NEMZETBIZTONSÁGI SZEMLE
11. évfolyam (2023) 4. szám 20–34. | DOI: 10.32561/nsz.2023.4.2

Sáfrán József[1]

A mesterséges intelligencia és a rendvédelmi szervek, valamint a közigazgatás kapcsolata[2]

Artificial Intelligence and the Relationship Between Law Enforcement and Public Administration

Az utóbbi időben a mesterséges intelligencia (Artificial Intelligence – AI) a figyelem középpontjába került, különösen a közigazgatási és biztonsági ágazatok területén. Nemcsak Magyarországon, de világszerte is, az AI lehetőséget teremt arra, hogy a biztonsági erők eredményesebben reagáljanak a különféle fenyegetésekre, miközben hatékonyságuk is növekszik. Az AI integrációjával azonban számos etikai és jogi kérdés is felmerül, különösen a személyes adatok védelmének és a polgári szabadságjogoknak a kontextusában, valamint az állami szerepvállalás terén. Ennek megértése érdekében fontos áttekinteni az AI-technológiát és a potenciális kihívásokat, amelyek demokratikus társadalmakban jelentkeznek annak alkalmazása során.

A tanulmányban elemzem az AI szabályozásának jelenlegi állapotát Magyarországon. Megvizsgálom azokat a normákat és irányelveket, amelyek szabályozzák annak alkalmazását a közszférában és a biztonsági erők körében. A mélyebb betekintés érdekében elitinterjút készítettem egy-egy vezető szakértővel a magyar biztonsági ágazatban, akik képet adnak arról, hogy jelenleg milyen formában és milyen mértékben alkalmazzák az AI-technológiát ezen a területen, illetve milyen jövőbeli lehetőségek állnak rendelkezésre. A tanulmány záró részében konklúziókat fogalmazok meg az AI és a magyar biztonsági szektor (a rendvédelmi szervek egy része és a Magyar Honvédség) közötti viszonyról, ideértve a pozitívumokat és a kockázatokat egyaránt, különös tekintettel a közigazgatásra. A nemzetközi összehasonlításban pedig megvizsgáljuk Magyarország viszonyulását az AI-hoz

[1] Adjunktus, Nemzeti Közszolgálati Egyetem Lőrincz Lajos Közigazgatási Jogi Tanszék, e-mail: safran.jozsef@uni-nke.hu

[2] A tanulmány a Kulturális és Innovációs Minisztérium ÚNKP-22-4-I-NKE-76 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

más országok gyakorlatával összevetve, ennek során kiemelünk néhány lehetséges fejlesztési irányt és legjobb gyakorlatot.

A vizsgálat fő célja, hogy átfogó képet adjon az AI és a magyar biztonsági erők közötti viszony dinamikájáról, fókuszálva a közigazgatásra és a jogra gyakorolt potenciális hatásaira.

Kulcsszavak: *mesterséges intelligencia, biztonság, kiberbiztonság, Magyar Honvédség, nemzetbiztonsági szolgálatok.*

In recent times, artificial intelligence (AI) has garnered significant attention, especially within the realms of public administration and security sectors. Not only in Hungary but globally, AI offers the prospect for security forces to respond more effectively to diverse threats, enhancing their overall efficiency. However, the integration of AI raises numerous ethical and legal concerns, particularly regarding personal data protection, civil liberties, and the role of the state. To comprehend this, it is imperative to review AI technology and the potential challenges that arise in its application within democratic societies.

This study analyzes the current state of AI regulation in Hungary, examining the standards and directives that govern its use in the public sector and among security forces. Additionally, the role of the information society and media in shaping public perception of AI, as well as its influence on the security sector, is scrutinized. For a deeper insight, we conduct an interview with a leading expert in the Hungarian security sector, who elucidates on the current extent and form of AI application in this domain and potential future avenues. In the concluding section of the study, we articulate insights about the relationship between AI and the Hungarian security sector (part of the law enforcement agencies and the Hungarian Defence Forces), including its advantages and risks, with a special focus on public administration. In an international comparison, we evaluate Hungary's approach to AI against practices in other countries, highlighting potential development directions and best practices.

The primary objective of this research is to provide a comprehensive understanding of the dynamic relationship between AI and Hungarian security forces, focusing on potential impacts on public administration and legal considerations.

Keywords: *Artificial Intelligence, Security, Cybersecurity, Hungarian Defence Forces, National Security Services.*

Bevezetés

A mesterséges intelligencia egyre fontosabb technológiává vált, és számos különböző területen széleskörűen alkalmazható. A mesterségesintelligencia-programozási szoftverek, mint például a C++, a Python és a Java, a mesterségesintelligencia-rendszerek fejlesztése során a legszélesebb körben használt programozási nyelvekké váltak.[3] Ebben a tanulmányban

[3] Tiobe 2023, lásd: www.tiobe.com/tiobe-index/

a mesterséges intelligencia felhasználását vizsgáljuk a civil világban és a biztonsági szolgálatokban, beleértve a titkosszolgálatokat és a hadsereget, különös tekintettel a felhasználás etikai és jogi vonatkozásaira.

A civil világban a mesterséges intelligencia számos iparágat forradalmasíthat, az egészségügytől a pénzügyeken át a közlekedésig és a szórakoztatásig. A mesterségesintelligencia-rendszereket már most is használják hatékonyabb és eredményesebb diagnosztikai eszközök kifejlesztésére, a pénzügyi piacok elemzésére, az ellátási lánc logisztikájának optimalizálására és az ügyfélkiszolgálás javítására számos különböző ágazatban. A mesterséges intelligencia széles körű alkalmazása várhatóan növeli a termelékenységet, és új lehetőségeket teremt a gazdasági növekedés számára. A McKinsey Global Institute jelentése szerint a mesterséges intelligencia 2030-ra 13 billió dollárral növelheti a globális gazdasági teljesítményt.[4]

