, vagy akár egy nyomozást segítő elemző szoftver. Ugyancsak magas kockázatúnak minősül minden biometrikus azonosító rendszer, amely nem valós idejű módon működik, például egy utólagos arcfelismerő szoftver. Bár az ilyen utólagos azonosítás nincs teljesen betiltva, a jogalkotó komoly veszélyként tekint rá, ezért szigorú szabályokhoz köti. A magas kockázatú kategóriában találjuk még az MI alkalmazását a határellenőrzésben (pl. menedéjogi kérelmek automatikus kiértékelése), a kritikus infrastruktúrákban (pl. közlekedésbiztonsági AI rendszerek), az oktatásban (felvételi algoritmusok, vizsgákat osztályozó MI) vagy a munkaerő-toborzásban (önéletrajzokat előszűrő MI) – ezek ugyan nem kapcsolódnak szorosan a bűnmegelőzéshez, de jól mutatják, hogy a szabályozás mely területeket itéli érzékenynek. Ami a bűnüldözést illeti, gyakorlatilag minden olyan MI-alkalmazás, amely rendőrök döntéseit befolyásolja (legyen az egy prediktív rendészeti szoftver vagy akár egy automatikus rendszámfelismerő rendszer, ami alapján intézkednek), ide tartozik.

A magas kockázatú MI-rendszerekre a rendelet részletes követelményrendszert állapít meg (9–15. cikkek). Mielőtt egy ilyen rendszert forgalomba hoznak vagy használatba vesznek, számos feltételnek meg kell felelnie:

- **Kockázatkezelési rendszer**
A fejlesztőknek és felhasználóknak *szisztematikus kockázatelemzést* kell végezniük. Azonosítaniuk kell az MI által jelentett lehetséges károkat (például téves riasztások, torzított output, adatvédelmi incidensek), és megfelelő intézkedésekkel mérsékelni azokat. Ezt a folyamatot a rendszer teljes életciklusa során folyamatosan fenntartják.
- **Adatminőség és adatirányítás**
A magas kockázatú MI-t csak olyan adatokkal szabad megtanítani és működtetni, amelyek megfelelő minőségűek, reprezentatívak és nem vezetnek rendszerszintű diszkriminációhoz. Például egy arcfelismerőnél elvárás, hogy különböző bőrszínű és korú arcokon is teszteljék a modellt, ne csak egy homogén csoporton, ezzel minimalizálva az elfogult működést. Az adatokat dokumentálni kell, a hiányosságokra pedig fel kell hívni a figyelmet.

- **Automatikus naplózás és nyomon követhetőség**
Az ilyen rendszerek működését naplózni kell – azaz rögzíteni, mikor, milyen inputra milyen eredményt adtak. Ez biztosítja az utólagos *auditálhatóságot*: egy incidens után vissza lehessen keresni, mi történt.
- **Részletes dokumentáció és tájékoztatás**
A fejlesztőknek kötelességük technikai dokumentációt készíteni a rendszerükről, amelyből a felügyeleti hatóságok megérthetik a működését, célját és korlátait. E dokumentáció kiterjed például a modellek architektúrájára, a tanítási adatok forrására, a pontossági mutatókra stb. Emellett a rendszer *használóit* (például a rendőrséget) is el kell látni világos utasításokkal és információkkal arról, hogy mire képes és mire nem a szoftver.
- **Humán felügyelet**
Kötelező emberi felügyeleti intézkedéseket bevezetni. Ez azt jelenti, hogy az MI nem működhet önállóan kritikus döntésekben. A szabályozás akár azt is előírhatja, hogy a végfelhasználó (rendőr) megfelelő kiképzést kapjon az MI működéséről, és legyen joga felülbírálni vagy figyelmen kívül hagyni az automatikus javaslatot.
- **Robusztusság, biztonság, pontosság**
A magas kockázatú MI-rendszereknek meg kell felelniük bizonyos teljesítménykritériumoknak. Elvárt a megfelelő pontosság (hibaarány meghatározott határok között tartása), a kiberbiztonság (ne lehessen könnyen feltörni vagy meghekkelni a rendszert, hiszen pl. egy rendőrségi MI manipulálása súlyos következményekkel járhat), és a megbízhatóság akár extrém körülmények között is.

A magas kockázatú MI-rendszereket a piacra kerülés vagy a tényleges alkalmazás előtt megfelelőségértékelésnek kell alávetni. Az MI-rendelet előírja, hogy egy független szervezet, illetve bizonyos esetekben maga a fejlesztő, belső eljárás keretében igazolja a jogszabályi követelmények teljesülését. Amennyiben a rendszer megfelel ezeknek az előírásoknak, megfelelőségi nyilatkozatot kap, amely funkciójában a CE-jelölés. Ennek birtokában az alkalmazás jogszerűen forgalmazható és használható az Európai Unión belül. A megfelelőség igazolása azonban nem zárja le az ellenőrzési folyamatot. A jogszabály a forgalomba hozatalt követően is folyamatos felügyeletet ír elő. A gyártónak piacfelügyeleti mechanizmust kell működtetnie, nyomon kell követnie a rendszer teljesítményét a valós környezetben, valamint köteles bejelenteni az esetleges súlyos incidenseket és működési zavarokat. A felhasználókra is jelentős felelősség hárul. Így például egy rendészeti szervnek biztosítania kell, hogy az MI-rendszert kizárólag rendeltetésszerűen alkalmazzák.

Emellett folyamatosan monitorozniuk kell az eredményeket is. Amennyiben a pontosság romlik vagy rendellenes működés tapasztalható, haladéktalanul intézkedniük kell. Ez a megelőző jellegű ellenőrzési rendszer hozzájárul ahhoz, hogy az MI teljesítménye ne romoljon le észrevétlenül, és ne alakuljon ki olyan helyzet, amely hosszabb távon veszélyeztetheti a jogszerű és biztonságos működést.

Korlátozott és minimális kockázatú MI-rendszerek

Az MI-rendelet a magas kockázatú kategórián túl megkülönböztet korlátozott és minimális kockázatú MI-rendszereket is. Ezekre enyhébb szabályozási követelmények vonatkoznak, mivel alkalmazásuk jellemzően kisebb veszélyt jelent az alapvető jogokra és a társadalom egészére.

A korlátozott kockázatú rendszerek esetében a rendelet elsősorban átláthatósági kötelezettségeket ír elő. Ide tartoznak például az úgynevezett deepfake-technológiák, valamint az MI-alapú chatbotok. Ezeknél alapvető elvárás, hogy a felhasználót egyértelműen tájékoztassák arról, ha mesterséges intelligenciával kerül kapcsolatba. Így például egy ügyfélszolgálati csevegőrobot esetében jelezni kell, hogy nem emberi ügyintézőről van szó. Ebben a kategóriában jelenik meg a generatív mesterséges intelligencia is, különösen a nagy nyelvi modellek alkalmazása. Ezeknél a rendelet elsősorban önkéntes magatartási kódexek és szakmai ajánlások kialakítását ösztönzi. Céljuk, hogy a mesterségesen előállított tartalom felismerhető maradjon, például megfelelő jelölések alkalmazásával szövegek, képek vagy egyéb médiatartalmak esetében.

A minimális vagy csekély kockázatú MI-rendszerekre a szabályozás már nem állapít meg különösebb kötelezettségeket. Ide sorolhatók például a spam-szűrők vagy egyes videojátékokban alkalmazott intelligens rendszerek. Ezeknél a jogalkotó álláspontja szerint elegendő védelmet nyújt a piaci önszabályozás, valamint a meglévő általános jogi keretek, így különösen a fogyasztóvédelmi és polgári jogi szabályozás.

A rendelet hatálybalépése és átmeneti időszakok

Fontos megjegyezni, hogy bár a MI-rendelet 2024. augusztus 1-jén *hatályba lépett*, az előírások nem azonnal váltak kötelezővé minden részletükben. A jogalkotó a szabályozás alkalmazását több lépcsőben vezeti be, figyelembe véve azt, hogy mind az iparági szereplőknek, mind a hatóságoknak megfelelő időre van szükségük az új követelményekhez való alkalmazkodáshoz. A rendelet kimondja, hogy a főbb rendelkezések 24 hónappal a hatálybalépés után, azaz 2026. augusztus 2-től lesznek

alkalmazandók a tagállamokban. Van azonban néhány kivétel, amelyek korábban életbe lépnek: így például a tiltott gyakorlatokra vonatkozó tilalmak és az úgynevezett MI-műveltségi kötelezettségek már 2025. február 2-től érvényesek. Ez azt jelenti, hogy a valós idejű arcfelismerés tilalma, a social scoring tiltása stb. már 2025 elejétől betartandó – függetlenül attól, hogy a részletes szabályok (pl. a magas kockázatú rendszerek tanúsítása) csak 2026-tól alkalmazandók. További kivétel, hogy a *generatív MI modellek* (mint pl. a ChatGPT) egyes kötelezettségei 2025. augusztus 2-től léptek életbe, illetve bizonyos, más jogszabályokba integrált MI-rendszereknél (például orvosi vagy gépjárműbiztonsági MI) 2027-ig hosszabb átmeneti idő is van. E többfázisú alkalmazás fontos a bűnmegelőzés szempontjából is: mivel a rendőrségi MI eszközök többsége a magas kockázatú kategóriába esik, a velük kapcsolatos konkrét kötelezettségek (pl. a tanúsítási kötelezettség) 2026-tól lesz közvetlenül számonkérhető. Ugyanakkor a tiltott gyakorlatok (pl. az előző fejezetben elemzett tömeges megfigyelés békés tüntetők ellen) már 2025. elejétől uniós jogba ütköznek, függetlenül attól, hogy egy adott tagállamban ezt engedné-e a helyi törvény.

A végrehajtás intézményrendszere

Az MI-rendelet csak akkor érheti el célját, ha hatékonyan betartatják. Ennek érdekében a jogszabály létrehoz egy több szintű *kormányzási és felügyeleti struktúrát*. EU-s szinten felállításra került az Európai MI Hivatal (European AI Office), amely a Bizottság felügyelete alatt működő új ügynökségként koordinálja a végrehajtást. Feladatai közé tartozik az egységes szabályalkalmazás elősegítése, az iránymutatások kidolgozása, a nemzeti hatóságok munkájának összehangolása és a piaci szereplők támogatása a megfelelésben. Munkáját egy Európai MI Tanács (AI Board) segíti, melyben a tagállami hatóságok képviselői ülnek, továbbá létrejön egy Tudományos Testület és egy Tanácsadó Fórum is, hogy szakmai inputot adjon a szabályozás továbbfejlesztéséhez. A tagállamoknak a rendelet értelmében ki kell jelölniük egy vagy több *nemzeti felügyeleti hatóságot*, amelyek a saját területükön ellenőrzik a szabályok betartását. Ez lehet egy újonnan létrehozott hatóság vagy valamely meglévő intézményre (pl. Magyarországon várhatóan részben a NAIH-ra és tervek szerint a magyar Mesterséges Intelligencia Hivatalra) ruházható át ez a funkció. A nemzeti hatóságok vizsgálhatják a piacra kerülő MI-rendszereket (piacfelügyelet), kezelhetik a panaszokat, szankciókat szabhatnak ki a jogsértőkre – utóbbi akár jelentős összegű bírság is lehet, a GDPR-hoz hasonlóan.

Emellett minden tagállamnak kötelező lesz létrehoznia legalább egy MI-regulációs tesztkörnyezetet (sandbox) 2026-ig. Ezek olyan kontrollált környezetek, ahol a cégek és hatóságok együttműködve kipróbálhatnak új MI-megoldásokat valós környezetben, átmeneti felügyeleti könnyítésekkel, hogy innováció közben is biztosítható legyen a jogkövetés. A bűnmegelőzés terén egy ilyen szabályozói sandbox például lehetővé teheti, hogy a rendőrség kísérleti jelleggel használjon egy prediktív algoritmust, miközben az adatvédelmi szakértők folyamatosan monitorozzák az eredményeket és javaslatokat tesznek a szabályok finomítására.

Érdemes megjegyezni, hogy az MI-rendelet elfogadása során jelentős nézeteltérések alakultak ki az uniós intézmények és a tagállamok között, különösen a rendészeti felhasználások szabályozása kapcsán. Egyes tagállamok – köztük Franciaország – következetesen amellett érveltek, hogy a bűnüldöző szervek számára szélesebb mozgásteret kell biztosítani a mesterséges intelligencia alkalmazásában, elsősorban a közbiztonság védelmére hivatkozva. Ezzel szemben az Európai Parlament tárgyalási álláspontjában hosszú ideig szigorúbb korlátozásokat szorgalmazott, különösen a valós idejű biometrikus azonosítás tekintetében. A végleges rendelet ennek eredményeként kompromisszumos megoldást tartalmaz. Alapvetően tiltja a nyilvános helyeken történő, rendőrségi célú valós idejű távoli biometrikus azonosítást, ugyanakkor szűk körben kivételt enged meg, szigorú feltételek és előzetes engedélyezési eljárás mellett. A kivételek kizárólag meghatározott, különösen súlyos bűncselekményekhez vagy közvetlen veszélyhelyzetekhez kapcsolódhatnak, és alkalmazásuk minden esetben arányossági és szükségességi vizsgálathoz kötött. Emellett a rendelet előírja, hogy a biometrikus keresések csak konkrét, jogszerű cél érdekében végezhetők. Tilos az olyan általános vagy tömeges adatfeldolgozás, amely védett tulajdonságokon alapuló profilalkotásra irányulna. E szabályozási megoldások jól tükrözik azt a törekvést, hogy a jogalkotó egyensúlyt teremtsen a közbiztonság iránti igény és az alapvető jogok védelme között. Ugyanakkor a rendelkezések gyakorlati alkalmazása várhatóan komoly értelmezési és végrehajtási kihívásokat vet majd fel a tagállamok számára.

Összességében az EU 2024-es MI-rendelete új standardot állít fel a mesterséges intelligencia szabályozásában. A bűnmegelőzés területére is jelentős hatást gyakorol: világos vészfékeket épít be (tiltások formájában), ugyanakkor utat enged a biztonságos innovációnak a szigorú feltételek mellett. A siker azonban nagyban függ attól, hogyan implementálják a rendelkezéseket a tagállamok, mennyire lesznek képesek a hatóságok kikényszeríteni az előírásokat, és hogy az érintett szervek – így a rendőrségek – mennyire

készülnek fel a változásokra. A következő fejezetben ezt a kérdést nemzetközi szinten vizsgálom meg: megnézem, hogyan integrálták eddig az MI-t a bűnmegelőzésbe néhány országban (az Egyesült Királyságban, Franciaországban, az USA-ban és Kínában), és milyen tanulságokkal szolgálnak ezek a tapasztalatok.

Nemzetközi rendészeti gyakorlatok AI-integrációja – összehasonlító elemzés (Egyesült Királyság, Franciaország, USA, Kína)

A mesterséges intelligencia bűnmegelőzési célú alkalmazása világszerte eltérő formában és eltérő intenzitással valósul meg. Egyes országok kifejezetten nyitottan közelítenek az új technológiák bevezetéséhez, míg mások inkább fokozatos, óvatos megközelítést alkalmaznak. A következőkben négy meghatározó példa kerül bemutatásra: az Egyesült Királyság, Franciaország, az Amerikai Egyesült Államok és Kína gyakorlata. Ezek az országok mind jelentős lépéseket tettek az MI-alapú eszközök rendészeti integrációja terén, és tapasztalataik sok szempontból irányadónak tekinthetők. Ugyanakkor mindegyik esetben megjelentek szakmai, jogi és társadalmi kritikák is, amelyek rávilágítanak az alkalmazás korlátaira és kockázataira. Az összehasonlító elemzés lehetőséget teremt a közös tendenciák és az eltérő megoldások feltárására. Egyúttal hozzájárul ahhoz is, hogy a magyar jogalkalmazás számára releváns tanulságok vonhatók le a nemzetközi tapasztalatok alapján.

Egyesült Királyság: az intenzív megfigyelés hagyománya és az AI kísérletek

Arcfelismerés és megfigyelő kamerák

A valós idejű arcfelismerés bevezetésében úttörő szerepet játszott a South Wales Police és a londoni Metropolitan Police Service. Már a 2010-es évek közepén megindultak az első tesztprojektek, amelyeket később nyilvános rendezvényeken is kipróbáltak. Ilyen helyszín volt például a Notting Hill-i karnevál, ahol élő arcfelismerő rendszert alkalmaztak a tömegből való azonosítás céljából. A kísérletek vegyes tapasztalatokat hoztak (Court of Appeal 2020; Big Brother Watch 2018). Egyes esetekben valóban sikerült körözött személyeket kiszűrni, ugyanakkor jelentős számú téves riasztás is előfordult. Ezek gyakran ártatlan személyek indokolatlan igazoltatásához vezettek, ami komoly társadalmi és jogi vitákat váltott ki.

A technológia jogszerűsége különösen a 2020-as Bridges kontra South Wales Police -ügy (Bridges v South Wales Police) kapcsán került a figyelem középpontjába. A brit fellebbviteli bíróság ebben az eljárásban megállapította, hogy a dél-walesi rendőrség által alkalmazott élő arcfelismerési gyakorlat nem felelt meg teljes mértékben az adatvédelmi és alapjogi követelményeknek. A döntés elsősorban a garanciák hiányosságaira és a célhoz kötöttség elégtelen érvényesülésére hívta fel a figyelmet. Ugyanakkor a bíróság nem tiltotta meg elvi szinten az arcfelismerés alkalmazását, hanem annak szigorúbb jogi feltételekhez kötését írta elő.

