

inAtrhteifCicoinalteIxntte olfliCgreinmce és a büntető

JELENTÉS A KOREAI KRIMINOLÓGIAI INTÉZET SZÁMÁRA

igazságszolgáltatás

ACritmificialndIntCerilmigeinnacle JusticeContext of

Benoît Dupont, Yuan Stevens, Hannes Westermann, Michael Joyce

Kanadai kutatói szék a kiberbiztonság területén

Nemzetközi Összehasonlító Kriminológiai Központ - Université de Montréal

Jelentés a Koreai Kriminológiai Intézet számára december,



Nemzetközi Összehasonlító Kriminológiai Központ

URL:<https://www.cicc-iccc.org/en>



Kanadai kutatói tanszék a kiberbiztonság területén Université de Montréal, Montreal, Kanada

URL:<https://www.umontreal.ca/>

Dr. Benoît Dupont

E-mail cím: benoit.dupont@umontreal.ca

Köszönetnyilvánítás

Köszönjük a Montreali Egyetem Kiberbűnözés Laboratóriumának, az Összehasonlító Kriminológia Nemzetközi Központjának és Dr. Carlo Morselli igazgatónak a támogatást.

Külön köszönetet mondunk Dr. Jea Hyen Soungnak és a Koreai Kriminológiai Intézet Nemzetközi Együttműködési Központjának munkatársainak a jelentés elkészítésében nyújtott segítségükért.

TARTALOMI OLDAL

<i>Előszó</i>	iv
<i>Előszó</i>	vi
<i>Összefoglaló</i>	ix
1. BEVEZETÉS	1
2. A MESTERSÉGES INTELLIGENCIA MEGHATÁROZÁSA: MIA MESTERSÉGES INTELLIGENCIA, ÉS MIÉRT FONTOS A BÜNTETŐ IGAZSÁGSZOLGÁLTATÁS SZÁMÁRA?	9
2.1. Mi az AI?	9
2.1.1. Mesterséges intelligencia	9
2.2. A szűk mesterséges intelligencia megközelítésének története	11
2.2.1. Szabályalapú rendszerek	12
2.2.2. Gépi tanulás	13
2.2.3. Mély tanulás	15
2.3. A gépi tanulás módszerei	18
2.3.1. Felügyelt tanulás	18
2.3.2. Nem felügyelt tanulás	20
2.3.3. Erősítéssel tanulás	21
2.3.4. Generáció	21
2.4. A mesterséges intelligencia kockázatai	23
2.4.1. Általános AI	23
2.4.2. Szűk AI	24
2.4.2.1. Adatvédelem	24
2.4.2.2. Nudging	25
2.4.2.3. Diszkrimináció	26
2.4.2.4. Opacitás	28
2.5. Következtetés	29

3.	AZ AI MINT A BŰNÖZÉS VEKTORA: A "BŰNÜGYI AI" MEGJELENÉSE	31
3.1.	A mesterséges intelligencia demokratizálása	33
3.1.1.	Adatok	33
3.1.2.	Szoftver és szakértelem	36
3.1.3.	Hardver	37
3.2.	A mesterséges intelligencia káros felhasználása	38
3.3.	A rosszindulatú mesterséges intelligencia megközelítései	39
3.3.1.	Social Engineering	40
3.3.1.1.	Adathalászat	40
3.3.1.2.	Vishing	43
3.3.1.3.	Astrourfing	45
3.3.2.	Generáció	48
3.3.3.	Kiberbiztonság	51
3.3.3.1.	Sebezhetőség felfedezése	52
3.3.3.2.	Kihhasználás	55
3.3.3.3.	Post-Exploitation & adatlopás	56
3.3.4.	A telepített mesterséges intelligencia felhasználása	57
3.3.4.1.	Ellenséges támadások	58
3.3.4.2.	A mesterséges intelligencia rendszerek mérgezése	59
3.4.	Következtetés	61
4.	MESTERSÉGES INTELLIGENCIA A BŰNÜLDÖZÉS BEN	64
4.1.	AI és bűnfelderítés	65
4.1.1.	A technológia és a bűnfelderítés története	65
4.1.2.	A mesterséges intelligencia képességeinek taxonómiája	68
4.1.2.1.	Tárgyak osztályozása	68
4.1.2.2.	Tárgyfelismerés (beleértve az arcfelismerést is)	72
4.1.2.3.	Rendőrségi testkamerák	79
4.1.2.4.	Beszéd felismerés	81
4.1.2.5.	Lövésérzékelés	82
4.1.2.6.	DNS-elemzés	84
4.1.2.7.	Digitális kriminalisztika	86
4.2.	AI a bűnözés előrejelzéséhez és megelőzéséhez	87

4.3.	Következtetés: A szakirodalom hiányosságai és etikai aggályok	90
4.3.1.	A mesterséges intelligenciával kapcsolatos kérdések feltérképezése a bűnüldözésben	91
4.3.2.	Előremutató utak	96
5.	MESTERSÉGES INTELLIGENCIA A BÜNTETŐELJÁRÁSBAN	116
5.1.	Hogyan használják már a mesterséges intelligenciát a büntetőeljárásokban	116
5.1.1.	A mesterséges intelligencia alkalmazása az óvadékkal kapcsolatos döntésekben	117
5.1.2.	New Jersey közbiztonsági értékelő eszköze	120
5.1.3.	A mesterséges intelligencia alkalmazása az ítélethozatalban	127
5.1.4.	A COMPAS használata az ítélethozatal során	128
5.2.	Hiányosságok a szakirodalomban és etikai aggályok	132
5.2.1.	Van bizonyíték arra, hogy ezek az eszközök pontosabbak, mint a már meglévő rendszerek? Van-e bizonyíték arra, hogy a mesterséges intelligencia alkalmazása a jogi eljárásokban beváltja az ígéretekét?	133
5.2.2.	Egy adott kontextusban létrehozott és/vagy használt mesterséges intelligencia eszközt kell-e használni a más igényei?	135
5.2.3.	A technológia tervezésekor és bevezetésekor bizonyítottan átláthatóságra, a veszélyeztetett népcsoportokat érő károk mérséklésére és a következőkre vonatkozó követelményre törekednek-e? lehetővé teszi a tájékozott beleegyezést az általa jelentett kockázatokra vonatkozóan?	136
6.	KÖVETKEZTETÉS ÉS AJÁNLÁSOK	142
6.1.	Etikai kihívások	142
6.2.	Hatékonysági kihívások	147
6.3.	Közbeszerzési kihívások	152

6.4. Kihívások az előírányzathoz.....	158
Hivatkozások listája.....	161

Előszó

Nagy örömmre szolgál, hogy bemutathatom a Mesterséges intelligencia a bűnözés és a büntető igazságszolgáltatás kontextusában című, a Koreai Kriminológiai Intézet és a Montréali Egyetem második közös kutatási projektjét. A Koreai Kriminológiai Intézet nevében szeretném hálásan megköszönni Benoît Dupont professzor és a Montréali Egyetem Nemzetközi Összehasonlító Kriminológiai Központjának (ICCC) kutatói által tett jelentős erőfeszítéseket.