A biztonsági szolgáltatások területén is egyre nagyobb jelentőséget kap az AI, különösen a hírszerzés és -elemzés terén. A titkosszolgálatok és a hadsereg az AI-technológiákat a helyzetfelismerés fokozására, nagy mennyiségű adat elemzésére és a potenciális fenyegetések azonosítására használják. A mesterséges intelligenciával működő drónokat és autonóm járműveket is fejlesztik, hogy fokozott megfigyelési és felderítési képességeket biztosítsanak. A mesterséges intelligencia alkalmazása a biztonsági szolgálatoknál azonban aggályokat vet fel a magánélet védelmével, az emberi jogokkal, valamint a visszaélésekkel és a visszaélések lehetőségével kapcsolatban.[5]

A mesterséges intelligencia polgári és biztonsági szolgálatokban való alkalmazásának etikai és jogi következményei egyaránt rendkívül fontosak. Ahogy a mesterséges intelligencia egyre elterjedtebbé válik, alapvető fontosságú annak biztosítása, hogy etikai és jogi kereteket hozzanak létre az e technológia által támasztott kihívások kezelésére. Az átláthatóság, az elszámoltathatóság és a méltányosság a felelős mesterségesintelligencia-fejlesztés és -alkalmazás kritikus elemei. Fontos figyelembe venni a mesterséges intelligencia alkalmazásával kapcsolatos lehetséges kockázatokat és nem szándékolt következményeket, és proaktív lépéseket kell tenni ezek mérséklésére.[6]

A polgári és biztonsági területeken a mesterséges intelligencia használatának etikai és jogi következményeinek megértését célzó kutatási és szakpolitikai erőfeszítések folyamatban vannak. A világ minden országában foglalkoznak ezekkel a kérdésekkel, és a mesterséges intelligencia etikáját és irányítását taglaló tudományos irodalomhoz többek között az Amerikai Egyesült Államok és Magyarország tudósai is jelentős mértékben hozzájárultak. Ez a tanulmány a mesterséges intelligencia biztonsági szolgálatokban történő felhasználásának vizsgálatával kíván hozzájárulni ehhez a folyamatban lévő beszélgetéshez, különös tekintettel az alkalmazás etikai és jogi következményeire.[7]

A mesterséges intelligencia alkalmazása a biztonsági szolgáltatásokban az elmúlt években nagy érdeklődés és aggodalom tárgyát képezte. A Szövetségi Nyomozó Iroda (Federal Bureau of Investigation, FBI) és a Központi Hírszerző Ügynökség (Central Intelligence Agency, CIA) az Egyesült Államok két legfontosabb biztonsági szerve, és a mesterséges

4 Chui 2018.
5 Buchanan–Konaev–Fedasiuk 2021.
6 Rowe 2022.
7 European Commission 2019.

intelligenciával és annak lehetséges alkalmazásaival kapcsolatos hozzáállásuk az idők során változott.

Az FBI és a CIA a megbízhatósággal és a magánélet védelmével kapcsolatos aggályok miatt csak lassan fogadta el a mesterségesintelligencia-technológiákat. A gépi tanulás és a természetes nyelvi feldolgozás terén a közelmúltban elért eredmények azonban egyre nagyobb érdeklődést váltottak ki ezekben az ügynökségekben a mesterséges intelligencia iránt. A mesterséges intelligenciát különösen a megfigyelés, a terrorizmus elleni küzdelem és a hírszerzési elemzés fokozásának potenciális eszközeként tartják számon.[8]

2017-ben az FBI Büntetőjogi Információs Szolgáltatások (Criminal Justice Information Services, CJIS) részlege bejelentette, hogy tervezi egy mesterségesintelligencia-alapú rendszer bevezetését az ujjlenyomat-elemzés pontosságának javítása érdekében. A Next Generation Identification (NGI) System nevű rendszer már gépi tanulási algoritmusokat használ az ujjlenyomatok gyorsabb és pontosabb elemzésére és összehasonlítására.

Egy 2020-as beszédében Christopher Wray, az FBI igazgatója kiemelte az ügynökség azon erőfeszítéseit, hogy a mesterséges intelligenciát és a gépi tanulást a kínai tevékenységek azonosítására és megszakítására használják. Megemlítette az AI által nyújtott lehetőségeket, mint például a sebezhetőségek felderítését, a kódírást, a célzott adathalászati kísérletek fejlesztését, amit például a kínaiak is aktívan használnak, valamint a virtuális emberrablások fejlett végrehajtását, ahol az AI képes utánozni egy gyermek hangját, így hitelesebbé téve a fenyegetéseket. Ezenfelül kifejezte az aggodalmát az AI-technológiák ellopása miatt is, különösen mivel Amerika vezető szerepet tölt be az AI-technológiában, és Kína különösen érdeklődik az amerikai AI-technológiák megszerzése iránt[9]

A CIA igazgatójaként Gina Haspel hangsúlyozta a technológia és az emberi tényező együttes fontosságát a hírszerzési műveletekben. Bár konkrétan a mesterséges intelligencia alkalmazására nem tér ki a McConnell Központban tartott beszédében, Haspel kiemelte az ügynökség elkötelezettségét a legújabb technológiák iránt. Ezen technológiák célja a rutinfeladatok automatizálása és az elemzői kapacitás felszabadítása volt, hogy az ügynökség szakemberei nagyobb hangsúlyt fektethessenek az összetettebb, stratégiai jelentőségű feladatokra. Haspel azon megközelítése, hogy a technológiai innovációkat az emberi tényezővel ötvözve kell alkalmazni, azt sugallja, hogy a CIA nem csupán a legfejlettebb eszközök bevetésére törekszik, hanem arra is, hogy azokat az ügynökség emberi erőforrásainak erősítésére használja.[10] Ez az integrált megközelítés lehetővé teheti az ügynökség számára, hogy hatékonyabban azonosítsa a nagy adathalmazokban rejlő mintákat és összefüggéseket, miközben fenntartja az emberi elemzés mélyreható, kritikus perspektíváit.Ezt erősíti meg Boda József és Dobák Imre írása, amely az új technológiák, köztük a mesterséges intelligencia hatását tárgyalja a hírszerzési adatok gyűjtésére és elemzésére. Megjegyzik, hogy a mesterséges intelligencia alkalmazása a hírszerzési munkában nagymértékben javíthatja az adatelemzés hatékonyságát és pontosságát. A mesterséges intelligencia hírszerzési munkában való alkalmazásának egyik fő előnye, hogy hatalmas mennyiségű adatot képes nagy sebességgel elemezni. Az AI-rendszerek gyorsan át tudják rostálni a nagy mennyiségű információt, például a közösségi médiában

