A mesterséges intelligencia belügyi és biztonsági célú alkalmazása

Necz Dániel

Pázmány Péter Katolikus Egyetem, Jog- és Államtudományi Kar, Budapest

Beérkezett: 2020. szeptember 22.; Elfogadva: 2020. november 3.

Összefoglalás

A tanulmány célja a mesterséges intelligencia (MI) belügyi és biztonsági célú alkalmazásának bemutatása, különös figyelemmel az arcfelismerő rendszerek és egyéb MI alapú megoldások rendvédelmi, nemzetbiztonsági, valamint önkormányzati és vízgazdálkodási területen való alkalmazásának lehetőségeire, adatvédelmi és kibervédelmi szempontjaira. A tanulmány ennek kapcsán mind az irányadó magyar és európai uniós előírásokat és célkitűzéseket, mind az MI-re irányadó hatósági gyakorlatot számba veszi és ismerteti, valamint ezek tanulságait összefoglalja és kiértékeli az egyes MI alapú megoldások sajátosságainak figyelembevételével.

Kulcsszavak: MI, biztonság, nemzetbiztonság, arcfelismerés, adatvédelem

The application of AI related solutions for security purposes and concerning internal affairs

Daniel Necz

Pázmány Péter Catholic University, Faculty of Law and Political Sciences, Budapest, Hungary

Summary

The purpose of the study is to take a closer look on the application of artificial intelligence (AI) concerning internal affairs and for security purposes, with a key focus on facial recognition systems and other solutions used by law enforcement and national security agencies to answer new challenges posed by cybercrime and criminal networks spreading through the cyberspace. In the light of the above, the study further takes into account the risks associated with the usage of AI solutions concerning internal affairs and for security purposes and tries to find possible measures to minimize them.

Bearing this in mind, the study highlights the key relevant Hungarian and European Union requirements and goals, including the approach of the European Union concerning biometric identification and the Hungarian AI Strategy's vision on the usage of AI based solutions for administrative, law enforcement, defense and military national security purposes.

The study further analyzes the practical aspects of the usage of AI solutions by law enforcement agencies and the key aspects of facial recognition systems and other similar solutions. This includes the territory affected by the system, the period of monitoring, the human revision of the results presented by the algorithms, as well as data security minimum requirements and the rights of data subjects affected by AI solutions (e.g. sufficient information provided on the processing of their data in accordance with the national and public interests related to the usage of AI solutions).

In addition to the above, the study further discusses the use of AI solutions by national security agencies, including the aspects of monitoring dark web activities conducted by criminal and terrorist organizations and ways for national agencies to intercept messages and gather evidence by new solutions in line with data protection and constitutional requirements.

Finally, the study helps us understand, how AI based solutions can be used for facilitating everyday work of local governments (with a key focus on chatbot services and self-service opportunities) and for solving water management related tasks more efficiently, thus creating a more modern administration, where citizens can easily interact with administrative bodies and technical or simpler tasks are undertaken by algorithms.

All in all, the study outlines how AI is currently used concerning internal affairs and for security purposes and how it can be used to help law enforcement and national security agencies fight new forms of crime empowered by technology or to further modernize local governments and water management systems and apply AI based solutions in accordance with data protection requirements and procedural laws.

Keywords: AI, security, national security, facial recognition, data protection

Bevezetés, vizsgálati szempontok

A mesterséges intelligencia (MI) napjaink egyik legjelentősebb technológiai vívmánya, amely egyre több területén válik meghatározóvá. A segítségével gyorsítható a termelés, hatékonyabban vehetjük fel a harcot a betegségekkel szemben, valamint a technológia arra is képes, hogy előre jelezze a fontosabb környezeti változásokat, amelyekre így időben felkészülhetünk. Természetesen az MI mindennapjaink könnyebbé tételén és az általa képviselt gazdasági és tudományos lehetőségeken túl jelentősen képes növelni a bűnüldözés hatékonyságát, valamint támogatni a nemzetbiztonsági és az egyéb belügyi célú tevékenységeket, továbbá érdemben megkönnyíteni a napi ügyintézéssel járó munkaterhet is. Így az MI célú rendszerek éppúgy alkalmazhatók a belügyi szervek kibervédelmi megoldásainak támogatására, mint körözött személyek kézre kerítésére vagy éppen az emberi munka kiváltására az egyszerűbb, adminisztratív feladatok terén.