A pilóta nélküli járművek, sebészeti robotok, ipari robotok és más mesterséges intelligencia (AI) egységek világszerte elterjedtek. Az ilyen felhasználás lehet személyes, orvosi, katonai, kereskedelmi vagy ipari. Ez a kutatás az AI-technológiák jelenlegi és jövőbeli használatát, valamint a büntető igazságszolgáltatási rendszer főbb szereplőire gyakorolt lehetséges hatásait vizsgálja. E tekintetben a KIC és az Université de Montréal közös kutatása nagy jelentőséggel bír abban, hogy segítse a bűnügyi igazságügyi igények - például a bűncselekményekkel vagy a közbiztonsággal kapcsolatos videókon szereplő személyek és tetteik azonosítása, a DNS-elemzés, a lövések felderítése és a bűnügyi előrejelzés - terén a mesterséges intelligencia alkalmazása terén vezető szerepet tölthet be. Nincs kétségem afelől, hogy ez a kiadvány értékes lépést jelent majd a mesterséges intelligencia bűnügyi igazságügyi célokra történő felhasználása iránt érdeklődő tudósok és szakemberek számára világszerte. Remélem, hogy ez a kiadvány megkapja azt a széleskörű olvasottságot, amelyet megérdemel, és hogy a Korea és Kanada közötti kriminológiai partnerség továbbra is virágzik.

Még egyszer szeretném kifejezni elismerésemet a KIC és az Université de Montréal összes kutatójának és tagjának kemény munkájáért, akik lehetővé tették ezt a kiadványt.

A handwritten signature in black ink, reading "In Sup Han". The script is cursive and fluid, with the first letters of each name being capitalized and prominent.

In Sup Han, a Koreai Kriminológiai Intézet
elnöke

Előszó

Talán nincs még egy jelenleg fejlesztés alatt álló technológia, amely annyi reményt, felhajtást és félelmet kelt, mint a mesterséges intelligencia (AI). A kormányok és a vállalatok dollármilliárdokat ölnek olyan kutatólaboratóriumokba és startupokba, amelyek azt remélik, hogy egész gazdasági ágazatokat fognak felforgatni, és javítani fogják az emberek kognitív képességeit. Az emberi tevékenység egyetlen területét sem hagyja érintetlenül a mesterséges intelligencia megjelenése, amint azt a Go bajnok Lee Sedol is megtapasztalta, amikor 2016 ötjátszmás mérkőzést veszített a Google leányvállalata, a DeepMind által létrehozott AlphaGo ellen, amely a dél-koreai Go Szövetség 4-1-es győzelmét követően a legmagasabb nagymesteri rangot kapta.

Bár a mesterséges intelligencia jelenlegi felhasználása a nyelvi fordítás, a képosztályozás és általában a mintafelismerés területén hozta a leglenyűgözőbb eredményeket, a kormányok egyre szélesebb körben vizsgálják a mesterséges intelligencia olyan területeken történő alkalmazásának lehetőségeit, ahol a várakozások szerint a mesterséges intelligencia előrejelző képességei javítani fogják a szolgáltatásnyújtás minőségét és az állami beavatkozások hatékonyságát. Az egyik olyan alkalmazási terület, amely eddig nagy médiafigyelmet kapott, de még mindig nagyon kevés tudományos kutatással rendelkezik, a büntető igazságszolgáltatás, amelyet ebben a jelentésben úgy határozunk meg, mint a kölcsönhatások és intézmények összetett hálóját, amely a bűnelkövetőket, a rendőröket, a bírósági tisztviselőket és a büntetés-végrehajtási szakembereket egyesíti.

Úgy véljük, hogy ennek az intenzív érdeklődésnek az egyik oka a sci-fi disztópiák elterjedésében rejlik.

intelligens gépek, amelyek képesek előre jelezni az egyes bűncselekményeket, mielőtt azok bekövetkeznének, és korlátozzák a polgárok egyéni szabadságjogait, hogy mindenáron fenntartsák a törvényt és a rendet. Az ilyen rémisztő kimenetel valószínűleg nem fog bekövetkezni, de ez nem jelenti azt, hogy a büntető igazságszolgáltatási intézmények simán átveszik az AI-technológiákat, vagy hogy ezek az új eszközök meghozzák mindazokat az előnyöket, amelyeket tervezőik és támogatóik hirdetnek. Számos csalódásra és kudarcra lehet számítani, amelyek közül néhány kiszámíthatatlan és igazságtalan kimenetelű lesz. Más szóval, a mesterséges intelligencia büntető igazságszolgáltatásban való felhasználásának jövője inkább Franz Kafkára emlékeztethet, mint George Orwellre vagy Philip K. Dickre.

Ezért ez a jelentés megkísérli feltérképezni azt a hétköznapiabb valóságot, amely valószínűleg kialakul, valamint azokat a számos kihívást, amelyekkel a büntető igazságszolgáltatási intézményeknek a mesterséges intelligenciával való kísérletezésük eredményeként meg kell majd küzdeniük. Miután rövid áttekintést adtunk a rendelkezésre álló különböző típusú gépi tanulási technológiákról és azok várható hatásáról a társadalom egészére, megvizsgáljuk a mesterséges intelligencia tényleges és lehetséges felhasználását a büntető igazságszolgáltatási rendszerben interakcióban álló szereplők és érdekeltek négy fő kategóriája - az elkövetők, a bűnüldöző szervek, a bírúk és a büntetés-végrehajtási tisztviselők - által. Az egyes fejezetek felvázolják a mesterséges intelligencia ismert felhasználási módjait az egyes csoportoknál, a még nem megvalósult, de a közeljövőben várható potenciális alkalmazásokat, valamint az etikai vagy működési akadályokat, amelyekkel ezek a felhasználások találkozhatnak, továbbá az igazságszolgáltatásra gyakorolt becsült hatásukat. A jövőre vonatkozó jóslatok megfogalmazása mindig veszélyes, ezért tartózkodunk a sci-fi forgatókönyvektől, amelyek jó szórakozást nyújtanak, de gyakran nem tudják elképzelni a büntető igazságszolgáltatási bürokráciák unalmasabb valóságát. Az

utolsó fejezetben összefoglaljuk a négy fő kihívást, amelyekről úgy véljük, hogy a következőkre vonatkoznak

amelyekkel a politikai döntéshozóknak, a gyakorlati szakembereknek és a kutatóknak foglalkozniuk kell a mesterséges intelligencia rendszerek büntetőjogi környezetben való alkalmazásán gondolkodó szakembereknek: ezek a kihívások etikai, technikai, adminisztratív és kulturális jellegűek. Bár az etikai dilemmák és az általuk elkerülni kívánt előítéletek foglalják el a mesterséges intelligenciáról szóló beszélgetések nagy részét, a három másik, egymással összefüggő kihívás is mind figyelmet érdemel.

A mesterséges intelligencia nem az első - és nem is az utolsó - olyan technológia, amely a büntető igazságszolgáltatási rendszer megzavarására törekszik, és azt állítja, hogy képes hatékonyabbá és eredményesebbé tenni annak intézményeit. Számos ilyen technológia nem hozta meg a várt előnyöket. Annak megértése érdekében, hogy az ilyen ígéretes innovációk miért buknak el folyamatosan, e jelentés utolsó ajánlása az etnográfiai tanulmányok ösztönzése, amelyek célja annak megértése, hogy az emberek és a mesterséges intelligencia által működtetett gépek új együtteseik hogyan működnek a mindennapi gyakorlatban, hogy túllépjünk az algoritmusok jelenlegi fetiszmusán.

Benoît Dupont professzor

Kanadai kutatói tanszék a kiberbiztonság területén - Université de Montréal

Összefoglaló

A hírek nap mint nap emlékeztetnek minket arra, hogy a mesterséges intelligencia (AI) a digitális forradalom egyik legmegrendítőbb technológiája lesz. A sakk- és góvilágbajnokokat olyan gépek győzik le, amelyek könyörtelen hatékonysággal győzik le ellenfeleiket, miközben az adatközpontok energiafelhasználását irányító mesterséges intelligencia lenyűgöző energiamegtakarítást eredményez, az orvosi algoritmusok pedig úgy tűnik, képesek felismerni a rákos daganatokat, mielőtt azok a felvételeken megjelenének. A közeljövőben az autonóm járművek a közúti balesetek halálos áldozatainak számának jelentős csökkentését ígérik, az univerzális fordítók pedig a nyelvek közötti jobb kommunikációt teszik lehetővé, mindezt olyan gépi tanulási technológiák segítségével, amelyek az emberi tevékenységek minden aspektusát optimalizálják. Jelenleg dollármilliárdokat fektetnek be a kormányok, a kockázati tőkecégek és az olyan internetes óriások, mint a Microsoft, a Facebook, az Amazon és az Apple, hogy a mesterséges intelligencia megoldásokat beépítsék szolgáltatásaikba és termékeikbe.