8 Lásd: https://emerj.com/ai-sector-overviews/artificial-intelligence-fbi/

9 Wray 2020.

10 Lásd: www.cia.gov/stories/story/remarks-for-central-intelligence-agency-director-gina-haspel-mcconnell-center-at-the-university-of-louisville/

közzétett bejegyzéseket vagy műholdas képeket, és képesek olyan mintákat és összefüggéseket azonosítani, amelyeket az emberi elemzők esetleg nem vesznek észre. Ez segíthet a hírszerző ügynökségeknek abban, hogy gyorsabban és pontosabban azonosítsák a potenciális fenyegetéseket, és hatékonyabban osszák be az erőforrásokat. A szerzők azonban azt is megjegyzik, hogy a mesterséges intelligencia hírszerzési munkában való alkalmazása aggályokat vet fel a mesterségesintelligencia-rendszerek megbízhatóságával és elszámoltathatóságával kapcsolatban. Az AI-rendszerek csak annyira megbízhatóak, amennyire a rájuk képzett adatok, és ha az adatok elfogultak vagy hiányosak, az AI-rendszer pontatlan vagy megbízhatatlan eredményeket produkálhat. Ez különösen a hírszerzési munkában jelenthet gondot, ahol a pontatlan vagy elfogult adatok súlyos következményekkel járhatnak.[11]

Ezen erőfeszítések ellenére mind az FBI, mind a CIA szembesült kritikákkal és aggodalmakkal a mesterséges intelligencia műveleteikben való felhasználásával kapcsolatban. A kritikusok aggályokat fogalmaztak meg azzal kapcsolatban, hogy a mesterséges intelligencia elfogult vagy diszkriminatív lehet, és hogy a mesterségesintelligencia-alapú megfigyelés sértheti a polgári szabadságjogokat. Ezen aggályok kezelése érdekében az FBI és a CIA hangsúlyozta az átláthatóság és az elszámoltathatóság fontosságát a mesterséges intelligencia alkalmazása során.[12]

Összefoglalva: az FBI és a CIA növekvő érdeklődést mutat a mesterséges intelligencia és annak a biztonsági szolgálatokban való lehetséges alkalmazása iránt. Bár a mesterséges intelligencia alkalmazásával kapcsolatban vannak aggályok és kihívások, ezek az ügynökségek olyan felelős és etikus mesterségesintelligencia-rendszerek kifejlesztésén dolgoznak,[13] amelyek fokozhatják műveleteiket és javíthatják a nemzetbiztonságot.

Módszertan

Az elemzésemhez megvizsgáltam a demokrácia és a mesterséges intelligencia általános viszonyát, majd a mesterséges intelligencia általános felhasználását a rendvédelmi szervezeteknél, a katonaságnál és a nemzetbiztonsági szolgálatoknál. Kérdéssort állítottam össze, amely alapján interjút készítettem a különböző szervezetek releváns képviselőivel. Az interjúk során a következő személyekkel készítettem riportot:

- A Rendőrségnél Babus Andrea, Juhász Gyöngyike és Szabó János álltak rendelkezésemre.
- A Magyar Honvédség képviseletében prof. dr. Kovács László nyújtott bepillantást munkájába.
- A Katonai Nemzetbiztonsági Szolgálat részéről Svigruha Gyula válaszolt kérdéseimre.
- Végül a Nemzetbiztonsági Szakszolgálattól dr. Szabó Hedvig osztotta meg szakértelmét velem.

11 Boda–Dobák 2016.
12 Horowitz–Kreps 2021.
13 Roff–Asaro 2018.

Az elitinterjú használata az állapotanalízis során, különösen a mesterséges intelligenciával kapcsolatban, több lényeges ok miatt is kínálja magát. Elsődlegesen a mesterséges intelligencia területén dolgozó döntéshozók és vezetők véleménye gyakran nyújt mély betekintést a technológia aktuális helyzetébe, kihívásaiba és jövőbeli irányvonalaihoz. Azok, akik a társadalom elitjéhez tartoznak ezen a területen, gyakran rendelkeznek olyan specifikus és exkluzív információkkal, amelyek a szélesebb közönség számára nem mindig elérhetőek. A félig strukturált interjúk jellege lehetővé teszi, hogy a beszélgetések egy bizonyos irányvonalat kövessenek, ugyanakkor teret hagynak az interjúalanyoknak a spontán és saját szavaikkal való kifejezésre. Az ilyen interjúkban gyakran kerülnek felszínre az alapvető motivációk, elvárások és az MI-re vonatkozó stratégiai nézetek. Továbbá, az elitinterjúval feltárhatók a mesterséges intelligencia területén lévő társadalmi hálózatok, amelyek kulcsfontosságú információs forrásokká válhatnak a technológia állapotának jobb megértéséhez. Az interjúk során nemcsak az egyéni véleményeket értékeljük, hanem azokat a társadalmi és szervezeti kontextusokat is, amelyek meghatározzák ezeket a nézeteket és döntéseket.[14]

A vizsgálattal célom egy olyan állapotanalízis felállítása, amelynek segítségével megismerhetjük a magyar rendvédelmi szervek egy részének általános hozzáállását a mesterséges intelligencia felhasználásához, és ezt kiegészítem a Magyar Honvédséggel, hogy a jövőbeni kutatásokban még tágabb képet kapjunk a fegyveres szervek attitűdjéről.

A demokrácia és a mesterséges intelligencia viszonya

A demokrácia és az információs társadalom közötti kapcsolat az elmúlt években jelentős vita tárgyát képezte, különösen a mesterséges intelligencia térnyerésével. Miközben a mesterséges intelligencia számos pozitív módon átalakíthatja a társadalmat, jelentős kihívások elé állítja a demokráciát és az információs társadalom működését. Ebben az elemzésben a demokrácia és az információs társadalom kapcsolatának a mesterséges intelligenciával kapcsolatos problémás területeit és az ezek mögött meghúzódó okokat tárjuk fel.