A brit kormány és a rendészeti vezetés mindezek ellenére továbbra is nyitottnak mutatkozik a technológia iránt. 2023-ban a Belügyminisztérium arra ösztönözte a rendőri vezetőket, hogy növeljék az arcfelismerési keresések számát, és mérlegeljék az élő rendszerek alkalmazását például sporteseményeken. A cél elsősorban a körözött személyek hatékonyabb kiszűrése volt. Ez a törekvés arra utal, hogy politikai szinten az Egyesült Királyság a fokozott MI-használat irányába mozdult el. Ugyanakkor az országon belül sem alakult ki teljes egység ezen a területen. Skócia például egy időszakban moratóriumot vezetett be az arcfelismerés rendőrségi alkalmazására, amíg egy független szakértői testület nem vizsgálta meg annak jogi és társadalmi következményeit.

A londoni rendőrség 2023-as beszámolója szerint (UK Home Office 2025) az utólagos, úgynevezett retrospektív arcfelismerő keresések száma jelentősen emelkedett, és ezek több esetben hozzájárultak erőszakos bűncselekmények gyanúsítottjainak azonosításához. Mindez azt mutatja, hogy megfelelő jogi ellenőrzés mellett a technológia fokozatosan beépült a brit rendészeti gyakorlatba, miközben továbbra is élénk szakmai és társadalmi vita övezi alkalmazását.

Prediktív rendészet és adatelemzés

A brit rendőrség az adataalapú rendészetben is kísérletezett. Az egyik legnagyobb szabású projekt az ún. National Data Analytics Solution (NDAS) volt, amelyet a Nyugat-Midlands-i Rendőrség vezetésével fejlesztettek, jelentős kormányzati támogatással. Az NDAS célja egy központosított, mesterséges intelligenciára épülő elemző platform létrehozása volt, amelyet több rendőri szerv is használhat. A rendszer keretében fejlesztették ki a Most Serious Violence (MSV) nevű modult is, amely arra törekedett, hogy az adatbázisban szereplő személyek körében azonosítsa a súlyos erőszakos bűncselekmények elkövetésének fokozott kockázatát.

Az elemzés középpontjában a középtávú kockázatbecslés állt, különös tekintettel az ismételt vagy eszközalódó erőszakos magatartás lehetőségére. A rendszer fejlesztése során több millió személyhez kapcsolódó adat került feldolgozásra, ideértve a rendőrségi nyilvántartásokat, a bűnügyi hírszerzési információkat és a büntetőjogi előéletre vonatkozó adatokat. Ezek alapján a modell célja az volt, hogy kockázati pontszámot rendeljen az egyes személyekhez, és előre jelezze a súlyos erőszakos cselekmények elkövetésének valószínűségét. Az NDAS-projekt azonban a várakozásokhoz képest nem hozott áttörést. A 2020 körül nyilvánosságra került értékelések szerint (Saunders–Hunt–Hollywood 2016) az MSV-modell működésében jelentős technikai és módszertani problémák merültek fel, amelyek megkérdőjelezték az előrejelzések megbízhatóságát. A rendszer tényleges pontossága elmaradt a kezdetben kommunikált értékektől, miközben adatvédelmi és etikai szakértők is komoly aggályokat fogalmaztak meg a gyakorlati alkalmazással kapcsolatban. A fejlesztésben részt vevő szakemberek később elismerték, hogy az MSV-modul jelenlegi formájában nem alkalmas operatív használatra. Ennek következtében a projekt ezen részét leállították, és átfogó felülvizsgálat indult a módszertani alapok újragondolására. A tapasztalatok jól rávilágítottak az egyéni szintű bűnelőrejelzés sajátos nehézségeire. Technikai szempontból problémát jelent, hogy az erőszakos bűncselekmények viszonylag ritka események, amelyek előrejelzése statisztikailag rendkívül bizonytalan. Emellett súlyos etikai kérdések is felmerülnek, például azzal kapcsolatban, hogy miként kezelhető egy olyan lista, amely potenciális elkövetőként jelöl meg személyeket pusztán valószínűségi alapon. Mindazonáltal az NDAS más területeken tovább működött. Különösen a hálózatelemzés és a bűnözői csoportok kapcsolatrendszerének feltérképezése terén maradt meg a gyakorlati hasznosíthatóság. A brit rendőrség több alkalommal is jelezte, hogy a jövőben is számol a mesterséges intelligencia alkalmazásával, ugyanakkor nagyobb hangsúlyt kíván helyezni a korábbi tapasztalatok feldolgozására és a kockázatok kezelésére. A központi program mellett helyi szinten is zajlottak kísérletek (His Majesty's Inspectorate of Constabulary and Fire & Rescue Services 2017; Burgess 2020). A Kent Police egy időszakban az amerikai PredPol szoftvert tesztelte a betörések előrejelzésére. A Greater Manchester Police területén pedig humán erőforrás-folyamatokban alkalmaztak mesterséges intelligenciát a jelentkezők előszűrésére. Ezeket a megoldásokat később megszüntették, miután kiderült, hogy torzításokat és nem kívánt mellékhatásokat eredményeznek.

Szabályozás és társadalmi reakciók

Az Egyesült Királyságban jelenleg nincs kifejezetten a mesterséges intelligenciára vonatkozó, átfogó külön törvény. Az MI rendészeti alkalmazására elsősorban a Data Protection Act 2018, valamint a Human Rights Act 1998 (United Kingdom Data Protection Act 2018; United Kingdom Human Rights Act 1998) rendelkezései irányadók. Ezek a jogszabályok biztosítják az adatvédelemhez és az alapvető jogokhoz kapcsolódó garanciák érvényesülését az új technológiák használata során is. A brit adatvédelmi felügyeleti szerv, az Information Commissioner's Office (2021) több alkalommal is útmutatást adott ki a rendőrségi MI-alkalmazásokkal kapcsolatban. Ezekben rendszeresen hangsúlyozza az adatvédelmi hatásvizsgálat (DPIA) elvégzésének jelentőségét minden új rendszer bevezetése előtt, különösen akkor, ha az személyes adatok tömeges feldolgozásával jár. A technológia társadalmi megítélése szintén élénk viták tárgya. Civil jogvédő szervezetek, így például a Big Brother Watch és a Liberty rendszeresen kampányolnak a túlzott megfigyelés ellen. A Liberty 2019-ben átfogó jelentést tett közzé a prediktív rendészet kockázatairól, és felszólította a rendőrséget, hogy vizsgálja felül az ilyen rendszerek alkalmazását azok aránytalansága és társadalmi hatásai miatt. E társadalmi és szakmai kritikák hatására a prediktív szoftverek alkalmazása az Egyesült Királyság nagyvárosaiban egyelőre nem vált általánossá. Az arcfelismerő technológiák használata is ellenállásba ütközött. Londonban és Cardiffban több alkalommal szerveztek tiltakozó megmozdulásokat az élő arcfelismerő kamerák alkalmazása ellen, miközben a közvélemény továbbra is megosztott maradt a kérdésben. Ugyanakkor a terrorfenyegetettség és a súlyos bűncselekmények elleni fellépés igénye jelentős befolyást gyakorol a politikai döntéshozatalra. Ennek következtében a kormányzati és rendészeti vezetés jellemzően továbbra is támogatja az MI-eszközök alkalmazását, amennyiben azok jogilag és technikailag megfelelő keretek között működnek.

Összességében az Egyesült Királyság gyakorlata a pragmatikus kísérletezés példaként értékelhető. Számos innovatív megoldást teszteltek, egyes projekteket később visszavontak, ugyanakkor a mesterséges intelligencia hosszú távú alkalmazásáról nem mondtak le. A hangsúly egyre inkább a szabályozott, átlátható és ellenőrizhető felhasználás irányába tolódik el.

Ezt tükrözi a londoni rendőrség, a Metropolitan Police Service 2023-ban kiadott etikai iránymutatása (Live facial recognition: Data Protection Impact Assessment (DPIA2) is, amely az MI használatát

független szakértői ellenőrzéshez, belső felügyeleti mechanizmusokhoz és rendszeres értékeléshez köti.

Franciaország: high-tech megfigyelés vs. erős adatvédelmi tradíciók

Franciaország a rendvédelmi MI alkalmazása terén kettős képet mutat. Egyrészt a francia hatóságok komoly lépéseket tettek a modern technológiák bevezetésére a közbiztonság terén, másrészt az ország erős adatvédelmi és polgári szabadságjogi hagyományai miatt a gyakorlatot szigorú felügyelet és vita övezi.

Algoritmikus videómegfigyelés és a 2024-es olimpia

Az egyik legjelentősebb francia példa a 2024-es párizsi olimpiai játékok kapcsán bevezetett algoritmikus videómegfigyelés. A francia parlament 2023. májusában elfogadott egy külön törvényt (2023-380. sz. törvény) az olimpia biztonságáról, amely kísérleti jelleggel engedélyezte MI-algoritmusok alkalmazását a közterületi kamerarendszerekben 2025. március végéig. A törvény részletesen meghatározta a technológia megengedett felhasználási körét. A rendszer kizárólag előre rögzített eseménytípusokat észlelhet az élő kameraképeken, így például a tömeges tolongást, a szokatlanul sűrű csoportosulást, az elhagyott tárgyakat, a fegyver jelenlétét, a földön fekvő személyt, a tüzesetet vagy a közlekedési szabályok megsértését. Amennyiben a szoftver ilyen helyzetet azonosít, riasztást küld az emberi kezelőknek, akik ezt követően értékelik a helyzetet és döntenek a további lépésekről. A kísérleti program keretében (France: Allowing Mass Surveillance at Olympics Undermines EU Efforts to Regulate AI 2023) négy vállalat megoldásait tesztelték: a Orange, a Videtecs, a Wintics és a ChapsVision fejlesztéseit. Kiemelt jelentőségű korlátozás volt ugyanakkor, hogy a jogszabály kifejezetten megtiltotta a biometrikus azonosítást. A rendszerek nem alkalmazhattak arcfelismerést, és nem végezhetek személyazonosítást, kizárólag viselkedési és eseményalapú elemzésre voltak jogosultak. Tehát a szoftver *anonim módon* figyeli a jeleneteket, és csak a fenti eseményekre koncentrál, az embereket nem próbálja meg azonosítani. Ez a kompromisszum jól mutatja, hogy Franciaország igyekezett egyensúlyozni a biztonsági igény és a polgári jogok között. A törvény ugyanakkor erősen vitatott volt: a Nemzeti Adatvédelmi Hatóság (CNIL) és több jogvédő szervezet (pl. Amnesty International) aggodalmát fejezte ki, hogy mindez a tömeges megfigyelés kapuját nyitja meg és *aláássa az EU AI-szabályozás szellemét*.

A kormány azzal érvelt, hogy a bevezetett rendszer nem sérti a személyes jogokat, mert nincs emberi azonosítás, csupán a biztonságot növeli. Az MI-támogatású kamerák az olimpia idején működtek (pl. Párizsban ~400-500 kamera MI-vel figyelte a köztereket), és a tapasztalatok alapján a rendőrség szeretné a technológiát a jövőben is használni nagy rendezvények biztosítására. Párizs rendőrfőnöke a sajtóban is szorgalmazta, hogy az olimpia után se bontsák le az MI-megfigyelési rendszert, mert az a terrorizmus elleni küzdelemben és a mindennapi bűnmegelőzésben is hasznos lehet. Ezt az igényt azonban valószínűleg újabb jogi és politikai vita fogja övezni, különös tekintettel az EU MI-rendelet vonatkozó előírásaira.

Arcfelismerés és biometrikus adatok Franciaországban

Franciaországban az arcfelismerés kérdése legalább annyira érzékeny, mint máshol Európában. Jelenleg a francia jog *nem engedélyezi széles körben* az arcfelismerő kamerák használatát a közterületen (France 1978). A rendőrség ugyanakkor használ belső adatbázisokat (pl. bűnügyi nyilvántartások arcképei alapján) nyomozások során. 2023-ban a Disclose oknyomozó portál belső dokumentumokra hivatkozva arról számolt be (Disclose 2023), hogy a francia rendőrség már évek óta alkalmaz arcfelismerési technológiákat bizonyos belső eljárásokban. A beszámoló szerint ezek használatának jogi háttere hosszú időn keresztül nem volt teljes mértékben rendezett, ami további adatvédelmi és alkotmányossági kérdéseket vetett fel. A jelentés szerint e módszer használata jogilag kérdéses, és a CNIL vizsgálatot is indított az ügyben. A francia adatvédelmi hatóság, a CNIL korábban több alkalommal is fellépett az önkormányzati szintű arcfelismerési gyakorlatokkal szemben. 2022-ben több dél-franciaországi települést is megbírságot, amiért „okos kamerákat” telepítettek arcfelismerési funkcióval. A hatóság megállapította, hogy ezek a rendszerek jogsértőek, ezért az érintett városok végül megszüntették azok használatát. Hasonló álláspontra helyezkedett 2021-ben a francia legfelsőbb közigazgatási bíróság, a Conseil d'État is. Döntésében kimondta, hogy Marseille tervezett, arcfelismerésen alapuló iskolai beléptetőrendszere aránytalan és adatvédelmi szempontból kifogásolható lenne. A határozat nyomán a projekt megvalósítása megghiúsult.

A végleges kompromisszum – amint arra a korábbi részek is utaltak – alapvetően tiltja a valós idejű biometrikus azonosítást, ugyanakkor szűk körben lehetőséget ad annak alkalmazására.

A felvételtől történő, utólagos arcfelismerés súlyos bűncselekmények gyanúsítottjainak azonosítása érdekében engedélyezhető, míg a valós idejű használat csak kivételes esetekben, szigorú feltételek és előzetes engedélyezési eljárás mellett lehetséges. E rendelkezések végrehajtása várhatóan a francia gyakorlatot is érdemben befolyásolja. A tiltó szabályok tagállami szintű alkalmazását követően Franciaország nem vezethetne be általános jelleggel valós idejű arcfelismerést anélkül, hogy az ellentétbe kerülne az uniós joggal. Az MI-rendelet megsértése ugyanis az European Union jogrendje szerint jogsértési eljárást vonhat maga után, amelyet a francia kormány nyilvánvalóan igyekszik elkerülni. Mindez arra utal, hogy Franciaország a jövőben is egyensúlyozni próbál majd saját biztonságpolitikai törekvései és az uniós alapjogi és adatvédelmi követelmények között.

Prediktív elemzések és kísérletek

Franciaországban a prediktív rendészet kevésbé vált ismertté, mint egyes angolszász országokban, ugyanakkor itt is zajlottak kísérleti projektek. A legismertebb ezek közül a „Paved” elnevezésű program volt, amelynek célja az erőszakos bűncselekmények mintázatainak elemzése és előrejelzése volt több nagyvárosban. Egy 2020-ban készült kutatói jelentés, amely a La Quadrature du Net megbízásából készült, arról számolt be, hogy több rendőri szerv is tesztelt prediktív szoftvereket. Ezek között szerepeltek a térbeli és időbeli „forrópontokat” jelző modellek, valamint a visszaeső elkövetők kockázatelemzésére irányuló kísérletek is. A jelentés ugyanakkor éles kritikát fogalmazott meg. Rámutatott az algoritmusok átláthatatlanságára és a diszkrimináció kockázatára, ezért a szervezet a prediktív rendészet alkalmazásának korlátozását, illetve betiltását sürgette. Ennek hatására, valamint a jogi bizonytalanságok miatt a francia rendőrség végül nem vezette be széles körben ezeket a rendszereket. A francia büntető igazságszolgáltatás hagyományosan az egyéni felelősségre és a ténylegesen elkövetett cselekményekre helyezi a hangsúlyt. Ez a szemlélet alapvetően idegenkedik az „előrelátó igazságszolgáltatás” gondolatától, ami szintén visszatartó tényezőt jelentett. Mindemellett a bűnügyi adatelemzés korszerűsítése Franciaországban is folyamatos. A rendőrség és a csendőrség közös elemző rendszereket használ, amelyek támogatják a bűncselekmény-sorozatok felismerését és az összefüggések feltárását. Ezek azonban elsősorban felderítő célú elemzések, nem pedig jövőbeni magatartás előrejelzésére szolgáló eszközök.

Szabályozói háttér és civil kontroll

Franciaországban az adatvédelmi felügyelet kiemelkedő szerepet tölt be. A CNIL Európa egyik legrégebbi és legtekintélyesebb adatvédelmi hatósága, amely szigorúan ellenőrzi a hatósági adatkezeléseket. Az MI alkalmazásával kapcsolatban 2022-ben részletes állásfoglalást adott ki (French Government), amelyben óvott a tömeges megfigyelés normalizálódásától, és hangsúlyozta a világos törvényi felhatalmazás szükségességét. A francia politikai kultúrában erősen jelen van a polgári szabadságjogok védelme. Amennyiben egy kormányzat túlzott megfigyelési intézkedéseket vezetne be, az rendszerint jelentős társadalmi ellenállást vált ki. Erre jó példa volt a 2020-as „globális biztonsági törvény” körüli vita, amely tömegtüntetésekhez és jogszabályi módosításokhoz vezetett.

Összességében Franciaország példája azt mutatja, hogy egy ország egyszerre lehet technológiailag nyitott és jogilag óvatos. Jó példa erre Nice, amely az egyik legintenzívebben kamerázott francia város, és ahol a helyi vezetés kifejezetten támogatja az intelligens megfigyelési rendszerek alkalmazását. Ugyanakkor országos szinten továbbra is érvényesülnek a jogi és társadalmi fékek. A rendőrség igyekszik kihasználni a modern technológiák nyújtotta lehetőségeket, részben a terrorfenyegetettség tapasztalataira hivatkozva. E törekvéseket azonban össze kell egyeztetni a francia és uniós jogi normákkal. Ennek eredményeként Franciaországban az MI integrációja óvatos, fokozatos formában valósul meg. A gyakorlatot pilot projektek, ideiglenes engedélyezések, utólagos ellenőrzések és folyamatos társadalmi vita jellemzi, amelyek együttesen alakítják a jövőbeni irányokat.