Természetesen azonban az MI alapú megoldások felhasználásával járó előnyök mellett jelentős adatvédelmi kockázatok is felmerülhetnek, tekintettel arra, hogy az MI alapú megoldások egy része (például: különböző arcfelismerő rendszerek) nagyban beavatkozik az érintettek magánszférájába, emellett az algoritmusok által hozott döntések jellemzően emberi felülvizsgálatra szorulnak, amelynek hiánya különösen a bűnügyi vagy nemzetbiztonsági célú adatkezelések tekintetében jelenthet kockázatot. Emellett a jogalkotónak és a jogalkalmazóknak napjainkban még a technológia kiforratlanságából eredő kockázatokkal is számolnia kell, és olyan formában, illetve módon kell szabályoznia az MI alapú megoldások alkalmazását, amely az érintettek jogaira és szabadságaira vonatkozó veszélyeket minimálisra csökkenteni. Figyelemmel pedig arra, hogy jelenleg az interneten folyó tevékenységek, valamint a gyakran ezek kapcsán érvényesülő új jelenségek bűnüldözési, nemzetbiztonsági vagy akár kibervédelmi érdekek védelmében való monitorozása is igen kevéssé szabályozott, így mindenképpen szükséges a létrejövő új szabályozás kialakításához szükséges szempontrendszereket is feltárnunk *(Klein 2018: 221)*, hogy a problémakört minél hatékonyabban közelíthessük meg.

A fentiekre figyelemmel jelen tanulmányomban azt vizsgálom, hogy belügyi, valamint biztonsági célú kérdésekben milyen módon és feltételekkel alkalmazhatóak MI alapú megoldások, emellett feltárom azokat a szempontokat is, amelyek alapján az MI alapú megoldásokkal kapcsolatos kockázatok csökkenthetők, és így a technológia adta előnyök a legszélesebb körben használhatók ki. A fentieken túl kísérletet teszek arra is, hogy az MI belügyi célú alkalmazásának azon főbb szabályozási területeit is felvázoljam, ahol fokozottan merülhet fel a jogalkotó közbeavatkozásának szükségessége.

Az MI rendészeti célú alkalmazása, az arcfelismerő rendszerek alkalmazásának adatvédelmi és kibervédelmi szempontjai

Az MI alapú megoldások a bűnüldöző szervek munkáját is nagyban képesek megkönnyíteni, alkalmazásukkal például hamarabb derülhet fény egy-egy bűncselekmény elkövetésére, hatékonyabban segíthetők az áldozatok és vonhatók felelősségre az elkövetők. Gyakori például MI alapú megoldások alkalmazása bűnüldöző szerveknél az ún. raszter-nyomozások területén, amelynek során az adott program előre meghatározott szempontok szerint tömegesen gyűjt ki adatokat bizonyos rendszerekből, ezeket pedig egymással összehasonlítva különböző műveleteket, értékeléseket végez *(Miskolczi–Szathmáry 2018: 192)*. Az Egyesült Királyságban például egy, Cellebrite nevű szoftverfejlesztő cég által fejlesztett MI alapú megoldás segítségét vette igénybe a rendőrség. A megoldás képes arra, hogy elemezze a gyanúsított mobiltelefonján lévő képeket, kommunikációs mintákat és egyéb adatokat, így a megoldás által gyűjtött információk révén a hatóságok könnyebben juthatnak el az elkövetőkhöz *(Baraniuk 2019)*.

A különböző MI alapú megoldások támogatásához azonban kellő mennyiségű erőforrás, valamint adat rendelkezésre állása is szükséges, ezek egy része pedig nem feltétlenül foglal magában személyes adatokat (például: statisztikai adatösszesítések, gazdasági társaságokra, eszközökre vonatkozó adatok kezelése), így esetükben a személyes adatok védelmére vonatkozó szigorú adatvédelmi követelményeknek való megfelelést sem szükséges biztosítani. Akár személyes, akár nem személyes adatokról beszélünk azonban, vitathatatlan tény, hogy olyan elektronikus infrastruktúra kialakítására van szükség, amely – az irányadó jogszabályi követelményekkel összhangban – biztosít lehetőséget szakértők részére elemzések elvégzésére, valamint különböző algoritmusok végrehajtására (*Lovas 2017: 373*) a fentiekhez hasonló megoldások területén.