Az egyik legproblematikusabb terület az adatvédelem és a felügyelet kérdése. A mesterségesintelligencia-technológiák nagymértékben támaszkodnak nagy adathalmazokra az algoritmusok betanításához, amelyek gyakran személyes adatokat is tartalmaznak. Ennek következtében fennáll a veszélye annak, hogy ezekkel az adatokkal visszaélnek, márpedig visszaélnek, ami jelentős következményekkel járhat az egyéni magánéletre és a demokráciára nézve. A mesterséges intelligencia megfigyelési célú felhasználása, különösen autoriter rezsimekben, szintén jelentős veszélyt jelenthet az emberi jogokra és a demokráciára. David Lyon és David Murakami Wood tudósok *Surveillance and Democracy* című tanulmányukban azzal érvelnek, hogy a megfigyelési technológiák, köztük a mesterséges intelligencia növekvő használata jelentős kockázatot jelent a demokratikus értékekre és intézményekre nézve.[15]

[14] Németh 2020: 390.
[15] Lyon–Wood 2013.

Egy másik problémás terület az elfogultság és a megkülönböztetés kérdése. A mesterséges intelligenciát alkalmazó rendszereket elfogult adatokon lehet betanítani, ami állandósíthatja és felerősítheti a meglévő társadalmi előítéleteket és diszkriminációt. Ez jelentős következményekkel járhat a marginalizált csoportokra, köztük a színes bőrűekre és a nőkre nézve, akik hátrányos megkülönböztetéssel szembesülhetnek olyan területeken, mint a foglalkoztatás és a büntetőjog. Kate Crawford és Ryan Calo tudósok *There is a Blind Spot in AI Research* című tanulmányukban azzal érvelnek, hogy a sokszínűség és a képviselet hiánya a mesterségesintelligencia-rendszerek fejlesztése során elfogult eredményekhez vezethet, és megerősítheti a meglévő hatalmi struktúrákat.[16]

A harmadik problémás terület az elszámoltathatóság és az átláthatóság kérdése. Az AI-rendszerek és döntéshozatali folyamataik összetettsége miat bonyolult lesz annak megértése, hogy hogyan jutottak egy adott döntésre. Ez megnehezítheti az AI-rendszerek felelősségre vonását döntéseikért, különösen az olyan területeken, mint a büntető igazságszolgáltatás és az egészségügy. A *Transparency in Algorithmic and Human Decision-Making: Is there a Double Standard?* című tanulmányban Margot Kaminski és Andrea Matwyshyn azzal érvelnek, hogy az átláthatóság és az elszámoltathatóság elengedhetetlen ahhoz, hogy az AI-rendszerek igazságosak és demokratikusak legyenek.[17]

Bár a mesterséges intelligencia számos pozitív módon átalakíthatja a társadalmat, jelentős kihívásokat is jelent a demokrácia és az információs társadalom működése szempontjából. Az adatvédelem és -felügyelet, az előítéletesség és diszkrimináció, valamint az elszámoltathatóság és átláthatóság problémás területei különösen aggasztóak, mivel jelentős következményekkel járnak – akár fegyverként is felhasználva[18] – az egyén magánéletére és a demokráciára nézve. Elengedhetetlen, hogy ezekkel a kérdésekkel foglalkozzunk annak biztosítása érdekében, hogy a mesterséges intelligenciát a demokratikus értékekkel és intézményekkel összhangban lévő módon fejlesszük és használjuk.

A mesterséges intelligencia általános felhasználása a rendvédelmi szervezeteknél, a katonaságnál és a nemzetbiztonsági szolgálatoknál

Fehér András Tibor és Négyesi Imre több példát is bemutatnak a mesterségesintelligencia-alapú kibertámadási modellekre. Az egyik ilyen modell gépi tanulási algoritmusokat használ nagy mennyiségű adat elemzésére és a célrendszerek sebezhetőségének azonosítására. Ez magában foglalhatja a hálózati forgalom és a rendszer naplóinak elemzését, hogy olyan tevékenységi mintákat azonosítson, amelyek potenciális gyenge pontra utalhatnak. Egy másik modell megerősítő tanulást használ a támadási stratégiák optimalizálására. Ebben a megközelítésben a mesterséges intelligenciát szimulált, tesztkörnyezetben képzik ki, hogy megtanulja, hogyan kell azonosítani és kihasználni a célrendszer sebezhetőségeit.

16 Crawford–Calo 2016: 311–313.
17 Kaminski–Matwyshyn 2016: 139–181.
18 Scharre 2018.

A szerzők a mesterséges intelligencia lehetséges előnyeit is tárgyalják a kibervédelemben. A mesterséges intelligencia például nagy mennyiségű adat elemzése és a támadásra utaló tevékenységi minták azonosítása révén gyorsan azonosíthatja a fenyegetéseket, és reagálhat rájuk. Emellett bizonyos feladatok, például a rendszerfrissítések és a javításkezelés automatizálására is használható, ami segíthet csökkenteni az emberi hibák kockázatát. A szerzők azonban azt is megjegyzik, hogy a mesterséges intelligencia katonai műveletekben való alkalmazása etikai aggályokat vet fel, különösen az autonóm fegyverek használata tekintetében. Az autonóm fegyverek olyan fegyverek, amelyek emberi beavatkozás nélkül képesek kiválasztani és megtámadni a célpontokat. Ez kérdéseket vet fel az elszámoltathatósággal és a nem szándékolt következmények lehetőségével kapcsolatban. A szerzők szerint fontos, hogy alaposan mérlegeljük a mesterséges intelligencia katonai műveletekben való alkalmazásának etikai következményeit, és hogy megfelelő politikákat és szabályozásokat dolgozzunk ki annak biztosítására, hogy az alkalmazás felelősségteljes és etikus módon történjen.[19]

Négyesi Imre *A mesterséges intelligencia katonai felhasználásának társadalmi kérdései* című cikkében megállapítja, hogy a mesterséges intelligencia felhasználható a döntéshozatali folyamatok támogatására, például a logisztika, az erőforrás-elosztás és a kockázatértékelés területén. Az AI segíthet megjósolni a berendezések meghibásodásának vagy az ellátási lánc megszakadásának valószínűségét, lehetővé téve a hadsereg számára, hogy proaktívan megelőző intézkedéseket hozzon.