Amerikai Egyesült Államok: az úttörő innovációk és a szabályozatlanság dilemmája

Az Amerikai Egyesült Államok a mesterséges intelligencia rendészeti alkalmazásának egyik legfontosabb nemzetközi központja. Számos, világszerte használt kereskedelmi megoldás innen indult, így például a PredPol rendszere vagy a Palantir Technologies elemzőplatformjai. Emellett több amerikai város rendőrsége már viszonylag korán megkezdte a prediktív modellek és az arcfelismerő technológiák tesztelését. Ugyanakkor az Amerikai Egyesült Államokban nem alakult ki egységes, szövetségi szintű MI-szabályozás. Ennek következtében a jogi környezet rendkívül széttagolt. Az egyes államok és városok eltérő szabályokat alkalmaznak, ami jelentős különbségeket eredményez a rendészeti gyakorlatban is.

Prediktív rendészet az amerikai városokban

A prediktív rendészet a 2010-es évek elején vált széles körben ismertté az Amerikai Egyesült Államokban. Több nagyváros, köztük Los Angeles, Chicago, New York és Seattle is kísérleti programokat indított ezen a területen. Los Angeles különösen ismertté vált, amikor a Los Angeles Police Department bevezette a PredPol szoftvert. A rendszer a korábbi bűncselekmények időbeli és térbeli adatai alapján próbálta előre jelezni a várható „forrópontokat”. A kezdeti időszakban több kedvező beszámoló született a járőrözés hatékonyabb szervezéséről és egyes bűncselekménytípusok visszaeséséről (Perry–McInnis–Price–Smith–Hollywood 2013). Hasonló kezdeményezések indultak New Yorkban és Chicagóban is. Chicagóban például létrejött az úgynevezett „Heat List”, amely a leginkább veszélyeztetettnek tartott személyeket tartalmazta, valamint elindult az „Operation Langston” program a bandák mozgásának elemzésére. A rendőrség egy időben a gyilkosságok számának csökkenéséről számolt be, amelyet részben ezekhez a modellekhez kötött (La Ford 2021). Ezeket az eredményeket azonban később több kutató is vitatta. Felhívták a figyelmet arra, hogy a pozitív trendek más rendészeti intézkedéseknek is betudhatók, és hosszabb távon nem bizonyultak fenntarthatónak.

Az elmúlt években egyre több kritika érte a prediktív rendészeti programokat. A American Civil Liberties Union és más jogvédő szervezetek kutatásai és jogi fellépései rávilágítottak a rendszerek torzító hatásaira. Chicago esetében például kiderült, hogy a „Heat List” nem csökkentette érdemben az áldozattá válás kockázatát, viszont aránytalanul sok fiatal, főként afroamerikai férfit vont a rendőrség figyelmének középpontjába. Los Angelesben pedig 2019-ben leállították a PredPol alkalmazását, miután belső vizsgálatok megállapították, hogy a modell rendszeresen ugyanazokat, jellemzően hátrányos helyzetű városrészeket jelölte meg magas kockázatúként (Sankin–Mattu 2023). Egy 2020-ban a New York University kutatói által végzett vizsgálat arra is rámutatott, hogy több amerikai városban a prediktív algoritmusok a korábbi rendészeti elfogultságokat tükrözték vissza. Ennek hatására egyes közösségek még erősebb rendőri ellenőrzés alá kerültek (AI Now Institute 2019). Mindezek következtében több város korlátozta vagy megszüntette a prediktív rendszerek alkalmazását. Jó példa erre Santa Cruz, amely 2020-ban teljes körű tilalmat vezetett be a prediktív rendészet alkalmazására (American Friends Service Committee 2020).

A kritikai hullám ellenére az Amerikai Egyesült Államokban nem szűnt meg teljesen az MI alkalmazása a rendészetben. Inkább szemléletváltás figyelhető meg. A hangsúly egyre inkább az úgynevezett „real-time crime center” modellek felé tolódik el. Ezekben az integrált központokban valós idejű adatgyűjtéssel és elemzéssel támogatják a rendőri munkát. Ilyen rendszer működik például New Yorkban is. Az MI itt jellemzően szűkebb, jól körülhatárolt feladatokat lát el, például videóelemzést vagy lövésérzékelést. Ebben a megközelítésben a mesterséges intelligencia inkább technikai segédeszközként jelenik meg, nem pedig átfogó döntéstámogató rendszerként. A cél a korábbi kritikákból tanulva egy kiegyensúlyozottabb, ellenőrizhetőbb alkalmazás kialakítása.

Arcfelismerés az USA-ban

A szövetségi szervek mellett számos helyi rendőri egység is alkalmaz kereskedelmi arcfelismerő megoldásokat. Ezek közül a legismertebb a Clearview AI, amely nyilvánosan elérhető képekből épített fel nagyméretű adatbázist. A vállalat beszámolói szerint szolgáltatását több ezer rendészeti szerv próbálta ki vagy használta, és befektetők felé azt kommunikálta, hogy számos ügy felderítéséhez járult hozzá (Hinkle 2020). Az arcfelismerés szerepet játszott több nagy horderejű nyomozásban is, például a Capitolium 2021. januári ostromában részt vevő személyek azonosításában, valamint egyes gyermekekkel szembeni bűncselekmények felderítésében. Ezeket az eseteket a technológia támogatói jelentős sikerként értékelték. Ugyanakkor számos visszaélés és téves azonosítás is nyilvánosságra került. Több dokumentált esetben afroamerikai férfiakat azonosítottak tévesen arcfelismerő rendszerek alapján, különösen Detroitban és New Jersey egyes területein. Ezek az ügyek ártatlan személyek letartóztatásához vezettek, és komoly társadalmi felháborodást váltottak ki (Lohr 2020). E tapasztalatok nyomán több nagyváros – köztük San Francisco, Boston és Portland – 2019-2020. folyamán megtiltotta a városi rendőrség számára az arcfelismerő technológiák alkalmazását. A döntések mögött elsősorban az a megfontolás állt, hogy a technológia jelenlegi formájában nem kellően megbízható és nem megfelelően szabályozott.

Szövetségi szinten mindeddig nem született átfogó törvény az arcfelismerés egységes szabályozására. Az egyes ügynökségek elsősorban saját belső irányelveik alapján járnak el. A Kongresszusban több alkalommal is benyújtottak jogszabálytervezeteket – például a Facial Recognition and Biometric Technology Moratorium Act-et –, ezek azonban nem váltak kötelező erejű jogszabállyá. Ennek következtében az Amerikai Egyesült Államokban a rendőrség viszonylag nagy

mozgástérrel rendelkezik az MI-eszközök használatában, különösen az európai gyakorlathoz képest. Ugyanakkor ez gyakran a társadalmi bizalom csökkenésével jár. A technológiai vállalatok részéről is megjelent az önkorlátozás. 2020-ban az IBM bejelentette, hogy megszünteti arcfelismerési üzletágát. Hasonlóan, az Amazon és a Microsoft is ideiglenes moratóriumot hirdetett rendszereik rendőrségi értékesítésére. Ezeket a lépéseket elsősorban az etikai és társadalmi kockázatokkal indokolták. Mindez azt jelzi, hogy az Amerikai Egyesült Államokban az arcfelismerés alkalmazása körül intenzív szakmai és közéleti vita zajlik.

Összességében az amerikai tapasztalat egyfelől jól mutatja, milyen lehetőségeket kínál a mesterséges intelligencia a bűnmegelőzés és a nyomozás területén. A nagy mennyiségű adat és a fejlett algoritmusok kombinációja valóban új eszközöket biztosíthat a rendészeti szervek számára. Másfelől ugyanakkor rávilágít arra is, milyen kockázatokkal jár mindez megfelelő jogi és intézményi kontroll nélkül. Az Amerikai Egyesült Államokban gyakran a technológiai alkalmazás megelőzte a szabályozást, és csak később jelentek meg a korrekciós mechanizmusok civil perek, helyi tiltások és politikai kezdeményezések formájában. A gyakorlat jelenleg is erősen széttagolt: egy seattle-i rendőrség eltérő szabályok szerint működik, mint egy dallasi. Emiatt amerikai szakértők is egyre gyakrabban hangsúlyozzák az országos iránymutatások szükségességét. Ezt a törekvést jelzi, hogy 2022-ben a White House közzétette az úgynevezett AI Bill of Rights dokumentumot, amely alapelveket fogalmaz meg az algoritmikus diszkrimináció tilalmáról és az átlátható döntéshozatalról. Bár ennek nincs kötelező jogi ereje, egyértelműen jelzi, hogy szövetségi szinten is felismerték a szabályozás hiányából fakadó problémákat.

Kína: átfogó megfigyelőrendszer és állami kontroll

Kína a rendészeti technológiák terén a legátfogóbb megfigyelőrendszert építette ki. A Közbiztonsági Minisztérium országosan összekapcsolja a városi és vidéki kamerahálózatokat, és ezekre élő arcfelismerő algoritmusokat illeszt. Az ún. Skynet program (Freedom House 2019) elsősorban a nagyvárosokban működik, minden kameraképet központi adatbázisokkal vetnek össze gyanús személyek kiszűréséhez. Párhuzamosan a Sharp Eyes kezdeményezés – 2015 óta – vidéki területeken létesít új kamerákat, ráadásul még a lakosságot is bevonja a megfigyelésbe (például az emberek speciális tévévevőkészülékeken nézhetik a közeli utcák élőképeit és jelezhetnek a rendőrségnek).

A kampány eredményeként a statisztikák szerint Kínában már több százmillió bel- és magán kamera gyűjti a felvételeket országosan. Az infrastruktúrát kínai nagyvállalatok építik: például a Hikvision a „Sharp Eyes” xi’ani rendszerének teljes megvalósítását magára vállalta (Human Rights Watch 2019).

Az arcfelismerés és egyéb biometrikus technológiák élesben is működnek: a kínai rendszerek képesek tömegben valós időben ellenőrizni a jelenlévő személyek arcát, és riasztani, ha körözött gyanúsítottat vagy más gyanúsítást észlelnek. Egyes beszámolók szerint (Sixth Tone 2017; Mozur 2017) kínai algoritmusok úttörőnek számítanak a pontosságban, ám mások – nemzetközi kutatók és emberi jogi csoportok – szerint a technológia torzított is lehet. Különösen probléma ez az etnikai kisebbségek térségében: a nyugat-kínai Szingjiang (Xinjiang) tartományban alkalmazott IJOP (Integrated Joint Operations Platform) rendszer például automatizált módon jelöl ki „gyanús” személyeket, személyes adatok alapján (például túl sok gyermek, VPN-használat vagy szokatlan üzemanyag-felhasználás szerint). Jogvédő szervezetek – köztük a Human Rights Watch – dokumentálták, hogy ezek az algoritmusok gyakran ujjur és más kisebbségi etnikumú embereket céloznak meg, a „Kemény fellépés a terrorizmus ellen” kampány keretében pedig sokukat fogolytáborokba vitték. Mindezek rámutatnak, hogy Kínában az arcfelismerő és megfigyelő szoftvereket elsősorban a nemzeti biztonság és a rendőrségi célok szolgálatába állítják, sokkal kevésbé az egyéni jogok védelmére – szemben a nyugati hagyományokkal, ahol az ilyen rendszerek bevetését jogi keretek, független kontrollok és társadalmi viták kísérik.

A prediktív rendszert és az adatvezérelt elemzések terén Kína szintén jelentős kísérleteket folytat. Egyes városokban és tartományokban hatalmas adatbázisokat építettek ki. Jó példa erre Hangzhou városa, ahol 2019-re egy úgynevezett „rendőrségi felhő” rendszer keretében több száz adatfajtát és rendkívül nagyszámú rekordot dolgoztak fel (Human Rights Watch 2019). Ezeket az adatokat egy központi big data-platfornon elemezték, amelynek célja a bűnözési mintázatok feltárása és a kockázati területek előrejelzése volt. Amennyiben a rendszer egy adott körzetben megnövekedett lopási vagy egyéb bűnözési kockázatot jelzett, a rendőrség célzottan erősítette meg ott a járőrszolgálatot. Emellett a kínai rendőrség létrehozott külön MI-alapú egységeket is. 2023-tól a Jiangsu tartományi Kunshan városában működik egy „MI-rendőr” csapat, amely saját fejlesztésű gépi tanulási modellt alkalmaz a gyanús viselkedések kiszűrésére és a csalások felderítésére (China Daily 2024). A beszámolók szerint ezek a rendszerek több esetben rövid idő alatt jelentős anyagi károkat okozó bűncselekményeket segítettek felderíteni.

A rendészeti fejlesztések hátterében széles körű állami és vállalati együttműködés áll. Ennek részeként Kínában nagyméretű adatelemző és nyelvi modelleket is fejlesztenek, például a DeepSeek által létrehozott rendszereket. Ezeket egyes tartományokban több adatforrás összekapcsolására és kockázati térképek készítésére használják, különösen az erőszakos bűncselekmények megelőzése érdekében. Összességében ilyen módon a kínai gyakorlatban a mesterséges intelligencia elsősorban az állami adatvagyon nagymértékű felhasználására épül. A cél a rendőri erőforrások rugalmasabb irányítása és a potenciális veszélyhelyzetek korai felismerése, még mielőtt azok ténylegesen megjelennének a közterületeken.

A kínai, erősen központosított modell feletti ellenőrzés jogalkotási és társadalmi szinten korlátozott. Az ország sajátos jogi és politikai környezetében a rendészeti és megfigyelési rendszerek felett nem érvényesül olyan mértékű külső kontroll, mint a nyugati demokráciákban. Nem működik független adatvédelmi ombudsmani rendszer, és a nyilvános társadalmi vita lehetősége is szűkebb keretek között zajlik. A civil érdekérvényesítés mozgástere korlátozott, így a mesterséges intelligencia etikus alkalmazásával kapcsolatos kritikák elsősorban nemzetközi fórumokon jelennek meg. Ezzel párhuzamosan az állami kommunikáció rendszerint a technológiai fejlesztések sikerét hangsúlyozza, és aktívan támogatja azok további kiterjesztését. E megközelítést több nemzetközi szervezet is bírálta. A Freedom House és a Human Rights Watch rendszeresen felhívják a figyelmet arra, hogy Kínában egyfajta „digitális tekintélyuralmi” modell formálódik. Értékelésük szerint a technológiai újítások jelentős részét a lakosság megfigyelésére és a politikai ellenőrzés erősítésére használják fel. Számos elemzés arra is rámutat, hogy bár a kínai rendészeti MI-rendszerek hatékonyak ígérkeznek a bűnözés elleni fellépésben, alkalmazásuk komoly kockázatokat hordoz az alapvető szabadságjogokra nézve. Különösen aggasztónak tartják a megfigyelési technológiák tömeges exportját, valamint az úgynevezett „social credit” jellegű értékelési mechanizmusok nemzetközi terjedésének lehetőségét. E rendszerek az európai jogi szemlélet szerint könnyen vezethetnek diszkriminációhoz, aránytalan megkülönböztetéshez és a szerzett jogok korlátozásához. Mindez jól mutatja, hogy a kínai modell alapvetően eltérő értékrendi és intézményi háttérre épül, mint az európai vagy észak-amerikai megközelítés.

Összességében a kínai rendészeti MI-alkalmazások a technológiai fejlettség és a közbiztonsági célok szoros összehangolásán alapulnak.

A tapasztalatok azt mutatják, hogy ahol a kormányzat kiemelt stratégiai érdeknek tekinti e rendszerek bevezetését, ott azok alkalmazása rendkívül gyorsan és széles körben valósulhat meg. Ennek azonban szükségszerű következménye, hogy a társadalmi kontroll és az egyéni jogok védelme háttérbe szorul a nyugati demokráciák gyakorlatához képest. A kínai modell ezért alapvetően eltérő megközelítést és sajátos társadalmi kompromisszumokat tükröz. Bár a rendszer számos területen hatékonynak bizonyulhat a bűnüldözésben, működése jelentős alapjogi kockázatokkal is együtt jár. Magyarország számára ezek a tapasztalatok elsősorban figyelmeztetésként értelmezhetők. A kínai példák jól szemléltetik, hogy a rendészeti mesterséges intelligencia komoly hatékonyságnövelő potenciállal rendelkezik. Ugyanakkor azt is világosan mutatják, milyen veszélyeket hordozhat, ha az alkalmazás nem átlátható jogi és etikai keretek között történik. Mindez alátámasztja annak jelentőségét, hogy a hazai gyakorlat kialakítása során a technológiai fejlődés és az alapvető jogok védelme között tartós egyensúly jöjjön létre.

Összehasonlító megállapítások

Mind a négy vizsgált ország tapasztalata azt mutatja, hogy az MI integrációja a rendőrségbe egy *tanulási folyamat*. Az Egyesült Királyság és Franciaország EU-tagállamként igyekszik összhangban maradni az uniós joggal, míg az USA saját útját járja, de ott is erősödőben a szabályozási igény. Közös bennük, hogy a technológiai lehetőségek adottak és vonzóak, a bűnüldöző szervek pedig nyitottak rájuk, ha azok hatékonyságot ígérnek. Ugyancsak közös a konfliktus a polgárjogi szférával: sehol nem fogadják el kritika nélkül a tömeges megfigyelést vagy az automatizált profilalkotást. Ahol nem volt előzetes szabály, ott utólag a bíróságok vagy a törvényhozás lépett közbe (ld. US városok tiltásai, brit bírósági ítélet, francia CNIL fellépések). Kínában a technológiai eszközök alkalmazása is kiemelt politikai cél (például a közbiztonság növelése) – ezzel együtt az állampolgári jogvédők szerint a kínai rendszerben a megfigyelés és az ún. „social credit” kritikus pontokat jelent.

