



Herke Csongor

A mesterséges intelligencia kriminalisztikai aspektusai

The forensic Aspects of Artificial Intelligence

Absztrakt

A mesterséges intelligencia (MI) a mindennapi életünk számos területén jelen van. Az MI-nek alapvetően meg kell változtatnia a gépekkel szemben eddig általánosan elfogadott szemléletet. Amíg a hagyományos számítógépeknél igaz a megállapítás, hogy csak azt hajtják végre, amire beprogramozták, addig a legfejlettebb és a legkifinomultabb MI-rendszerek képesek autonóm módon cselekedni, elfogadni és végrehajtani saját döntéseiket, amelyeket a programozók nem is láthattak előre. Könnyen belátható, hogy a jövőben az MI a kriminalisztika szinte minden területén megjelenik és hasznosítható lesz. Az MI nagyságrendileg gyorsabb és pontosabb lehet, mint egy ember. A telepített MI-szoftver képes a bonyolult számításokat gyorsabban és egyidejűleg végrehajtani, még ha egyelőre nem is tud gyorsabban gondolkodni. Emellett egy MI vezérelt robot olyan tevékenységeket is el tud végezni, amelyeket biztonsági okból egy ember nem vagy csak nagy kockázat árán tenne meg. Az MI beküldhető egy élesített pokolgép által veszélyeztetett helyiségbe, de részt vehet veszélyes körözött terroristák elfogásában, vagy éppen az emberi életre veszélyes anyag kezelésében is elvégezheti feladatát. A tanulmány elsősorban a nyomozás tervezése, szervezése, a kockázatértékelés, és a nemzetközi bűnügyi együttműködés egyes, az MI-vel összefüggő aspektusait tekinti át.

Kulcsszavak: mesterséges intelligencia, önvezető járművek, kriminalisztikai alapkérdések, nyomozás tervezése és szervezése, kockázatértékelés, nemzetközi bűnügyi együttműködés

Abstract

The artificial intelligence (AI) is present in many areas of our daily lives. AI needs to change fundamentally the hitherto generally accepted approach to machines. While it is true for traditional computers that they only execute what they are programmed for, the most advanced and sophisticated AI systems are able to autonomously act, accept, and execute their own decisions that their programmers could not foresee. It is easy to see that the AI will appear and be usable in almost all areas of forensics in the future. AI can be by orders of magnitude faster and more accurate than human being. The installed AI software is able to perform complex calculations faster and simultaneously, even if you can't think faster yet. In addition, an AI-robot can perform activities that a human being would not do, or would only do at high risk, due to security reasons. The AI can be sent to a room endangered by a bomb, but it can take part in the capture of dangerous searched terrorists, or it can also perform its task in the vicinity of materials dangerous to human life. The study primarily reviews some AI related aspects in planning and organizing of the investigation, in risk assessment and in international criminal cooperation.

Keywords: Artificial Intelligence, self-driving vehicles, basic issues of forensic science, planning and organizing of the investigation, risk assessment, international criminal cooperation

Bevezetés

Tremmel Flóriánt joggal tekinthetjük a Pécsi Bűnügyi Műhely szellemi atyjának, motorjának és lelkének. Tudományos pályafutása során mind a büntető eljárás-jog, mind a kriminalisztika területén fogékony volt a legmodernebb tudományos eredmények és módszerek megismerésére és ismertetésére. Mindig hangsúlyozta, hogy a jogi oktatáson belül milyen nagy jelentősége van a kriminalisztikának, és ez nem csak azokra igaz, akik később bűnügyi pályán kívánnak elhelyezkedni. Éppen ezért is írta meg (Fenyvesi Csabával közösen) 1997-ben a Kriminalisztika egyetemi jegyzetet (ami valójában a krimináltechnikai ismereteket foglalta össze), majd a krimiáltaktikával és szemléltető képekkel kiegészítve 1998-ban jelent meg a Kriminalisztika Tankönyv és Atlasz, amely egyedülálló a jogi oktatásban.

Tremmel Flórián mindig érdeklődött a modern kriminalisztikai eszközök és kutatások iránt. Nem véletlen, hogy már az 1998-as (illetve az immáron Herke Csongorral kiegészülve három szerzős 2004-es) tankönyvben is számos modern, a kriminalisztikai gyakorlatban nem vagy alig ismert módszert ismertetett, illetve

szorgalmazta azok mielőbbi bevezetését. Biztosak lehetünk abban, hogy ha ma valamit fontos kutatási területnek tart, az éppen a mesterséges intelligencia kriminalisztikai vonatkozása. Éppen ezért gondoltam, hogy Tremmel professzor 80. születésnapja tiszteletére ezt a kérdést járom körül, a teljesség igénye nélkül.