A zavarok fájdalommal is járnak majd, a legrosszabb előre jelzett hatás a munkahelyek millióinak megsemmisülése lesz. A legpesszimistább tanulmányok szerint a fejlett gazdaságokban a munkahelyek csaknem felét fenyegeti az automatizálás veszélye. A fizikai, ismétlődő munkát nyilvánvalóan kiemelik, de a tudásalapú munka és a szakmai szolgáltatások, például a jog és az orvostudomány is veszélyeztetetté válnak. Egyes szélsőséges esetekben a mesterséges intelligenciát egyéni elkövetők és bűnözői csoportok is felhasználják majd arra, hogy soha nem látott számú áldozatot károsítsanak meg. Erre válaszul a büntető igazságszolgáltatási szervezetek már most fontolgatják a következők alkalmazását

a mesterséges intelligencia technológiákat az eljárásaik hatékonyságának és eredményességének javítása érdekében, és néhány kísérleti alkalmazást jelenleg a bűnüldöző szervek, a bíróságok és a büntetés-végrehajtási szolgálatok alkalmaznak. Minden bizonnyal nem ez az első olyan technológiai innovációs hullám, amely átalakítja az igazságszolgáltatást az idők során, de az általa bevezetett potenciális torzítások, valamint a magyarázhatóság és az elszámoltathatóság hiánya komoly kihívást jelent a demokratikus értékek számára.

Ez a feltáró jelentés a világ minden tájáról gyűjtött példák széles körére támaszkodva áttekintést nyújt arról, hogy a mesterséges intelligencia milyen szerepet fog játszani a büntető igazságszolgáltatásban. Olyan szekvenciális megközelítést alkalmaz, amely tükrözi a bűncselekmény kibontakozását, az elkövetők általi elkövetéstől a bűnüldöző szervek általi felderítésig, majd a büntetőbíróságok általi elbírálásig, végül pedig a büntetés végrehajtásától a büntetés-végrehajtási szolgálatokig.

Annak érdekében, hogy megértsük azokat a mögöttes technikai koncepciókat, amelyek a mesterséges intelligenciát a bűnügyi igazságszolgáltatási szervek számára ilyen zavaró technológiává teszik, a 2. fejezet a mesterséges intelligencia történetét és jellemzőit igyekszik ismertetni, különös hangsúlyt fektetve a számítógépes programozás más formáitól való eltérésekre. Ez a fejezet feltérképezi a mesterséges intelligencia fejlődését a szabályalapú rendszerektől kezdve, amelyeket már az 1950-es években bevezettek a számítástechnikában, majd az 1980-as években felváltották a gépi tanulás megközelítései, amelyek kifejlesztették a tapasztalattal való automatikus javulás képességét. Végül a Deep Learning a gépi tanulás egyik alcsoportjaként most virágzik, és az emberi agyból inspirálódott többrétegű architektúrára támaszkodik, amely automatikusan megtalálja a releváns jellemzőket a strukturálatlan adatok óceánjában. A mélytanulás drámai javulást eredményezett olyan területeken, mint például a

képosztályozás,

x

beszéd felismerés és természetes nyelvi feldolgozás. Páratlan lehetőségei ellenére a mélytanulásnak számos buktatója is van, például az, hogy olyan tulajdonságokat is felfedhet, amelyeket az emberek inkább titokban szeretnének tartani, hogy nagymértékben befolyásolhatja az embereket anélkül, hogy ezek az emberek észrevennék, hogy manipulálták őket, hogy reprodukálja és felerősíti az adatokba ágyazott elfogultságokat és diszkriminációt, amelyeket előrejelzések készítéséhez használ, valamint hogy strukturális átláthatatlanságot biztosít az okok tekintetében, amelyek miatt egy adott következtetésre jutott. A mesterséges intelligencia körüli jelenlegi hype-ot tápláló Deep Learning technológia ezen korlátai tehát megerősíthetik a status quo-t és fenntarthatják a szisztematikus diszkriminációt.

A fejezet a mesterséges intelligenciára mint a bűnözés vektorára összpontosít³. A mesterséges intelligencia demokratizálódása azt jelenti, hogy a nyilvánosság tagjai hozzáférnek a saját mesterséges intelligencia-eszközök (adatok, szoftverek és hardverek) használatához és fejlesztéséhez szükséges kulcsfontosságú erőforrásokhoz, ami a rosszindulatú szereplőket is képessé teheti arra, hogy a mesterséges intelligenciát aljas célokra használják. A mesterséges intelligencia által jelentett bűnügyi kockázatok három kategóriába sorolhatók: meglévő bűnügyi fenyegetések, amelyek a mesterséges intelligencia által lehetővé tett automatizálás miatt bővülnek, új fenyegetések, amelyeket a mesterséges intelligencia azon képessége vezet be, hogy egy személy hangját vagy képét utánozó adatokat képes generálni, hibrid fenyegetések, amelyek a célzottabb, hatékonyabb és kevésbé tulajdonítható támadások miatt alakulnak ki. A mesterséges intelligencia által elősegített vagy lehetővé tett bűncselekmények közül ez a jelentés kiemeli a social engineering támadásokat (adathalászat, vishing és astroturfing), a rendkívül valóságúnak tűnő képek, videók vagy hangfoszlányok létrehozására épülő generatív támadásokat (deep fakes), valamint a technikai jellegű

kibertámadásokat, amelyek során a mesterséges intelligencia rendszereket ismeretlen szoftversebezhetőségek felfedezésére és kihasználására használják. Szó esik továbbá az ellenséges támadásokról, amelyek során a mesterséges intelligenciával működő rendszerek alááshatók vagy megmérgezhetők.

A 4. fejezet azt vizsgálja, hogy a bűnüldöző szervek világszerte hogyan kezdték el használni a mesterséges intelligencia alapú technológiákat a bűncselekmények felderítésére, kivizsgálására, megelőzésére, sőt időnként még a bűncselekmények előrejelzésére is. A technológia bűnügyi nyomozásban való felhasználásának hosszú története van, de a mesterséges intelligencia használata képes a felügyelet és a társadalmi ellenőrzés eddig soha nem látott szintjét elősegíteni. Először is, a mesterséges intelligencia vonzó technológia a bűncselekmények felderítésére a mintafelismerési és tárgyszortályozási képességei miatt: A mesterséges intelligencia képes például megtanulni azonosítani azt a helyet, ahol egy kép vagy videó készült, vagy bizonyos tetoválásokat bizonyos bandákhoz való tartozáshoz vagy jelentéshez társítani. Az arcfelismerő technológia és annak élőben követési képessége szintén nagymértékben támaszkodik a mesterséges intelligenciára, és Kína széles körben használja azt a városi központokban. A bűnfelderítés egyéb felhasználási területei közé tartoznak a testen viselt kamerák, a beszéd felismerő technológia (például telefonlehallgatáshoz), a lövések felderítésére szolgáló rendszerek, valamint a DNS és a digitális törvényszéki elemzés. A bűnüldöző szervek a mesterséges intelligenciát a bűncselekmények megelőzésére és előrejelzésére is használják, olyan termékekkel, mint például a PredPol, amelyek azt állítják, hogy képesek meghatározni a jövőbeli események helyét, lehetővé téve ezzel a proaktív és elrettentő rendőri jelenlétet. Az ilyen előrejelző megközelítés hatékonyságát alátámasztó tudományos bizonyítékok a legjobb esetben is ellentmondásosak, miközben egyes kiszolgáltató csoportok (különösen a látható kisebbségek) esetében jelentős a tisztességtelen profilalkotás kockázata.