Ami a „sikeres integrációt” illeti – a kérdés, mit tekintünk sikernek. Technikai értelemben a brit rendőrség talán a leginkább integrálta a napi rutinba az MI-t (arcfelismerés és bizonyos analitikák formájában). Franciaország egyelőre inkább eseti jelleggel, nagy eseményekre fókuszálva alkalmazza. Az USA-ban pedig válogatást látunk: van, ahol rutinszerű (pl. New Yorkban a rendszámfelismerő kamerahálózat és a valós idejű központ integráltan működik, Chicagóban a *Strategic Decision Support Centers* része a szoftveres elemzés).

A „siker” másik oldala, a társadalmi elfogadottság, már vegyesebb: ott tekinthető talán valamelyest sikeresnek az integráció, ahol működnek fékek és ellensúlyok, tehát a közvélemény látja, hogy a technológia nem kontrollálatlanul terjed. Ebből a szempontból az EU megközelítése (szigorú alapelvek lefektetése) hosszú távon fenntarthatóbb bizalmat ígér, mint az USA eleinte laissez-faire hozzáállása, amit utólag kellett korrigálni. Kínában a rendőrség igen gyorsan és kiterjedten alkalmazott MI-t, de a „siker” itt elsősorban a központi hatékonyságban mérhető – a lezárt és elszigetelt társadalmi diskurzusban a polgári bizalom kérdése kevésbé jelenik meg. A kínai modell tehát erős eredményeket hozhat a bűnözők azonosításában, miközben az állami ellenőrzés mértéke miatt a nyugati értelemben vett társadalmi elfogadottság nem jut szóhoz.

A nemzetközi példák tanulsága mindenesetre az, hogy az MI rendészeti alkalmazása nem vákuumban történik: az adott ország jogi keretei, intézményi kultúrája és társadalmi értékei meghatározzák, milyen módon lehet integrálni az új eszközöket. E tanulságokkal felvértezve a következő fejezetben Magyarország helyzetét tekintem át: milyen a magyar jogi és intézményi környezet, és hogyan lehet(ett) idehaza megkezdeni az MI-eszközök integrációját a bűnmegelőzésbe.

A magyar jogrend és intézményrendszer helyzete: az MI-eszközök integrációjának lehetőségei és korlátai

Magyarországon a mesterséges intelligencia bűnmegelőzési alkalmazása még kezdeti szakaszban jár, de az utóbbi évek fejleményei azt mutatják, hogy a téma egyre inkább napirendre kerül. A kérdés az, hogyan illeszthetők be ezek az új technológiák a hatályos jogi és intézményi keretekbe. E fejezetben először áttekintem a releváns magyar jogszabályokat és alapelveket, majd a jelenlegi gyakorlatot (vagy annak hiányát), végül azonosítom az integráció fő akadályait és lehetőségeit.

Alkotmányos keretek és alapjogok

A magyar jogrend csúcsán az Alaptörvény (Magyarország Alaptörvénye 2011) biztosítja azokat az alapvető jogokat, amelyek egyben korlátot is szabnak a bűnmegelőzés során bevezethető eszközöknek. Ide tartozik a VI. cikk (1) bekezdése, amely kimondja mindenkinek a magán- és családi élet, otthon, kapcsolattartás és jó hírnév tiszteletben tartásához való jogát – vagyis a *magánszféra védelmét*. Ugyanez a cikk (3) bekezdésében rendelkezik a személyes adatok védelméről.

Ezek az alkotmányos rendelkezések alapvetően *információs önrendelkezési jogként* és a magánélet szférájának sérthetatlenségeként értelmezendők. A gyakorlatban azt jelentik, hogy az állam csak törvény által, a szükségesség-arányosság elvének betartásával avatkozhat be e jogokba – például csak törvényi felhatalmazás alapján figyelheti meg polgárait, és akkor is a lehető legkisebb mértékben. Szintén lényeges az Alaptörvény VIII. cikke, amely a gyülekezési jogot garantálja. Ez kimondja, hogy mindenkinek joga van békésen gyülekezni, és e jog gyakorlását csak nagyon szűk körben lehet korlátozni (pl. a nemzetbiztonság vagy közbiztonság érdekében). Egy olyan intézkedés, amely egy tüntetés résztvevőit tömegesen megfigyeli és azonosítja MI segítségével, felveti e cikk sérelmét is, ahogyan azt a korábbi fejezetekben láttuk a „Pride megfigyelés” kapcsán. Fontos még megemlíteni az Alaptörvény IV. cikkét (szabadsághoz és személyi biztonsághoz való jog, benne az ártatlanság vétele), illetve a XXVIII. cikket (tisztességes eljárásához való jog, nullum crimen elv), amelyek azt húzzák alá, hogy *előre senkiről sem tételezhető fel bűnösség*. Ez összefügg a prediktív algoritmusok problémakörével: ha a hatóság csupán egy MI által generált „kockázati profil” alapján lép fel valakivel szemben, az adott esetben összeütközésbe kerülhet ezen alapelvekkel.

Ágazati törvények – rendőrség, büntetőeljárás, adatvédelem

Az MI-eszközök integrálásának vizsgálatakor kiemelten fontos a rendőrséget szabályozó törvény, a 1994. évi XXXIV. törvény a Rendőrségről (Rtv.). Az Rtv. számos ponton szabályozza a rendőrség adatgyűjtési, megfigyelési jogosítványait. Például rendelkezik arról, hogy a rendőrség közterületen technikai eszközökkel (pl. kamera) megfigyelést folytathat bűnmegelőzési vagy bűnfelderítési céllal, de ennek feltételei vannak. Az Rtv. 42. §-a kimondja, hogy a rendőrség nyilvános helyen technikai megfigyelést végezhet, ha bűncselekmény megelőzése, felderítése indokolja, viszont a felvételek kezelését szigorú adatvédelmi szabályokhoz köti (pl. a felvételeket bizonyos időn túl törölni kell, csak meghatározott célra használhatók). Az MI integrációja itt azt jelentheti, hogy a hagyományos kamera mellé *elemző szoftver* kerül – de jogilag még nincs explicit utalás a „szoftver általi automatikus azonosításra” vagy hasonlóra. A rendőrségi törvény 69. §-a tartalmaz rendelkezéseket a biometrikus adatok (pl. ujjlenyomat, DNS, arckép) nyilvántartásáról: a bűnügyi nyilvántartásban kezelhető gyanúsítottak és elítéltek biometrikus adatai. Ez jogalapot ad a rendőrségnek, hogy egy *bűnügyi arcképfelismerő rendszert* működtessen – ilyen a magyar rendőrség valóban rendelkezik is (a

Nemzeti Szakértői és Kutató Központtal (NSZKK) együttműködésben egy arcfelismerő szoftver segíti a nyomozásokat, amely a bűnügyi nyilvántartó fotóit használja referencia-adatbázisként). Ez eddig főként *utólagos* azonosításra szolgált: ha van egy bűncselekményről felvétel, a rendszer megpróbálja kikeresni, hogy a képen látható személy szerepel-e a nyilvántartásban. 2023-2024. során azonban a jogi környezetben változás történt Magyarországon, ami lehetővé tette e rendszer *közel valós idejű* alkalmazását is demonstrációk résztvevőinek azonosítására – erre hamarosan visszatérek.

Az adatvédelemmel kapcsolatban ki kell emelni a 2011. évi CXII. törvényt (Infótörvény), amely a GDPR hazai átültetését és a nemzeti specifikumokat tartalmazza. Az Infótörvény hatálya kiterjed a rendőrségi adatkezelésre is, amennyiben arra nem a külön 2018. évi XXX. törvény (a bűnüldözési célú adatkezelésről, az EU 2016/680 irányelv implementálása) vonatkozik. E jogszabályok kimondják, hogy a személyes adatok (pl. biometrikus adatok is) kezelésének jogalapja lehet *közhatalmi jogosítvány gyakorlása*, ha azt törvény felhatalmazza. Az arcfelismerésre például a felhatalmazást a rendőrségi törvényben és a szabálysértési törvényben kellett megteremteni. Itt érünk el a 2025-ös tavaszi jogszabályi változásokhoz.

Az ún. „Pride-törvény” és a biometrikus megfigyelés kibővítése

2025 tavaszán az Országgyűlés rövid idő alatt több törvénymódosítást fogadott el, amelyekről a kormányzati kommunikáció elsősorban a Pride-rendezvények korlátozásának szándékát hangsúlyozta. A módosítások 2025. április 15-én léptek hatályba, és többek között a szabálysértési, valamint a gyülekezési jog területét érintették. A változtatások egyik központi eleme az volt, hogy a rendőrség számára tágabb jogi lehetőség nyílt biometrikus technológiák alkalmazására bizonyos közterületi eseményekkel összefüggésben. Egyes jogértelmezések szerint ez a gyakorlat akár békés demonstrációk résztvevőinek azonosítására is kiterjedhet, ami érdemi elmozdulást jelent a korábbi, szűkebb alkalmazási körhöz képest. Korábban az ilyen eszközök használata elsősorban súlyos bűncselekmények megelőzéséhez vagy felderítéséhez kapcsolódott. Az új szabályozás viszont lehetőséget teremthet arra is, hogy kisebb súlyú jogsértések esetén alkalmazzák a technológiát, például *utólag* jogellenesnek minősített rendezvények résztvevőinek azonosítása céljából.

A módosítások elfogadását követően több civil jogvédő szervezet, köztük a Társaság a Szabadságjogokért, jogi elemzésekben fejezte ki aggályait. Álláspontjuk szerint az új szabályozás egyes elemei ellentétbe kerülhetnek az Európai Unió mesterséges intelligenciáról szóló rendeletével, valamint az uniós alapjogi követelményekkel. Az uniós AI-rendelet 5. cikke főszabály szerint tiltja a valós idejű távoli biometrikus azonosítást nyilvános helyeken, és csak kivételes esetekben enged eltérést. A békés gyülekezések résztvevőinek tömeges azonosítása jellemzően nem tartozik ezen kivételek közé. Amennyiben a hazai gyakorlat a helyszínen, közel valós időben történő azonosítást tesz lehetővé, az jogilag a valós idejű biometrikus megfigyelés kategóriájába sorolható. A kérdés uniós szinten is visszhangot váltott ki. Több európai politikai és jogi szereplő nyilvánosan jogi aggályokat fogalmazott meg a magyar szabályozás uniós joggal való összhangját illetően. Az European Commission szintén jelezte, hogy vizsgálni kívánja a módosítások megfelelőségét, különös tekintettel a technológia alkalmazásának módjára és időbeliségére. A magyar kormány ezzel szemben azt hangsúlyozta, hogy álláspontja szerint a módosítások összhangban állnak az alkotmányos és uniós előírásokkal. A kialakult helyzet ugyanakkor jelentős jogértelmezési bizonytalanságokat hordoz, amelyek hosszabb távon akár uniós jogvitákhoz is vezethetnek. A kialakult jogi konfliktus egyelőre rendezetlen, és nem zárható ki, hogy végső soron az Európai Unió Bíróságának kell majd állást foglalnia a kérdésben, különösen akkor, ha az Európai Bizottság kötelezettségszegési eljárást indít Magyarországgal szemben.

A Pride-törvény esete egyfelől azt illusztrálja, hogy a magyar jogalkotó nyitott az MI-eszközök engedélyezésében, másfelől rámutat arra, milyen kihívások merülnek fel a *jogállamisági és alapjogi* szempontok érvényesítése terén. E lépéssel Magyarország részben eltér a nyugat-európai gyakorlattól – ahol óvatosabb megközelítés érvényesül az ilyen technológiák használatával kapcsolatban. A jelenlegi hazai jogi környezet formálisan lehetőséget biztosít bizonyos biometrikus technológiák alkalmazására, azonban az uniós AI-rendelet teljes körű hatálybalépését követően e gyakorlat jogszerűsége egyre inkább vitatottá válhat. A magyar szabályozási környezet ezért jelenleg átmeneti és alakulóban lévő állapotban van. Az uniós rendelet és a hazai joggyakorlat közötti összhang végleges formája a következő időszakban válhat egyértelművé.

A kutatás empirikus vizsgálatának eredményei: belső rendőrségi tapasztalatok és szakértői vélemények

A tanulmány empirikus része célzott adatfelvételre épül, amelynek célja annak feltárása volt, hogy Magyarországon, a mindennapi rendészeti gyakorlat szintjén, milyen szerepet tölt be jelenleg a mesterséges intelligencia a bűnmegelőzésben és a bűnüldözésben. Az adatgyűjtés nem egy technológiai „leltár” összeállítására irányult, hanem arra, hogy feltérképezze, miként értékelik a lehetőségeket és a kockázatokat azok a szakemberek, akik vezetői, nyomozói, informatikai vagy adatvédelmi szerepkörben közvetlen kapcsolatban állnak a rendszerek működtetésével. Ennek megfelelően a kutatás elsősorban kvalitatív jellegű volt. Célja az volt, hogy részletes, belső tapasztalatokon alapuló képet adjon a rendőrségi gyakorlatról, nem pedig statisztikailag reprezentatív eredményeket mutasson be.

Az empirikus vizsgálat alapját a rendőrségen belül, illetve a rendőrségi működéshez kapcsolódó szakértők körében felvett kérdőívek képezték. Összesen huszonöt kitöltött kérdőív került feldolgozásra, amelyek a következő csoportokból származtak: rendőrségi vezetők és szakemberek (9 fő), nyomozók és operatív munkakörben dolgozók (9 fő), informatikai szakértők (6 fő), valamint adatvédelmi és civil területről érkező szakértő (1 fő). A válaszadók jellemzően saját szakmai szerepükből kiindulva fogalmazták meg tapasztalataikat és véleményüket. A kutatás során – az anonimitás és a személyes biztonság biztosítása érdekében – az elemzés kizárólag szerepkörök szerinti bontásban történt, egyéni azonosításra alkalmas adatok felhasználása nélkül.

A célzott adatfelvétel keretei és korlátai

A kutatás egyik legnagyobb erőssége, hogy több, egymástól szakmailag eltérő nézőpontot fog össze egyetlen elemzésben. A vezetői elvárások, a mindennapi operatív tapasztalatok, az informatikai fejlesztési és üzemeltetési szempontok, valamint az adatvédelmi megfontolások ugyanarra a kérdéskörre reflektálnak, mégis eltérő hangsúlyokkal. Már önmagában is sokatmondó, hogy ugyanaz a téma – például az, hogy jelen van-e a mesterséges intelligencia a napi munkában – a különböző szerepkörökben egészen másként jelenik meg. Ez nem ellentmondásként értelmezhető, hanem inkább azt jelzi, hogy az új technológiák bevezetése a szervezeten belül széttagolt módon zajlik: nem minden területen egyszerre, és nem azonos intenzitással.

A kutatás korlátja ugyanakkor abból fakad, hogy a kérdőíves válaszok elsősorban a kitöltők saját tapasztalatait és rálátását tükrözik.

Több vezetői és nyomozói válaszban is megjelent az a megjegyzés, hogy „nincs információ” vagy „nem használom” az adott eszközt. Ez egyrészt utalhat arra, hogy az adott területen valóban nincs még érdemi MI-alapú alkalmazás, másrészt arra is, hogy a fejlesztések, kísérleti projektek és technológiai újítások belső kommunikációja nem mindig átlátható és egységes. Ennek megfelelően a fejezet megállapításai nem egy átfogó, országos helyzetképet kívánnak felrajzolni, hanem a válaszadók által jelzett tapasztalatok és mintázatok bemutatására törekednek.

A rendőrségi MI-használat jelenlegi képe a kérdőívek alapján

A kérdőívek válaszai alapján egyértelműen kirajzolódik, hogy a rendőrségen belül jelenleg nem zajlik önálló, emberi beavatkozás nélküli MI-alapú döntéshozatal. A mesterséges intelligenciát a megkérdezettek túlnyomó többsége nem „robotrendőrként”, hanem elsősorban támogató eszközként értelmezi, amely megkönnyíti az adatfeldolgozást, segíti az eligazodást az információk között, illetve csökkenti az adminisztratív terheket.

A vezetői válaszok ezt következetesen megerősítik: többen hangsúlyozták, hogy az MI szerepe kizárólag kiegészítő jellegű lehet, és a szakmai, illetve jogi felelősség továbbra is az intézkedő rendőröknél marad. Egyik vezető sem tartotta elfogadhatónak, hogy a technológia önállóan határozzon meg rendészeti lépéseket. A nyomozói válaszok ennél sokszor még direkter formában fogalmaztak: több kitöltő egyértelműen rögzítette, hogy az MI csak ellenőrzött környezetben alkalmazható, és a döntéseknek „emberi szinten” kell megszületniük.

A vezetői válaszok tematikus mintázatai: motivációk, pilotok, kommunikáció

A rendőrségi vezetők által kitöltött kérdőívek alapján az MI alkalmazásának motivációja viszonylag egységes képet mutat. A válaszadók elsősorban abban látják a technológia jelentőségét, hogy egyes, időigényes és ismétlődő munkafolyamatok automatizálásával tehermentesíti az állományt, és így több kapacitás marad az érdemi rendészeti feladatokra. Többen hangsúlyozták, hogy az MI nem önmagáért való innováció, hanem eszköz a hatékonyabb szervezeti működéshez. Ez a szemlélet összhangban van azzal a törekvéssel, hogy a digitális fejlesztések elsősorban a mindennapi munka gyakorlati támogatását szolgálják.