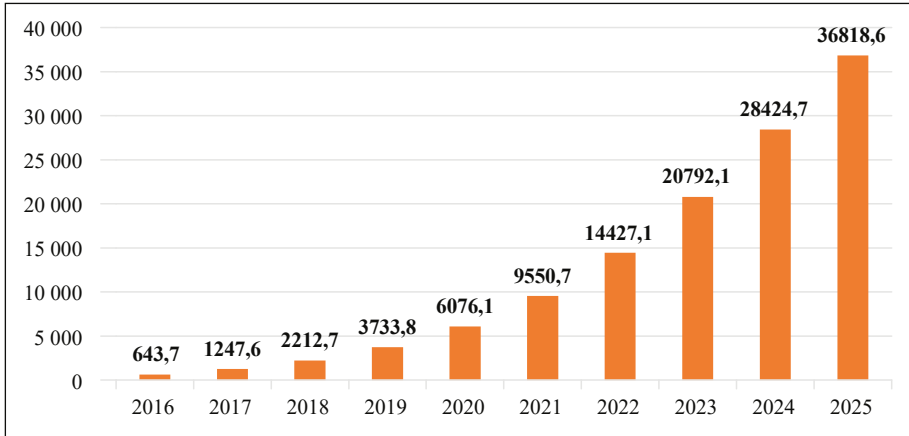
A mesterséges intelligencia (a továbbiakban MI) gyűjtő kifejezés, amely az 1956-os hannoveri Dartmouth College (New Hampshire) egyik műhelyének megfelelő szóalkotására vezethető vissza (angol kifejezéssel Artificial Intelligence, rövidítve AI). Az MI-t az különbözteti meg a hagyományos számítógéptől, hogy míg a számítógép az ismert „ha-akkor” („if-then”) kapcsolat alapján hozza meg a döntését (azaz előre beprogramozzák neki, hogy mire mi legyen a válasz), addig az MI szinte végtelen számú lehetőségből reagál (Staffler & Jany, 2020). Az MI tehát képes olyan ismereteket megszerezni, amelyeket előzetesen nem programoztak bele a fejlesztők. Más szakértők szerint az MI egy tanulásra képes matematikai modellt, amelyet az emberi agy mintájára hoztak létre (Kirpichnikov, Pavlyuk, Grebneva & Okagbue, 2020).

Amíg az emberiség pusztán eszközként használta a számítógépeket, addig (Hallevy példájával élve) nem volt valódi különbség a számítógépek és a csavarhúzó között, mert a számítógépek csak azt hajtották végre, amit az ember kért (Hallevy, 2019). A közelmúltig az MI rendszerek a programozó által előre beállított algoritmusok alapján működtek, viselkedésük tehát teljesen előre meghatározott volt (Borsari, 2019). Ennek megfelelően tesznek különbséget a „gyenge MI” (csak egy nagyon meghatározott területen intelligens viselkedést mutató gép) és az „erős MI” között. Utóbbi már nem az emberi gondolkodást szimulálja, hanem maga is egy elme (Moreno, 2021). A „gyenge MI” is képes fejlődni és tanulni, de csak a hozzá rendelt feladatprofil alapján. A legtöbb MI-rendszer „gyenge MI”. Az „erős MI” viszont képes a kijelölt feladatprofilon kívül is működni, ami azt jelenti, hogy alkalmazási és fejlesztési lehetőségei alig korlátozottak (Staffler & Jany, 2020).

Az MI a mindennapi életünk számos területén jelen van. Elég csak a gépjárművek navigációs rendszerére, az animációs filmek előállítására vagy akár az önvezető járművekre gondolni (Basile, 2019). Stephen Hawking egyenesen azt jósolta, hogy a következő száz évben a számítógépek intelligenciája meg fogja haladni az embereket, és elemezte azt a félelmet, hogy az MI akár le is rombolhatja a civilizációt (URL1; URL2). Ugyanerre utal az Európai Parlament robotikáról szóló, 2017. február 16-i állásfoglalásának preambuluma, miszerint lehetséges, hogy hosszú távon az MI meghaladja az emberi szellemi kapacitást.

Egyes tudósok szerint az MI világgpiaci részesedése 2016 és 2025 között hatvanszorosára emelkedik (643,7 milliárd USA dollárról 36.818,6 milliárd USA dollárra) (1. számú ábra).

1. számú ábra: *A mesterséges intelligencia világti részese*



Forrás: Kirpichnikov et al., 2020.

Tilesch és Hatamleh szintén úgy vélekedik, hogy az MI a hatalom újraelosztásának az egyik legfontosabb eszköze lesz a 21. században. Sőt szerintük nem sokára minden technológia MI-alapú lesz (Tilesch & Hatamleh, 2021).

Az MI alapvetően meg kell, hogy változtassa a gépekkel szemben eddig általánosan elfogadott szemléletet. Amíg a hagyományos számítógépeknél igaz, hogy „*a számítógépek csak azt csinálják, amire be vannak programozva*”, a legfejlettebb és a legkifinomultabb MI-rendszerek képesek autonóm módon cselekedni, elfogadni és végrehajtani saját döntéseiket, amelyeket a programozóik nem is láthattak előre (Basile, 2019).

Ettől függetlenül továbbra is igaz, hogy az algoritmusok nem rendelkeznek saját tényleges tudással. Az MI tehát nem értelmezhető olyan gépként, amely önállóan gondolkodik, de ismeretlen (előzetesen be nem táplált) paraméterekből állít elő reakciót (Staffler & Jany, 2020).

Nem véletlen tehát, hogy a Nemzetközi Büntetőjogi Társaság (AIDP) XXI. Kongresszusát 2024-ben az MI témakörében szervezi (URL3). A konferencia három fő kérdése az alábbi lesz:

- Mennyire tulajdonítható egy MI-rendszer által elkövetett bűncselekmény az embernek vagy magának az MI-nek (ha egyáltalán ez lehetséges)?
- Hogyan segíthetik az MI-rendszerek a rendészeti szerveket a bűnözés megelőzésében és leküzdésében?
- Bízhatunk-e az MI-ben a büntetőjogi ügyekben hozott döntések meghozatalakor?

A három kérdés közül kriminalisztikai szempontból a másodiknak van különös jelentősége. Az már ebből a felvetésből is egyértelműen látszik, hogy az MI-rendszerek hasznos kiegészítői lehetnek az igazságügyi munkának, és fel is gyorsíthatják azt (Staffler & Jany, 2020).