Hangsúlyozzuk azonban, hogy az MI alapú rendszerek által hozott döntések jelentős mértékben emberi felülvizsgálatra szorulnak, valamint azok igénybevétele nem vezethet a hatósági, ügyészi vagy bírósági döntéshozatal „robotizálásához", különösen nem a büntetőeljárás területén. Így a nyomozóhatóság, az ügyészség vagy a bíróság feladatai sem válthatók ki algoritmusok segítségével, azonban a döntéshez alapul szolgáló információk összegyűjtése, rendszerezése, valamint a szakértői munka megkönnyítése kapcsán már napjainkban is képes a mesterséges intelligencia segítséget nyújtani, így ezen rendszerek és megoldások inkább támaszai lehetnek a fenti szervek munkájának, mintsem „gépesített" döntéshozók.

A gyakorlatban szintén egyre nagyobb elterjedést mutatnak a különböző arcfelismerő rendszerek, amelyeket jellemzően a közterületi elektronikus megfigyelőrendszerekhez kapcsoltan alkalmaznak a bűnüldöző hatósá-

gok, és amelyek elvileg képesek arra, hogy például segítségükkel súlyos bűncselekményekkel gyanúsított, illetve körözött személyek is azonosíthatók legyenek. Ezen rendszerek azonban napjainkban még sok esetben pontatlan eredményeket produkálnak, amely érthető módon komoly veszélyekkel jár az érintettek jogaira nézve. A rendszerek megbízhatóságán kívül azonban egyéb szempontok is azok alkalmazása ellen szólhatnak, ideértve különösen a közbiztonság egyéb, az érintettek jogaira és szabadságaira enyhébb hatást gyakorló eszközökkel történő fenntarthatóságát, valamint a rendszerekkel kapcsolatos adatkezelés átláthatóságát. Franciaországban például nemrég ezen okokkal összefüggésben tiltotta meg a marseille-i közigazgatási bíróság arcfelismerő rendszerek alkalmazását két gimnázium bejáratánál (*Narendra 2020*).

Tekintettel a technológia szabályozatlanságára, valamint az annak alkalmazásával kapcsolatos problémákra, az utóbbi időben az Európai Bizottság is aktívan foglalkozott az arcfelismerő rendszerek szabályozásának kérdésével. A nemrég nyilvánosságra hozott, „*Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése*" elnevezésű white paper dokumentumban a Bizottság kitér például a mesterséges intelligencia távoli biometrikus azonosítás céljára (például arcfelismerő rendszerek keretében) való felhasználására, e körben hangsúlyozva, hogy az ilyen technológiák csak kellő indokkal, arányos mértékben, valamint megfelelő biztosítékok mellett alkalmazhatók. Előrebocsátja továbbá, hogy széleskörű európai vitát indít a kapcsolódó körülményekről, valamint biztosítékokról *(Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése 2020: 26–27)*. A vonatkozó konzultáció eredményei, valamint ezek későbbi felhasználása természetesen izgalmas kérdéseket tartogat még a jövőre nézve, amely során az európai jogalkotónak a tagállami, társadalmi, gazdasági és szakmai szempontokat is megfelelő mértékben kell majd összehangolnia.

Ugyancsak kiemelendők a nemrégiben megjelent, Magyarország Mesterséges Intelligencia Stratégiájának témába vágó meglátásai. A dokumentumban ugyanis jelentős hangsúlyt kap az MI közigazgatási, rendvédelmi, honvédelmi és katonai nemzetbiztonsági célú felhasználása is, ideértve többek között a rendvédelmet szolgáló különböző ellenőrzési rendszerek bevezetését, meglévő rendszerek (pl. Robotzsaru program) továbbfejlesztését, komplex modellezési, szimulációs rendszerek fejlesztését, MI-vel támogatott védelmi megoldások kialakítását *(Magyarország Mesterséges Intelligencia Stratégiája 2020: 38, 52)*.