A pilotprojektekre vonatkozó válaszok alapján a vezetői szinten elsősorban olyan kísérleti megoldások jelentek meg, amelyek döntés-előkészítő vagy elemző

funkciót látnak el. Leggyakrabban az intelligens térképi elemző modul került említésre, amely a bűncselekmények és rendbontások térbeli mintázatait elemzi, és úgynevezett „forrópontokat” jelöl ki. Emellett több válaszadó számolt be adminisztratív célú szövegfeldolgozó rendszerek teszteléséről is, különösen jegyzőkönyvek és jelentések előkészítésének támogatására. Ezek a példák arra utalnak, hogy a pilotok első hulláma elsősorban alacsonyabb kockázatú, támogató jellegű területeken indult el.

A konkrét eredményeket illetően a vezetők visszafogott, de alapvetően pozitív képet rajzolnak. Több válasz szerint a térképi elemző rendszer már rövid távon is hasznos információkkal szolgált, például bizonyos rendbontási gócpontok előrejelzésében. Ugyanakkor ezek az eredmények jellemzően még nem intézményesített értékelési rendszeren alapulnak, hanem inkább tapasztalati visszajelzések formájában jelennek meg. Ez arra utal, hogy a hatékonyság mérésének módszertana egyelőre nem kiforrott.

Az erőforrásokkal kapcsolatban a vezetői válaszok egyaránt említik a technikai és humán feltételek fontosságát. Kiemelt szerepet kap a megfelelő adatkezelési kapacitás, a stabil informatikai infrastruktúra, valamint a képzett elemzők és informatikusok jelenléte. Többen úgy fogalmaztak, hogy ezek az alapfeltételek részben már adóttak, ugyanakkor hosszabb távon további fejlesztésekre és beruházásokra lesz szükség. Ez különösen igaz a nagyobb adatmennyiségek feldolgozására és az összetettebb MI-modellek üzemeltetésére.

A képzés és kompetenciafejlesztés területén a vezetői válaszok viszonylag tudatos megközelítést tükröznek. Több kitöltő számolt be tematikus belső képzésekről, amelyekben külön hangsúlyt kap az etikus és jogszertű MI-használat. Ugyanakkor az is érzékelhető, hogy ezek a képzések nem minden szervezeti egységben azonos intenzitással jelennek meg, és jelenleg inkább részmegoldásokként működnek, semmint egységes, országos rendszerként. A technológiával szembeni esetleges bizalmatlanság kezelésében a vezetők elsősorban a belső kommunikációt tartják kulcsfontosságúnak. Több válasz hangsúlyozza, hogy a kollégák számára érthetővé kell tenni a rendszerek működését, korlátait és céljait, valamint lehetőséget kell biztosítani számukra a visszajelzésre. Ez a megközelítés arra utal, hogy a vezetés tisztában van azzal: az MI elfogadottsága nem pusztán technikai, hanem szervezeti és pszichológiai kérdés is.

Az adatvédelmi és etikai dimenzió a vezetői válaszokban rendszeres ellenőrzésekhez és külső szakértők bevonásához kapcsolódik.

A kitöltők többsége úgy látja, hogy az MI-rendszerek bevezetése csak akkor tartható fenn hosszú távon, ha azok folyamatos jogi és etikai kontroll alatt állnak. Ez a szemlélet összhangban van azzal a törekvéssel, hogy az innováció ne veszélyeztesse a rendőrség társadalmi legitimációját. A nyilvánosság felé irányuló kommunikációban a válaszadók elsősorban a „felelős technológiahasználat” hangsúlyozását tartják fontosnak. Többen kiemelték, hogy kerülni kell a túlzó ígéretek, és világossá kell tenni, hogy az MI nem helyettesíti a rendőri munkát, hanem annak támogatását szolgálja. Ugyanakkor nem minden válaszadó rendelkezett pontos információval az intézményi szintű kommunikációs stratégiáról, ami arra utal, hogy ezen a területen még van tér a tudatosabb szervezésre.

A hosszú távú fejlesztési tervekben a vezetői válaszok egy moduláris, rugalmasan bővíthető MI-ökoszisztéma irányába mutatnak. A cél egy olyan rendszer kialakítása, amely alkalmazkodni tud a változó rendészeti igényekhez, és fokozatosan, kockázatarányos módon épül be a működésbe. Összességében a vezetői kérdőívek azt jelzik, hogy a döntéshozói szinten megvan az innováció iránti nyitottság, ugyanakkor ezt óvatos, lépésről lépésre haladó megközelítés jellemzi, amelyben a hatékonyság, a jogszerűség és a szervezeti bizalom egyszerre jelenik meg szempontként.

Operatív tapasztalatok: nyomozói és végrehajtói nézőpontok

A nyomozói kérdőívek összképe alapján a mesterséges intelligencia használata a mindennapi terepmunkában jelenleg még nem tekinthető általánosnak. A válaszadók jelentős része egyértelműen úgy nyilatkozott, hogy rendszeresen nem alkalmaz ilyen eszközöket, és többen azt is jelezték, hogy nincs kialakult módszerük az esetleges MI-alapú megoldások hatékonyságának mérésére. Ennek oka részben az, hogy ezek az eszközök sok helyen még nem érhetőek el, részben pedig az, hogy a használatukhoz nem kapcsolódik intézményi értékelési rendszer.

Ugyanakkor két visszatérő szempont szinte minden kérdőívben megjelent. Az egyik az átláthatóság iránti igény: sok nyomozó számára alapvető fontosságú, hogy pontosan értse, mit és hogyan „számol ki” egy rendszer. A másik a bizonytalanság, amely abból fakad, hogy a felhasználók gyakran maguk sem tudják egyértelműen megítélni, egy adott szoftver valóban mesterséges intelligenciát alkalmaz-e, vagy csupán hagyományos automatizmusokra épül.

Amikor a válaszadók konkrét felhasználási területeket neveznek meg, ezek jellemzően az adminisztratív és elemző feladatok köréből kerülnek ki.

Ilyen például a jelentések és összefoglalók készítése, az iratjegyzékek összeállítása, a statisztikai adatok feldolgozásának támogatása, a mintázatok keresése vagy a hanganyagok leiratozása. A válaszokból kirajzolódó kép ebben a tekintetben jól illeszkedik az informatikai és vezetői elképzelésekhez: az MI-t elsősorban ott tartanák hasznosnak, ahol nagy mennyiségű szöveges és ismétlődő adminisztratív munka terheli az állományt, és ahol a humán kapacitás felszabadítása valódi gyakorlati előnyt jelenthet.

Külön figyelmet érdemel egy olyan válasz, amely egy konkrét alkalmazási példát is bemutat. Egy nyomozó beszámolója szerint gyermekpornográfiával kapcsolatos ügyekben lefoglalt felvételek előszűrésére már használtak MI-alapú eszközt, amely érzékelhetően gyorsította a munkafolyamatot. Ugyanakkor ebben az esetben is megjelentek minőségi problémák – például a leiratozás pontatlansága vagy rendezetlensége –, valamint az a körülmény, hogy a hatékonyság megítélése nem intézményi mutatók, hanem személyes tapasztalat alapján történt. Ez az egyedi példa jól mutatja, hogy szűk, jól körülhatárolt területeken már megjelent az MI-támogatás, miközben a minőségbiztosítás és a kockázatkezelés még nem épült be rendszerszinten.

A nyomozói állomány technológiához való viszonya összességében kifejezetten sokszínű képet mutat. Egyes válaszadók pragmatikus módon elsősorban az infrastrukturális feltételek hiányát emelik ki, mások a döntések objektív megalapozásának lehetőségét hangsúlyozzák („objektív adatokra van szükség”). Ugyanakkor olyan vélemények is megjelennek, amelyek már alapvetően elutasító jellegűek („veszélyes”, „nem kellene használni”), és kifejezetten veszélyesnek tartják az MI szélesebb körű alkalmazását. Ez a véleménybeli sokféleség arra utal, hogy a mesterséges intelligencia rendészeti bevezetése nem pusztán technikai kérdés, hanem szorosan összefügg a szervezeti kultúrával, a bizalommal és a szakmai identitással is.

Belső rendőrségi tapasztalatok: a fejlesztői–üzemeltetői perspektíva

Az informatikai területen dolgozó válaszadók összességében úgy jellemzik a jelenlegi helyzetet, mint egy előkészített, de még nem teljesen kiforrott állapotot. A mesterséges intelligencia alkalmazása jelenleg elsősorban fejlesztési és kísérleti környezetben jelenik meg: ilyen például a szöveges és dokumentumalapú anyagok feldolgozása, hangfelvételek elemzése, automatikus összefoglalók készítése, illetve különféle adatkinyerési megoldások tesztelése. Ezek a megoldások jellemzően még nem a napi működés részét képezik, inkább próbajellegű fejlesztések formájában vannak jelen.

Több válaszadó hangsúlyozta azt is, hogy jelenleg a rendőrség nem futtat mesterséges intelligenciát közvetlenül a saját, teljes körű adatállományán. Ugyanakkor már megkezdődtek azok az előkészítő folyamatok, amelyek ezt a jövőben lehetővé tehetik: ilyen az adatok tisztítása, strukturálása, egységesítése, valamint az adatminőség javítása. Ezek a háttér munkák kevésbé látványosak, de a későbbi MI-használat szempontjából meghatározó jelentőségűek.

A fejlesztések bevezetését a válaszok nem egyetlen nagy, központi rendszer megjelenéseként írják le, hanem fokozatos, szerkezeti és folyamatok átalakításaként. Ennek része az egységesebb adatkezelés kialakítása, az API-alapú (Application Programming Interface: alkalmazásprogramozási interfész) kapcsolatok fejlesztése, az ügykezelési rendszerek MI-kompatibilissé tétele, valamint a tesztelést lehetővé tevő, úgynevezett *sandbox* környezetek³ létrehozása. Ezek célja, hogy az új megoldásokat biztonságos környezetben lehessen kipróbálni, mielőtt éles működésbe kerülnének.

A válaszokban visszatérő elem a kapacitáshiány kérdése is. Többen jelezték, hogy az informatikai erőforrások jelenleg több feladat között oszlanak meg, és az MI-fejlesztések csak az aktuális prioritások függvényében kapnak hangsúlyt. Több kitöltő szerint hosszabb távon elkerülhetetlenné válik külön, erre specializálódott szakemberek vagy dedikált fejlesztői csoportok kialakítása, mert a jelenlegi struktúra csak korlátozott mértékben alkalmas összetettebb MI-rendszerek fenntartására.

A kockázatkezelés területén az informatikai válaszok különösen következetesek és szigorúak. Gyakran megjelenik az *on-premise*⁴ működés iránti igény, a többszintű jogosultságkezelés, a részletes naplózás, az auditálható frissítési folyamatok, valamint a kormányzati hálózati környezethez igazodó biztonsági elvárások hangsúlyozása. Több válaszadó egyértelműen kijelenti, hogy a rendészeti alkalmazások esetében az átláthatatlan, „*black box*”⁵ jellegű megoldások nem elfogadhatók.

Emellett többen kiemelik, hogy a gyakorlatban rendkívül magas pontossági és megbízhatósági elvárások érvényesülnek, helyenként szinte hibamentes működést várnak el a rendszerektől. Ez a hozzáállás nem technológiai túlzásként jelenik meg a válaszokban, hanem a rendészeti felelősség természetes következményeként: egy téves riasztás, hibás elemzés vagy félrevezető döntéstámogatás ebben a környezetben közvetlen jogi, szakmai és társadalmi

következményekkel járhat. Ennek megfelelően az informatikai oldal elsődleges célja nem az innováció gyorsítása, hanem a biztonságos, ellenőrizhető és stabil működés megteremtése.

Adatvédelmi és civil nézőpont: kockázatok, audit, központi keretrendszer

Az adatvédelmi és civil kérdőív válaszai alapján jól látható, hogy a jelenlegi rendészeti gyakorlat még nem alkalmazkodott teljes mértékben az új uniós és hazai MI-szabályozáshoz. A mindennapi működésben gyakran nem egyértelmű, hogy egy adott technológia pontosan milyen jogi megítélés alá esik, és milyen eljárási kötelezettségek kapcsolódnak hozzá. A válaszadó szerint a szervezetek még tanulási szakaszban vannak ezen a téren.

A kérdőív hangsúlyozza azt is, hogy a rendőrségi adatvagyon kezelése új szemléletet igényel. Az adatok egyre inkább stratégiai értékűként jelennek meg, ami fokozott felelősséget ró az intézményekre, mind jogi, mind szervezeti szempontból. Kockázatként három terület emelkedik ki. Az első az MI-rendszerek pontatlansága vagy „*hallucinációja*”, amely rendészeti környezetben súlyos eljárási következményekkel járhat. A második a nem engedélyezett, ellenőrizetlen eszközhasználat (*Shadow AI*), amely adatbiztonsági veszélyt jelent. A harmadik az *átláthatóság* kérdése: az információk megosztása önmagában is új kockázatokat teremthet, ha nem megfelelően szabályozott. A válaszadó egyértelműen szükségesnek tartja a *független szakmai auditok* rendszeres alkalmazását, valamint egy központi, *minisztériumi szintű keretrendszer* kialakítását. Ez biztosíthatná az egységes eljárásrendet és a jogszerű működést az egész rendészeti szférában. Fontos elemként jelenik meg a *civil szervezetek* bevonásának igénye is. A válasz szerint a jogvédő és felhasználói szempontok korai figyelembevétele hozzájárulhat a társadalmi bizalom fenntartásához és a későbbi konfliktusok megelőzéséhez.

Összességében az adatvédelmi és civil nézőpont arra mutat rá, hogy a rendészeti MI-használat csak akkor lehet hosszú távon fenntartható, ha azt világos jogi keretek, független ellenőrzés és tudatos intézményi felelősségvállalás kíséri.

³ A *sandbox* (homokozó) az informatikai biztonság területén programok elkülönített futtatására szolgáló biztonsági mechanizmus

⁴ *On-premise* működés: helyi vagy helyszíni telepítésű informatikai infrastruktúra

⁵ A *black box* (feketedoboz) kifejezésnek több jelentése is van a kontextustól függően, de mindegyik arra utal, hogy egy rendszer belső működése rejtve marad, és csak a bemenetre (input) és kimenetre (output) fókuszálunk

Következtetések: a kérdőíves kutatás eredményeiről

A kérdőíves válaszok összegzése alapján az rajzolódik ki, hogy a rendőrségi mesterségesintelligencia-használat Magyarországon jelenleg inkább egy formálódó, kísérleti szakaszban van, semmint egy kiforrott, stabilan működő rendszer része. A vezetői és informatikai területen dolgozó válaszadók körében egyértelműen megjelenik a nyitottság az olyan megoldások iránt, amelyek csökkentik az adminisztratív terheket és támogatják a döntéshozatalt. Ezzel szemben a nyomozói válaszok jelentős része még mindig arról tanúskodik, hogy a mindennapi munkában az MI-használat alig jelenik meg, és több esetben bizalmatlanság is érzékelhető a technológiával szemben. Ez az eltérés jól illeszkedik egy tipikus átmeneti időszak képéhez: a fejlesztési és stratégiai elképzelések sok esetben előrébb járnak, mint a gyakorlati alkalmazás, miközben a szervezeten belüli bizalom és rutin még nem tudott lépést tartani az innováció ütemével.

A kérdőíves anyagból egyértelműen kirajzolódik, hogy a sikeres és fenntartható bevezetéshez több, egymásra épülő feltétel együttes teljesülése szükséges:

- szabályozási és felelősségi keret (mit lehet, milyen célból, milyen kontrollok mellett alkalmazni)
- biztonságos technológiai környezet (különösen az ON-PREM működés és a jogosultságkezelés fontossága)
- minőségbiztosítás és audit (a „black box” megoldások elutasítása, folyamatos tesztelés, naplózás és ellenőrizhetőség)
- kompetencia és belső kultúra fejlesztése (képzések, gyakorlati útmutatók, a Shadow AI kockázatainak kezelése)
- óvatos, átlátható bevezetés (pilotprojektek alkalmazása, a lakossági bizalom megőrzése).

Összességében a válaszok arra utalnak, hogy a rendőrségi MI-integráció nem egyetlen döntés eredménye, hanem hosszabb, fokozatos intézményi folyamat. Számos kisebb lépés, kísérlet, visszacsatolás és korrekció szükséges ahhoz, hogy a technológia valóban beépüljön a mindennapi működésbe. A technológiai lehetőségek vonzereje – a gyorsabb elemzés, a hatékonyabb adatkezelés és a kapacitások felszabadítása – a válaszokban világosan megjelenik. Ugyanakkor ezzel párhuzamosan ugyanolyan hangsúlyt kapnak a rendészeti munka sajátosságai is: a tévedés kockázata, a felelősség személyes jellege, a magas biztonsági elvárások, valamint a társadalmi bizalom megőrzésének kényszere.

Hosszabb távon, éppen e tényezők egyensúlya fogja meghatározni, hogy a mesterséges intelligencia a magyar rendészetben valódi, stabil döntéstámogató eszközzé válik-e, vagy továbbra is elszigetelt kísérletek és eseti megoldások szintjén marad meg.

Szabálysértési eljárások és arcképelemzés a magyar rendészetben

A szabálysértési terület külön tárgyalása azért indokolt, mert ezen a ponton válik igazán láthatóvá, miként alakul át egy eredetileg eseti jelleggel alkalmazott nyomozati technológia fokozatosan mindennapi, rutinszerű azonosítási eszközzé. Míg más eljárástípusokban az arcképelemzés jellemzően kivételes megoldás marad, a szabálysértési ügyek magas száma miatt itt már tömeges igénybevételről beszélhetünk.

