



Mesterséges intelligencia egyenruhában Rendvédelmi MI-rendszerek nemzetközi sikerei és kudarcai jogi szempontból

Artificial intelligence in uniform

The international successes and failures of law enforcement
AI systems from a legal perspective

Szabó Hedvig

Dr., PhD, tudományos munkatárs
Széchenyi István Egyetem,
Deák Ferenc Állam- és Jogtudományi Kar
szabo.hedvig@sze.hu



Absztrakt

Cél: A tanulmány a mesterségesintelligencia-alapú rendvédelmi rendszerek nemzetközi alkalmazásának szisztematikus elemzésével azonosítja azon jogi és intézményi tényezőket, amelyek meghatározzák ezen rendszerek sikerét vagy kudarcát.

Módszertan: Esettanulmány-alapú összehasonlító elemzés nyolc kiemelt nemzetközi projektről, a spanyol VioGén 2, az EU IAMI és az angolszász modellek, valamint a holland SyRI, spanyol VERIPOL, német és francia biometrikus azonosítással összefüggő kezdeményezések vizsgálata.

Megállapítások: A rendszerek jogszerű működése három pillér egyidejű meglététől függ: egyértelmű jogszabályi felhatalmazás, átláthatóság biztosítása és független felügyeleti mechanizmusok működése. E hármas követelményrendszer hiánya rendszerint a projekt leállításához vagy alapjogi jogsértések megállapításához vezetett.

Érték: A tanulmány jogtudományi szempontú összehasonlító elemzést végez az EU AI Act hatálybalépését követő időszak sikeres és sikertelen rendvédelmi

A szerző a kéziratot magyar nyelven nyújtotta be. Benyújtás ideje: 2025. 12. 25. Átdolgozás: 2026. 02. 07. Elfogadás: 2026. 02. 16.



MI-projektek tapasztalatairól, összekapcsolva a normatív előírásokat a gyakorlati alkalmazás tapasztalataival. Hiánypótló a magyar szakirodalomban, konkrét javaslatokat megfogalmazva a hazai jogalkotás és jogalkalmazás számára.

Kulcsszavak: mesterséges intelligencia, rendvédelem, EU AI Act, alapjogvédelem

Abstract

Aim: This study identifies the legal and institutional factors determining the success or failure of artificial intelligence-based law enforcement systems through a systematic analysis of their international applications.

Methodology: A case study-based comparative analysis of eight prominent international projects, examining the Spanish VioGén 2, the EU IAMI, Anglo-Saxon models, as well as the Dutch SyRI, Spanish VeriPol, and German and French biometric identification-related initiatives.

Findings: The lawful operation of these systems depends on the simultaneous presence of three pillars: clear legal authorization, ensuring transparency, and functioning independent oversight mechanisms. The absence of this tripartite requirement system typically led to project termination or findings of fundamental rights violations.

Value: The study conducts a comparative analysis from a legal science perspective on the experiences of successful and unsuccessful law enforcement AI projects in the period following the entry into force of the EU AI Act, linking normative requirements with practical implementation experiences. It fills a gap in Hungarian academic literature by formulating concrete recommendations for domestic legislation and legal practice.

Keywords: artificial intelligence, law enforcement, EU AI Act, fundamental rights protection

Elméleti és normatív keretek

A mesterséges intelligencia (továbbiakban: MI) rendvédelmi alkalmazása az elmúlt évtizedben paradigmaváltást hozott a közbiztonság fenntartásának eszköztárában. A prediktív analitikától a biometrikus azonosításon át az automatizált kockázatelemzésig terjedő technológiai megoldások bevezetése azonban nemcsak a hatékonyság javításának ígérését hordozza, hanem alapvető jogállami és alkotmányos kérdéseket is felvet. Az Európai Unió, EU 2024/1689

számú, mesterséges intelligenciáról szóló rendeletének (továbbiakban: EU AI Act) 2024. augusztus 1-jei hatálybalépése, valamint a tiltott gyakorlatokra vonatkozó rendelkezések 2025. február 2-i alkalmazhatóvá válása új normatív keretet teremtett, amely a technológiai innováció és az alapjogvédelem egyensúlyának megteremtését tűzi ki célul.

Jelen tanulmány a nemzetközi tapasztalatok szisztematikus feldolgozásán keresztül arra keresi a választ, hogy mely tényezők határozzák meg az MI-alapú rendvédelmi rendszerek sikerét vagy kudarcát, különös tekintettel a jogi megfelelőség szempontjaira. A vizsgálat módszertani alapját az esettanulmány-alapú összehasonlító elemzés képezi, amely egyaránt kiterjed a (részben) sikeres implementációkra – így a spanyol VioGén 2 családon belüli erőszak előrejelző rendszerre, az Európai Unió IAMI biometrikus azonosítási projektjére, valamint az alkalmazott angolszász modellekre – és a megszüntetett vagy alkotmányossági aggályok miatt leállított kezdeményezésekre, mint a holland SyRI, a spanyol VERIPOL vagy a német és francia biometrikus azonosítási törekvések.

A kutatás szerint az MI-alapú rendvédelmi rendszerek társadalmi elfogadottsága és jogszerű működése három pillér egyidejű meglététől függ (Entcheva & Mazilescu, 2024), az egyértelmű jogszabályi felhatalmazástól, az átláthatóság biztosításától, valamint a független felügyeleti mechanizmusok működésétől. E hármas követelményrendszer hiánya – amint azt a nemzetközi példák igazolják – rendszerint a projekt leállításához vagy alapjogi jogsértések megállapításához vezetett.

(Részben) Sikeres implementációk, a jogszerű működés esetleges modelljei a rendvédelmi mesterséges intelligencia területén

VioGén 2 – Spanyolország családon belüli erőszak előrejelző rendszere¹

A spanyol belügyminisztérium 2025. január 15-én indította újra a VioGén 2-t, amelynek elődje a VioGén már 2007-ben megkezdte működését. A rendszer több mint hatmillió családon belüli erőszak értékelését végezte el (López-Osorio et al., 2018). A rendszer elindításának alapja a 2004. évi 1. számú törvény (Ley Orgánica 1/2004), amely átfogó intézkedéseket írt elő a nemi erőszak ellen. A rendszer működésének igazolásában a jogszabály mellett kulcsfontosságú volt, hogy a spanyol alkotmánybíróság 2008 májusában – a nembeli egyenlőtlenségre hivatkozó kifogások ellenére – alkotmányosnak ítélte az ilyen típusú védelmi rendszereket (STC 59/2008).