A fejezet a bíróságokra és a büntetés-végrehajtásra összpontosít⁵, bemutatva, hogyan épül be a mesterséges intelligencia a bírósági és büntetés-végrehajtási döntéshozatali folyamatokba. A jelentés azonosít néhány kulcsfontosságú területet, például az óvadékkal és büntetés-kiszabással

kapcsolatos tárgyalásokon hozott kockázatértékelési döntéseket, ahol a mesterséges intelligencia technológiákat stratégiaileg értékesítik. Esettanulmányt nyújt egy konkrét értékelési eszközről, amelyet az Egyesült Államokban fejlesztettek ki a következők korlátozására

a túlzott elítélés, megmutatva, hogy a mesterséges intelligencia hogyan használható az emberi előítéletek semlegesítésére, amelyek aránytalanul nagy mértékben sújtanak egyes kisebbségi csoportokat. Más értékelő eszközöket, például a COMPAS szoftvert újságírók és kutatók is alaposan megvizsgálták, és felfedezték, hogy előrejelzéseik pontossága ellentmondásos, és a fekete vádlottakkal szembeni rendszerszerű faji előítéletekre utal. Bár ezen mesterséges intelligencia termékek tervezői és forgalmazói vitatják az ilyen megállapításokat, jelenleg nagyon kevés független bizonyíték áll rendelkezésünkre, amely lehetővé tenné, hogy megbízható értékeléseket készítsünk pontosságukról - vagy annak hiányáról. Az ilyen eszközöket működtető algoritmusok átláthatóságának hiánya és a felülvizsgálatuk nehézségei csak fokozzák az óvatosságot, amelyet az alkalmazásuk mérlegelésekor alkalmazni kell.

Az utolsó fejezet a mesterséges intelligencia eszközeinek a büntető igazságszolgáltatásban való alkalmazása által felvetett kihívások négy fő kategóriáját vizsgálja az egyéni szabadságjogokra gyakorolt lehetséges hatásuk miatt. Ezek a kihívások nemcsak etikai jellegűek, hanem a mesterséges intelligencia hatékonyságával, a beszerzésének bonyolultságával és a büntető igazságügyi szakemberek általi elsajátításának szeszélyeivel is foglalkoznak. Ez a négy kihívás szorosan összefügg egymással, és felerősítik egymást. Alaposan meg kell őket oldani, mielőtt a mesterséges intelligencia rutinszerűen beépülne a büntető igazságszolgáltatási eljárásokba. A központi kihívás, amely eddig a legnagyobb figyelmet kapta, etikai jellegű: bár a mesterséges intelligencia potenciálisan igen jelentős előnyökkel járhat, a döntéshozatal automatizálása az igazságszolgáltatásban számos erkölcsi dilemmát vet fel, amelyek olyan alapelvekhez kapcsolódnak, mint a méltányosság és a törvény előtti egyenlőség. Technikai szinten a legmodernebb gépi tanulási megközelítések alkalmazása is bizonytalan a bizonytalan területeken, ahol az általánosításokat korlátozott számú, a következő esetekben gyűjtött adatokból

kell levonni: "A gépi tanulás nem a legmegfelelőbb módszer..."

dinamikus kontextusban. Az ember még mindig előnyben maradhat a gépekkel szemben bizonyos bűnügyi kockázatok felderítésében és értékelésében. A mesterséges intelligenciával működő rendszerek bűnügyi igazságszolgáltatási szervek általi beszerzése etikai és teljesítménybeli következményeket is maga után von, ha nem megfelelően kezelik azokat. Az e piacra AI-megoldásokat fejlesztő vállalatok vonakodnak hozzáférést biztosítani algoritmusaik "titkos mártásához", de az átláthatóságnak nem lenne vitatható a büntető igazságszolgáltatásban, ahol az emberi jogok nagy tétje van. Végezetül, a bűnügyi igazságügyi szakemberek nem fogják zökkenőmentesen elfogadni a mesterséges intelligencia rendszereket: ahogy a korábbi technológiák története is mutatja, az emberi felhasználók mindig nagyfokú ügynöksége megmarad, amely különböző formákat ölthet, a szelídítéstől az ellenálláson át a szabotázsig.

1. BEVEZETÉS

Naponta érkeznek hírek a mesterséges intelligencia (AI) által kínált lenyűgöző lehetőségekről. A mesterséges intelligenciával működő rendszerek már most számos kihívást jelentő játékokban felülmúlják az emberek képességeit. 2011-ben az IBM által kifejlesztett Watson nevű rendszer legyőzte a Jeopardy című televíziós játékműsor világbajnokát.¹ 2016-ban a Google által kifejlesztett, "DeepMind" nevű mesterségesen intelligens számítógépes rendszer legyőzte Lee Sedolt, a világ egyik legjobb "Go" játékosát.² Ez a győzelem figyelemre méltó volt, tekintve, hogy a Go egy rendkívül összetett játék. Nagyban támaszkodik a játékos intuíciójára, ezért úgy gondolták, hogy a számítógépek számára rendkívül nehéz elsajátítani.³ 2017 decemberében a DeepMind újabb mérföldkövet ért el az AlphaZero rendszerével (az AlphaGo továbbfejlesztett változata), amely kevesebb mint négy óra alatt megtanította magát sakkozni, és 100 játszmas mérkőzésen legyőzte a világbajnok sakkprogramot.⁴

¹ "IBM Watson a Jeopardy világbajnok", *Forbes* (2011. február 28.), <http://www.forbes.com/sites/bernardmarr/2011/02/28/ibm-watson-the-inside-story-of-watsons-jeopardy-victory/>

² David Silver, "In Two Moves, AlphaGo Redefines Go", *MIT Technology Review* (2016. december 26.), <http://www.technologyreview.com/2016/12/26/399272/in-two-moves-alpha-go-redefined/>

³ Samuel Gibbs, "AlphaZero AI veri a championness programot tanítja magát négy óra alatt", *The Guardian* (2017. december 7.), <https://www.theguardian.com/technology/2017/dec/07/alphazero-online>: google után.

A mesterséges intelligencia egyre növekvő képességei és a korábban az emberre korlátozódó feladatokban való látszólagos jártassága jelentős kérdéseket vet fel azzal kapcsolatban, hogy ez a technológia milyen hatással lehet a bűnözésre és a büntető igazságszolgáltatásra. A mesterséges intelligencia technológia nemcsak a bűncselekmények elkövetésére, hanem a bűnüldözés és a büntető igazságszolgáltatási rendszer működésére is hatással lehet. Természetesen ezek a drasztikus változások nem korlátozódnak az igazságszolgáltatásra, mivel az emberi tevékenység minden ágazatát meg fogja zavarni a mesterséges intelligencia. Számos szakértő és elemző egyetért ezzel: Carl Benedikt Frey közgazdász és Michael A. Osborne gépi tanulási szakértő tanulmánya szerint az amerikai munkaerő 47%-át fenyegeti az automatizálás veszélye.⁵ A tanulmány szerint különösen veszélyeztetettek a szállításban és logisztikában, a szolgáltatóiparban, az irodai és kisegítő munkások, valamint a fizikai munka egyes formái. Például az egymillió 3.5kamionsofőr a