Ebben a környezetben különös jelentőséget kapnak azok a garanciális elemek, amelyek a kutatás korábbi szakaszaiban is hangsúlyosan megjelentek: a humán kontroll fenntartása, az átláthatatlan „black box” megoldások elutasítása, valamint a biztonságos és ellenőrizhető üzemeltetés követelménye. A szabálysértési eljárások volumenéből fakadóan ugyanis nem csupán elvi kérdés, hanem gyakorlati jelentőségű tényezővé válik, hogy a rendszer milyen feltételek mellett működik, milyen mértékben támaszkodik szakértői értékelésre, és milyen arányban képes valóban használható, megbízható találatokat biztosítani.

A szabálysértési alkalmazás így jól szemlélteti azt az átmeneti állapotot, amelyben a technológiai hatékonyság iránti igény és az alapjogi, valamint szakmai garanciák iránti elvárás egyszerre van jelen. Ebben a szegmensben különösen élesen kirajzolódik, hogy az arcképelemzés hosszú távú elfogadhatósága nem pusztán technikai kérdés, hanem intézményi, jogi és bizalmi tényezők összjátékának eredménye.

Szabályozási háttér és a kiterjesztés üteme

A magyar állóképes arcképelemzés jogi keretét alapvetően a 2015. évi CLXXXVIII. törvény adja, amely meghatározza az arcképelemző nyilvántartás, az arcképelemző rendszer és az igénybevételre jogosult szervek rendjét. A részletszabályokat a miniszteri rendeleti szint (különösen a működtetés és igénybevétel feltételei) bontja ki, és a rendszer a gyakorlatban szerződéses és informatikai együttműködési láncan keresztül működik.

A szabálysértések irányába történő kiterjesztésnek két jól azonosítható lépcsője volt. Elsőként a 2024. évi XXV. törvény a 2015. évi CLXXXVIII. törvényt úgy módosította, hogy az arckép-profil nyilvántartás céljai közé bekerültek a szabálysértési elzárással is büntethető szabálysértések, és ezzel összefüggésben a bíróság/előkészítő eljárást lefolytató szerv jogosultsága is megjelent az arcképelemző tevékenység igénybevételére. A második lépcsőben a 2025. évi III. törvény már általánosabban, „minden szabálysértésre” kiterjesztette a célmeghatározást és az igénybevételi jogosultságot.

A jogszabályi változások a rendőrségi belső szabályozásban is leképződtek. A sajtóban is visszhangot kapott, hogy a rendőrségi utasítások szintjén 2025. május közepén olyan módosítás történt, amely a szabálysértési eljárások körében már nem csak az elzárással fenyegetett esetekre szorította az arcképelemző rendszer igénybevételét.

Az Állóképes Arckép Azonosító Rendszer működése és a szakértői kontroll

A szabálysértési ügyeknél döntő jelentőségű, hogy a hazai rendszer nem „automatikus döntést” hoz, hanem egy többlépcsős, humán kontrollal átszőtt eljárásrendben működik. Az Állóképes Arckép Azonosító Rendszer (ÁAAR) 2016-ban indult, majd 2017-től az NSZKK feladatkörébe került; a mozgóképes azonosítás ezzel szemben a Nemzetbiztonsági Szakszolgálathoz kapcsolódik. Az NSZKK-n belül az Arcképfelismerő Elemző Osztály a törvényi keretek között „szaktanácsadói” szerepben jár el: informatikai összehasonlítást és szakértői kiértékelést kombinál.

A gyakorlatban a megkeresés zárt csatornán érkezik (például az IPL vagy a RobotZsaru Neo útján), és az eljárás egyik lényegi eleme az anonimizálás: a kérelem és az arcképmás nyilvántartási szinten nem „névhez kötött”, a szakterület deklaráltan nem személyazonosító adatot kezel, hanem azonosításra alkalmas technikai hivatkozást ad vissza. A folyamatban a szoftver kandidátusi listát generál, de a tényleges szakmai értékelés két egymástól független elemzőn keresztül történik, majd egy további kontroll után kerül visszaadásra a találat (technikai kapcsoló szám formájában). A „szakértői komponens” tehát nem díszítő elem, hanem a rendszer egyik tartópillére: épp ez az, ami a szabálysértési alkalmazhatóságot jogilag és szakmailag is értelmezhetőbbé teszi. A tevékenység minőségbiztosított (ISO 9001:2015), 0–24 órában elérhetővé vált, és akkreditációs folyamat is fut.

Statisztikai kép a szabálysértési ügyekben

A szabálysértési kiterjesztés egyik legfontosabb következménye, hogy a rendszer használata itt már nem „ritka kivétel”, hanem mérhető volumenű gyakorlat. Az NSZKK által készített, kifejezetten a szabálysértési célhoz kapcsolt egyszerűsített kimutatás szerint 2024. július 1. és 2024. december 31. között összesen 1352 kérelem érkezett (havi bontásban: 113–297 közötti értékekkel).

A rendelkezésre álló, összesített rendőrségi adatok (amelyek külön bontásban tartalmazzák a kezdeményezett beazonosítások számát és az eredményességi mutatókat is) a korábban ismert számokhoz képest magasabb igénybevételi szintet jeleznek. Eszerint 2024. második félévében 1700 feletti kezdeményezés történt elzárással sújtható szabálysértésekben, és 900 feletti esetben volt eredményes a beazonosítás; 2025. első félévében pedig 2900 feletti kezdeményezés és 1650 feletti eredményes beazonosítás szerepel. (A „több mint” jelleg miatt ezek minimumértékek; alsó becsléssel számolva az eredményességi arány 2024. II. félévben legalább ~53%, 2025. I. félévben legalább ~57%.)

A két adatsor összevetése jól mutatja, hogy ezek érdemben kiegészítik egymást: a 2024. július–decemberi 1352-es adat jól mutatja a szabálysértési ág gyors megerősödését a kiterjesztést követően, míg a rendőrségi összesítés a kezdeményezések és az eredményes találatok arányát teszi láthatóvá. A statisztikai következtetések szempontjából azonban fontos rögzíteni, hogy a különböző kimutatások eltérő módszertant (szűrést, definíciót, időmetszetet) követhetnek, ezért a dolgozatban célszerű feltüntetni, hogy mely számok milyen adatforrásból és milyen célú összesítésből származnak.

Mit jelentett a 2025-ös kiterjesztés a gyakorlatban

A 2024-es jogszabályi lépcső – amely az elzárással fenyegetett szabálysértések körét vonta be – még viszonylag jól körülhatárolt ügycsoportot érintett. Ezekben az esetekben a jogalkotói megközelítés a szükségesség és arányosság szempontjából könnyebben igazolható volt, hiszen a kiszabható jogkövetkezmények súlyosabbak. A 2025-ös kiterjesztés ezzel szemben már azt eredményezte, hogy az arcképelemzés elvileg kisebb súlyú szabálysértések esetében is alkalmazhatóvá vált. Ez a változás nemcsak az ügyforgalom növekedését vetíti előre, hanem az intézményi kockázatkezelés szempontjából is új helyzetet teremt: ugyanazt az eszközt eltérő társadalmi és alapjogi környezetben kezdik el használni.

A gyakorlati működés felől nézve a kiterjesztésnek egy kevésbé látványos, ugyanakkor rendkívül jelentős „közigazgatási” dimenziója is van. Amennyiben az arcképlelemzés a szabálysértési előkészítő eljárásban bizonyítási eszközzé válik, úgy az a rendőrség és az eljáró hatóságok számára nem rendkívüli megoldásként, hanem a mindennapi eljárásrend részeként épülhet be. Ez rövid távon hozzájárulhat a felderítési hatékonyság növeléséhez – különösen tömegesen elkövetett, kamerával dokumentált jogsértések esetében –, középtávon azonban csak akkor maradhat fenntartható, ha világos belső kritériumok rögzítik, milyen esetekben indokolt az arcképlelemzés alkalmazása, és mikor nem.

Garanciák és a szakértői szerep jelentősége

A szabálysértési alkalmazás egyik legfontosabb jelenlegi „védőkorlátja” a szakértői közreműködés ténye. A rendszer szoftveres jelzése önmagában nem jelent azonosítást: a több szereplős kontrollmechanizmus – két egymástól független elemző és egy további ellenőrzési szint – eleve csökkenti annak kockázatát, hogy egy automatizmus „vakon”, emberi mérlegelés nélkül váljon döntéssé. Ez a garanciarendszer ugyanakkor csak akkor maradhat hosszú távon is védhető, ha az igénybevétel tömegesedése nem gyengíti el a szakértői kontroll tényleges működését, vagyis, ha a kapacitás, a minőségbiztosítás és az auditálhatóság képes lépést tartani a növekvő volumennel.

A fejezet elején bemutatott empirikus tapasztalatok ezen a ponton is visszaigazolódnak. A szabálysértési kör kiterjesztésével párhuzamosan különösen felértékelődik a világos szabályozási és felelősségi keret, a biztonságos technológiai környezet, valamint a minőségbiztosítás és a megfelelő szakmai kompetencia szerepe. Ezek hiányában az arcképlelemzés könnyen pusztán „technikai rutinná” alakulhat, miközben a jogi és társadalmi következményeket a rendszer már csak utólag, korrekciós jelleggel próbálja kezelni.

Összegző megállapítások

A szabálysértési terület különösen jól érzékelteti az MI-jellegű (vagy MI-hatású) rendszerek rendészeti bevezetésének alapvető dilemmáját. Miközben a technológia egyre könnyebben hozzáférhetővé válik, és használata mindennapibbá lesz, ezzel párhuzamosan folyamatosan erősíteni kellene a jogállami garanciákat is. A 2024–2025-ös kiterjesztés nyomán a hazai gyakorlat már nem pusztán elméleti lehetőségként jelenik meg, hanem statisztikailag is kimutatható, növekvő intézményi gyakorlatként.

A kérdőíves és belső adatok alapján egyértelműen látható, hogy ebben a folyamatban továbbra is meghatározó szerepe van a szakértői közreműködésnek.

Az arcképlelemzés nem önálló döntéshozó eszközként működik, hanem olyan döntés-előkészítő mechanizmusként, amelyben a humán értékelés és a többlépcsős ellenőrzés biztosítja az eljárás szakmai és jogi legitimációját. A következő fejezet szempontjából ebből az következik, hogy a szabálysértési alkalmazás hosszabb távon csak akkor maradhat társadalmilag és jogilag is stabil, ha az igénybevétel küszöbrendszere, az auditálás és a képzési-competencia háttér képes együtt növekedni a rendszer használatának volumenével.

Javasolt szabályozási és eljárási modell az MI felelős rendészeti alkalmazására

A fentiekben részletesen áttekintésre kerültek a mesterséges intelligencia bűnmegelőzési szerepének technológiai, jogi, nemzetközi és hazai aspektusai. A tanulmány zárásaként egy olyan modellkoncepciót vázolok fel, amely irányt mutathat a magyar jogalkotóknak és rendészeti szervezeteknek az MI eszközök felelős, jogszerű és hatékony integrációjához. Fontos egy olyan egysúlyi keret kialakítása, amely egyaránt szolgálja a közbiztonság növelését és az alapvető jogok szilárd védelmét.

Jogszabályi keretek konszolidációja és harmonizációja

- Javasolt egy külön jogi keret létrehozása – akár az alaptörvény erejű Rtv. (rendőrségi törvény) kiegészítéseként, akár önálló törvény formájában –, amely meghatározza a „magas kockázatú MI-rendszerek” fogalmát a rendőrségen belül, és előírja alkalmazásuk feltételeit. Ez a szabályozás tartalmazhatná például a kockázatértékelést, dokumentációs kötelezettséget, humán felügyeletet és tesztelési előírásokat, amelyek az EU AI Act (2024) általános rendelkezéseiből következnek. Emellett biztosítani kell, hogy a rendőrség csak olyan MI-eszközt szerezzen be, amely megfelelősségi tanúsítással (pl. CE-jelöléssel) rendelkezik, vagy ha saját fejlesztésű, akkor belső megfelelőség-értékelés előzze meg a használatát.
- Bírói kontroll és jogorvoslati mechanizmusok: egyes MI-alapú beavatkozások – különösen a valós idejű biometrikus megfigyelés – esetén indokolt az előzetes bírói engedély intézményének bevezetése, hasonlóan a titkos információgyűjtésre vonatkozó szabályokhoz. Ez azt biztosítja, hogy a szükségesség és arányosság elvei érvényesüljenek, és a jogalkalmazók számára világos felülvizsgálati lehetőségek álljanak rendelkezésre.

Hasonlóképp, ha egy prediktív algoritmus valakit „kockázatosnak” minősít, az ilyen jelzések kihatással lehetnek hatósági intézkedésekre, ezért jogorvoslati lehetőségeket kell biztosítani, amelyekben a döntéshozatal nem kizárólag szoftveres eredményre épül, hanem emberi mérlegelés is történik.

- A rendészeti MI-alkalmazások is alá tartoznak a személyes adatok kezelésére vonatkozó általános elveknek: célhoz kötöttség, adattakarékosság, időbeli korlátozás, valamint privacy by design. Például olyan mechanizmusokat kell előírni, amelyek biztosítják, hogy a nem releváns – vagy már nem indokolt – biometrikus adatok ne maradjanak hosszabb ideig nyilvántartásban, és technikai szinten is minimalizálják a személyazonosító adatok felesleges tárolását. Az uniós AI Act (2024) mellett az adatvédelmi szabályok megerősítése hazai szinten további garanciákat adhat az érintettek jogainak védelmére, beleértve a tájékoztatási, törlési és helyesbítési jogokat.

Intézményi garanciák és felügyelet

- A felelős rendészeti MI-használat egyik kulcskérdése, hogy világosan meghatározott intézményi keretek között történjen az ellenőrzés és az elszámoltathatóság. A technológiai eszközök önmagukban nem képesek garantálni a jogszerűséget és az arányosságot: ehhez stabil, működőképes felügyeleti struktúrára van szükség. Az AI Act (2024) végrehajtása nyomán Magyarországon is formálódóban van az MI-felügyeleti intézményrendszer. Ennek részeként folyamatban van a Magyar Mesterséges Intelligencia Hatóság létrehozása, amely várhatóan központi szerepet kap a magas kockázatú rendszerek ellenőrzésében, regisztrációjában és felügyeletében. A rendészeti MI-alkalmazások esetében ezért indokolt, hogy a jövőben ez a hatóság – a NAIH-al együttműködésben – érdemi ellenőrzési jogosítványokkal rendelkezzen.
- Nemzeti Felügyeleti Hatóság kijelölése: a felügyeleti rendszer egyik pillérét továbbra is a NAIH jelentheti, különösen az adatkezelési és alapjogi megfelelés területén. A gyakorlatban ez azt jelenti, hogy az új vagy jelentősen módosított rendészeti MI-rendszerek bevezetését megelőzően kötelező hatásvizsgálatot és adatvédelmi elemzést kell lefolytatni, amelyhez hatósági jóváhagyás is kapcsolódhat.

Emellett indokolt, hogy a felügyeleti szervek rendszeres és eseti ellenőrzéseket is folytathassanak a működés, a naplózás és az adatkezelési gyakorlat tekintetében.

Az intézményi garanciák másik fontos eleme egy belső, szakmai-etikai kontrollmechanizmus megerősítése. A Belügyminisztérium keretein belül célszerű egy állandó, több szakterületet képviselő MI-etikai és szakmai testület működtetése, amelyben jogászok, informatikusok, rendészeti szakemberek és külső szakértők egyaránt részt vesznek. Ez a testület nem csupán véleményező fórumként működhetne, hanem aktívan részt vehetne az új technológiák előzetes értékelésében, pilotprojektek felügyeletében, valamint a nemzetközi tapasztalatok beépítésében is.

- Belső protokollok és felelősségi lánc: fontos, hogy a rendőrség szervezeti szinten is lefedtesse: ki felel az MI döntésekért. Javasolt, hogy minden MI-rendszerhez rendeljenek egy felelős emberi tisztviselőt (pl. az adott elemző osztály vezetőjét), aki monitorozza a rendszer outputját és döntéshozóként jóváhagyja vagy elutasítja azokat. Ez a gyakorlatban biztosítja a „human-in-the-loop” elvet. Az MI ne lehessen „gazdátlan”: mindig legyen felelőse, és ha az MI hibázik, a felelős vizsgálja ki, korrigálja a folyamatot. A protokoll írja elő, hogy a rendőr nem hivatkozhat kizárólag a gépre, indokolnia kell saját meggyőződését is. Például, ha egy prediktív térkép alapján küld több járőrt valahova, később értékelje, bevált-e a modell vagy sem.
- Naplózás és nyomonkövethetőség: minden MI-rendszer működését – amennyiben azt a jogszabály kéri – naplózni kell. Ideértve: milyen adatokat vitt be, mit adott ki, ki fért hozzá, milyen emberi beavatkozás történt. Ezek a logok szükség esetén független audit (pl. bíróság vagy felügyelet) által ellenőrizhetők legyenek. Például, ha valakit MI javaslatra tartóztattak le, utólag visszakéreshető legyen, mire alapozott a javaslat és ki hagyta jóvá. Ez egyrészt védi a polgárt (ha hiba történt, felfedezhető), másrészt védi a rendőrt (ha helyesen járt el, bizonyítható).