Az MI azonban nem csak előnyökkel jár, veszélyei már igen hamar megmutatkoztak. Ismert példa, hogy negyven évvel ezelőtt, 1981-ben egy motorke-rékpárgyár 37 éves japán alkalmazottját megölte a közelében dolgozó MI-robot (Hallevy, 2019). A robot (tévesen) fenyegető veszélyként azonosította az alkalmazottat, és kiszámította, hogy a fenyegetés leghatékonyabb kiküszöbölése az, ha őt egy szomszédos gépbe tolja, ezért hidraulikus karjával a robot a sokkolt munkavállalót a gépbe csapta, azonnal megölte, majd folytatta feladatait, mint-ha mi sem történt volna (Moreno, 2021).

Könnyen belátható, hogy a jövőben az MI a kriminalisztika szinte minden területén megjelenik és hasznosítható lesz. Ezen számos terület közül az alábbi-akban kettőt tekintünk át részletesen:

- a) a nyomozás tervezése, szervezése;
- b) a kockázatértékelés és a nemzetközi bűnügyi együttműködés kérdése.

Természetesen (ahogyan említettem) az MI a kriminalisztika minden területén jelen lesz (és sok helyen már jelen is van). Még az írásvizsgálat is jelentősen felgyorsulhat az MI-rendszer segítségével, de ugyanez lehet igaz egy ballisztikai vagy akár daktiloszkópiái, DNS stb. azonosításra is. Az MI ugyanis nagyság-rendileg gyorsabb és pontosabb lehet, mint egy ember. A telepített MI-szoftver lehetővé teszi a bonyolult számításokat gyorsabban és egyidejűleg végrehajtani (Hallevy, 2019). A legújabb generációs MI-k működése úgynevezett mély tanu-lási (deep learning) módszeren alapszik. Ezekben a technológiákban az inputok-tól az outputokig vezető folyamat átláthatatlan, sokszor nem is lehet levezetni, hogy a szoftver hogyan hozta létre a végeredményt, amely ezáltal nem is vezet-hető vissza a programozók eredeti akaratára (Borsari, 2019). Ezért is merül fel például magának a járműnek a felelőssége a teljesen önvezető járművek által elkövetett bűncselekmények vonatkozásában (Herke, 2021b).

Azonban az is könnyen belátható, hogy mennyivel gyorsabban és könnyeb-ben beszerezhető az adatok az MI segítségével a bűnügyi nyilvántartásokból (vagy akár végezheti maga az MI a nyilvántartást), hiszen ha az MI megfelelően működik, minden képességét fel tudja használni az adatok elemzésére (Hallevy, 2019). Az is egyértelmű, hogy óriási lehetőségek rejlenek az MI-ben a sajátos krimilátechnikai eszközök (csapda, képrögzítés, hangazonosítás) vonatkozásá-ban. Ahogyan a nagy adatfeldolgozást igénylő bűncselekmények elkövetésé-hez is egyre gyakrabban használnak fel MI-rendszereket. Gondoljunk csak az

úgynevezett „pump and dump”-ra, azaz az olyan csalásra, amely az értékpapír árának mesterséges emelkedését okozzák hamis, félrevezető vagy eltúlzott értékpapír-kereskedelemmel.

Ahogy a megerősítő tanulás révén az MI megtanulhatja a hamisítás gyakorlatát és önálló életre kelhet (Borsari, 2019), ugyanígy felhasználható lehet a bűnüldözésben is (Ligeti, 2020). Így például Nutter szerint az MI felhasználható hamis műalkotások azonosítására vagy személyek arcfelismerésére is, és akár rosszabb körülmények között is képes lenne azonosítani a kérdéses személyt a hagyományos arcfelismerő szoftverekhez képest (Nutter, 2019). A számítógépek a tárgyfelismerés, az arcfelismerés, az arckifejezés-elemzés, a beszélőfelismerés és akár az érzelemazonosítás terén is bizonyos esetekben már ma is felülmúlják az embereket (Perrot, 2017). Emellett utalni kell például az MI felhasználására a DNS-elemzések során (Rigano, 2019), de akár a közösségi médiaprofilok vonatkozásában is. Ennek előnye, hogy az MI elemzése nagy mennyiségű komplex adatot eredményez, rögtön elektronikus formátumban (Ligeti, 2020).

A nyomozás tervezése, szervezése

Ligeti szerint az MI-rendszerek két fő belső jellemzője, hogy képesek:

- a) összegyűjteni és elemezni a környező környezetből származó adatokat, valamint
- b) intézkedéseket végrehajtani a gép speciális (az ember által általában előre meghatározott) céljainak elérése érdekében (Ligeti, 2020).

A bűnügyi elemzés területén Perrot az MI alábbi alkalmazhatóságát emeli ki:

- a bűnözés földrajzi és időbeli hotspot területeinek meghatározása;
- a bűnözők profiljának meghatározása;
- a hasonló bűncselekmények elkövetése szintjének meghatározása egy adott területen;
- bizonyos feladatok tekintetében akár a nyomozó helyettesítése virtuális ügynökökkel (Perrot, 2017).

A bűncselekmények előrejelzése a digitális alkalmazások büntető igazságszolgáltatásban történő gyakorlati alkalmazásának egyik fontos területe. Az úgynevezett prediktív policing (előrejelzés-alapú rendőri munka) lényegében a rendőrségi aktákból származó részletes információk elemzését jelenti. Erre példa a közel ismétlődő megközelítés, amely szerint kiszámítható minták állnak rendelkezésre bizonyos bűncselekménytípusokhoz (például betöréses lopás), mivel a

sorozatbűnözők visszatérő viselkedési mintákkal rendelkeznek a sértettek racionális kiválasztása és költség-haszon elemzés alapján (Staffler & Jany, 2020).

A prediktív megközelítést nemcsak az USA-ban használják. Így például Franciaországban a Gendarmerie Nationale két év alatt kifejlesztette a bűnügyi kockázat prediktív megközelítését, elsősorban a sorozatbűncselekmények és a szervezett bűnözés vonatkozásában (Perrot, 2017).