Az Egyesült Államokban valószínűleg hamarosan önvezető teherautók váltják majd fel, ha a kutatók megállapításai igazak.⁶ A Waymo, a Google kezdeményezése, már most is üzemeltet autonóm vezetésre képes tesztjárműveket a

<https://www.theverge.com/2017/10/10/16410440/autonomous-trucks>

⁵ Carl Benedikt Frey & Michael A. Osborne, "The Future of Employment: How susceptible are jobs to computerisation?" (2013) 11(4) *Journal of Economic Surveys* 157-175. doi:10.1016/j.econsurv.2013.09.004

⁶ Tom H. Davenport & D.J. Patil, "Data Science in the 21st Century", *Journal of Data Science* 10(2017), 43-62. doi:10.1080/15257580.2017.1345072

<https://www.theguardian.com/technology/2017/oct/10/autonomous-trucks>, "Truck drivers' jobs at risk as Google tests self-driving trucks", *The Guardian* (2017) 17. <https://www.theguardian.com/technology/2017/oct/10/autonomous-trucks>

autonóm vezetésre képes tesztjárműveket a

0 17), :

https://www.abcnews.com/business/autos/millions-professional-drivers-
-lesz-helyettesítjük-önvezető-járművek-

2

n817356.

Arizona útjai.⁷ A kiszámítható fizikai munka 78%-a, például a hegesztés vagy a futószalagok, állítólag automatizálható.⁸ Állítólag még a tudásalapú munkát vagy az olyan szakmai szolgáltatásokat, mint a jog és az orvostudomány, is veszélyezteti a mesterséges intelligencia. Eszközök kifejlesztés alatt állnak, amelyek képesek gyorsan átvizsgálni a több ezer dokumentumot, és kiválaszthatja a relevánsakat, vagy a helyszínen

a szerződésekben szereplő kérdéseket átlagosan 94%-os pontossággal, szemben az emberi jogászok 85%-os átlagos pontosságával.¹⁰

Elon Musk, a Tesla elektromosautó-gyártó és a SpaceX űrvállalat mögött álló vállalkozó a világra szabadított mesterséges intelligencia veszélyeire figyelmeztet, még akkor is, ha az véletlenül történik.¹¹ Ray Kurzweil ezzel szemben úgy véli, hogy a mesterséges intelligencia 2029-re felülmúlja az emberi általános intelligenciát - de ez inkább megerősíti, mint fenyegeti az emberiséget.¹² Ezek a

⁷ <http://www.theverge.com/1/7/16615290/waymo-self-driving-2017>

⁸ www.muse.com

⁸ hdi Miremadi, "Where machines can't (yet)", McKinsey (2016),

www.mckinsey.com/industries/automotive-and-assembly/our-insights/autonomous-driving-will-change

⁹ Enrt-lynet W. inick, "Lawyer-bots are shaking up jobs", MIT Technology

www.technologyreview.com/2017/02/27/401701/robot-lawyer-jobs

www.technologyreview.com/2017/02/27/401701/robot-lawyer-jobs //ügyvédi 609556robotok-az-rendország-u-Apl-jovbss /.

¹⁰ "Ügyvédek", LawGeex Blog (2018. 26február), online:

www.lawgeex.com/insights/robot-lawyer-jobs Boirleli-oanc-cDuorlaltaer-tChrauns-

¹¹ www.technologyreview.com/2017/02/27/401701/robot-lawyer-jobs, (26 M)
p az A. I. www.haniviteyfai.com/ Favis/2017

m207), :
℔ sko-nbliinlieon-dollar-

~~0116~~

12 , " weil azt állítja, hogy a szingularitás lesz

a hangok a mesterséges intelligencia fejlődése által előidézett utópisztikus és disztópikus jövőképeket egyaránt megidézik. E forgatókönyvek bármelyike természetesen óriási hatással lenne a társadalom viselkedésére és a büntetőjogi intézmények szerepére. Ezek az eshetőségek egy közös feltételezésen alapulnak. A beszámolók és cikkek mind hisznek a mesterséges intelligencia természetfeletti képességében, hogy képes lesz utánozni, sőt talán még fejleszteni is az emberi mivoltunk egy részét.

Az ipar és a tudományos élet egyaránt felfigyelt erre. Számos nagy technológiai vállalat jelentős összegeket fektet be a mesterséges intelligencia kutatásába. A McKinsey amerikai tanácsadó cég becslése szerint a magánszektor 2016-ban 20-30 milliárd USD-t fektetett be a mesterséges intelligenciába.¹³ A Google például 2014-ben felvásárolta a DeepMindot.¹⁴ Ez a vállalat felelős az AlphaGo és az AlphaZero fejlesztéséért. A legtöbb más technológiai óriás, például a Microsoft, a Facebook, az Apple és az Amazon is nagymértékben használja a mesterséges intelligenciát termékeiben.¹⁵

Az ilyen hatalmas beruházások nem korlátozódnak a Szilícium-völgyre. Kína is dollármilliárdokat önt a fejlesztésbe.

¹³ Jacques Bughin et al., "Mesterséges intelligencia: The Next Digital Revolution?", *McKinsey Quarterly*, 2017. június, <https://www.mckinsey.com/insights/ai-and-analytics/advanced-ai-2017>.

¹⁴ "Google acquires DeepMind", *Google*, 2014. február 25., <https://www.google.com/pressroom/articles/20140225-google-acquires-deepmind/>.

¹⁵ "The world's most innovative companies are investing heavily in AI", *McKinsey Quarterly*, 2017. június, <https://www.mckinsey.com/insights/ai-and-analytics/advanced-ai-2017>.

¹⁶ "The world's most innovative companies are investing heavily in AI", *McKinsey Quarterly*, 2017. június, <https://www.mckinsey.com/insights/ai-and-analytics/advanced-ai-2017>.

és a mesterséges intelligencia termékek méretarányos bevezetése.¹⁶ A mesterséges intelligencia körüli startup-világ ugyanilyen virágzó. Decemberben az AngelList2017., a startupokat és a befektetőket összekötő platform közel 4000 startupot sorolt fel a mesterséges intelligencia területén.¹⁷ A Pitchbook pénzügyi kutatócég szerint a kockázati tőkebefektetők 2017-ben több mint 10 milliárd USD-t fektettek be AI-startupokba, ami 2016-hoz képest csaknem kétszeres növekedés.¹⁸ Az Element AI, egy kanadai vállalat, amely a cégek mesterséges intelligencia bevezetésének segítésére összpontosít, egymillió 102USD-t gyűjtött be.¹⁹ Az érdeklődés nem kevésbé intenzív az akadémiai szférában sem. 2017-ben közel 20 000 tanulmányt publikáltak a mesterséges intelligencia témájában.²⁰

A mesterséges intelligencia körüli irracionális túlzással szemben azonban egyre több kritikus is megszólal. Egy népszerű blogbejegyzésében Filip Piekiewicz, az AI szakértője az "AI-tél" eljövételét jósolja, amely a mesterséges intelligencia kutatásának jelentős lehülését jelenti.²¹

¹⁶ [Name], d, Nae/SuYpoerkpU:Chinga, év
 Redeer, (, : G/Mu/M-harcanodrth, 2018).