Összességében az intézményi felügyelet akkor tekinthető működőképesnek, ha több szinten is érvényesül: külső hatósági kontroll, belső szakmai-etikai ellenőrzés, egyértelmű vezetői felelősség és technikailag biztosított átláthatóság formájában. Csak ilyen többszintű rendszer képes hosszú távon garantálni, hogy a rendészeti MI-használat ne váljon öncélú technológiai gyakorlattá, hanem valóban jogállami keretek között maradjon.

Technológiai és adatbiztonsági feltételek

Az MI-rendszereket úgy kell integrálni, hogy azok minimálisra csökkentsék a jogsérelem kockázatát. Ennek érdekében:

- Beépített adatvédelem és anonymizálás: alapvető elvárás, hogy az alkalmazott rendszerek ne kezeljenek több személyes adatot, mint amennyi a konkrét rendészeti cél eléréséhez feltétlenül szükséges. A gyakorlatban ez azt jelenti, hogy a megfigyelő vagy elemző rendszerek működését úgy kell kialakítani, hogy azok alapállapotban ne tároljanak tömegesen azonosítható képfelvételeket. Csak indokolt esetben induljon el az egyedi azonosítási folyamat. Egyes európai példák azt mutatják, hogy technikailag is megvalósítható az arcok automatikus kitarakása vagy anonimizálása, amely csak külön engedély birtokában oldható fel. Az ilyen megoldások alkalmazása hozzájárulhat ahhoz, hogy a biometrikus adatok kezelése valóban kivételes eszköz maradjon, és ne váljon rutinszerű adattárolássá.
- Adatminőség és reprezentativitás: különösen a prediktív és az arcfelismerő rendszereknél is gondoskodni kell arról, hogy a használt adatok ne legyenek torzítóak. Ehhez lehetőleg *független szakértők bevonásával* át kell tekinteni a tanító adatbázist. Pl. a bűnügyi adatokat meg lehet tisztítani bizonyos elfogultságoktól (ha mondjuk kiderül, hogy egyes kerületek túlréprezentáltak a statisztikában a fokozott ellenőrzések miatt, ezt figyelembe lehet venni a modellben). Az arcfelismerő rendszernél ellenőrizni, hogy a nyilvántartott arcképek minősége, változatossága megfelelő-e (ha pl. csak idős férfiak képe van meg, fiatal nőket nem jól ismer fel – akkor bővíteni vagy finomhangolni kell).
- Kiberbiztonság és felhasználás-biztonság: mivel ezek a rendszerek szenzitív adatokat kezelnek, erősíteni kell a védelmüket a kibertámadások ellen. Javasolt, hogy minden új MI-rendszert a NBSZ (Nemzeti Biztonsági Szakszolgálat) kiberbiztonsági auditnak vessen alá bevezetés előtt. Emellett a felhasználói jogosultságokat is szigorúan szabályozni kell: csak az férjen hozzá a nyers adatokhoz vagy a rendszer beállításaihoz, akinek feltétlen szükséges (need-to-know elv). Legyen belső szankciórendszer az illetéktelen MI-használatra (pl. ha valaki kíváncsiságból magáncélra futtat le valakit a rendszerben, az fegyelmi vétség legyen).

Képzés, tudatosság és társadalmi párbeszéd

A modell utolsó, de nem elhanyagolható eleme a humán faktor kezelése.

- Rendőrségi oktatás: be kell építeni a rendészeti képzésbe (tisztképzés, továbbképzés) az MI és adatvezérelt rendészet ismereteit. Ez magában foglalná az adott eszközök kezelésének gyakorlati oktatását, de a jogi-etikai háttér oktatását is. A cél, hogy minden rendőri felhasználó értse: az MI nem tévedhetetlen döntéshozó, csak egy segédeszköz, és tisztában legyen azzal is, milyen jogi határok között mozoghat. Legyenek belső irányelvek arra, hogyan ellenőrizzék másodlagosan az MI eredményeit.
- Szakszerű kommunikáció: fontos a rendőrség részéről a nyilvánosság felé is kommunikálni arról, milyen MI-eszközöket használnak és mire. A transzparencia erősíti a közbizalmat: ha a lakosság érti, hogy pl. a kamera nem a "megfigyelő állam" eszköze, hanem bűnözőket segít elkapni, de őt nem listázza ok nélkül, akkor nagyobb elfogadottság fogja övezi. Javasolt a rendszeres tájékoztatás, akár adatközlések (pl. évente jelentés: hány esetben használták az arcfelismerőt, mennyi bűnözőt fogtak el így). Ahol hibák történtek, azt tanulásként kommunikálják, mit változtattak, hogy ne fordulhasson elő. Ez a nyíltság hozzájárul, hogy a társadalom ne ellenséggént tekintsen a technológiára, hanem olyasmire, amit kontroll alatt tartanak.
- Civil kontroll és párbeszéd: érdemes bevonni civil szervezeteket, adatvédelmi és jogvédő szakembereket konzultatív módon. Például a javasolt Etikai Bizottságban is lehet helyük, de akár nyilvános fórumokat is lehet szervezni, ahol a rendőrség meghallgatja a lakosság vagy civil csoportok véleményét egy-egy újítás előtt. Például, ha a rendőrség drónokat akar bevezetni tömegmegfigyelésre, előtte tart egy szakmai vitát meghívott civilekkel, és esetleg integrálja a felvetéseiket (pl. tiltott területek kijelölése, adatmegőrzési idő csökkentése stb.). Ez a fajta *kooperatív szabályozás* csökkenti a későbbi konfliktusokat és peres ügyeket, mert már az elején figyelembe veszi a lehetséges aggályokat.

Folyamatos felülvizsgálat és alkalmazkodás

Végül a modellnek tartalmaznia kell a dinamizmust. Az MI-technológia gyorsan fejlődik, így a szabályozásnak is adaptívnak kell lennie. Javasolt, hogy a Belügyminisztérium készítsen évente egy *MI-rendészet értékelő jelentést*, ami összegzi a tapasztalatokat: mi működött, mi nem, milyen új eszköz jelent meg a piacon, kell-e módosítani a szabályokat. Ezt a jelentést terjesszék az Országgyűlés illetékes bizottsága elé is, biztosítva a törvényhozói felügyeletet. Ha pl. kiderül, hogy egy rendszer sorozatosan diszkriminatív eredményt ad, a jelentés javasolhatja a felfüggesztését vagy cseréjét. Az EU AI Board és Office ajánlásait is integrálni kell az ilyen felülvizsgálatokba, hiszen EU-s szinten is lesz tapasztalatcsere.

Konklúzió: a fenti javaslatcsomag megvalósítása révén Magyarország kialakíthat egy kiegyensúlyozott modellt a mesterséges intelligencia rendészeti alkalmazására. Az MI eszközök így valóban a közbiztonság szolgálatába állíthatók anélkül, hogy aláásnák a demokratikus értékeket és jogokat. A technológia nyújtotta előnyök – gyorsabb bűnfelderítés, hatékonyabb megelőzés – összeegyeztethetők a személyes szabadságjogokkal, ha a használatukat megfelelő jogi és etikai korlátok közé szorítjuk. A javasolt modell lényege épp ez: *fegyelmezett innováció* – a rendvédelem modernizálása úgy, hogy közben megtartjuk mindazt, ami a jogállami rendőrséget a polgárok szemében legitimé teszi (arányosság, átláthatóság, elszámoltathatóság). Ezzel teremthető meg az a bizalmi viszony, amely hosszú távon mind a közbiztonságot, mind a szabadságot erősíti.

Összegzés

A tanulmány elején feltett kérdésre – milyen szerepet tölthet be a mesterséges intelligencia a bűnmegelőzésben a 21. századi demokratikus jogállamban – vizsgálódásom egy árnyalt választ adott. Az MI technológiák, úgymint az arcfelismerő rendszerek, az intelligens megfigyelőkamerák és a prediktív algoritmusok, kétségtelenül új dimenziót nyitnak a bűnüldözésben. Képesek hatalmas adatmennyiséget feldolgozni, rejtett összefüggéseket feltárni és villámgyorsan reagálni olyan jelekre, amelyeket ember talán észre sem venne. A gyakorlati példák – Egyesült Királyság, Franciaország, USA, Kína – mutatják, hogy az MI eszközök hozzájárulhatnak veszélyes bűnelkövetők kézre kerítéséhez, terrorcselekmények megelőzéséhez vagy épp a rendőri erők optimális elosztásához. Ugyanakkor azt is megtanulhattuk a nemzetközi tapasztalatokból, hogy mindez csak akkor válik igazi sikertörténétté, ha

kordában tartjuk a technológiát. Fékezés nélkül az MI könnyen csúszhat át a polgárok magánszféráját teljesen felszámoló, disztópikus megfigyelőgépezetté – erre figyelmeztetnek a jogvédők és az EU új szabályai is. A kulcs az egyensúly: a demokratikus jogállamiság alapelveinek (joguralom, átláthatóság, alapjogok tisztelete) és a közbiztonsági érdekeknek kiegyensúlyozása.

Dolgozatom magyar vonatkozású elemzése azt tárta fel, hogy hazánkban e téren még számos teendő van. A jogi környezet jelenleg *ellentmondásos*: bizonyos új szabályok (pl. a 2025-ös biometrikus megfigyelési kiterjesztés) egyértelműen szembemennek az európai normákkal, ami nem csak jogi konfliktust szül, hanem a közbizalmat is aláássa. Ugyanakkor az is látszik, hogy a magyar rendvédelmi szervek érdeklődnek az MI iránt és kísérleti lépéseket már tettek is, de hiányzik a stabil keretrendszer és a társadalmi párbeszéd e lépések körül. Empirikus kutatásom rávilágított, hogy a rendőrségen belül is megfogalmazódott az igény a *szabályozott, felelős innovációra*. A legtöbben hatékonyságnövelő eszközöket látnak benne, nem pedig a polgári szabadságjogok elleni fegyvert – ezt a szemléletet érdemes támogatni és hivatalos normákba önteni.

A kidolgozott javaslatcsomag azt a modellt vázolta fel, amelyben a mesterséges intelligencia a jogállami korlátok tiszteletben tartásával válik a bűnmegelőzés integráns részévé. E modell pillérei – a koherens jogszabályi háttér, az intézményi felügyelet és átláthatóság, a technikai garanciák, valamint a képzés és társadalmi kontroll – együttesen biztosítják, hogy a technológia ne uralja, hanem szolgálja a társadalmat. Ha ezen elvek mentén haladunk, a mesterséges intelligencia nem ellensége, hanem támogatója lesz a rendőrségnek és a közösségeknek egyaránt. Segítségével *gyorsabb, proaktívabb és eredményesebb* bűnmegelőzés valósulhat meg – de mindez nem a jogállam rovására, hanem annak erősítésével, hiszen a hatékony rendvédelem is a közjó és az emberi jogok védelmének része.

Zárásként hangsúlyozni szükséges, hogy a technológia fejlődése nem áll meg, sőt, az elkövetkező években még újabb kihívásokkal szembesülhetünk (gondoljunk csak a deepfake videókra vagy a még fejlettebb tömeges megfigyelési eszközökre). Ezért a most megalkotandó kereteket is *folyamatosan értékelni és szükség szerint módosítani* kell. A jogállam rugalmassága abban áll, hogy képes reagálni az új jelenségekre anélkül, hogy feladná alapértékeit. A mesterséges intelligencia bűnmegelőzésben betöltött szerepéről szóló vizsgálódás eredményei azt igazolják: meg lehet és meg is kell találni azt a finom egyensúlyt, ahol az MI kihasználja mindazt a potenciált, amit a bűnözés elleni harcban nyújthat, ugyanakkor a jog korlátai között marad, tiszteletben tartva az emberi méltóságot és szabadságot.

Ez az egyensúly teszi lehetővé, hogy a mesterséges intelligencia valóban a 21. századi rendvédelem értékes és legitim eszközévé váljon, a társadalom bizalmát élvezve.

Irodalomjegyzék

Jogszabályok, uniós jogi aktusok és alapjogi dokumentumok

2024. évi XXV. törvény a belügyi ágazati feladatellátást támogató egyes törvények módosításáról.
<https://njt.hu/jogszabaly/2024-25-00-00.0> [Letöltve: 2026.01.06.].
2015. évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről.
<https://njt.hu/jogszabaly/2015-188-00-00> [Letöltve: 2026.01.06.].
2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotörvény).
<https://net.jogtar.hu/jogszabaly?docid=a1100112.tv> [Letöltve: 2025.11.15.].
1994. évi XXXIV. törvény a Rendőrségről (Rtv.).
<https://net.jogtar.hu/jogszabaly?docid=99400034.tv> [Letöltve: 2025.11.15.].
- Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024) a mesterséges intelligenciáról (AI Act). Az Európai Unió Hivatalos Lapja, L 168. 113. cikk (5)–(6) bekezdés.
- Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024) a mesterséges intelligenciáról (AI Act). Az Európai Unió Hivatalos Lapja, L 168. 113. cikk.
- Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024) a mesterséges intelligenciáról (AI Act). Az Európai Unió Hivatalos Lapja, L 168. 4., 5., 52–53. és 113. cikk.
- Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024) a mesterséges intelligenciáról (AI Act). Az Európai Unió Hivatalos Lapja, L 168. 64–66. cikk.
- Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024) a mesterséges intelligenciáról (AI Act). Az Európai Unió Hivatalos Lapja, L 168. 67–68. cikk.
- Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024) a mesterséges intelligenciáról (AI Act). Az Európai Unió Hivatalos Lapja, L 168. 70–74. cikk.
- Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024) a mesterséges intelligenciáról (AI Act). Az Európai Unió Hivatalos Lapja, L 168. pp. 17–21.
https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=OJ:L_202401689 [Letöltve: 2025.09.20.].
- Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024) a mesterséges intelligenciáról. Az Európai Unió Hivatalos Lapja, L 168.
https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=OJ:L_202401689 [Letöltve: 2025.09.20.].
- Az Európai Parlament és a Tanács 2000/43/EK irányelve (2000).
- Az Európai Parlament és a Tanács 2000/78/EK irányelve (2000).
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016) General Data Protection Regulation – GDPR, különösen 5. cikk, 6. cikk és 9. cikk.
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016) General Data Protection Regulation – GDPR, különösen 51–59. cikk.
- Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016) Law Enforcement Directive – LED, különösen 4. cikk és 8–10. cikk.
- Az Európai Unió Alapjogi Chartája (2012/C 326/02) 7–8. cikk – A magán- és a családi élet tiszteletben tartása; A személyes adatok védelme.
- Az Európai Unió Alapjogi Chartája (2012) 12. cikk – Gyülekezési és egyesülési szabadság.
- Az Európai Unió Alapjogi Chartája (2012) 47. cikk – Hatékony jogorvoslatához való jog.
- France (2023) Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions.
<https://www.legifrance.gouv.fr/eli/loi/2023/5/19/2023-380/jo/texte> [Letöltve: 2026.04.29.].
- France (1978) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/> [Letöltve: 2026.04.29.].
- Magyarország 2015. évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről.
<https://net.jogtar.hu/jogszabaly?docid=a1500188.tv> [Letöltve: 2025.11.15.].
- Magyarország Alaptörvénye (2011. április 25.) VI. cikk.
<https://net.jogtar.hu/jogszabaly?docid=a1100425.atv> [Letöltve: 2025.11.15.].
- United Kingdom (2018) Data Protection Act 2018.
<https://www.legislation.gov.uk/ukpga/2018/12/contents> [Letöltve: 2026.04.29.].

United Kingdom (1998) Human Rights Act 1998.
<https://www.legislation.gov.uk/ukpga/1998/42/contents> [Letöltve: 2026.04.29.].

Bíróági döntések

Bridges, R. v South Wales Police (2020) EWCA Civ 1058.
 England and Wales Court of Appeal.
<https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html> [Letöltve: 2025.10.13.].

Court of Appeal (England and Wales) (2020) R (Bridges) v Chief Constable of South Wales Police and others [2020] EWCA Civ 1058.
<https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf> [Letöltve: 2026.04.29.].

Hatósági, kormányzati és intézményi dokumentumok

Council of Europe (2019) Guidelines on Artificial Intelligence and Data Protection. Strasbourg.
<https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/16809f9d8> [Letöltve: 2025.09.20.].

European Commission (2025) Regulatory Framework for Artificial Intelligence (Artificial Intelligence Act).
<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> [Letöltve: 2025.09.14.].

European Commission – High-Level Expert Group on Artificial Intelligence (2019) Ethics Guidelines for Trustworthy Artificial Intelligence. Brussels.
<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> [Letöltve: 2025.09.20.].

European Parliament (2025) Regulation on Artificial Intelligence (AI Act) – Legislative Process. Legislative Train.
<https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence> [Letöltve: 2025.10.05.].

European Parliament (2020) Artificial Intelligence in Law Enforcement: Impact on Fundamental Rights. European Parliamentary Research Service, Brussels.

French Government (n.d.) Commission nationale de l'informatique et des libertés (CNIL).
<https://www.info.gouv.fr/organisation/commission-nationale-de-l-informatique-et-des-libertes-cnil> [Letöltve: 2026.04.29.].

His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (2017) PEEL: Police effectiveness 2016: An inspection of Kent Police.
<https://assets-hmicfrs.justiceinspectorates.gov.uk/uploads/peel-police-effectiveness-2016-kent.pdf> [Letöltve: 2026.04.29.].

Information Commissioner's Office (2021) The use of live facial recognition technology in public places. 2021, June 18.
<https://ico.org.uk/media2/migrated/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf> [Letöltve: 2026.04.29.].

Metropolitan Police Service (2024) Live facial recognition: Data Protection Impact Assessment (DPIA2).
<https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/impact-assessments/lfr-dpia2.pdf> [Letöltve: 2026.04.29.].

Nemzeti Adatvédelmi és Információszabadság Hatóság (2025) Hivatalos honlap.
<https://www.naih.hu> [Letöltve: 2025.09.20.].