Habár nehéz lenne megjósolni az egyes tagállamok vagy a Bizottság szempontjainak találkozását a technológia jövőbeli alkalmazása kapcsán, azonban álláspontom szerint ennek ellenére – a jelenleg rendelkezésünkre álló információk alapján is – meghatározhatók olyan intézkedések és megoldások, amelyek tükrében az arcfelismerő rendszerek alkalmazásával az érintettek jogaira és szabadságaira jelentett kockázatok megfelelően lecsökkenthetők, ideértve különösen az alábbiakat:

- *Az adatkezelés céljának megválasztása:* az arcfelismerő rendszerek alkalmazása csak kivételes esetekben lehet indokolt (például: a közbiztonságot fenyegető súlyos veszélyek elhárítása, járványveszély megfékezése). Ehhez mérlegelni kell természetesen az adatkezelés egyéb lentebb tárgyalt körülményeit is, valamint azon garanciákat, amelyekkel megfelelően csökkenthetők az érintettekre gyakorolt adatvédelmi kockázatok.
- *A rendszer által érintett terület és az alkalmazás időtartama:* az arcfelismerő rendszer alkalmazását megelőzően szükséges felmérni a rendszer által megfigyelt terület jellemzőit, valamint arcfelismerő rendszerrel ellátott kamerák esetén a kamerák látószögét. Így – hasonlóan az elektronikus megfigyelőrendszerek általi adatkezelés általános szabályaihoz – az arcfelismerő rendszer sem alkalmazható olyan területen, ahol a megfigyelés az érintettek emberi méltóságát a megfigyelés időtartama alatt sértheti, ideértve például a mellékhelyiséget vagy az öltözőt. A rendszer megfelelő pontossága, és további garanciák megléte esetén adott esetben alkalmazható lehet azonban például pályaudvarok vagy repülőterek utasforgalom által érintett nyilvános részein, lévén, hogy ezen területek fokozott terrorveszélynek vannak kitéve, valamint a járványok terjedésének megállítása és körözött bűnelkövetők kézre kerítése is indokolhatja arcfelismerő rendszerek alkalmazásának szükségességét. Az arcfelismerő rendszerek tényleges, gyakorlati alkalmazását megelőzően azonban javasolt azokat szimulációs körülmények között – például erre kijelölt területen –, akár több periódusban is tesztelni, az így gyűjtött tapasztalatokat pedig például egy hatásvizsgálati dokumentációban összegezni. Szintén kifejezetten ajánlott lehet a rendszerek alkalmazása előtt az adatvédelmi hatósággal is konzultálni a rendszerrel kapcsolatos adatvédelmi kockázatokról, valamint az azok csökkentését célzó intézkedésekről.
- *A rendszerek felülvizsgálata és az érintettek jogai:* a rendszerek alkalmazása során az emberi felülvizsgálat lehetőségét folyamatosan garantálni kell, ideértve különösen azon MI általi adatkezeléssel érintett információkat, amelyeket büntetőeljárásban bizonyítékként kívánnak felhasználni, illetve amelyek alapján az érintettekkel szemben hatósági intézkedést foganatosítanak. Mindemellett ki kell dolgozni az érintettek jogainak biztosítására vonatkozó módszereket (például: az érintett észrevételezési joga). Ezeket értelemszerűen összhangba kell hozni azon eljárások szabályaival, amelyekben az arcfelismerő rendszerek által elemzett felvételeket felhasználják (ideértve különösen a büntetőeljárási szabályokat).
- *Adatbiztonsági szempontok:* tekintettel az arcfelismerő rendszerekkel kapcsolatos kockázatok körére, valamint a rendszerek pontosságával kapcsolatos jelenlegi bizonytalansági tényezőkre, kijelenthető, hogy az arc-

felismerő rendszerek kapcsán kiemelten magas adatbiztonsági szintet szükséges garantálni. Ez kiterjed mind az adatbiztonság megszervezésére (ideértve például a rendszert alkalmazó, valamint a rendszer által elemzett felvételekhez hozzáférő személyek adatvédelmi oktatását, a rendszerhez való hozzáférési jogok szigorú meghatározását), mind az azzal kapcsolatos technikai intézkedések alkalmazására (például: megfelelő kibervédelmi intézkedések alkalmazása a rendszer kapcsán).