1 Sistema de Seguimiento Integral en los casos de Violencia de Género.

Azonban a rendszer működését alapjaiban kellett felülvizsgálni, mikor 2024-ben a *New York Times* oknyomozó újságírói megállapították a rendszer kritikus gyengeségeit, többek közt, hogy számos alacsony kockázatúnak minősített áldozat később erőszak vagy halál áldozata lett (Satariano & Toll Pifarré, 2024). Ez alapján levonható az a következtetés, hogy még a jogi szempontból kifogástalan rendszerek is kudarcot vallhatnak, ha a rendszer alapját képező MI algoritmusának pontossága nem elegendő (Éticas Foundation & Ana Bella Foundation, 2022).

A VioGén 2 már 37 kockázati változót értékel, többek között az erőszak súlyosságát, az elkövető előéletét, az áldozat sebezhetőségét és a kiskorúak jelenlétét az elkövetésnél (Interoperable Europe Portal, 2024). A VioGén új modellje már megszüntette a „nincs kockázat” kategóriát, így minden családon belüli erőszakra vonatkozó bejelentés esetén kötelező a kockázatértékelés (Ministerio del Interior Sistema VioGén). A modellben az adatok kezelését a GDPR 9. cikk szerinti különleges adatkategóriák feldolgozásának megfelelően szigorú garanciák övezik, csak arra jogosult szakemberek férnek hozzá (rendőrök, ügyészek, bírók, szociális munkások), és a 2016/680 irányelv (továbbiakban: LED) alapján csak „szigorúan szükséges” esetben, esetről esetre igazolt módon

IAMI – Az EU biometrikus azonosítási projektje²

Az IAMI a Horizon Europe keretében finanszírozott kutatási projekt, amelyet a Bajorországi Közszerzőláti Főiskola vezet 18 konzorciumi taggal, köztük biometrikus azonosítással foglalkozó cégekkel és szabályozási megfelelési szakértőkkel. A projekt iránytűként szolgálhat, mivel kifejezett célja, hogy már a tervezési fázisban integrálja az EU AI Act előírásait.

Az EU AI Act alapján a bűnüldözési célú biometrikus azonosítás magas kockázatú MI-rendszernek minősül (III. melléklet, 1. és 6. pont), ami szigorú kötelezettségeket jelent. Az 5. cikk különösen fontos a projekt szempontjából, hiszen 2025. február 2-től – szűk kivétellel – nyilvános helyeken tiltott a valós idejű távoli biometrikus azonosítás.

A projekt kifejezetten törekszik a szabályozásnak való megfelelésre, ennek keretében alapvető jogok érvényesülésének az értékelését és adatvédelmi hatásvizsgálatot is végeznek. A projekt befejezését követően mintaként is szolgál valamennyi uniós tagállam rendvédelmi szerve számára, mivel valamennyi nagy kockázatú rendvédelmi rendszer esetén minden tagállamban külön engedélyt kell beszerezni az alkalmazás telepítése előtt, és be kell jegyezni az EU

2 Identity Attributes Matrix Initiative – Személyazonosítási Tulajdonságmátrix Program.

adatbázisába. Mindemelett figyelembe kell venni, hogy a LED 10. cikke szerint a biometrikus adatok feldolgozása csak „szigorúan szükséges” esetben megengedett, és az Európai Adatvédelmi Testület 05/2022-es iránymutatása szigorú korlátokat szab azoknak az arcfelismerő technológiáknak is, amelyeket a büntetőügy területén használnak.

Truleo és Find and Profile Tool – angolszász rendvédelmi MI-modellek

Az amerikai Truleo egy testkamera hangfelvételeket elemző, MI-n alapuló rendszer, amelyet számos amerikai rendvédelmi szerv alkalmaz pilot vagy operatív jelleggel. A rendszer természetes nyelvfeldolgozási technológiák segítségével automatikusan elemzi a testkamerák hangfelvételeit, elsősorban a rendőri kommunikáció professzionalitását.

A Truleo által alkalmazott technológia és adatbiztonsági keretrendszer az Egyesült Államok szövetségi rendészeti és kormányzati informatikai követelményeihez igazodik. A rendszer működése összhangban áll az FBI Criminal Justice Information Services (CJIS) biztonsági előírásaival, valamint a Szövetségi Kockázat- és Engedélykezelési Program (FedRAMP) követelményeivel. Az infrastruktúra jellemzően az AWS GovCloud környezetben működik, FIPS 140-2 szabványnak megfelelő titkosítással. Ezek a keretek ugyanakkor elsősorban technikai és információbiztonsági megfelelést biztosítanak, és nem jelentenek önmagukban demokratikus vagy alkotmányos jogalapot a rendőri működés MI-alapú ellenőrzésére. A rendszer egyik legjelentősebb strukturális hiányossága a demokratikus felhatalmazás és a független intézményi felügyelet korlátozott volta. Megállapítható, hogy az Egyesült Államokban a testkamerákhoz és az azokhoz kapcsolódó MI-alapú elemző eszközökhöz fűződő szabályozás fragmentált és hiányos; a bevezetésről és az alkalmazás módjáról jellemzően maguk a rendőri szervek döntenek, átfogó jogalkotási vita és egységes normarendszer nélkül (Heydari et al., 2025).

Az egyértelmű jogi felhatalmazás hiánya miatt egyes amerikai rendőri szerveknél szakmai és szakszervezeti ellenállás bontakozott ki a rendőri viselkedést monitorozó MI-funkciókkal szemben. Több esetben viták alakultak ki arról, hogy az ilyen rendszerek belső fegyelmezési vagy teljesítményértékelési eszközzé válhatnak, ami pilot projektek felfüggesztéséhez vagy a technológia alkalmazásának újratárgyalásához vezetett (Open Vallejo, 2023).