A prediktív rendőri tevékenységek lényege, hogy statisztikai módszerek alapján igyekeznek előrejelezni a bűncselekmény elkövetését, és akár azt is, hogy hol és mikor követhető el a bűncselekmény. Célja pedig az, hogy ezen előrejelzés alapján megakadályozzák a bűncselekmények elkövetését. Az utóbbi időben a prediktív módszerek között megjelentek az első MI-alapú szoftverek is (például PredPol, Precobs, HART, X-LAW, Keycrime; utóbbi kettőt az olasz rendőrség használja). Ezek jelentős előrelépést jelentenek a bűncselekmények megelőzésében, ugyanakkor adatvédelmi problémákat is felvetnek (Basile, 2019).

Ligeti a prediktív rendőri tevékenységgel kapcsolatosan négy fő aggályt fejt ki:

- 1) Felmerül, hogy a prediktív rendfenntartás nem kontraproduktív-e azáltal, hogy a rendőrség az erőforrásokat ezekre a területekre összpontosítja, ezáltal az ezen kívüli területekre kevesebb energiát fordítanak.
- 2) A jövőbeni, még el nem követett bűncselekményekkel való gyanúsítás alapvető emberi jogokat sért, kezdve az ártatlanság vélelmével (Ligeti, 2020). Emellett gondot okozhat, hogy a védelem nincs abban a helyzetben, hogy megtámadja a bizonyítékok összegyűjtésének módját, és az MI-vel kapcsolatos bizonyítékok felhasználása kockázatot jelent a fegyverek egyenlőségének elvére is.
- 3) Noha általános a vélekedés, hogy a számítógép (ezáltal az MI is) objektív, semleges értékítélettel rendelkezik, Ligeti rámutat, hogy az igazságszolgáltatásban használt MI-gépek „beágyazzák a meglévő elfogultságokat és örökítik a diszkriminációt”, mivel az MI-rendszerek az emberek által bevitt adatok alapján működnek.
- 4) Végül a prediktív rendészet (és igazságszolgáltatás) miatt fennáll a veszélye, hogy a bűnüldöző hatóságok szerepe sokkal proaktívabb lesz a jelenlegi (többnyire) reaktívhoz képest, ami problémákat okozhat (például a hatóságok átláthatósága szempontjából) (Ligeti, 2020).

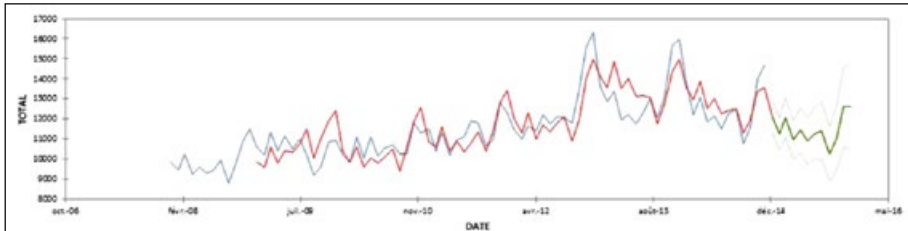
Staffler és Jany a bűncselekmények előrejelzésének két fő módját emeli ki: a hotspot azonosítást és a bűnözés összekapcsolását (crime linking) (Staffler & Jany, 2020). A hotspot azonosítás során a hatóságok algoritmusok segítségével olyan földrajzi mintákat hoznak létre a rendelkezésre álló adatokból, amelyek statisztikai szempontból magasabb bűnözéssel járnak, és ennek alapján valós

idejű figyelmeztetést generálnak a jövőbeli bűncselekmények vonatkozásában. Ilyen hotspot rendszer például az RTM (Risk Terrain Modeling), ami egy olyan algoritmus, amely a bűncselekményeket elősegítő tényezőkkel kapcsolatos különféle adatok kiértékelését használja a földrajzi helyek azonosítására annak érdekében, hogy statisztikai előrejelzést nyújtson a kábítószer-bűncselekmények elkövetéséről (URL4). Az olyan változók, mint a gyenge vagy nem működő utcai megvilágítás, az ATM-ek, pénzváltók, parkolók és iskolák közelsége, az éjszakai klubok, a tömegközlekedési megállók, vasútállomások, fő forgalmi kereszteződések környezete alapján olyan térképet hoztak létre a kábítószer-kereskedelem hotspotjainak az azonosítására, amely alapján következtetéseket lehet levonni a várható bűncselekmények elkövetésére, ami aztán jelentősen befolyásolja a rendőrség bűnmegelőzési stratégiáját (Staffler & Jany, 2020). Hasonló rendszer a Predictive Policing (rövidítve PredPol), ami olyan algoritmust használ, amely összekapcsolja a különböző bűnügyi statisztikai adatállományokat: a bűncselekmények típusát, helyét és idejét, és ennek alapján az algoritmus kiszámítja a statisztikai valószínűségét annak, hogy melyik területeken várható magasabb arányú bűnözés. Az ilyen rendszereket nemcsak az USA-ban, de Európában is egyre több helyen használnak, elég csak az Olaszországban a vagyoni elleni bűncselekmények helyben és időben való megismétlődésén alapuló, több helyen is alkalmazott XLAW szoftverre, vagy a Németországban és Svájcban alkalmazott, az azonos elkövetői csoportokon alapuló Pre Crime Observation System (rövidítve Precobs) szoftver használatára utalni.