Négyesi Imre kitér a mesterséges intelligencia lehetséges felhasználására is a hírszerzés területén, beleértve a különböző forrásokból származó nagy mennyiségű adat elemzését. A mesterséges intelligencia felhasználható az adatokban található minták és anomáliák azonosítására, ami segíthet a potenciális fenyegetések felderítésében, vagy betekintést nyújthat a stratégiai tervezésbe.[20] A mesterséges intelligencia például felhasználható a közösségi média és más online platformok megfigyelésére, hogy a nyugtalanságra vagy terrorista tevékenységre utaló jeleket keressenek.[21] *Magyarország Mesterséges Intelligencia Stratégiája* az említett konkrét alkalmazások mellett hangsúlyozza az AI-kutatásba és -fejlesztésbe való befektetés, valamint az akadémiai intézményekkel és a magániparral való partnerségek kiépítésének fontosságát is. A dokumentum megjegyzi, hogy a hadseregnek arra kell törekednie, hogy vezető szerepet töltsön be az AI-technológiák fejlesztésében és alkalmazásában, hogy megőrizze technológiai előnyét, és biztosítsa felkészültségét a jövőbeli kihívásokra.[22] A mesterséges intelligencia egyéb lehetséges katonai felhasználási területei közé tartozik az autonóm fegyverrendszerek – például drónok és robotok – kifejlesztése felderítésre, megfigyelésre és egyéb feladatokra.[23] Az autonóm fegyverek alkalmazása azonban etikai aggályokat vet fel, és a nemzetközi közösségben sok vita tárgyát képezi. Elmondható, hogy a mesterséges intelligencia katonai alkalmazása nagymértékben

19 Fehér–Négyesi 2021: 85.
20 Négyesi 2008: 97–100.
21 Négyesi 2021: 136–137.
22 *Magyarország Mesterséges Intelligencia Stratégiája, 2020–2030.* 2020.
23 Fehér–Négyesi 2021: 85.

növelheti a különböző feladatok és műveletek hatékonyságát és eredményességét.[24] Fontos azonban alaposan mérlegelni a mesterséges intelligencia lehetséges kockázatait és etikai következményeit, és biztosítani, hogy alkalmazása összhangban legyen a nemzetközi normákkal és értékekkel.[25]

Magyarország és a mesterséges intelligencia

A hadiipar és a védelmi ágazat a 20. század közepétől fogva folyamatosan integrálja a mesterséges intelligencia megoldásait, ami döntő mértékben alakította át a katonai műveleteket. A gépi tanulás és az autonóm rendszerek mellett a drónok, a robotok és az autonóm fegyverek is megjelentek, amelyek az automatizálás új korszakát hozták el. Az orosz védelmi reformok szerint 2030-ra a hadseregük harmada robotosított lesz, míg az Amerikai Egyesült Államok korlátozottan használja az autonóm rendszereket. Az autonóm fegyverek kihívást jelentenek, mivel potenciálisan az emberi döntéshozatali szerepüket veszélyeztetik, mint az atomfegyverek esetében.

A 2020-as nemzeti biztonsági stratégia kiemeli a mesterséges intelligencia kihívásait, míg Magyarország stratégiája részletesebb iránymutatást ad, és a Katonai Nemzetbiztonsági Szolgálatot felelőssé teszi az AI-ban rejlő nemzeti kockázatok kezeléséért.[26] Jelenleg a magyar kibervédelmi rendszerben a fejlesztési törekvések nem maradnak el a nemzetközi szint mögött. A rendőrségi és a biztonsági ágazatban a mesterségesintelligencia-képzések iránti igény fokozódik.

*Magyarország Mesterséges Intelligencia Stratégiájá*nak előzménye az EU 2018–2019-ben készített AI-fejlesztési terve és a 2020-as, az Európai Bizottság által kiadott AI fehér könyv. Magyarország AI Koalíciója ezen iránymutatások alapján dolgozta ki saját stratégiáját, amely a mesterséges intelligencia különböző területeire helyezi a hangsúlyt. A magyar kormány célja az AI-stratégiával, hogy gyorsítson a technológiai fejlődésen, és az állampolgárok számára elérhetővé tegye az AI előnyeit, garantálva az információs biztonságot. A stratégia kiemeli az ember és gép közötti harmonikus együttműködés fontosságát. Az 5G és 6G technológia központi szerepet játszik a világban, és Magyarország is prioritásként kezeli. A Huawei és a ZTE példája rámutat a nemzetbiztonsági kockázatokra, amelyek az ilyen rendszerek kivitelezői miatt adódhatnak. Az EU is elismeri a 5G biztonsági kockázatait, és figyelmezteti a tagállamokat a beszállítók nemzetbiztonsági profiljának mérlegelésére.[27]

Állapotanalízis

Az interjúalanyok által adott válaszokat az 1. táblázat foglalja össze:

[24] Négyesi 2021: 136–137.
[25] Négyesi 2008: 97–100.
[26] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
[27] *Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése* 2020.