Az egyesült királyságbeli Find and Profile Tool, az USA-beli viselkedés-monitorozó eszközökkel ellentétben, szigorú jogi keretben működik. A 2018. évi adatvédelmi törvény 3. része, a 2012. évi szabadságvédelmi törvény és a 2023. szeptemberi NPCC AI Covenant hat alapelve (jogszerűség, átláthatóság,

magyarázhatóság, felelősség, elszámoltathatóság, robusztusság) biztosítja a garanciákat.³

A rendszer többek között az automatikus rendszámfelismerő adatokat elemzi a county lines kábítószer-kereskedelem azonosítására.⁴ A rendszer jogszerű és arányos működését többszintű garanciarendszer biztosítja, amely magában foglalja a független szakmai felügyeletet ellátó Independent Advisory Group (IAG) működését, az adatvédelmi hatóság (Information Commissioner's Office) felügyeleti ellenőrzéseit, valamint a hozzáférések teljes körű és visszakövethető naplózását (*Liberty Investigates*, 2025).

A sikeres MI-alapú rendvédelmi rendszerek mellett olyan sikertelen kezdeményezések is bemutatásra kerülnek, amelyeknél a jogi felhatalmazás, a szükségesség-arányosság vagy az átláthatóság hiánya miatt nem lehetett továbbműködtetni.

MI-alapú rendszerek kudarcai, alkotmányossági korlátok

SyRI – A holland adatelemző MI-rendszer működésének tapasztalatai

A System Risk Indication (SyRI) adatelemző rendszert Hollandiában 2014-től alkalmazták a szociális ellátásokkal kapcsolatos visszaélések feltárása érdekében, melynek keretében több állami és önkormányzati adatbázist összekapcsoltak és automatizált kockázatelemzést végeztek. A Hágai Kerületi Bíróság 2020. február 5-én hozott ítéletében (C-09-550982) megállapította, hogy a rendszer működtetése sérti az Emberi Jogok Európai Egyezményének 8. cikkében biztosított magán- és családi élet tiszteletben tartásához való jogot. Ennek következtében a bíróság hatályon kívül helyezte a SyRI alkalmazását lehetővé tevő SUWI⁵ törvény rendszerre vonatkozó részeit (*AI Law Hub*, 2020).

A bíróság megállapította, hogy az algoritmus nem volt átlátható, az érintetteket nem tájékoztatták, és a rendszer pontos működését még a bíróság sem tudta megállapítani. A kormány álláspontja szerint ennek az volt az oka, hogy a rendszer működésének közzététele esetén az állampolgárok „kijátszották volna” a rendszert. Mindamellet a rendszert kizárólag „problémás” negyedekben alkalmazták:

- 3 Egyesült Királyságban a National Police Chiefs' Council által elfogadott, jogilag nem kötelező erejű (soft law) normatív keretrendszer, amely a rendészeti célú MI-alkalmazások fejlesztésére és használatára vonatkozó alapelveket rögzíti.
- 4 County lines: az Egyesült Királyságban azonosított kábítószer-kereskedelmi működési modell, amelynek lényege városi bünszervezetek vidéki terjeszkedése, a mobiltelefon-hálózatok és közlekedési infrastruktúra rendszeres használata, valamint a kiszolgáltatott személyek bevonása a terjesztésbe.
- 5 Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI): a holland szociális és foglalkoztatási igazgatás intézményi és adatkezelési kereteit szabályozó törvény.

alacsony jövedelmű, magas bevándorló arányú területeken. Az ENSZ különleges jelentéstevője véleményében megfogalmazta, hogy a rendszer működése „*indokolatlan kirekesztéshez, diszkriminációhoz és stigmatizációhoz vezethet*” (United Nations Special Rapporteur on Extreme Poverty and Human Rights, 2019).

A holland kormány nem élt jogorvoslattal a döntés ellen, helyette a rendszert véglegesen megszüntette. A döntés nemzetközi jelentőségűvé vált, mivel első esetben állítottak le rendvédelmi MI-rendszert emberi jogi indokok miatt.

VERIPOL – Módszertani hiányosságok

A spanyol nemzeti rendőrség 2018-tól alkalmazta a természetes nyelv feldolgozáson alapuló VERIPOL rendszert, a feltételezetten hamis rablási bejelentések kiszűrésére. A rendszer működését 2024 októberében megszüntették, azt követően, hogy a Valenciái Egyetem 2024 szeptemberében közzétett értékelő jelentése súlyos módszertani és jogi hiányosságokat tárt fel (Universitat de València, 2024).

A Valenciái Egyetem tanulmánya három kiemelten problematikus tényezőt azonosított. Egyrészt a rendszert mindössze 1122 rablási bejelentés alapján tanították be 2015-ben, ami a spanyolországi évi mintegy 60 000 rablási ügy kevesebb mint két százalékát jelenti, így a tanítóadat-állomány sem mennyiségében, sem reprezentativitásában nem volt alkalmas megbízható prediktív modell kialakítására. Másrészt az összes tanítóadatot egyetlen rendőrtiszt minősítette „kiterjedt kihallgatási és hazugságvizsgálati tapasztalata” alapján, ami jelentős szubjektív torzítás és intézményes előítéletek beépülésének kockázatát hordozta. Harmadrészt a rendszer alapfeltevése empirikusan megalapozatlan volt, abból indult ki, hogy mivel a rablási ügyek mintegy 80%-a megoldatlan marad, ezért a bejelentések 57%-a szükségszerűen hamis. Ezzel szemben a hivatalos statisztikák szerint a hamis rablási bejelentések aránya 2015-ben mindössze körülbelül 4% volt (Ministerio del Interior, 2016).

Adatvédelmi szempontból hiányossággként értékelhető, hogy nem áll rendelkezésre bizonyíték a GDPR 35. cikke szerinti adatvédelmi hatásvizsgálat (DPIA) elvégzésére, továbbá a személyes adatok kezelésének jogalapja a GDPR 6. cikke alapján nem került egyértelműen meghatározásra. Emellett felmerül a GDPR 22. cikkében rögzített, kizárólag automatizált döntéshozatal tilalmának megsértése is, mivel a VERIPOL által generált kockázati besorolás alapján a rendőrség hamis bejelentés gyanúja miatt indított eljárásokat, amelyek büntetőjogi következményekkel járhattak. Az érintetteket nem tájékoztatták az automatizált feldolgozás tényéről, nem biztosítottak számukra jogorvoslati lehetőséget, és nem férhettek hozzá a döntéshozatal logikájához sem (GDPR, 2016).

A tényszerű értékeléshez hozzátartozik, hogy a rendszer gyakorlati alkalmazása idővel jelentősen visszaesett, míg 2019-ben még 49 702 bejelentést elemeztek a VERIPOL segítségével, addig 2022-ben már csupán 3762 esetben alkalmazták, ami a rendszer szakmai és intézményi hitelvesztésére utal. A spanyol bíróságok következetesen elutasították a VERIPOL eredményeinek bizonyítékként történő felhasználását (García et al., 2025).