¹⁷ SadykAnggaalyrtwicasl, "ThJeaCnuarrreynt HypoCite in Artificial
 Intelligence", (2018) :

¹⁸ P/O/sksreynalytics .Yae/atr ypTeh-ecytcolpe-iVnC-
 ;2 017 ei-ncuRrerevnieth-
 arrtoifuicnidals-i& nteinllvigeesntocers.
 hP/"/, (2017),
 :/ /pPittichhbBooookk.00000/Aanrtaiclylesiss/2017-Dyeeacre-minb-review-t h eo-
 :

¹⁹ [Name] Ent AI, egy platform a vállalatok számára AI
 t/i/osnosc, tiesecshc\$runMhD", (The/Cur/20174/hammha
 shatpu iarla. c
 2017, :
 th, tformmlin-feo r-
 (p/2017/01/04/)

²⁰ [Name], [Name] njolsso & Jack Clark,

"Narotvifeimcibaler IntelligencieneIndex: 2017 Éves jelentés", AI Index
(2017. május 17):

21 [P/ækn. . oAg/winter2017 . B.](#)
" [ipowte way](#)", Pieknewskis' Blog
(2018. május 28.),

online:

5

Gary Marcus tudós 10 kihívást sorol fel a mélytanulással kapcsolatban egy tanulmányban, amelyet a jelentés utolsó fejezetében részletesebben is megvizsgálunk. Szerinte a mélytanulás (a mesterséges intelligencia egyik részterülete) messze meghaladja az emberi képességeket bizonyos feladatokban, például a bemeneti adatok osztályozásában. Más feladatok, például a nyelv megértése azonban a jelenlegi módszerek hatókörén kívül esik. Továbbá rámutat arra a problémára, hogy a mélytanulási algoritmus nem képes jól reagálni az algoritmus betanításához használt adatokon kívüli ingerekre.²²

Számos tanulmány kimutatta, hogy a modern mesterséges intelligencia olyan hibákat képes elkövetni, amelyek az ember számára teljesen értelmetlennek tűnhetnek. Ha egy bizonyos zajmintázatot adunk egy képhez, amely semmilyen módon nem változtatja meg a kép emberi szemmel való megjelenését, akkor az AI egy kutyát struccnak²³, vagy egy stop táblát kaput jelző táblának minősíthet.²⁴ Gyakran előfordul, hogy a mesterséges intelligenciának mutatott képek apró változtatásai - például egy elefánt hozzáadása egy képhez -²⁵ más tárgyak felismerését teljesen váratlan módon megghiúsítják. Melanie Mitchell informatikus szerint ez a "jelentés gátjának" köszönhető. Az emberek általános, józan tudással rendelkeznek a megértéshez.

²² Gary Marcus, "Ten Challenges for Deep Learning in Natural Language Processing," *Journal of Cognitive Neuroscience*, 2018, 30(12), pp. 1974-1992. <https://arxiv.org/abs/1808.08010>, online: <https://arxiv.org/abs/1808.08010>.

²³ Christian Szepesvári, "The Problem of Learning to Recognize Objects from Noisy Data," *Journal of Machine Learning Research*, 2013, 14, pp. 1-12. <https://arxiv.org/abs/1312.0991>, etownlinkse

²⁴ "The Problem of Learning to Recognize Objects from Noisy Data," *Journal of Machine Learning Research*, 2013, 14, pp. 1-12. <https://arxiv.org/abs/1312.0991>, etownlinkse

²⁵ "The Problem of Learning to Recognize Objects from Noisy Data," *Journal of Machine Learning Research*, 2013, 14, pp. 1-12. <https://arxiv.org/abs/1312.0991>, etownlinkse

világot, ami lehetővé teszi számunkra az általánosítást és az új helyzetek felismerését. A mesterséges intelligenciából hiányzik ez a józan ész. Szerinte ez azt jelenti, hogy a jelenlegi megközelítéssel nem biztos, hogy olyan mesterséges intelligenciát kapunk, amely megbízhatóan tud dönteni, és előbb egy lépést hátra kell lépnünk, mielőtt rábízunk magunkat.²⁶

E két gyökeresen eltérő nézőpontot látva nehéz lehet meghatározni, hogy mi is az a mesterséges intelligencia, és milyen hatással lesz a világra. Olyan forradalomról van szó, amely egész munkaköröket tesz feleslegessé, tömeges munkanélküliséget okoz, és végül kognitív képességekben felülmúlja az embert? Vagy, ahogyan azt a kritikusok egy része állítja, csupán egy statisztikai rendszer, amely néhány szűk feladatban képes utánozni az embert, de kudarcot vall, amikor a világ komplexitásával szembesül?

Ebben a jelentésben megvizsgálunk néhány választ ezekre a kérdésekre, különös hangsúlyt fektetve a büntetőjogi alkalmazásokra. Az ember alkotta technológiai eszközök használata a (megtorló, büntető vagy helyreállító) büntető igazságszolgáltatásról alkotott elképzeléseink megvalósítására az emberiség létezése óta létezik: gondoljunk csak a történelem során a helytelen magatartás kivizsgálására és a büntetés kiszabására használt technológiákra. Amint azt ez a jelentés bemutatja, a mesterséges intelligencia új korszakot nyitott a büntető igazságszolgáltatásban világszerte, amelyet a nagy adathalmazokon alapuló automatizált empirikus elemzés jellemez, és amely arra használható, hogy az embereket ösztönözze, vagy akár teljesen helyettünk hozzon döntéseket.

Ebben a feltáró jelentésben áttekintést nyújtunk a következők szerepéről

26 online: <http://arxiv.org/abs/1808.03305>. . os, " TheEle CaVnt
 26 "TheRoom" (2018) gJPohapnerK, alXis18 08.033 05[ph]

A mesterséges intelligencia a büntető igazságszolgáltatásban számos, a világ minden tájáról származó példára támaszkodva. Időrendi megközelítést alkalmazunk, amely nyomon követi, hogyan bontakozik ki egy bűncselekmény, beleértve (i) a bűncselekmény elkövetését, (ii) a felderítését, és végül (iii) a büntetőbíróságok és a büntetés-végrehajtási szolgálatok reakcióját. Először is arra a lehetőségre összpontosítunk, hogy a rosszindulatú szereplők elítélendő cselekmények elkövetésére használhatják a mesterséges intelligenciát, bár erre még nem volt példa. Másodszor, értékeljük a mesterséges intelligencia bűnüldözés általi alkalmazását, beleértve a rendőrség új képességét a bűncselekmények felderítésére és előrejelzésére. Harmadszor, megvizsgáljuk a mesterséges intelligencia és a büntetőeljárás közötti kapcsolatot, hogy bemutassuk, hogyan alkalmazzák a mesterséges intelligenciát az elkövetőkkel kapcsolatos különböző kockázatok értékelésére a tárgyalás előtti és utáni szakaszban. Végül a büntető igazságszolgáltatással összefüggésben a mesterséges intelligencia által támasztott kihívások négy átfogó kategóriájának elemzésével zárjuk: etika, hatékonyság, beszerzés és kisajátítás. Óvatosságra intünk minden olyan szervezetet, amely a mesterséges intelligenciát a büntető igazságszolgáltatási rendszerében kívánja alkalmazni: ezeket az egymással összefüggő kérdéskategóriákat kifejezetten és alaposan meg kell vizsgálni annak érdekében, hogy a mesterséges intelligencia rendszerek iteratív módon, tisztességesen és átlátható módon részt vehessenek a büntető igazságszolgáltatási döntésekben.

2. A MESTERSÉGES INTELLIGENCIA MEGHATÁROZÁSA:

MI AZ A MESTERSÉGES INTELLIGENCIA, ÉS

MIÉRT FONTOS A BÜNTETŐ

IGAZSÁGSZOLGÁLTATÁS SZÁMÁRA?