1. táblázat: A mesterséges intelligencia általános felhasználása a Magyar Rendőrségnél, a Magyar Honvédségnél, a Katonai Nemzetbiztonsági Szolgálatnál és a Nemzetbiztonsági Szakszolgálatnál

	Magyar Rendőrség	**Magyar Honvédség**	**Katonai Nemzetbiztonsági Szolgálat**	**Nemzetbiztonsági Szakszolgálat**
Mesterséges intelligencia használata	Prediktív modellezés, bűnmegelőzés, adatkezelés	Felismerés, tervezés, szimuláció, döntéstámogatás, robotika	Hírszerzés, adatgyűjtés, elemzés, kibervédelem	OSINT, adatgyűjtés, elemzés
Demokrácia és MI	Felelős AI-használat, etikai és jogi keretek betartása	Tiszteletben tartja a demokratikus értékeket, betartja az etikai normákat	Etikai és jogi keretek betartása, átláthatóság	Felelős AI-használat, etikai és jogi keretek betartása
Jogszabályok és MI	GDPR betartása, adatkezelési jogszabályok	GDPR betartása, adatkezelési jogszabályok	GDPR betartása, adatvédelmi jogszabályok	GDPR betartása, adatvédelmi jogszabályok
Kooperáció és közigazgatási kapcsolatok	Kooperáció más hatóságokkal és szervezetekkel, jó kapcsolatok a közigazgatással	Intenzív együttműködés más szervekkel, közigazgatási kapcsolatok	Együttműködési kapcsolatok, közigazgatási kapcsolatok	Széles körű együttműködés, közigazgatási kapcsolatok
Pénzügyi helyzet	Jelentős beruházások szükségessége az MI-fejlesztésbe	Beruházások az MI-technológiákba, fokozott költségvetési szükségletek	Jelentős beruházások, technológiai fejlesztések	Jelentős beruházások, adatelemző eszközök fejlesztése, stratégiából adódóan feladat a fejlesztés – erre többletköltségek vannak
MI hatása a munkaerőre	Új szerepkörök, átképzések, a hagyományos munkahelyek átalakítása	Specializált munkaerőképzés, munkahelyek átalakítása	Új szerepkörök, specializált képzések	Alacsony hatás, specializált személyzet
Kooperáció és közigazgatási kapcsolatok	Kormányzati és nemzetközi együttműködés, belügy-minisztériumi kapcsolatok	Hazavédelmi kooperáció, nemzetközi katonai együttműködés	Együttműködés a nemzetbiztonsági struktúrákkal, nemzetközi hírszerző szervezetekkel	Intenzív kormányzati kapcsolat, együttműködés más nemzetbiztonsági szervekkel, de még nincs egységes koordináció!
Legfőbb problémák	Jogszabályi környezet, technológiai kérdések	Képzési hiányosságok, technológiai frissítések	Szigorú biztonsági követelmények, technológiai kihívások	Szigorú titkosítási követelmények, technológiai hozzáférési problémák

Forrás: a szerző szerkesztése

Az előző pontok alapján készült státuszanalízis a következő képet mutatja a magyar rendvédelmi szervek és a honvédség mesterségesintelligencia-alkalmazásáról:

Felhasználási területek: Mind a négy vizsgált szervezet – a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Rendőrség és a Nemzetbiztonsági Szakszolgálat – aktívan alkalmazza az MI-technológiákat számos területen. Ezt elsősorban az adatelemzés és a döntéstámogatás terén látjuk, ahol az MI hozzájárul a gyors és pontos információfeldolgozáshoz. A technológia felhasználása a bűncselekmények és a nemzetbiztonsági fenyegetések előrejelzésében és a honvédelmi operációk támogatásában is fontos szerepet játszik.

Demokrácia és MI: Bár az MI-technológiák hozzájárulnak a hatékony információfeldolgozáshoz és döntéshozatalhoz, fontos, hogy ezek a technológiák összhangban legyenek a demokratikus elvekkel. Jelenleg ezek a szervezetek rendelkeznek a megfelelő jogszabályi keretekkel, hogy biztosítsák a demokratikus elszámoltathatóságot és a személyes adatok védelmét. Ugyanakkor további kutatásra és vitára van szükség arról, hogy hogyan lehet a legjobban összeegyeztetni az MI alkalmazását a rendvédelmi és honvédelmi szektorban a demokratikus normákkal és elvekkel.

Jogi kihívások: Az MI alkalmazása számos jogi kérdést vet fel, beleértve az adatvédelmet, a személyiségi jogokat és a biztonsági kérdéseket. Bár Magyarország és az EU rendelkezik az adatvédelmi és a biztonsági kérdésekkel foglalkozó jogszabályokkal, a dinamikusan fejlődő MI-technológia gyors változásai új kihívásokat jelenthetnek. Ezért folyamatos jogszabályi frissítésekre és a technológia fejlődésével lépést tartó új jogszabályokra van szükség.

Gyűjtött adatok minősége: Az MI alkalmazásának hatékonysága nagymértékben függ a használt adatok minőségétől. Az adatok gyűjtése, tárolása és feldolgozása során a négy vizsgált szervezetnek biztosítania kell az adatok integritását és relevanciáját, mivel az adatok minősége közvetlen hatással van az MI által generált eredmények pontosságára. Továbbá, az adatgyűjtés során szem előtt kell tartani az adatvédelmi jogszabályokat és az etikai irányelveket.

Technológiai kihívások: Az MI-technológiák alkalmazásának gyors növekedése technológiai kihívásokat is jelent, amelyek között szerepel a megfelelő infrastruktúra kiépítése, a szükséges hardver- és szoftvereszközök rendelkezésre állása, valamint a megfelelő tudással és képességekkel rendelkező munkaerő biztosítása. Mindezen szempontok megkövetelik a folyamatos befektetést, oktatást és fejlesztést, hogy ezek a szervezetek lépést tudjanak tartani az MI-technológia fejlődésével.

Humán erőforrások: Az MI-technológiák alkalmazása változást hoz a munkaerő szerkezetében és a munkavégzés módjában. Míg az MI csökkentheti az emberi erőforrások igényét bizonyos területeken – mint például az adatelemzés –, ugyanakkor növeli az igényt olyan szakértőkre, akik képesek fejleszteni, üzemeltetni és felügyelni ezeket a rendszereket. Ezért fontos, hogy a szervezetek stratégiai szinten foglalkozzanak a munkaerő képzésével és toborzásával.

Biztonsági kockázatok: Az MI alkalmazása új biztonsági kockázatokat is magával hoz, beleértve a kibertámadásokat és az adatszivárgásokat. A négy vizsgált szervezetnek biztosítania kell az adatok és az infrastruktúra megfelelő védelmét a különböző kibertámadásokkal szemben. Ebben a kontextusban a megfelelő kiberbiztonsági protokollok és eljárások kidolgozása elengedhetetlen, ezért már több ilyet is kidolgoztak a szervezetek, de fejlesztik is ezeket.