Nemzeti Szakértői és Kutató Központ (2024) Az Állóképes Arckép Azonosító Rendszer (ÁAAR) működése, szervezeti és eljárási keretei. ORFK belső szakmai segédlet.

Országgyűlési képviselők (2025) T/11201. számú törvényjavaslat a gyülekezési jogról szóló 2018. évi LV. törvény módosításáról. Budapest, 2025. március 17.
<https://www.parlament.hu/irom42/11201/11201.pdf> [Letöltve: 2025.09.14.].

UK Home Office (2023) Police Urged to Double AI-Enabled Facial Recognition Searches.
<https://www.gov.uk/government/news/police-urged-to-double-ai-enabled-facial-recognition-searches> [Letöltve: 2025.10.13.].

UK Home Office (2025) Public attitudes to police use of facial recognition technology.
<https://www.gov.uk/government/publications/public-attitudes-to-police-use-of-facial-recognition-technology> [Letöltve: 2026.04.29.].

Szakirodalom, tanulmányok és jelentések

AI Now Institute (2019) *Discriminating Systems: Gender, Race, and Power in AI*. New York University, New York, 2019.
<https://ainowinstitute.org/wp-content/uploads/2023/04/discriminating-systems.pdf> [Letöltve: 2025.10.27.].

- Babuta, A. (2020) *Algorithmic Policing: The Risk of Driving Law Enforcement by the Numbers*. London, Royal United Services Institute for Defence and Security Studies.
https://static.rusi.org/rusi_pub_i65_2020_01_algorithmic_policing_babuta_final_web_copy.pdf
 [Letöltve: 2025.10.13.].
- Big Brother Watch (2018) Face Off: Az arcfelismerés törvénytelen növekedése az Egyesült Királyság rendőrségében.
<https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf> [Letöltve: 2026.04.29.].
- Braga, A. A.–Turchan, B. S.–Papachristos, A. V. (2019) Hot spots policing and crime reduction: An update of an ongoing systematic review and meta-analysis. *Journal of Experimental Criminology*, 15(3). pp. 289–311. doi: 10.1007/s11292-019-09372-3
<https://psycnet.apa.org/record/2019-52100-001>
 [Letöltve: 2026.05.07.].
- Buolamwini, J.–Gebru, T. (2018) Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, Vol. 81. pp. 1–15.
<https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> [Letöltve: 2025.09.20.].
- Cook, S. (2020) Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence Since 2017. Washington, Freedom House.
<https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone> [Letöltve: 2025.11.12.].
- Crawford, K.–Calo, R.–Schultz, J.–Richardson, J. (2019) The Documentarian Gaze: Rethinking Surveillance Law in the Age of Big Data and Artificial Intelligence. *New York University Law Review*, Vol. 94.
<https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf> [Letöltve: 2025.09.16.].
- Creemers, R. (2018) China's Social Credit System: An Evolving Practice of Control. *Iberchina*.
https://www.iberchina.org/files/2018/social_credit_china.pdf [Letöltve: 2025.11.12.].
- Freedom House (2019) Freedom in the World 2019: China.
<https://freedomhouse.org/country/china/freedom-world/2019> [Letöltve: 2026.04.29.].
- Garvie, C. (2019) Garbage in, garbage out: Face recognition on flawed data. *Georgetown Law Center on Privacy & Technology*, 2019, May 16.
<https://www.law.georgetown.edu/privacy-technology-center/publications/garbage-in-garbage-out-face-recognition-on-flawed-data/>
 [Letöltve: 2026.04.29.].
- Garvie, C.–Bedoya, A.–Frankle, J. (2016) The Perpetual Line-Up: Unregulated Police Face Recognition in America. Washington, *Georgetown Law Center on Privacy & Technology*.
<https://www.perpetuallineup.org/> [Letöltve: 2025.09.14.].
- Hinkle, C. (2020) The End of Anonymity – How Facial Recognition Technology Will Worsen Online Harassment. *Georgetown Journal of Gender and the Law*.
https://www.law.georgetown.edu/gender-journal/wp-content/uploads/sites/20/2020/09/Online-Article-3_Final-Draft_ch1263.pdf [Letöltve: 2025.11.04.].
- Human Rights Watch (2019) *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*. New York, Human Rights Watch.
<https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass> [Letöltve: 2025.11.04.].
- Koula, A. (2024) *AI-Driven Mass Surveillance at 2024 Olympics: The Human Rights Issues and Recommendations*. Policy Report. Manchester, Manchester Metropolitan University.
<https://www.mmu.ac.uk/sites/default/files/2024-06/AI-driven%20Mass%20Surveillance%20at%202024%20Olympics%20-%20The%20Human%20Rights%20Issues%20and%20Recommendations.pdf> [Letöltve: 2025.09.14.].
- La Fors, K. (2021) Review of “Predict and Surveil: Data, Discretion, and the Future of Policing”. *Surveillance & Society*, 19(2). pp. 274–276.
https://www.researchgate.net/publication/354175774_Predict_and_surveil_Data_discretion_and_the_future_of_policing_by_Sarah_Brayne_A_review_by_Karina_La_Fors [Letöltve: 2025.10.27.].
- La Quadrature du Net (2025) PolPred – Prediktív rendészet Franciaországban: Elemzés és Aggályok. Paris, Queried Report.
<https://www.laquadrature.net/wp-content/uploads/sites/8/2025/05/polpred050525.pdf>
 [Letöltve: 2025.10.21.].

- Lum, K.–Isaac, W. (2016) To Predict and Serve? *Significance*, Vol. 13. No. 5. pp. 14–19. doi: 10.1111/j.1740-9713.2016.00960.x <https://rss.onlinelibrary.wiley.com/doi/10.1111/j.1740-9713.2016.00960.x> [Letöltve: 2025.09.16.].
- Marr, B. (2018) Artificial Intelligence in Practice: Examples Across Industries. *Journal of International Scientific Publications: Ecology & Safety*, Vol. 15. pp. 163–168. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10898100/> [Letöltve: 2025.09.16.].
- Perry, W. L.–McInnis, B.–Price, C. C.–Smith, S. C.–Hollywood, J. S. (2013) *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, RAND Corporation. pp. 3–5. https://www.rand.org/pubs/research_reports/RR233.html [Letöltve: 2025.09.16.].
- Qiang, X. (2019) *The Road to Digital Unfreedom: President Xi's Surveillance State*. Boise, Frank Church Institute, Boise State University. p. 45. <https://www.boisestate.edu/sps-frankchurchinstitute/wp-content/uploads/sites/128/2019/01/Road-to-Digital-Unfreedom.pdf> [Letöltve: 2025.11.04.].
- Richardson, R.–Schultz, J.–Crawford, K. (2019) Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York City Law Review*. <https://www.nycds.org/wpcontent/uploads/2019/03/3/Dirty%20Data%20Bad%20Predictions.pdf> [Letöltve: 2025.09.16.].
- Saunders, J.–Hunt, P.–Hollywood, J. S. (2016) Predictions put into practice: A quasi-experimental evaluation of Chicago's predictive policing pilot. RAND Corporation. <https://www.nacdl.org/getattachment/9d276b57-0d3f-477a-90fb-5a00c003edff/rand-ssl-study.pdf> [Letöltve: 2026.04.29.].
- Welsh, B. C.–Farrington, D. P. (2009) Public area CCTV and crime prevention: An updated systematic review and meta-analysis. *Justice Quarterly*, 26(4), pp. 716–745. <https://doi.org/10.1080/07418820802506206>
- West, S. M.–Whittaker, M.–Crawford, K. (2019) *Discriminating Systems: Gender, Race, and Power in AI*. AI Now Institute, New York, New York University. <https://ainowinstitute.org/wp-content/uploads/2023/04/discriminatingystems.pdf> [Letöltve: 2025.10.27.].

Sajtó, hírportálok és online források

- 24.hu (2025) Kisebb szabálysértések esetében is használhatja a rendőrség az arcképfelismerő rendszert. 2025. 05. 15. <https://24.hu/belfold/2025/05/15/arcfelismero-rendszer-szabalysertes-orfk-utasitas-valtozas-hivatalos-ertesito/> [Letöltve: 2026.01.06.].
- American Friends Service Committee (2020) Santa Cruz Becomes First U.S. City to Ban Predictive Policing. *European Digital*. <https://afsc.org/newsroom/santa-cruz-becomes-first-us-city-ban-predictive-policing> [Letöltve: 2025.10.27.].
- Amnesty International (2023) France: Allowing Mass Surveillance at Olympics Undermines EU Efforts to Regulate AI. <https://www.amnesty.org/en/latest/news/2023/03/france-allowing-mass-surveillance-at-olympics-undermines-eu-efforts-to-regulate-ai/> [Letöltve: 2025.10.15.].
- ArtificialIntelligenceAct.eu (2025) *What Is the EU AI Act?* <https://artificialintelligenceact.eu> [Letöltve: 2025.10.05.].
- Burgess, M. (2020) A British AI Tool to Predict Violent Crime Is Too Flawed to Use. *Wired*. <https://www.wired.com/story/a-british-ai-tool-to-predict-violent-crime-is-too-flawed-to-use/> [Letöltve: 2025.10.13.].
- Carpentier, A. (2024) How Algorithmic Video Surveillance Was Used during the Paris Olympics. *Le Monde*. https://www.lemonde.fr/en/france/article/2024/08/16/how-algorithmic-video-surveillance-was-used-during-the-paris-olympics_6716745_7.html [Letöltve: 2025.10.15.].
- Christakis, T.–Lodie, A. (2023) The French Supreme Administrative Court finds the use of facial recognition by law enforcement agencies to support criminal investigations “strictly necessary” and proportional. 2023, January 11. *AI-Regulation.com*. <https://ai-regulation.com/facial-recognition-law-enforcement-agencies/> [Letöltve: 2025.10.21.].
- Cuvelliez, C.–Quisquater, J.-J. (2024) La Police Prédictive à l'Épreuve du Crime Spectacle. *La Tribune*. <https://www.latribune.fr/idees/tribunes/opinion-la-police-predictive-a-l-epreuve-du-crime-spectacle-1025380.html> [Letöltve: 2025.10.21.].

- Deloitte (2025) Surveillance and Predictive Policing through AI. *Deloitte Insights*.
<https://www.deloitte.com/na/en/Industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html> [Letöltve: 2025.09.14.].
- Disclose (2023) The French national police is unlawfully using an Israeli facial recognition software.
<https://disclose.ngo/en/article/the-french-national-police-is-unlawfully-using-an-israeli-facial-recognition-software> [Letöltve: 2026.04.29.].
- E-gov Hírlével (2025) Jön a magyar Mesterséges Intelligencia Hivatal.
<https://hirlevel.egov.hu/2025/06/22/jon-a-magyar-mesterseges-intelligencia-hivatal/> [Letöltve: 2025.10.05.].
- European Digital Rights (2020) Open letter: EDRi calls on IBM to clarify stance on facial recognition. 2020, June 25.
<https://edri.org/our-work/open-letter-edri-calls-on-ibm-to-clarify-stance-on-facial-recognition/> [Letöltve: 2025.11.04.].
- Faiola, A. (2023) Artificial Intelligence Is Powering a Revolution in Policing, at the Olympics and Beyond. *The Washington Post*.
<https://www.washingtonpost.com/world/2023/12/18/ai-france-olympics-security/> [Letöltve: 2025.09.14.].
- Feiner, L. (2020) Microsoft Says It Will Not Sell Facial Recognition Software to Police until There Is a Federal Law. *CNBC*. 2020. június 11.
<https://www.cnbc.com/2020/06/11/microsoft-says-will-not-sell-facial-recognition-software-to-police.html> [Letöltve: 2025.11.04.].
- Foley, T. (2023) Use of Facial Recognition Systems Leads to Sanctions in France. *Vital Law*.
<https://www.vitalaw.com/news/use-of-facial-recognition-systems-leads-to-sanctions-in-france/cspdoid7dc8a5fcbac4eaoa5aec5bf219c15b1#> [Letöltve: 2025.10.21.].
- France (2023) Allowing Mass Surveillance at Olympics Undermines EU Efforts to Regulate AI. *Amnesty International*.
<https://www.amnesty.org/en/latest/news/2023/03/france-allowing-mass-surveillance-at-olympics-undermines-eu-efforts-to-regulate-ai/> [Letöltve: 2026.04.29.].
- Hill, K. (2020) Wrongfully accused by an algorithm. *The New York Times*. 2020, June 24.
<https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> [Letöltve: 2026.04.29.].
- Horák, R. (2025) Hungary's Facial Recognition Plan Lands It on an EU Watchlist. *Politico*. 2025. 04. 30.
<https://www.politico.eu/article/hungary-eu-watchlist-facial-recognition-surveillance-lgbtq-pride/> [Letöltve: 2025.11.15.].
- ID Tech Wire (2023) Report Flags French Police's 'Illegal' Use of Facial Recognition.
<https://idtechwire.com/report-flags-french-polices-illegal-use-of-facial-recognition/> [Letöltve: 2025.10.21.].
- Jogászvilág (2025) Részben hatályba lépett a „Pride” törvény. 2025. 03. 20.
<https://jogaszvilag.hu/szakma/reszben-hatalyba-lepett-a-pride-torveny/> [Letöltve: 2025.11.15.].
- Jun, G.–Xiaomin, Z. (2024) AI Police Improve Rate of Solving Crime. *China Daily Global*. 2024. október 23.
<http://global.chinadaily.com.cn/a/202410/23/WS6718580ca310f1265a1c9146.html> [Letöltve: 2025.11.12.].
- Laanstra-Corn, A.–Sewell, T. (2024) Algorithmic Surveillance Takes the Stage at the Paris Olympics. *Lawfare*.
<https://www.lawfaremedia.org/article/algorithmic-surveillance-takes-the-stage-at-the-paris-olympics> [Letöltve: 2025.10.15.].
- Lohr, S. (2020) Facial Recognition Leads to Misidentifications and Wrongful Arrests. *The New York Times*. 2020. június 24.
<https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> [Letöltve: 2025.11.04.].
- McConvey, J. R. (2023) French Police May Have Been Unlawfully Using Facial Recognition since 2015. *BiometricUpdate*.
<https://www.biometricupdate.com/202311/french-police-may-have-been-unlawfully-using-facial-recognition-since-2015> [Letöltve: 2025.10.21.].
- Mozur, P. (2017) China uses facial recognition to identify wanted suspects at beer festival. *The Guardian*. 2017, September 1.
<https://www.theguardian.com/world/2017/sep/01/facial-recognition-china-beer-festival> [Letöltve: 2026.04.29.].
- Pailliez, C. (2022) French Court Sentences Eight on Trial over 2016 Truck Attack in Nice. *Reuters*.
<https://www.reuters.com/world/europe/french-court-sentences-eight-trial-over-2016-truck-attack-nice-2022-12-13/> [Letöltve: 2025.09.14.].
- Rainie, L.–Funk, C.–Anderson, M.–Tyson, A. (2022) Public more likely to see facial recognition use by police as good, rather than bad for society. *Pew Research Center*. 2022, March 17.
<https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/> [Letöltve: 2025.11.04.].

- Rescan, M.–Berdah, A. (2024) How Algorithmic Video Surveillance Was Used during the Paris Olympics. *Le Monde*.
https://www.lemonde.fr/en/france/article/2024/08/16/how-algorithmic-video-surveillance-was-used-during-the-paris-olympics_6716745_7.html
 [Letöltve: 2025.09.14.].
- Sankin, A.–Mattu, S. (2023) Predictive Policing Software Is Terrible at Predicting Crimes. *The Markup*.
<https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes> [Letöltve: 2025.10.27.].
- Sixth Tone (2017) Face recognition spots wanted suspects at Qingdao beer festival. 2017, August 28.
<https://www.sixthtone.com/news/1000773/face-recognition-spots-wanted-suspects-at-qingdao-beer-festival> [Letöltve: 2026.04.29.].
- Sly, L. (2023) France's Security Tech Gamble: Artificial Intelligence and Olympics Surveillance. *The Washington Post*.
<https://www.washingtonpost.com/world/2023/12/18/ai-france-olympics-security/> [Letöltve: 2025.09.14.].
- Stone, L. (2020) UK Police Scrap AI Prototype Designed to Predict Serious Violence. *AI Business*.
<https://aibusiness.com/responsible-ai/uk-police-scrap-ai-prototype-designed-to-predict-serious-violence> [Letöltve: 2025.10.13.].
- The Policing Project (2024) How Policing Agencies Use Artificial Intelligence.
<https://www.policingproject.org/ai-explained-articles/2024/9/6/how-policing-agencies-use-ai>
 [Letöltve: 2025.09.14.].
- Thomson Reuters Legal (2025) Predictive Policing: Navigating the Challenges.
<https://legal.thomsonreuters.com/blog/predictive-policing-navigating-the-challenges> [Letöltve: 2025.09.16.].
- Társaság a Szabadságjogokért (2025) Magyarország új biometrikus megfigyelési törvényei sértik az Európai Unió mesterséges intelligencia rendeletét.
<https://tasz.hu/cikkek/magyarorszag-uj-biometrikus-megfigyelesi-torvenyei-sertik-az-eu-mestersegesintelligencia-rendeletet/> [Letöltve: 2025.09.14.].
- Wong, J. C. (2021) LAPD's Predictive Policing Systems Face Overhaul amid Surveillance Reform Push. *The Guardian*.
<https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform> [Letöltve: 2025.09.16.].
- Zsíros, S. (2025) Exclusive: Hungary's Gay Pride Surveillance Would Breach the EU's AI Act, Says Leading MEP. *Euronews*.