A fenti szempontok egy része más MI alapú megoldások vonatkozásában is alkalmazandó (ideértve például az adatbiztonság kiemelten magas szintjének megkövetelését), azonban valamennyi MI alapú megoldás esetén elsősorban az alkalmazás célja és egyéb körülményei, illetve sajátosságai szerint határozhatók meg a vonatkozó adatvédelmi és kibervédelmi szempontok is.

Mint az a fentiekkel összhangban megállapítható, az MI alapú megoldások rendőrségi alkalmazása jelenleg még gyerekcipőben jár, azonban ennek ellenére már most is elérhetők olyan alkalmazások a piacon, amelyek, például bizonyítékok gyűjtését vagy elemzését teszik könnyebbé. Biztosak lehetünk azonban benne, hogy ezen megoldások köre az elkövetkezendő években csak bővülni fog, valamennyi megoldás esetén kulcskérdésnek tekinthető azonban az adatvédelmi megfelelés garantálása, valamint ezen eszközöknek az érintettek jogait is számításba vevő alkalmazása. E körben hangsúlyozandó azonban, hogy az igazságszolgáltatási, az ügyészi, valamint a rendvédelmi tevékenységek a gyakorlatban jellemzően közhatalmi tevékenységnek tekinthetők, amelyek számos esetben – és az adatkezelés egyéb körülményeinek, valamint az adatkezelő jogosítványainak elemzésével – jogalapul szolgálhatnak az adatkezeléshez *(dr. Osztopáni 2018: 129)*, vagy egyébként olyan körülménynek tekinthetők, amelyek az MI alapú megoldások alkalmazásánál és a vonatkozó adatkezelés kialakítása kapcsán figyelembe veendők. Mindez természetesen nem jelenti azt, hogy ezen esetekben az érintettek jogait biztosító garanciák elhagyhatók, sőt ezek a fenti adatkezelések jogszerű és tisztességes végzése egyik biztosítékának is tekinthetők. Ennek kapcsán az elkövetkezendő időszakban mind az uniós, mind a tagállami jogalkotók egyik kiemelt feladata lesz az arcfelismerő rendszerek alkalmazásával kapcsolatos részletes szabályok kialakítása, valamint az ezzel kapcsolatos uniós, tagállami és egyéb szempontok helyes összehangolása.

Az MI nemzetbiztonsági célú alkalmazása

Az MI alapú megoldások természetesen jelentősen támogathatják a nemzetbiztonsági szolgálatok tevékenységeit is, azonban e körben kiemelt szempontot élvez az érintettek magánszférájának és személyiségi jogainak védelme. Hangsúlyozandó azonban, hogy ezen jogok tiszteletben tartása mellett a gyakorlatban azonban egyéb érdekek (például: nemzetbiztonság, terrorcselekmények vagy más súlyos bűncselekmények megelőzése, honvédelem) is megkövetelhetik a magánszférába való erősebb hatósági behatást, különös tekintettel a bűnözői csoportok technológiai kapacitásainak elmúlt években bekövetkezett rohamos fejlődésére. Mára például egyértelműen kijelenthető, hogy a különböző bűnbandák és terrorista csoportok tagjai gyakran kommunikálnak a hagyományos böngészők által el nem érhető ún. dark web-en (sötét web) keresztül *(Serbakov 2019: 120)*, amely a hagyományos böngészőknél jóval nagyobb anonimitást nyújt, így ennek révén számos bűncselekmény és kapcsolódó tranzakció felderítetlen maradhat. Habár az adatvédelmi és egyéb magánszemélyek megfigyelését szabályozó jogszabályi rendelkezések az ezen felületeken keresztül folytatott kommunikációkat is védik[1], ugyanakkor az MI alapú rendszerek megfelelő garanciák (például: a technológia alkalmazásáról való döntéssel kapcsolatos büntetőeljárási garanciák és az MI alapú rendszerek útján gyűjtött bizonyítékok felülvizsgálata) mellett történő alkalmazása komoly segítséget jelenthet a terrorcselekmények vagy egyéb súlyos bűncselekmények megelőzéséhez. A dark web-en keresztül folytatott cselekmények vonatkozásában pedig további szempont lehet, hogy a publikus böngészőkkel ellentétben ezen nagyfokú anonimitást biztosító csatornák használóinak fokozottabban kell számolniuk a magánszférájukba akár jelentősebb behatást is eredményező hatósági adatkezelés lehetőségével.