Nem hagyható figyelmen kívül a rendszer leállításának időzítése sem, az EU AI Act 2024. júliusi kihirdetését követően mindössze három hónappal, 2024 októberében került sor a rendszer megszüntetésére. Tekintettel arra, hogy a VERIPOL funkcionálisan „hazugságvizsgáló” jellegű kockázati profilalkotást végzett bűnüldözési célból, nagy valószínűséggel a rendelet szerinti magas kockázatú MI-rendszernek minősült volna, amely jelentős megfelelési kötelezettségeket vont volna maga után (European Union, 2024).

Németország és Franciaország: Az alkotmányosság határai

A német belbiztonsági jogalkotás 2024–2025-ben egymást követő, tartalmilag összefüggő kezdeményezések révén kísérletet tett a biometrikus adatfeldolgozás és az MI-alapú elemzési eszközök rendszeti alkalmazásának kiterjesztésére. Mind a 2024-es, mind a 2025-ös javaslat közös célja az volt, hogy az arcfelismerést és az internetes forrásokból történő adatfelhasználást a bűnüldözés rendszeres eszközévé tegye (Bundesministerium des Innern und für Heimat, 2024, 2025).

A 2024 augusztusában benyújtott törvénytervezet a Szövetségi Bünyügyi Rendőrség (Bundeskriminalamt, BKA) és a Szövetségi Rendőrség (Bundespolizei) számára tette volna lehetővé, hogy erőszakos bűncselekményekről készült videofelvételeken szereplő arcképeket nyilvánosan hozzáférhető internetes tartalmakkal, különösen közösségi médiában található képekkel vessenek össze (BMI, 2024). A javaslat adatvédelmi és alkotmányossági kritikákat váltott ki, mivel az internetes képek felhasználása szükségszerűen nagyszámú, „nem érintett” személy biometrikus adatának feldolgozásával járt volna. A szakmai elemzések rámutattak arra, hogy az ilyen típusú arcfelismerés sérti az információs önrendelkezéshez való jogot és az arányosság elvét, valamint a célhoz kötött adatkezelés sem valósul meg (AlgorithmWatch, 2024; Lewandowski, 2024). A javaslat végül nem jutott túl a politikai egyeztetés szakaszán, a Bundesrat szintjén is ellenállásba ütközött. Az újabb, 2025 nyarán előkészített új biztonsági csomag már rendszerszintű megközelítést alkalmazott. Ennek keretében a Szövetségi Belügyminisztérium két, 2025. június 26-i keltezésű törvénytervezetet

bocsátott előzetes egyeztetésre, amelyek jelenleg egyeztetési státuszban vannak. A tervezetek központi célja a rendészeti adatfeldolgozási kapacitások jelentős bővítése, amely egyrészt magában foglalja a biometrikus – elsősorban arckép – adatok nyilvánosan hozzáférhető internetes forrásokban történő kereshetőségének megteremtését, másrészt az automatizált, big data és MI-alapú adatelemzési módszerek rendészeti célú alkalmazását, továbbá lehetővé tenni informatikai rendszerek fejlesztését és tesztelését személyes adatok felhasználásával (BMI, 2025). A tervezetek széles körű civil és szakmai kritikát váltottak ki. Civil szervezetek szerint a javaslatok egy „gigantikus arckép adatbázis” létrehozásához vezetnének, amely válogatás nélkül gyűjtött online képekre épülne, és ellentétes lenne az uniós joggal (AlgorithmWatch, 2025). A Német Ügyvédi Kamara állásfoglalása hangsúlyozta, hogy az arcfelismerés nemcsak az érintett személyeket vizsgálja, hanem mindenkit, aki a megfigyelési körbe kerül, ami súlyos alapjogi beavatkozást jelent (Deutscher Anwaltverein, 2025).

Mindkét javaslat komoly alkotmányossági kockázatokat vet fel a Német Szövetségi Alkotmánybíróság ítélkezési gyakorlata alapján, amely következetesen szigorú feltételekhez köti az automatizált adatösszekapcsolást és prediktív elemzést (Bundesverfassungsgericht, 1983, 2016, 2023).

Uniós jogi szempontból a javaslatok különösen problematikusak az EU AI Act rendelkezéseivel összefüggésben. Az EU AI Act 2025 februártól hatályos szabályai kifejezetten tiltják a nyilvánosan hozzáférhető képek cél nélküli gyűjtésén alapuló arcfelismerő adatbázisok létrehozását, különösen rendészeti célokra (European Union, 2024). A 2025-ös német tervezet e tilalmat funkcionálisan megkerülni látszik, ami felveti az uniós jog közvetlen alkalmazandóságának kérdését is.

Franciaország a 2024-es párizsi olimpiai és paralimpiai játékok biztonságának garantálása érdekében kísérleti jelleggel vezette be az MI-alapú videómegfigyelésre vonatkozó jogi szabályozást. A szabályozás alapját a 2023. május 19-én elfogadott, 2023-380. számú törvény (Loi relative aux Jeux Olympiques et Paralympiques de 2024) 10. cikke képezte, amely 2025. március 31-ig engedélyezte az videókamerás védelmi rendszerek alkalmazását meghatározott körülmények között, elsősorban nagy tömegrendezvényeken és közlekedési csomópontokban.