Etikai kérdések: Végül, de nem utolsósorban, az MI alkalmazása számos etikai kérdést is felvet. E kérdések közé tartozik az adatvédelmi és személyes jogok tiszteletben tartása, az algoritmikus átláthatóság és elszámoltathatóság, valamint a potenciális diszkrimináció és előítéletesség kérdése, amelyeket az MI-rendszerek torzított, nem reprezentatív adatokból tanulhatnak. Ezenfelül az MI alkalmazásának hatása a társadalomra és a munkaerőre is jelentős etikai kérdéseket vet fel. A szervezeteknek foglalkozniuk kell ezekkel a kérdésekkel, és etikai irányelveket kell alkalmazniuk az MI-technológiák fejlesztésében és használatában.

Összefoglalva: a négy magyar rendvédelmi és honvédelmi szervezet már aktívan alkalmazza az MI-technológiákat, és jelentős előnyöket tapasztalnak a hatékonyság, a sebesség és a pontosság terén. Ugyanakkor számos kihívással is szembesülnek, amelyek között szerepelnek jogi, technológiai, munkaerő-, biztonsági és etikai kérdések. Az MI alkalmazásának jövője ezekben a szervezetekben nagymértékben attól függ, hogy mennyire képesek ezeket a kihívásokat kezelni és az MI-technológiákat etikusan és felelősségteljesen használni. Ez a képesség döntő jelentőségű lesz az MI-technológia további alkalmazásának és fejlődésének elősegítésében a rendvédelmi és a honvédelmi szektorban. A mesterséges intelligencia használatának egyik közös területe a négy szervezetnél a fenyegetések azonosítása és elemzése, ami lehetővé teszi a biztonsági kockázatok kezelését. Ez magában foglalja az adatok nagy mennyiségű elemzését és a potenciális veszélyek előrejelzését. Emellett az MI-t széles körben használják a logisztikai folyamatokban, ahol segíthet az erőforrások hatékonyabb elosztásában és a műveletek optimalizálásában. Ez különösen fontos a Honvédség esetében, ahol a logisztika kulcsfontosságú szerepet játszik a hadműveletek sikeres végrehajtásában. Az MI-nek emellett kiemelt szerepe van a kommunikációs rendszerekben is, ahol segíthet a hírszerzésben és a kommunikáció hatékonyságának növelésében. Az adatbiztonság és a kibervédelem terén az MI szintén nagy lehetőségeket rejt, például az anomália detektálás terén, amelynek segítségével képesek lehetünk azonosítani a szokatlan mintákat és a potenciális fenyegetéseket. Mindezek mellett az MI-t felhasználják továbbá a személyzet képzésében, az infrastruktúra-menedzsmentben és az adatgyűjtés területén is, ami a nemzetbiztonsági szolgálatoknál különösen fontos.

A legfőbb különbségeket az MI-hez való hozzáállásban a következőképp lehet összefoglalni:

Magyar Honvédség: Az etikai kérdések közé tartozhat, hogy miként használhatók fel a mesterségesintelligencia-rendszerek a hadműveletekben anélkül, hogy veszélyeztetnék az emberi jogokat vagy a humanitárius jogot. Jogi kihívások között lehetnek kérdések a mesterséges intelligencia nemzetközi konfliktusokban való használatával kapcsolatban, például autonóm fegyverrendszerek alkalmazásakor.

Katonai Nemzetbiztonsági Szolgálat: Itt a legfontosabb etikai kérdések közé tartozhat a személyes adatok védelme és az állampolgári jogok tiszteletben tartása a nemzetbiztonsági célú adatgyűjtés során. Jogi kérdések merülhetnek fel az információgyűjtés, -feldolgozás és -megosztás területén, valamint a kiberbiztonság és az információs hadviselés témakörében.

Rendőrség: Az etikai kérdések közé tartozhatnak a bűnüldözés és az adatgyűjtés módjai, különösen a magánélethez való jog és a diszkriminációmentesség szempontjából. Jogi kérdések lehetnek a mesterséges intelligencia bűnüldözésben való használatának határai, például az arc- és hangfelismerés alkalmazásának korlátai.

Nemzetbiztonsági Szakszolgálat: Az etikai kérdések közé tartozhat a személyes adatok védelme és a magánélethez való jog tiszteletben tartása az adatgyűjtés során. Jogi kérdések merülhetnek fel a kiberbiztonsággal, az adatvédelemmel és az információgyűjtés és -megosztás határaival kapcsolatban.

Érdekesség: Mit mond a ChatGPT az adatokról?

A ChatGPT az adatok alapján a következő rövid elemzést készítette:

Az általam készített elemzés demonstrálja, hogy a vizsgált intézmények – többek között a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Rendőrség, és a Nemzetbiztonsági Szakszolgálat – proaktívan integrálják az MI-technológiákat, főleg adatanalitikai és döntéstámogató funkcionalitásaik révén. Ezen alkalmazásuk elősegíti a hatékony információs feldolgozást, ami imperatív a kriminális és nemzetbiztonsági incidensek kezelésénél. Ezen szervezetek a demokratikus elszámoltathatóságot és adatvédelmi protokollokat szigorúan alkalmazzák az MI-technológiák keretein belül. Ugyanakkor a dinamikus technológiai fejlesztések komplex jogi kérdéseket vetnek fel, amelyek átfogó jogszabályi adaptációt és innovációt igényelnek.

Az adatok kvalitása esszenciális az MI-technológiák hatékonyságához, következésképpen az intézményeknek fokozottan kell monitorozniuk az adat integritását és relevanciáját, etikai és jogi keretek között. Technológiai szempontból a megfelelő infrastruktúra, eszközök és specifikusan képzett munkaerő elengedhetetlenek. Bár az MI potenciálisan redukálhatja a humán erőforrás szükségességét egyes területeken, párhuzamosan fokozott igény mutatkozik azokra a specialistákra, akik az MI-rendszereket tervezik, implementálnak és menedzselnek. Az MI integrációja új kiberbiztonsági kockázatokat is generál, például adatszivárgás vagy kibertámadások formájában, amelyek ellen adekvát védekezési mechanizmusokat és protokollokat kell kialakítani. Ezenfelül az MI által generált etikai kérdések, mint az adatvédelmi jogok, algoritmikus transzparencia és az esetleges diszkriminációs torzítások, kritikusak a technológia etikus és társadalmilag elfogadott alkalmazása szempontjából.