A fentebb írtakkal összhangban megállapítható, hogy a nemzetbiztonsági szolgálatok tevékenységéhez – különösen a nehezen figyelhető kommunikációs csatornák elemzéséhez, valamint az ezen keresztül folyó illegális tevékenységek felderítéséhez – jelentős segítséget jelenthet az MI alapú rendszerek alkalmazása, valamint az – közvetetten módon, a megfelelő információk birtokában való kormányzás útján – akár a kormányzati döntéshozatalt is segítheti *(Sabjanics István 2017: 103–104)*, azonban természetesen csak az érintettek jogainak védelmét szolgáló garanciák mellett.

Az MI alapú rendszerek önkormányzati és vízgazdálkodási területen való alkalmazása

Az MI alapú rendszerek az önkormányzati igazgatás területén is jelentős haszonnal kecsegtetnek, különösen ideértve az ügyintézési folyamatok drasztikus egyszerűsítését, valamint a döntések meghozatalához szükséges kisebb súlyú számítási feladatok átvállalását. Az Egyesült Királyság területén például már több önkormányzat is

[1] Hangsúlyozandó e körben, hogy a személyes adatok bűnüldözési, nemzetbiztonsági és honvédelmi célú kezelésére nem az (EU) 2016/679. sz. Európai Általános Adatvédelmi Rendelete (GDPR), hanem az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az (EU) 2016/680. sz. bűnügyi irányelv rendelkezéseit átültető, és az ilyen adatkezelések sajátosságait figyelembe vevő szabályai, valamint a vonatkozó szektorális jogszabályok adatvédelmi rendelkezései irányadók.

vezetett be a hivatali ügyintézés támogatása céljából chatbot és egyéb kognitív szolgáltatásokat vagy kezdett hasonló projektbe az elmúlt években. Ezen megoldások jelentős ügyterhet vesznek le az egyes hivatali egységekről, valamint megnövelik az állampolgárok által gyakran preferált, távolról is intézhető ügyek körét, és támogatják az új technológiai megoldásokon keresztüli önkiszolgálást (lásd: Oxford város önkormányzatának chatbotokkal és mesterséges intelligenciával kapcsolatos információs és projektoldala).

Az MI az önkormányzatok munkájának támogatásán túl hatékony segítséget jelenthet a modern vízgazdálkodás területén is. Így már jelenleg is elérhetők a piacon olyan szolgáltatások, amelyek segítik a vízgazdálkodással kapcsolatos számítások és tervezési feladatok elvégzését, az egyes infrastruktúrák és hálózatok kiépítését *(Joshi 2018)*. Ezen megoldások implementációja hatékonyabbá teheti mind a vízgazdálkodási hatósági tevékenységet, mind az egyes infrastruktúrák üzemeltetőinek napi munkáját, lévén pedig, hogy az ezen a területen kezelt információk jellemzően nem tartalmaznak személyes adatokat, így az adatvédelmi követelményeknek sem kell megfelelni esetükben.

A fentiekre tekintettel megállapítható, hogy az MI alapú megoldások használata az önkormányzati igazgatás, valamint a vízgazdálkodás területén is jelentős előnyökkel járhat, mind a hatósági döntés-támogatás, mind az állampolgárok és a hivatal közötti interakciók és a napi ügyintézés gördülékenyebbé tétele területén.

Összefoglaló gondolatok, következtetések levonása

Mint azt a fentiek tükrében is láthatjuk, az MI jelentős hatással bír a belügyi és biztonsági területen is. A segítségével csökkenthetők a nemzetbiztonsági kockázatok, valamint növelhető a bűnüldözés hatékonysága, ugyanakkor támogatható segítségével az önkormányzati ügyintézés, és csökkenthetők a vízgazdálkodás adminisztrációjával kapcsolatos terhek.