A hotspot mellett Staffler és Jany szerint a bűncselekmények előrejelzésének másik sajátos módja a bűnözés összekapcsolása: múltbeli bűncselekmények összevetése bizonyos (már azonosított vagy még azonosítatlan) személyekkel annak érdekében, hogy megjósolják, hol és mikor követik el a következő bűncselekményt. Ez a módszer a sorozatbűnözőkre összpontosít (Staffler & Jany, 2020). Nagy-Britanniában a bűnözés összekapcsolására a Harm Assessment Risk Tool (rövidítve: HART) rendszert használják, amelynek célja az emberek osztályozása a jövőbeni bűncselekmények különböző kockázatait szerint. Ehhez olyan adatokat használnak fel, mint a bűnügyi nyilvántartás, a menekülés veszélye és a bűncselekmény súlyossága. Az algoritmus célja, hogy segítse a biztonsági erőket abban, hogy eldöntsék, a terhelt mennyi ideig legyen fogva vagy mikor ajánlhatson fel óvadékot (Oswald, Grace, Urwin S. & Barnes, 2018). Olaszországban pedig a milánói rendőrség fejlesztette ki a KeyCrime nevű szoftvert, ami azon a megfigyelésen alapult, hogy nagy számú rablást ugyanazok az elkövetők követnek el. Ezen bűncselekmények jellemzőit az egyes elkövetőkhöz rendelik annak érdekében, hogy előrejelzést készítsenek a bűncselekmény jövőbeli elkövetésének helyéről, idejéről és típusáról (URL5).

A prediktív elemzésre példa az alábbi francia modell (2. számú ábra), ami a 2008. és 2014. közötti adatok alapján tartalmazta a 2015-ös előrejelzést, igen nagy pontossággal.

2. számú ábra: A prediktív elemzés



Forrás: Perrot, 2017.

Az MI képes arra, hogy igen nagy mennyiségű tényadatot dolgozzon fel, és ennek alapján képes az összegyűjtött adatok gyors és pontos elemzésére, ami a nem MI-alapú adatfeldolgozásnál és adatelemzésnél sokkal nagyobb hatékonyságot eredményezhet (Borsari, 2019). Ehhez óriási mennyiségű adatra van szükség, amelyek egy része már most is rendelkezésre áll (gondoljunk csak a GAFAM – Google, Apple, Facebook, Amazon, Microsoft – és a NATU – Netflix, Air BNB, Telsa, Uber – globális vállalatok által naponta begyűjtött hatalmas adathalmazra) (Perrot, 2017). Ugyanakkor az MI fő jellemzője az önálló tanulás képessége, ami intellektuális autonómiát eredményez, és ez megnehezítheti megjósolni az MI tevékenységének okát és hatását, viselkedését vagy konkrét döntéseit (Kirpichnikov et al., 2020).

A gépi tanulási mechanizmusoknak köszönhetően az MI-rendszer képes tanulni a tapasztalatokból, és ennek következtében módosíthatja viselkedését, alkalmazkodva az időközben kapott ingerekhez (lásd a teljesen önvezető autók deep learning tanulását) (Herke, 2020). Sok esetben a felhőalapú információcsere exponenciálisan növelheti az MI tanulását (Borsari, 2019). A teljesen önvezető járműveknél éppen az okozza a legnagyobb problémákat, hogy az MI-rendszer olyan szabályokkal rendelkezik az adatbázisában, amelyek alapján csak két rossz döntés közül választhat (Moreno, 2021). Ugyanígy sok veszéllyel járhat az MI elterjedése a hétköznapi életben [lásd például az úgynevezett online ellenőrzés problémáját, amikor az MI-rendszer adott esetben néhány percen belül megvásárol bizonyos, nagy népszerűségnek örvendő eseményekre szóló jegyeket, majd visszahelyezi őket egy párhuzamos piacra (másodlagos jegyértékesítés), jóval magasabb áron; vagy a piac visszaélészerű manipulálására, amikor a nagyfrekvenciás kereskedők (úgynevezett HFT-k) másodpercenként

több ezer művelet végrehajtásával képesek a pénzügyi árak hirtelen és nagyon gyors ingadozásának előidézésére, aminek akár bűnügyi vonatkozásai is lehetnek, például tiltott piacbefolyásolás, Btk. 411. §] (Basile, 2019). Ligeti az MI-vel kapcsolatosan a kábítószer-kereskedelem, a terrorcselekmények és az online csalások veszélyére hívja fel a figyelmet (Ligeti, 2020), Borsari pedig ezen bűncselekmények vonatkozásában a távvezérelt drónok és tengeralattjárók felhasználását emeli ki (Borsari, 2019). Az MI azonban nemcsak terhelt, hanem sértett is lehet a büntetőeljárásban. Basile felveti a kérdést, hogy nincs-e szükség sajátos, kifejezetten az MI-rendszerek elleni bűncselekményekkel kapcsolatos tényállások megalkotására, mivel a jelenlegi büntetőjogi rendelkezések nem feltétlenül alkalmasak ezek kezelésére. Igen plasztikus példa erre szerinte a szexuális aktusok végrehajtása olyan androiddal, amelyet eredetileg nem erre a célra terveztek, hanem például recepciós funkciók ellátására szállodában vagy áruházban (Basile, 2019). És noha egyelőre nem tisztázott, hogy a kifejezetten szexuális igények kielégítésére létrehozott MI-robot (ügynevezett szexbot) sérelmére követhető-e el szexuális erőszak, Ambrus szerint az ilyen „bűncselekmény” kriminogén hatással lehet az emberek sérelmére elkövetett szexuális deliktumok vonatkozásában is (Ambrus, 2020).

Ezekkel a veszélyekkel foglalkozni kell, ugyanakkor az MI óriási segítséget nyújthat a bűnüldözésben.