Ahhoz, hogy megértsük, hogyan használható a mesterséges intelligencia a büntető igazságszolgáltatásban, elengedhetetlen annak megértése, hogy pontosan mi is a mesterséges intelligencia. Először is elmagyarázzuk a mesterséges intelligenciával kapcsolatos főbb fogalmakat, és azt, hogy miben különbözik a számítógépes programozás más formáitól. Ezután elmélyedünk abban, hogy mi nem mesterséges intelligencia. Ezután áttekintést adunk arról, hogy a mesterséges intelligencia milyen különböző módon okozott és fog várhatóan okoz majd zavart azokban az ágazatokban, amelyekbe belép. Végül pedig ismertetjük, hogy a mesterséges intelligencia milyen különböző módon használható a büntető igazságszolgáltatás világában. Ez a fejezet hasznos bevezetésként szolgál ahhoz, hogy megértsük a mesterséges intelligencia képességeit, és hogy melyek azok, amelyek átültethetők a büntető igazságszolgáltatásba.

2.1. Mi az AI?

2.1.1. Mesterséges intelligencia

Az American Association for the Advancement of Artificial Intelligence a mesterséges intelligenciát úgy írja le, mint "a gondolkodás és az intelligens viselkedés alapjául szolgáló mechanizmusok tudományos megértését és ezek gépekben való megtestesülését".²⁷ Ez nagyon tág hálót vet ki, mivel

bármilyen intelligensnek tűnő viselkedést magában foglal, amelyet egy gép képes végrehajtani. Egy egyszerű csevegőfelület, amely

²⁷ ~~Reza Aslan, "Ita' Gogal Us!' a bOnha n Mye Adhyt~~
Reza Aslan, "Ita' Gogal Us!' a bOnha n Mye Adhyt"
50 a

címen.

3.

kérdéseket tesz fel Önnek, de csak igennel vagy nemmel válaszol, például az intelligencia jeleit mutatja. Egy másik példa egy elektromos szárítógép, amely leáll, amikor érzékeli, hogy a ruhák megszáradtak.²⁸

A mesterséges intelligenciát általában két kategóriára osztják: Általános mesterséges intelligencia és szűk mesterséges intelligencia. Az általános mesterséges intelligencia (vagy erős mesterséges intelligencia) olyan számítógépes rendszer, amely minden területen emberi vagy magasabb intelligenciát mutat. Képes lenne az egyik területről származó tudást átvenni és átültetni egy másik területre.²⁹ Számos tesztet javasoltak annak megállapítására, hogy egy mesterséges intelligenciával rendelkező rendszer erős mesterséges intelligenciát mutat-e. A leghíresebb talán a Turing-teszt, amely során a bírácoknak azt kell eldönteniük, hogy egy számítógéphez vagy egy emberhez beszélnek-e egy csevegőfelületen keresztül.³⁰ Egy másik javasolt teszt a Wozniak Coffee teszt - képes-e egy gép bemenni egy ismeretlen házba és elkészíteni egy csésze kávé?³¹ Az általános mesterséges intelligencia óriási hatással lehet az emberiségre, és potenciálisan kiválthat minden emberi munkát. Ez azonban valószínűleg még nagyon messze van. A szakértők nem értenek egyet abban, hogy ez még a mi életünkben bekövetkezik-e, és hogy a mesterséges intelligencia jelenlegi útja el fog-e juttatni minket oda.³²

²⁸ Ibid.

²⁹ L. Teoh, "The Turing Test: A Review of the Test and Its Implications for Artificial Intelligence", *Journal of Artificial Intelligence Research*, 2013, pp. 1-11. https://www.researchgate.net/publication/261508483_The_Turing_Test_A_Review_of_the_Test_and_Its_Implications_for_Artificial_Intelligence

³⁰ B. Horvath, "The Turing Test: A Review of the Test and Its Implications for Artificial Intelligence", *Journal of Artificial Intelligence Research*, 2013, pp. 1-11.

³¹ Ibid. 141.

³² "From Narrow to General AI", *Intuition Machine 3* (October 2017), pp. 1-11.

Íps : János Várkonyi 25
6 15510 , Budapest, Magyarorszag

10

Bár az AlphaGo elképesztően jól játszik Go-t, mégsem tudja átültetni ezt a felsőbbrendű tudást egy másik területre (vagy akár egy csésze kávé készíteni).³³

A mesterséges intelligencia terén eddig elért minden emberi eredmény a szűk értelemben vett mesterséges intelligencia kategóriájába tartozik. Ez olyan mesterséges intelligencia, amely egy előre meghatározott probléma megoldásával foglalkozik, például egy társasjátékkal, képek azonosításával vagy autózéssel. ³⁴ A szűk értelemben vett mesterséges intelligencia önmagában is nagyon hasznos, és nagy hatással lehet a társadalomra azáltal, hogy hatékonyabbá teszi a munkásokat és automatizálja a feladatokat. Nem foglalkozik azonban teljesen tudatos, emberi szintű intelligenciával.

2.2. A szűk mesterséges intelligencia megközelítésének története

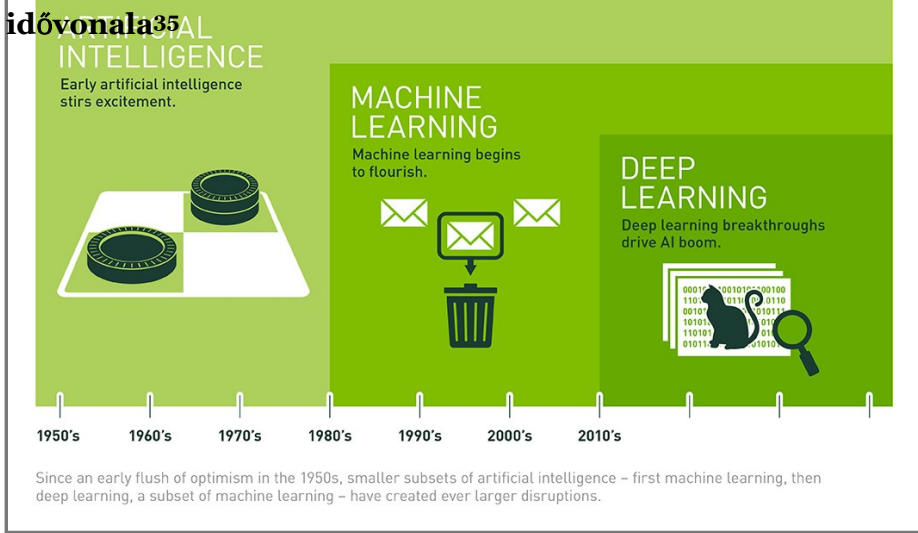
Ez a szakasz azt fejt ki, hogy milyen módszereket alkalmaztak az intelligens rendszerek létrehozása érdekében. Ezeket korszakokra³, illetve megközelítésekre oszthatjuk: Szabályalapú módszerek, gépi tanulás és mélytanulás.

Nem minden AI-alkalmazás fog megvalósulni", The Verge (27
2018), elérhető: [https://www.theverge.com/2018/11/27/14362143/ai-muvi-altalános-
l/i/gwenwcwe](https://www.theverge.com/2018/11/27/14362143/ai-muvi-altalános-
l/i/gwenwcwe).

³³ Atkinson, Supra note at 277.

³⁴ Ibid.

Ábra -1 A mesterséges intelligencia megközelítések



2.2.1. Szabályalapú rendszerek

A szakértői rendszerek létrehozásához a programozó pontosan kódolja a számítógépbe a megoldandó problémára vonatkozó ismereteket. Ennek eredményeképpen egy szakértői rendszer jön létre, amely egy korlátozott területen automatikusan képes szakértői segítséget nyújtani.³⁵ Bár a szakértői rendszerek számos területen lenyűgöző eredményekhez vezethetnek, számos nehézséggel küzdenek. Először is, ahogy a nevük is jelzi, a szakértő szakterületének ismereteitől függ, hogy a tudásukat megszerezzék. Például egy sakkmotort építő programozó a saját sakkozási ismereteit kódolná a számítógépbe. Ez azonban soha nem tudná meghaladni a sakkozás szintjét.