Hangsúlyozandó azonban, hogy az MI alapú rendszerek alkalmazásával járó egyes – különösen adatvédelmi természetű – kockázatok sem hagyhatók figyelmen kívül. Így a rendszerek alkalmazása előtt az adatkezelő szervnek fel kell mérnie, hogy feltétlenül szükséges-e a rendszer alkalmazása, és az nem váltható-e ki esetleg az érintettek magánéletére enyhébb hatással lévő eszközökkel és megoldásokkal. Amennyiben pedig az adott rendszer a fentiek szerint alkalmazható, úgy az adatkezelőnek olyan garanciákat kell biztosítania, amelyek az érintettek jogaira és szabadságaira gyakorolt negatív hatásokat csökkentik, valamint az érintettek adatvédelmi jogainak gyakorlását biztosítják.

Minderre tekintettel megállapítható, hogy a mesterséges intelligencia a jövő belügyi célú adatkezeléseinek egyik legfőbb támasza lehet, a segítségével pedig – annak helyes alkalmazása esetén és magas szintű adatvédelmi tudatosság mellett – hatékonyabb ügyintézés és a közbiztonság egy magasabb szintje érhető el.

Irodalomjegyzék

Könyv és tanulmánykötetben megjelenő írás

Klein, T. (2018) Az online nyilvánosság alkotmányjogi vonatkozásai. In: Klein, T. & Tóth, A. (ed.) Technológia jog – Robotjog – Cyberjog. Budapest, Wolters Kluwer Hungary Kft. pp. 219–261.

Lovas, R. (2017) Számításifelhő-alapú platformok alkalmazása a környezeti és társadalmi biztonság céljaira. In: Finszter, G. & Sabjanics, I. (ed.) Biztonsági kihívások a 21. században. Budapest, Dialóg Campus Kiadó. pp. 373–400.

Miskolczi, B. & Szathmáry, Z. (2018) Lehetőségek a büntetőeljárás előtt. In: Miskolczi B. & Szathmáry Z. Büntetőjogi kérdések az információk korában – mesterséges intelligencia, big data, profilozás. Budapest, HVG-Orac Lap- és Könyvkiadó Kft. pp. 190–203.

Osztopáni, K. (2018) Jogalapok, Közérdekű feladat ellátása és közhatalom gyakorlása. In: Péterfalvi, A., Révész, B. & Buzás, P. (ed.) Magyarázat a GDPR-ról. Budapest, Wolters Kluwer Hungary Kft. pp. 129–130.

Sabjanics, I. (2017) A nemzetbiztonság jogi koncepciója. In: Csink, L. (ed.) A nemzetbiztonság hatásainak kihívása a magánszférára. Budapest, Pázmány Press. pp. 103–123.

Serbakov, M. T. (2019) Az online felületek és okostelefonos alkalmazások mint a terrorcselekmények előrejelző rendszerei. In: Gaál, Gy. & Hautzinger, Z. (ed.) A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői. Pécs, Pécsi Határőr Tudományos Közlemények XXI., Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja. pp. 119–124.

Web-címek

Baraniuk, C. (2019.03.04) The new weapon in the fight against crime. https://www.bbc.com/future/article/20190228-how-ai-is-helping-to-fight-crime [Letöltve: 2020.10.30].

Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése. Brüsszel, 2020.02.19. COM(2020) 65 final, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_hu.pdf [Letöltve: 2020.10.30].

Joshi, N. (2018.10.10) 4 ways AI is helping with water management https://www.allerin.com/blog/4-ways-ai-is-helping-with-water-management [Letöltve: 2020.10.30].

Magyarország Mesterséges Intelligencia Stratégiája, lásd különösen: 38., 52. o. https://digitalisjoletprogram.hu/files/6f/3b/6f3b96c7604fd36e436a96a3a01e0b05.pdf [Letöltve: 2020.10.30].

Narendra, M. (2020.02.28) #Privacy: France issues first legal decision on facial recognition. https://gdpr.report/news/2020/02/28/privacy-france-issues-first-legal-decision-on-facial-recognition/ [Letöltve: 2020.10.30].

Oxford város önkormányzatának chatbotokkal és mesterséges intelligenciával kapcsolatos információs és projektoldala. https://local-digital.gov.uk/funding/oxford-city-council/ [Letöltve: 2020.10.30].