Konklúzióként az MI-technológiák paradigmaváltást hoznak a vizsgált szervezetek operatív működésében, de a hatékony implementáció érdekében az etikai, jogi és technológiai kihívások koherens kezelése, valamint a kvalitatív adatkezelés és a humán erőforrás optimalizálása esszenciális.

Megállapítások

A mesterséges intelligencia használatának egyik közös területe a négy szervezetnél a fenyegetések azonosítása és elemzése, ami lehetővé teszi a nemzetbiztonsági kockázatok kezelését. Ez magában foglalja az adatok nagy mennyiségű elemzését és a potenciális veszélyek előrejelzését. Emellett az MI-t széles körben használják a logisztikai folyamatokban, ahol segíthet az erőforrások hatékonyabb elosztásában és a műveletek optimalizálásában. Ez különösen fontos a Honvédség esetében, ahol a logisztika kulcsfontosságú szerepet játszik a hadműveletek sikeres végrehajtásában. Az MI emellett fontos szerepet tölt be a kommunikációs rendszerekben is, ahol segíthet a hírszerzésben és a kommunikáció hatékonyságának növelésében. Az adatbiztonság és a kibervédelem terén az MI szintén

nagy lehetőségeket rejt, például az anomália detektálása terén, amelynek segítségével képesek lehetünk azonosítani a szokatlan mintákat és a potenciális fenyegetéseket. Mindezek mellett az MI-t felhasználják továbbá a személyzet képzésében, az infrastruktúramenedzsmentben és az adatgyűjtés területén is, ami a nemzetbiztonsági szolgálatoknál különösen fontos.

Elmondható, hogy a mesterséges intelligencia használata a vizsgált szervezeteknél kulcsfontosságú eszközzé vált a hatékonyság növelésében, a fenyegetések kezelésében és az adatbiztonság javításában.

Felhasznált irodalom

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

Abadicio, Millicent (2019): Artificial Intelligence at the FBI – 6 Current Initiatives and Projects. *Emerj Artificial Intelligence Research,* 2019. május 19. Online: https://emerj.com/ai-sector-overviews/artificial-intelligence-fbi/

Boda, József – Dobák Imre (2016): Titkosszolgálatok fejlődése – technikai szemmel. *Nemzetbiztonsági Szemle,* 4(4), 17–25. Online: http://epa.oszk.hu/02500/02538/00016/pdf/EPA02538_nemzetbiztonsagi_szemle_2016_04_017-025.pdf

Buchanan, B. – Konaev, M. – Fedasiuk, R. (2021): AI and National Security: The Importance of the AI Ecosystem, Center for Security and Emerging Technology, Georgetown University, September.

Chui, Michael et al. (2018): Notes from the AI frontier. Insights from hundreds of use cases. McKinsey Global Institute, June.

Crawford, Kate – Calo, Ryan (2016): There is a Blind Spot in AI Research. *Nature,* 538(7625), 311–313. Online: https://doi.org/10.1038/538311a

Európai Bizottság (2020): *Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése*. Brüsszel, 2020. 02. 19. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A52020DC0065

European Commission (2019): *Ethics Guidelines for Trustworthy AI*. Online: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Fehér, András Tibor – Négyesi, Imre (2021): Mesterségesintelligencia-alapú kibertértámadási modellek. *Műszaki Katonai Közlöny,* 31(3), 73–87. Online: https://doi.org/10.32562/mkk.2021.3.5

Haspel, Gina (2018): Remarks by CIA Director Gina Haspel at the University of Louisville. Online: www.cia.gov/stories/story/remarks-for-central-intelligence-agency-director-gina-haspel-mcconnell-center-at-the-university-of-louisville/

Horowitz, Michael C. – Kreps, Sarah E. (2021): The Ethics of AI Ethics in National Security. *Texas National Security Review.*

Kaminski, Margot – Matwyshyn, Andrea (2016): Transparency in Algorithmic and Human Decision-Making: Is there a Double Standard? *University of Pennsylvania Law Review,* 165(1), 139–181.

Lyon, David – Wood, David (2013): *Surveillance and Democracy*. Surrey, UK: Ashgate Publishing.

Magyarország Mesterséges Intelligencia Stratégiája, 2020–2030. 2020. Online: https://digitalisjoletprogram.hu/files/2f/32/2f32f239878a4559b6541e46277d6e88.pdf

Négyesi Imre (2008): Az információgyűjtés jövőképe. *Hadtudományi Szemle,* 1(3), 97–100. Online: http://hdl.handle.net/20.500.12944/2255

Négyesi Imre (2021): A mesterséges intelligencia katonai felhasználásának társadalmi kérdései. *Honvédségi Szemle,* 1, 133–144. Online: https://doi.org/10.35926/HSZ.2021.1.10

Németh, Krisztina (2020): Az interjú. In Jakab, András – Sebők Miklós (szerk.): *Empirikus jogi kutatások. Paradigmák, módszertan, alkalmazási területek*. Budapest: Osiris – MTA Társadalomtudományi Kutatóközpont, 383–408.

Roff, H. – Asaro, P. (2018): Artificial Intelligence in the National Security Domain: Opportunities, Risks, and Key Governance Issues. *Journal of Cyber Policy*.

Rowe, Neil C. (2022). The Comparative Ethics of Artificial-Intelligence Methods for Military Applications. *Frontiers in Big Data,* 5. Online: https://doi.org/10.3389/fdata.2022.991759

Scharre, Paul (2018*): Army of None: Autonomous Weapons and the Future of War.* New York: W. W. Norton & Company.

Wray, Christopher (2020): FBI Director Christopher Wray's Remarks at the Hudson Institute. Online: www.hudson.org/national-security-defense/transcript-the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states