A törvényi felhatalmazást a 2023. augusztus 28-i 2023-828. számú végrehajtási rendelet részletezte, amely tételesen felsorolta azokat az eseménytípusokat, amelyek automatikus képelemzéssel detektálhatók. Az elemzés kizárólag nyolc, előre meghatározott esemény észlelésére volt használható (haladási irány megsértése; tiltott vagy érzékeny területre való belépés, illetve ott-tartózkodás; tömeg szokatlan mozgása; túlzott zsúfoltság, a tömeg rendellenes növekedése;

elhagyott csomag vagy tárgy jelenléte; fegyver jelenléte vagy használata; földön fekvő személy észlelése; tűz keletkezése). A francia jogalkotás kifejezetten kizárta az arcfelismerést, a biometrikus azonosítást, a személyek adatbázisokkal való összevetését, valamint a kizárólagos automatizált döntéshozatalt a modell működéséből. A rendszer logikája szerint az algoritmusok csupán riasztási jelzéseket adhatnak, amelyek értékelése és az esetleges intézkedés meghozatala minden esetben az „emberi” döntéshozó feladata. A szabályozás alkotmányosságát a Francia Alkotmánytanács a 2023. május 17-i 2023-850 DC határozatában vizsgálta. A testület a törvényt összességében alkotmányosnak ítélte, ugyanakkor hangsúlyozta, hogy az intézkedés csak szigorú garanciák mellett alkalmazható. Ezek közé tartozik különösen az időbeli korlátozottság, a célhoz kötöttség, a nyilvánosság előzetes tájékoztatása, valamint az a kötelezettség, hogy az engedélyt haladéktalanul vissza kell vonni, amennyiben az alkalmazás feltételei már nem állnak fenn. A jogalkotó ezen felül havi megújításhoz kötötte az engedélyezést, és előírta a kísérlet jövőbeni parlamenti értékelését. A rendszer bevezetését ennek ellenére jelentős civil és szakmai ellenállás kísérte. 2023 tavaszán 38 civil szervezet – köztük az Amnesty International és a Human Rights Watch – nyílt levélben figyelmeztetett arra, hogy a szabályozás a tömeges megfigyelés normalizálásához vezethet, és hosszabb távon „disztópikus megfigyelő állam” irányába tolhatja el Franciaországot. A kritikák hangsúlyozták, hogy bár a jogszabály formálisan kizárja a biometrikus azonosítást, az algoritmikus képelemzés fokozatos kiterjesztése funkcióbővüléshez (function creep) vezethet. A civil ellenállás 2024-ben új szintre lépett, amikor La Quadrature du Net panaszt nyújtott be a CNIL-hez⁶ amiatt, hogy francia közlekedési ágazatban már folytak olyan kutatás-fejlesztési projektek, amelyek valós környezetben tesztelték a videófelvételek automatizált elemzését. Ezek közé tartozott a francia állami vasúttársaság (SNCF) és a párizsi közösségi közlekedést üzemeltető vállalat (RATP) által koordinált Prevent PCP projekt, amely MI fejlesztését és kipróbálását célozta a közlekedési környezetben előforduló események (például elhagyott tárgyak vagy rendellenes mozgásminták) észlelésére, mivel a tesztelés kiterjedt a valós utasforgalmat figyelő kameraképekre is, valamint a projekt egyes szakaszai megelőzték az algoritmikus videómegfigyelésre vonatkozó törvényi felhatalmazást adó 2023-as olimpiai jogszabályt. A francia szabályozás megítélését tovább bonyolítja az Európai Adatvédelmi Testület (EDPB) 05/2022. számú iránymutatása. Az iránymutatás szerint a biometrikus adat fogalma nem korlátozódik kizárólag az arcképre, hanem kiterjedhet viselkedési jellemzőkre is, amennyiben azok technikai feldolgozása egy személy egyedi

6 Francia Nemzeti Adatvédelmi és Információszabadság Hatóság.

kiválasztását vagy megkülönböztetését teszi lehetővé a tömegből. A testtartás, a járás, a mozgásminták vagy gesztusok ilyen esetben – még személyhez nem kötötten is – biometrikus adatkezelésnek minősülhetnek. A francia jogalkotás előírta, hogy a kormánynak 2024. december 31-ig értékelő jelentést kell benyújtania a parlamentnek az algoritmikus videómegfigyelés hatékonyságáról és alapjogi következményeiről. Ennek ellenére 2025 elején már napirendre került a technológia közlekedési ágazatban történő állandósításának lehetősége, még az olimpiai értékelés teljes körű lezárása előtt. E törekvést azonban a francia Alkotmánytanács 2025. április 24-én megsemmisítette, arra hivatkozva, hogy a hosszabbítás tárgyidegen módosításként („cavalier législatif”) került volna be egy másik jogszabályba.

Tanulságok a magyar jogalkalmazás számára

A bemutatott nemzetközi esettanulmányok elemzése alapján megállapítható, hogy az MI-alapú rendvédelmi rendszerek sikere vagy kudarca döntően három tényezőtől függ: a jogszabályi felhatalmazás egyértelműségétől, az átláthatóság biztosításától, valamint a független felügyeleti mechanizmusok működésétől. Ez a három pillér – amelyet a spanyol VioGén 2, az EU IAMI projekt és az egyesült királyságbeli Find and Profile Tool sikeres működése igazol – Magyarországon is irányadónak tekinthető. A sikertelen projektek – így a holland SyRI, a spanyol VERIPOL és a német biometrikus azonosítási javaslatok – tanulságai egyértelműen rámutatnak arra, hogy az átláthatóság hiánya, a célhoz kötöttség elvének érvényesítése, valamint az arányossági teszt mellőzése ellehetetleníti a rendszerek sikerét (AI Law Hub, 2020; García et al., 2025). A francia olimpiai videómegfigyelési kísérlet ugyanakkor azt is mutatja, hogy megfelelő alkotmányos garanciák és időbeli korlátozások mellett a kísérleti jellegű bevezetés is lehetséges, bár a funkcióbővülés (function creep) veszélye ezekben az esetekben is valós fenyegetés lehet. Jelen tanulmány célja, hogy a nemzetközi tapasztalatok szintézisére építve stratégiai javaslatokat fogalmazzon meg a magyar jogalkotás és jogalkalmazás számára, különös tekintettel az EU AI Act tiltott gyakorlataira és a magas kockázatú MI-rendszerekre vonatkozó követelményekre. Az EU AI Act 2024. augusztus 1-jén lépett hatályba, és a tiltott gyakorlatokra vonatkozó rendelkezései 2025. február 2-től alkalmazandók. Magyarországon a 2025. évi LXXV. törvény 2025. december 1-jén lépett hatályba, amely megteremtette az EU AI Act végrehajtásának nemzeti kereteit. A törvény létrehozta a Magyar Mesterséges Intelligencia Hivatalt és a Magyar Mesterséges Intelligencia Tanácsot, kijelölte a piacfelügyeleti hatóságot (Nemzetgazdasági Minisztérium