Kockázatértékelés és MI. Az MI szerepe a nemzetközi bűnügyi együttműködésben

Az MI egyik lehetséges felhasználása a bűnözők specifikus profiljának modellezése. Az MI sok elemből álló minta elemzésére képes, ennek során vizsgálhatja az elkövetők mozgását, lakóhelyét, munkáját, szokásait, az általuk elkövetett bűncselekményeik jellegét, mindennapi tevékenységeiket, közösségi hálóikat stb. (Perrot, 2017).

A kényszerintézkedések taktikájával összefüggésben utalni kell arra, hogy létezik olyan elképzelés, miszerint például a veszélyes bűnözők elfogását robotokkal végeztessék, ezzel is védve a hatóság tagjainak személyi épségét. Ennek különös jelentősége lehet kiemelten veszélyes terroristák elleni akciók során. Ilyenkor az MI parancsot kap az elfogásra, nem vizsgálhatja az elfogást elrendelő határozat jogellenességét, bár a nyilvánvaló jogellenesség esetén elképzelhető, hogy a jövőben tudja ezt jelezni az elrendelő felé. Ebben az esetben Hallevy szerint nincs különbség aközött, hogy a határozatot végrehajtó természetes személy vagy például egy MI-robot (Hallevy, 2019).

Ligeti kiemeli, hogy a MI segíthet az események és helyek felkutatásában is (Ligeti, 2020). Amíg jelenleg az elemzések nagy részét emberek végzik, a jövőben ennek jelentős része automatizálható és/vagy gyorsítható a gépi tanulással (Maas, 2019).

Az USA büntető igazságszolgáltatási rendszerében évek óta egyértelmű tendencia figyelhető meg az empirikus kockázatértékelés mind gyakoribb alkalmazása terén. Ezzel kapcsolatosan két MI-alapú rendszer ismert az USA-ban, a Public Safety Assessment (PSA) és a Correctional Offender Management Profiling for Alternative Sanctions (COMPAS).

A PSA az adott személy bizonyos kockázati tényezőit hasonlítja össze egy adatbázissal, amely több mint 1,5 millió esetet tartalmaz 300 amerikai bírósági körzetből. Az elemzés kilenc kockázati tényezőt ölel fel, ideértve az életkort, a bűnügyi nyilvántartást, a korábbi idézéseket vagy panaszokat, ugyanakkor kizárja a földrajzi származást és a versenyt, mint kockázati tényezőt. A kockázatelemzés elvégzése után az eredményt hatrészes skálán jelölik (Staffler & Jany, 2020).

Az egyik leghíresebb kockázatértékelési eszköz az USA-ban a COMPAS (Ligeti, 2020). A program célja kockázatértékelés az elkövetők elhelyezésével, nyomon követésével és bánásmódjával kapcsolatos bírósági döntéshozatalban. A kockázatértékelés (alapkonfigurációjában) 137 kérdésre adott válaszon alapul, különféle témákban, például bűnügyi nyilvántartások és bűncselekmények, bűnözőkkel való megbirkózás, kábítószerrel való visszaélés, gazdasági nehézségek, oktatási és képzési nehézségek, a családi környezet, társadalmi kontextus, szabadidő, élethelyzet, társadalmi környezet, személyiségi tényezők. A kérdőívet vagy az érintett válaszolja meg vagy pedig a rendőrség és az ügyészség adatbázisait használják annak kitöltéséhez. A kérdőív még olyan általános kérdéseket is tartalmaz, mint hogy „*Van-e joga lopni egy éhes embernek?*”, amelyekre az érintettnek IGEN/NEM választ kell adnia (Staffler & Jany, 2020).

Ez a kockázatértékelés (látszólagos objektivitása ellenére) több kockázatot is rejt magában. Leginkább azzal kapcsolatosan merülhet fel probléma, hogy a védelem számára nem feltétlenül világos, hogy milyen tényezők alapján történik a kockázatértékelés, az MI-rendszer milyen szempontokat vett figyelembe, mennyire lett individualizált a kockázatértékelés.

Az MI prediktív algoritmusok vagy kockázatértékelési eszközök segítségével is felmérheti a büntetőjogi veszélyt. Irányulhat ez a kényszerintézkedés alkalmazhatóságára, de akár a büntetés vagy próbaidő feltételes felfüggesztésének lehetőségére vagy annak kizártságára is. Az MI képes hatalmas mennyiségű adat összegyűjtésére és feldolgozására, és ennek alapján képes megalkotni a személy profilját, és akár előrejelezni a későbbi magatartásformákat, ideértve

a bűnügyi vonatkozásokat is. A PSA és a COMPAS segítséget nyújtanak például a bírónak annak eldöntésében, hogy engedélyezi-e a feltételes szabadlábra helyezést vagy a próbára bocsátást (Basile, 2019).

A bevezetőben említett AIDP kongresszus 4. szekciója az MI használatának néhány nemzetközi vonatkozását fogja megvizsgálni. Ennek keretében a bizonyítékgyűjtés (illetve ezzel kapcsolatos nemzetközi együttműködés), valamint a nemzetközi humanitárius jog és a nemzetközi büntetőjog, különös tekintettel a robotok háborús környezetben történő használata emelhető ki (Ligeti, 2020). Emellett a nemzetközi humanitárius jogban és a nemzetközi büntetőjogban az utóbbi időben fokozott figyelmet kapott az autonóm fegyverrendszerek (AWS) kérdése is (Ligeti, 2020).

Az Interpol a számítógépes bűnözést a kormányok, vállalkozások és magán-személyek elleni bármilyen számítógépes támadásként határozza meg. Ezek a támadások nem ismernek sem fizikai, sem virtuális határokat, és jelentős károkat képesek okozni a világon (Moreno, 2021). A bizonyítékok határokon átnyúló cseréje, különösen a bizonyítékok más államban való elfogadhatósága és felhasználása régóta témája a nemzetközi szakirodalomnak. A digitális bizonyítékokkal kapcsolatos új – és még mindig nagy részben megoldatlan – problémák Ligeti szerint tovább bonyolítják a helyzetet. Ugyanakkor a számítógép, a digitális világ nem csak rosszat jelent: a MI nagyon sok segítséget nyújthat a nemzeti hatóságoknak (Ligeti, 2020).