keretén belül) és a bejelentő hatóságot (Nemzeti Akkreditáló Hatóság). A rendvédelmi célú MI-rendszerek szempontjából különös jelentőségű, hogy az EU AI Act 5. cikke kifejezetten tiltja a valós idejű távoli biometrikus azonosítást nyilvános helyeken, valamint a profilalkotásra és bűnözői előéletre alapozott prediktív rendészetet (Európai Parlament, 2024). A rendelet III. mellékletének 1. és 6. pontja értelmében a bűnüldözési célú biometrikus azonosítás magas kockázatú MI-rendszernek minősül, amely szigorú megfelelőségi kötelezettségeket von maga után, beleértve az alapjogi hatásvizsgálatot, az EU adatbázisba történő regisztrációt és a megfelelőségértékelési eljárást. A Nemzeti Adatvédelmi és Információszabadság Hatóság 2022-ben precedensértékű határozatot hozott egy pénzügyi intézmény MI-alapú hangelemző rendszerével kapcsolatban (NAIH-85/2022). A hatóság rekordösszegű bírságot szabott ki, megállapítva, hogy az adatkezelő nem rendelkezett joggalappal az ügyfélszolgálati hangfelvételek automatikus elemzéséhez, nem biztosította az átláthatóságot, és nem végezte el megfelelően az adatvédelmi hatásvizsgálatot (Bojnár & Pünkösty, 2022). Ez a döntés több szempontból is irányadó a rendvédelmi MI-rendszerek számára, megerősíti a GDPR 35. cikke szerinti adatvédelmi hatásvizsgálat kötelező jellegét, hangsúlyozza a GDPR 22. cikke szerinti automatizált döntéshozatal tilalmának érvényesülését, amennyiben az MI-rendszer döntése joghatással bír az érintettre. A LED 10. cikke szerint a biometrikus adatok feldolgozása csak „szigorúan szükséges” esetben megengedett, és az Európai Adatvédelmi Testület 05/2022-es iránymutatása szigorú korlátokat szab az arcfelismerő technológiák bűnüldözési célú alkalmazásának. Az iránymutatás szerint a biometrikus adat fogalma nem korlátozódik az arcképre, hanem kiterjedhet viselkedési jellemzőkre is, amennyiben azok technikai feldolgozása egy személy egyedi azonosítását teszi lehetővé.

Szabályozási és jogalkalmazási megfelelőség kulcselemei

A nemzetközi tapasztalatok alapján az alábbi stratégiai irányok javasolhatók Magyarország számára az MI-alapú rendvédelmi rendszerek esetében. A VERIPOL és SyRI kudarcából levonható legfontosabb tanulság, hogy az MI-rendszerek működésének átláthatónak kell lennie a jogállami keretek között. Így biztosítani kell, hogy minden rendvédelmi MI-rendszer működési logikája – legalább a döntéshozatali kritériumok szintjén – nyilvánosan hozzáférhető legyen. Alapjogi szempontból elvárható – az IAMI projektben megvalósított módon – már a tervezési fázisba integrált alapjogi hatásvizsgálat és adatvédelmi hatásvizsgálat kötelezővé tétele minden magas kockázatú rendszer esetén (Necz, 2020).

A VioGén 2 sikerének kulcsa, hogy 37 kockázati változót értékel, de minden változó szükségességét külön igazolták (López-Ossorio et al., 2018).

A magyar szabályozásnak – összhangban az Alkotmánybíróság információs önrendelkezésre vonatkozó gyakorlatával – meg kell határoznia az MI-alapú döntéshozatal konkrét feltételeit és korlátait. A francia olimpiai videómegfigyelési modell és az EU AI Act 57–62. cikkei által előírt szabályozói tesztkörnyezet kombinálása optimális megoldás, amelynek jogi kereteit meghatározta a 2025. évi LXXV. törvény, és amelyet a Magyar Mesterséges Intelligencia Hivatal fog működtetni.

A nemzetközi tapasztalatok alapján indokolt, hogy a tesztkörnyezetben működő rendszerek időbeli korlátozás alá esnek, és az értékelést független szakértői testület végezze. Az intézményi garanciák terén az egyesült királyságbeli Find and Profile Tool sikerének egyik kulcseleme egy független testület bevonása a rendszer működésének ellenőrzésébe. Magyarországon a NAIH jogosítványait ki kellene egészíteni az MI-specifikus felügyeleti hatáskörökkel, vagy az EU AI Act 70. cikkével összhangban a Magyar Mesterséges Intelligencia Hivatal keretében önálló, független felügyeleti testületet lehetne létrehozni. Az Európai Adatvédelmi Testület MI-auditálási projektje megfelelő módszertani alapot kínál a megvalósításhoz (EDPB AI Auditing).

A VioGén-ügy – amelyben a *New York Times* oknyomozó újságírói tártak fel kritikus hiányosságokat – rámutat arra, hogy még a jogilag megfelelő rendszerek is kudarcot vallhatnak, ha az MI pontossága nem megfelelő (Satariano & Toll Pifarré, 2024). A technikai követelmények vonatkozásában a VERIPOL kudarcának egyik fő oka az volt, hogy mindössze 1122 esetből álló, egyetlen rendőrtiszt által minősített tanítóadat-állomány nem volt reprezentatív az évi mintegy 60 000 rablási ügyre vetítve. A magyar szabályozásnak minimális adatminőségi és reprezentativitási követelményeket kell meghatároznia, összhangban az AI Act 10. cikkével.

A francia Alkotmánytanács hangsúlyozta, hogy az MI döntés javaslatainak értékelése és az intézkedés meghozatala minden esetben emberi döntéshozó feladata, amelyet az EU AI Act 14. cikke is kötelezővé tesz a magas kockázatú rendszereknél. A SyRI-ügyben az ENSZ különleges jelentéstevője rámutatott, hogy a rendszer alacsony jövedelmű, magas bevándorlói arányú területeken való kizárólagos alkalmazása „indokolatlan kirekesztéshez, diszkriminációhoz és stigmatizációhoz” vezethet (United Nations Special Rapporteur, 2019). A holland bíróság döntésében kimondta, hogy az átláthatóság hiánya és a hátrányos helyzetű csoportok aránytalanul magas érintettsége az Emberi Jogok Európai Egyezménye 8. cikkének sérelmét valósítja meg.