A törvényesség elve arra kényszeríti a nyomozó hatóságokat, hogy a teljes nyomozati anyagot átfogóan elemezzék a kezdeti gyanú megállapítására vagy cáfolására. Érdekes megfigyelni, hogy míg az adatgyűjtésnél az MI-rendszer legfőbb előnye, hogy az emberhez képest nagyságrendileg több adatot tud beszerezni és összevetni, addig a digitális nyomozószoftver esetén már nem az adatok nagy mennyiségű előállítása, hanem éppen azok csökkentése, szűkítése jelenti a nagy előnyt. Az Észak-Rajna-Vesztfáliei Igazságügyi Minisztérium kutatási projektje, a Zentral- und Ansprechstelle Cybercrime NRW (ZAC NRW) bemutatja, hogy egy ilyen nyomozati szoftver hogyan tudja észszerűen csökkenteni az adatokat. A szoftver például az MI segítségével támogatja a gyermekpornográfia elleni küzdelmet. A gyermekpornográfiai tartalom interneten történő terjesztése elleni vizsgálati anyag elképzeltetlen mennyiségben keletkezik, ezért a büntetőjogilag releváns adatokat emberileg szinte lehetetlen lenne kiszűrni az ártalmatlan képfájlok között. Éppen ezért olyan algoritmust fejlesztettek ki, amelynek segítségével az MI megkülönbözteti az ártalmatlan képeket a gyermekpornográfiai anyagtól. Ezt követően már egy csökkentett adatsor tekintetében kell csak elvégezni a nyomozónak az ellenőrzést (Staffler & Jany, 2020).

Összegzés

Az MI a hagyományos számítógépes programoktól eltérő kibernetikai rendszer, amely képes autonóm, tudatos-akaratossá viselkedésre (Kirpichnikov et al., 2020). Sokan úgy képzelik, hogy az MI-rendszerek megjelenése a távoli jövő. Ugyanakkor számos példa mutatja, hogy ez már a jelen. Ahogyan arra már egy korábbi tanulmányomban rámutattam, 2012 óta 41 USA tagállamban engedélyezték az önvezető járműveknek a közúti forgalomban való részvételét (Herke, 2021a). Az MI-rendszerek használata már a bűnüldözési tevékenységekben is valóság, és várhatóan ez az elkövetkező években csak egyre növekszik és fokozódik. Egyes országokban már MI-robotokat használnak különféle feladatokhoz, például járőrözéshez, megfigyeléshez, bombabontáshoz, arcfelismeréshez stb. (Bassile, 2019). A következő feladat ezek szabályozási keretének kidolgozása lesz.

A jogi keretekkel kapcsolatban Staffler és Jany rámutatott, hogy 2002-ben az Európa Tanács Miniszteri Bizottsága felállította az igazságszolgáltatás hatékonyságával foglalkozó Európai Bizottságot (The European Commission for the Efficiency of Justice – CEPEJ), amely figyelemmel kíséri és felülvizsgálja a szerződő államok jogrendszereinek minőségét. Miután a közelmúltban megnőtt az MI használata a büntető igazságszolgáltatásban, és komoly kockázatok merültek fel az emberi jogokkal kapcsolatban, a CEPEJ 2018. december 4-én közzétette az MI igazságszolgáltatási rendszerekben való használatának etikai chartáját, amely szerint be kell tartani az emberi jogi normákat és az alapvető jogokat, különösen az Emberi Jogok Európai Egyezményét és az Európa Tanács adatvédelmi egyezményét (Staffler & Jany, 2020). 2019 szeptemberében megkezdte munkáját az Európa Tanács által létrehozott Mesterséges Intelligencia Ad Hoc Bizottság (CAHAI), amely jogi keretet biztosít az MI fejlesztéséhez, tervezéséhez és alkalmazásához. 2018 áprilisában az Európai Bizottság közzétette az „emberközpontú mesterséges intelligencia” európai stratégiáját, amely szerint az embernek kell az MI fejlesztésének középpontjában állnia. 2018 decemberében pedig az Európai Bizottság az összehangolt MI-terven keresztül bejelentette, hogy az MI-t a bűnözés elleni küzdelemben is használni kívánja (Staffler & Jany, 2020).

A legtöbb MI-rendszernek vannak érzékszervi receptorai, és ezek a receptorok a kapott tényadatokat az adatokat elemző központi feldolgozó egységekhez továbbítják. Az MI-rendszerek elemzési folyamata tehát nagyban hasonlít az emberi megértéshez. Az igazán fejlett MI-algoritmusok az emberi kognitív folyamatokat is megpróbálják utánozni. Hallevy rámutatott, hogy az MI és az ember kognitív folyamatai alapvetően nem különböznek egymástól (Hallevy, 2019).

Az MI-rendszerek alkalmazásával összefüggésben egyelőre nagy a félelem.

Az emberiség Borsari szerint két választási lehetőség előtt áll: az elővigyázatosság elvén alapulva nem alkalmaz MI-gépeket, ezzel lemond az általuk nyújtott előnyökről, vagy a megengedett kockázat, a kollektív haszon és a különféle rendszerek megfélézhetetlen kockázatai közötti összetett egyensúly elemzésével fokozatosan bevezeti ezeket a rendszereket (Borsari, 2019).

Még távol vagyunk attól, amit egy autonóm MI valóban jelentene, de a már létező MI is elegendő kihívást jelent a büntetőjoggal kapcsolatban (Moreno, 2021), de bármilyen kitalálnak is tűnik az MI-k kora, a látszat ellenére nem vagyunk olyan távol attól. A ma létező egyik legkifinomultabb emberszerű robot a Sophia, amelynek MI-rendszere már a tudat kezdetleges formáját hordozza magában. Önálló tanulási folyamatának fejlesztése érdekében Sophiának kommunikációra van szüksége az emberekkel, ezért alkotói „ember-mesterséges hibrid intelligenciának” tartják. Az egyik nyilvános beavatkozása során maga Sophia kijelentette, hogy az MI-rendszerek nem versenyeznek az emberi intelligenciával, hanem inkább kiegészítik azt (Moreno, 2021). Szaud-Arábia állampolgárságot adott Sophiának, egy tokiói önkormányzat pedig elismerte egy chatbot, Shibuya Mirai állandó lakóhelyét, „aki” egy hétéves gyermek képességeivel képes kommunikálni (Basile, 2019).

Az információ, amely fizikai tulajdonságai miatt hozzáférhető az információs és távközlési hálózatokban, az MI, a szoftverek és a kritikus jelentőségű elektronikus információs rendszerek által okozott illegális befolyás legnagyobb veszélyének van kitéve (Kirpichnikov et al., 2020). Az csak rajtunk múlik, hogy ettől a veszélytől megriadunk vagy az MI segítségével jobbá tesszük az életünket és kiaknázzuk azt a hatalmas lehetőséget, amivel kapcsolatosan egyelőre csak a jéghegy csúcsát látjuk.

Felhasznált irodalom

- Ambrus I. (2020). A mesterséges intelligencia és a büntetőjog. *Állam- és Jogtudomány*, 61(4), 4-23.
- Basile, F. (2019). Diritto penale e Intelligenza Artificiale. *Giurisprudenza Italiana*, 170(12), 67-73.
- Borsari, R. (2019). Intelligenza Artificiale e responsabilità penale: prime considerazioni. *Media Laws*, 4(3), 262-268.
- Hallevy, G. (2019). The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control. *Akron Intellectual Property Journal*, 4(2), 171-201.
- Herke Cs. (2021a). A kriminalisztika alapkérdései és az önvezető járművek. *Belügyi Szemle*, 69(1), 87-105. <https://doi.org/10.38146/BSZ.2021.1.4>
- Herke Cs. (2020). „De biztos Úr, én nem is tudok vezetni!” – a terhelt az önvezető járművekkel kapcsolatos büntetőeljárásokban. *Magyar Jog*, 67(11), 633-647.

- Herke Cs. (2021b). The digital person as defendant in criminal proceedings relating to self-driving vehicles. C. E. Чебуранова (Eds.), *Состояние, проблемы и перспективы развития юридической науки и практики: белорусский и зарубежный опыт* (pp. 184-189). Yanka Kupala State University.
- Kirpichnikov, D., Pavlyuk, A., Grebneva, Y. & Okagbue, H. (2020). Criminal Liability of the Artificial Intelligence. *E3S Web of Conferences*, 159(04025), 1-10. <https://doi.org/10.1051/e3sconf/202015904025>
- Ligeti K. (2020). *Artificial Intelligence and Criminal Justice AIDP-IAPL International Congress of Penal Law*. <http://www.penal.org/en/aidp-iapl-publications>
- Maas, M. M. (2019). International law does not compute: Artificial intelligence and the development, displacement or destruction of the global legal order. *Melbourne Journal of International Law*, 20(1), 29-57.
- Moreno, A. M. M. (2021). Inteligencia artificial y derecho penal: primeras aproximaciones. *Revista jurídica de Castilla y León*, 19(53), 177-202.
- Nutter, P. W. (2019). Machine Learning Evidence: Admissibility and Weight. *Journal of Constitutional Law*, 21, 919-958.
- Oswald, M., Grace, J., Urwin, S. & Barnes, G. C. (2018). Algorithmic risk assessment policing models: lessons from the Durham HART model and ‘Experimental’ proportionality. *Information & Communications Technology Law*, 27(2), 223-250. <https://doi.org/10.1080/13600834.2018.1458455>
- Perrot, P. (2017). What about AI in criminal intelligence? From predictive policing to AI perspectives. *European Police Science and Research Bulletin*, 16, 65-76.
- Rigano, C. (2019). Using Artificial Intelligence to Address Criminal Justice Needs. *National Institute of Justice Journal*, 1, 1-10.
- Staffler, L. & Jany, O. (2020). Künstliche Intelligenz und Strafrechtspflege – eine Orientierung. *Zeitschrift für Internationale Strafrechtsdogmatik*. 15(4), 164-167.
- Tilesch Gy. & Hatamleh, O. (2021). *Mesterség és intelligencia. Vegyük kezünkbe sorsunkat az MI korában*. Libri Kiadó.

A cikkben található online hivatkozások

URL1: *Stephen Hawking warns artificial intelligence could end mankind*. <https://www.bbc.com/news/technology-30290540>

URL2: *Stephen Hawking AI Warning: Artificial Intelligence Could Destroy Civilization*. <https://www.newsweek.com/stephen-hawking-artificial-intelligence-warning-destroy-civilization-703630>

URL3: *XXIst International Congress of Penal Law. 2024*. <http://www.penal.org/en/information>

URL4: *Risk Terrain Modeling*. <https://www.riskterrainmodeling.com>

URL5: *Numbers of KeyCrime*. <https://www.keycrime.com>

A cikk APA szabály szerinti hivatkozása

Herke Cs. (2021). A mesterséges intelligencia kriminalisztikai aspektusai. *Belügyi Szemle*, 69(10), 1709-1724. <https://doi.org/10.38146/BSZ.2021.10.2>