Összegzés

A nemzetközi esettanulmányok elemzése egyértelműen alátámasztja, hogy az EU AI Act paradigmaváltást jelent a rendvédelmi technológiák szabályozásában. Míg a korábbi időszakban a tagállamok fragmentált és gyakran reaktív módon kezelték az MI-alapú rendészeti alkalmazásokat, addig az EU AI Act egységes normatív keretet teremt, amely ex ante – azaz már a fejlesztési és telepítési fázisban – érvényesíti az alapjogvédelmi követelményeket. A tiltott gyakorlatok 2025. február 2-i hatálybalépése és a magas kockázatú rendszerekre vonatkozó kötelezettségek alkalmazandóvá válása közötti átmeneti időszak lehetőséget biztosít a tagállamok, így Magyarország számára is, hogy a meglévő rendszereiket felülvizsgálják és a jogszerű működés feltételeit megteremtsék.

A vizsgált esetek rávilágítanak arra is, hogy az MI-alapú rendvédelmi rendszerek sikeressége nem kizárólag technológiai, hanem elsősorban jogállami kérdés. A holland SyRI, a spanyol VERIPOL és a német biometrikus javaslatok kudarca egyaránt azt mutatja, hogy a legfejlettebb technológiai megoldások is fenntarthatatlanná válnak, amennyiben hiányzik a demokratikus legitimitás, az átláthatóság és a független felügyelet hármasa. Ezzel szemben a spanyol VioGén 2, az EU IAMI projekt és az egyesült királyságbeli Find and Profile Tool sikere bizonyítja, hogy a jogszabályi felhatalmazás egyértelműsége, a célhoz kötöttség szigorú érvényesítése és a folyamatos értékelési mechanizmusok beépítése lehetővé teszi a hatékony és alapjogkonform működést. A magyar jogalkotásnak és jogalkalmazásnak ezen modellekből merítve kell kialakítania a hazai rendvédelmi MI-rendszerek szabályozási kereteit.

Jelen tanulmányban a vizsgált esetek többsége európai jogi környezetben értelmezhető, így az angolszász modellek adaptálhatósága további kutatást igényel. Ugyanakkor a nemzetközi tapasztalatok szintézise egyértelműen igazolja, hogy a technológiai innováció és az alapjogvédelem nem egymást kizáró, hanem egymást feltételező célok. Az MI rendvédelmi alkalmazása csak akkor szolgálhatja eredményesen a közbiztonságot, ha az a jogállami keretek tiszteletben tartásával, az emberi méltóság védelmével és a demokratikus elszámoltathatóság biztosításával valósul meg. Magyarország – az EU AI Act implementációjával, a Magyar Mesterséges Intelligencia Hivatal létrehozásával és a szabályozói tesztkörnyezet működtetésével – megfelelő alapokkal rendelkezik ahhoz, hogy a nemzetközi élvonalhoz tartozó, jogszerű és hatékony rendvédelmi MI-rendszereket alakítson ki, e cél megvalósítása azonban folyamatos szakmai párbeszédet, rendszeres hatásvizsgálatot és a nemzetközi fejlemények nyomán követését teszi szükségessé.

Az EU AI Act jövőbeli alkalmazását jelentősen befolyásolhatja az Európai Bizottság 2025. november 19-én közzétett Digitális Omnibusz csomagja (Digital Omnibus on AI), amely célzott módosításokat javasol az MI-re vonatkozó rendelet végrehajtásának egyszerűsítése érdekében. A csomag a magas kockázatú MI-rendszerekre vonatkozó kötelezettségek hatálybalépését 2027. decemberig halasztja, figyelembe véve a technikai szabványok kidolgozásának késedelmeit és a tagországok felkészülési igényeit. A rendvédelmi MI-alkalmazások szempontjából kiemelendő, hogy az omnibusz csomag nem érinti az EU AI Act 5. cikkében rögzített tiltott gyakorlatokat – így a valós idejű távoli biometrikus azonosítás tilalmát, a prediktív rendészet korlátait –, amelyek 2025. február 2-től változatlanul érvényesek. A módosítások ugyanakkor bővítik a szabályozói tesztkörnyezetek alkalmazási lehetőségeit, és ösztönzik a valós körülmények közötti tesztelést, ami a rendvédelmi MI-rendszerek jogszerű és hatékony fejlesztését szolgálhatja. A magyar jogalkotás és jogalkalmazás számára az omnibusz csomag egyértelművé teszi, hogy az alapjogvédelmi garanciakeret stabil marad, miközben a gyakorlati megvalósítás rugalmassága növekedhet.

Felhasznált irodalom

- AI Law Hub (2020). *The SyRI judgment*. <https://ai-lawhub.com/spring-2020-syri-judgment/>
- AlgorithmWatch (2024). *Stellungnahme zur biometrischen Datenverarbeitung*. AlgorithmWatch.
- AlgorithmWatch (2025). *Stellungnahme zur biometrischen Internetfahndung*. AlgorithmWatch.
- Amnesty International (2023). *France: Intrusive Olympics surveillance technologies could usher in a dystopian future*.
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR). *Az Európai Unió Hivatalos Lapja*, L 119, 1–88.
- Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a büncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról (LED). *Az Európai Unió Hivatalos Lapja*, L 119, 89–131.
- Bojnár K., & Pünköszt A. (2022). *Úttörő szerepben a NAIH a bizalomra épülő mesterséges intelligencia alkalmazások kiépítésében?* Ludovika.hu, ITKI Blog.
- Bundesministerium des Innern und für Heimat (2024). *Referentenentwurf eines Gesetzes zur Erweiterung polizeilicher Befugnisse im Bereich biometrischer Identifizierung*. BMI.

- Bundesministerium des Innern und für Heimat (2025, június 26.). *Referentenentwurf eines Sicherheitspakets zur Nutzung automatisierter Datenanalyse und biometrischer Daten*. BMI.
- Bundesverfassungsgericht (1983). Volkszählungsurteil. *BVerfGE* 65, 1.
- Bundesverfassungsgericht (2016). Automatisierte Kennzeichenerfassung. *1 BvR 142/15*.
- Bundesverfassungsgericht (2023). Automatisierte Datenanalyse in Polizeigesetzen der Länder. *1 BvR 1547/19; 1 BvR 2634/20*.
- Conseil constitutionnel (2023, május 17.). *Décision n° 2023-850 DC*.
- Conseil constitutionnel (2025, április 24.). *Décision relative à la prolongation de la vidéoprotection algorithmique*.
- Deutscher Anwaltverein (2025). *Stellungnahme Nr. 28/2025 zur automatisierten Datenanalyse und biometrischen Gesichtserkennung*.
- Entcheva, K., & Mazilescu, I. (2024). Artificial intelligence and digitalisation of judicial cooperation: The main provisions in recent EU legislation. *Eucrim*, 2024(3). <https://doi.org/10.30709/eucrim-2024-018>, <https://eucrim.eu/articles/artificial-intelligence-and-digitalisation-of-judicial-cooperation/>
- Eticas Foundation & Ana Bella Foundation (2022). *External audit of VioGén: Spain's algorithm designed to protect victims of gender violence*. Montreal AI Ethics Institute. <https://eticas-foundation.org/the-external-audit-of-the-viogen-system/>
- Európai Adatvédelmi Testület (2022). *05/2022 iránymutatás az arcfelismerő technológia bűnüldözési célú alkalmazásáról*. EDPB.
- Európai Parlament és Tanács (2024). Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról (AI Act). *Az Európai Unió Hivatalos Lapja*, L sorozat.
- European Commission (2025). *Proposal for a Regulation amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)* (COM(2025) 836)
- García, T., Torrecillas, C., Maqueda, A., & Cabo, D. (2025, március 19.). La Policía Nacional deja de usar Veripol, su IA estrella para detectar denuncias falsas. *Civio*. <https://civio.es/tecnologia/2025/03/19/la-policia-nacional-deja-de-usar-veripol/>
- Heydari, F., Isaacs, M., Kinsey, K., Friedman, B., Slobogin, C., & Heydari, A. M. (2025). Putting Police Body-Worn Camera Footage to Work: A Civil Liberties Evaluation of Truleo's AI Analytics Platform. *Cardozo Law Review*, 46(6). <https://doi.org/10.2139/ssrn.5030758>
- Human Rights Watch (2023, március 7.). *France: Reject Surveillance in Olympic Games Law*.
- Interoperable Europe Portal (2024). *Viogen 5.0: Discovering Spain's risk assessment system of gender-based violence*. European Commission. <https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/viogen-50-discovering-spains-risk-assessment-system-gender-based-violence>
- La Quadrature du Net (2024). *Plainte à la CNIL – Prevent PCP*.
- Légifrance (2023a). *Loi n° 2023-380 du 19 mai 2023 relative aux Jeux Olympiques et Paralympiques de 2024*.

- Légifrance (2023b). *Décret n° 2023-828 du 28 août 2023 relatif aux traitements algorithmiques de vidéoprotection.*
- Lewandowski, D. (2024). *Warum datenbankfreie Gesichtserkennung technisch nicht möglich ist.*
- Liberty Investigates (2025). *Police given AI tech to track 'suspicious' car journeys.* <https://libertyinvestigates.org.uk/articles/police-ai-anpr-track-drivers/>
- López-Ossorio, J. J., González-Álvarez, J. L., Buquerín Pascual, S., García, L. F., & Buela-Casal, G. (2018). Integral monitoring system in cases of gender violence: VioGén system. *Behavior & Law Journal*, 4(1), 29–48. <https://doi.org/10.47442/blj.v4.i1.56>
- Ministerio del Interior (2016). *Estadística de criminalidad 2015.* Gobierno de España.
- Ministerio del Interior (2016). *Sistema VioGén.* Secretaría de Estado de Seguridad, Gobierno de España.
- Necz D. (2020). A mesterséges intelligencia adatvédelmi szempontjai, különös tekintettel a belügyi szervek adatkezelési gyakorlatára. *Rendvédelem*, 9(1), 135–165.
- Nemzeti Adatvédelmi és Információszabadság Hatóság (2022). *NAIH-85/2022. számú határozat.* NAIH.
- Open Vallejo (2023). *Under union pressure, Vallejo police chief ends body-camera analysis program.* <https://openvallejo.org/2023/07/09/under-union-pressure-vallejo-police-chief-ends-body-camera-analysis/>
- Rechtbank Den Haag (2020). *C-09-550982-HA ZA 18-388, ECLI:NL:RBDHA:2020:1878.*
- Satariano, A., & Toll Pifarré, R. (2024, július 18.). An algorithm told police she was safe. Then her husband killed her. *The New York Times.* <https://www.nytimes.com/interactive/2024/07/18/technology/spain-domestic-violence-viogen-algorithm.html>
- Sénat (2025). *Rapport d'information sur la vidéoprotection algorithmique.*
- Sentencia del Tribunal Constitucional (2008). *STC 59/2008.*
- United Nations Special Rapporteur on Extreme Poverty and Human Rights (2019). *Amicus curiae intervention in the case concerning the System Risk Indication (SyRI), Netherlands.*
- Universitat de València (2024). *Evaluación crítica del sistema VERIPOL aplicado por la Policía Nacional.* Universitat de Valencia.
- Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI).*

Alkalmazott jogszabályok

- A holland szociális és foglalkoztatási igazgatás intézményi és adatkezelési kereteit szabályozó törvény
2025. évi LXXV. törvény az Európai Unió mesterséges intelligenciáról szóló rendeletének magyarországi végrehajtásáról

A cikk APA szabály szerinti hivatkozása

Szabó H. (2026). Mesterséges intelligencia egyenruhában: Rendvédelmi MI-rendszerek nemzetközi sikerei és kudarcai jogi szempontból. *Belügyi Szemle*, 74(7), 1861–1878. <https://doi.org/10.38146/bsz-aija.2026.v74.i7.pp1861-1878>

Nyilatkozatok

Összeférhetetlenség

A szerző nem jelentett összeférhetetlenséget.

Finanszírozás

A szerző nem kapott pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.

Etikai nyilatkozat

Jelen cikkhez nem kapcsolódik adatkészlet.

Nyílt hozzáférésről szóló tájékoztatás

A közlemény nyílt hozzáféréssel, a Creative Commons Attribution–NonCommercial–NoDerivatives 4.0 International License (CC BY-NC-ND 4.0) feltételei szerint jelenik meg. A közlemény változatlan formában, nem kereskedelmi célból, bármely médiumban és formátumban szabadon megosztható és újraközölhető, feltéve, hogy az eredeti szerző(k), a közlés helye és a licenc hivatkozása megfelelően feltüntetésre kerül. Módosított vagy átdolgozott változat terjesztése, valamint kereskedelmi célú felhasználása nem megengedett.

Levelező szerző

A cikk levelező szerzője Szabó Hedvig, aki a szabo.hedvig@sze.hu e-mail címen érhető el.