³⁵ Dreyfus, Hubert A. "What Computers Can't Do." In *Artificial Intelligence and the Future of Thinking*, edited by Marvin Minsky, 1965. MIT Press. (2000)

high
) , lared

difference-ar-ar-művi-
/i/gbelnocges- hrechalringde/pá/wingaid .

36 BuAcIMBuacghaazninaen, "A (V ery) rövid története a mesterséges
ø intelligencia" (2005).

12

a rendszert megvalósító személy tudása, mivel az csupán a létrehozó tudását valósítja meg.

Továbbá a mindennapi életben használt tudás nagy része implicit, és így nagyon nehéz explicit módon átültetni a kódba. Például egy embernek nagyon nehéz lenne formalizálni az összes tudást és izommozgást, amely a biciklizéshez szükséges, vagy az összes gondolatot, amely annak eldöntéséhez szükséges, hogy egy állat macska vagy kutya. Ha megpróbáljuk formalizálni ezeket az ösztönöket, az valószínűleg sok időt vesz igénybe, és nem valószínű, hogy megragadjuk az agy által végzett feladat teljes komplexitását.

A tudás algoritmusba való teljes kódolásának nehézsége miatt a szakértői rendszereknek az új információkra való általánosítás is problémát jelent. Amíg egy kérdés pontosan abba az osztályba esik, amelyet a szakértői rendszer létrehozója tervezett, addig az eredmény jó lesz. Amint azonban a bemenet kívül esik a megadott paramétereken, a rendszer képtelen lesz eredményt meghatározni. Egy egyszerű példa szemlélteti ezt a pontot. Egy egyszerű szakértői rendszer megkérdezhetné, hogy egy állatnak van-e bajusza, hogy megállapítsa, macska vagy kutya. Ha van bajusza, akkor macska, ha nincs, akkor kutya. Ez a rendszer sok esetben működik, de azonnal kudarcot vall, ha a macska elvesztette a bajuszát. Még ebben az egyszerű helyzetben sem tud jól általánosítani.

2.2.2. Gépi tanulás

A gépi tanulás (ML) másképp működik. Ahelyett, hogy a programozó megpróbálná a rendszerbe kódolni a tudását, a programozó megmutat az algoritmusnak néhány példát és egy címkét az adatokhoz. A gép ezután maga fogja kitalálni, hogy mi a közös ezekben a példákban. Minél több példát mutatnak neki, annál jobb a

algoritmus lesz - így képes vagy fejleszteni önmagát. Ezért az ML népszerű definíciója a következő:

"Az a terület, [amely] azzal a kérdéssel foglalkozik, hogyan lehet olyan számítógépes programokat készíteni, amelyek a tapasztalattal automatikusan javulnak."³⁷

A macska- vagy kutyapélda esetében ez a következőképpen működik. A programozó kiválasztana egy nagyszámú kutyás képet és egy nagyszámú macskás képet. Ezeket megmutatná a számítógépnek, és megmondaná neki, hogy melyik állatot ábrázolja egy-egy kép. Az összes adatot megvizsgálva és a mintákat azonosítva a számítógép felépítene egy modellt arról, hogy mitől lesz egy állat kutya vagy macska. Ezt követően a számítógép elé kerül egy olyan kép, amelyet korábban még nem látott, és a modell segítségével képes megjósolni a fajt.

Amint azt később részletesebben is ismertetjük, a hagyományos ML-algoritmusok jellemzően emberi beavatkozást igényelnek annak eldöntéséhez, hogy a valós világ mely jellemzőit vizsgálják meg.³⁸ Ez rengeteg időt és területi szakértelmet igényel, és nagyon megnehezíti a hagyományos ML használatát strukturálatlan adatok, például beszéd és képek elemzésére.³⁹ Több száz különböző algoritmus létezik a gépi tanulás végrehajtására. Az alábbiakban néhány különbséget ismertetünk. Példák az algoritmusokra a lineáris regresszió, a véletlen erdők és a támogató vektoros gépek. Az algoritmusok egy csoportja azonban, az ún.

³⁷ Tom Mitchell, *Machine Learning*, (New York: McGraw-Hill, 1997).

³⁸ Yann LeCun, Yoshua Bengio, Geoffrey Hinton, "Mélytanulás" (2015) 5 2:7553 & 436.

³⁹ Ibid.

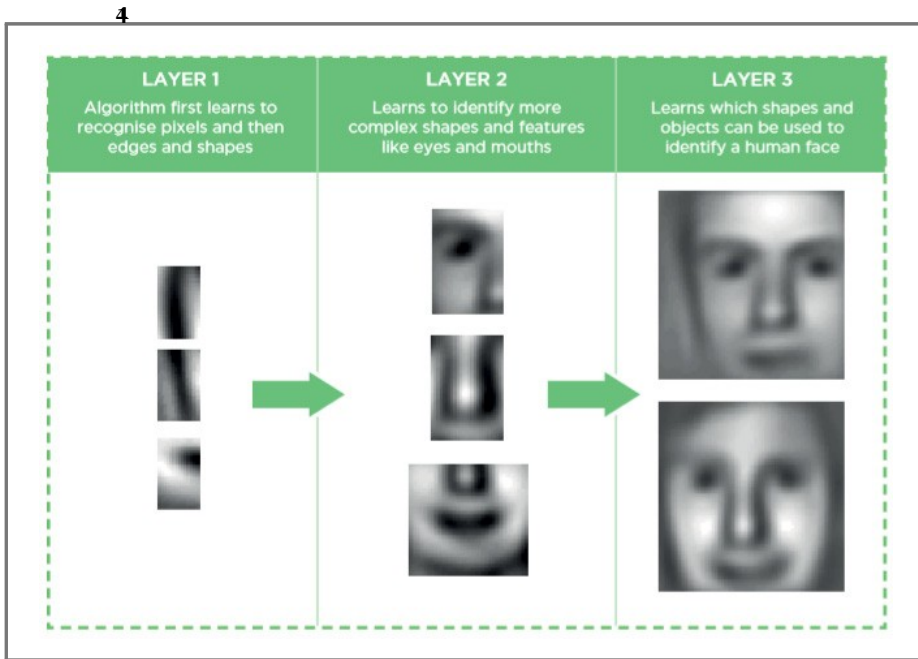
A mesterséges neurális hálózatok nemrégiben kerültek reflektorfénybe, mint az eddigi talán legerősebbek.

2.2.3. Mélytanulás

A mélytanulás (Deep Learning, DL) tehát a gépi tanulási algoritmusok egy részhalma. Jellemzően azokat a mesterséges hálózatokat nevezik Deep Learning rendszereknek, amelyek kettőnél több "rejtett réteggel" rendelkeznek. A különbség a hagyományos ML és a DL között az, hogy az utóbbi hierarchikus rétegekbe van strukturálva. Ahelyett, hogy a mérnök manuálisan vonja ki a jellemzőket az adatokból, az adatokat közvetlenül a Deep Learning algoritmusba táplálhatja, amely automatikusan megtalálja a releváns jellemzőket. Minden réteg az absztrakció egy magasabb szintjére lép. ⁴⁰ Macskák és kutyák esetében például az első réteg felismerhetné az alapvető vizuális mintákat, a második a bajuszokra, a farokra és a mancsokra összpontosíthatna, míg a harmadik a kutyák és a macskák magasabb szintű jellemzőit észlelné. Ma a kutatók több tíz ilyen rétegből álló modelleket építenek. Ez azt jelenti, hogy a hagyományos ML-hez képest sokkal kifinomultabb modelleket képesek megtanulni a valóságról.

⁴⁰ Ibid.

Ábra - 2.1 Reprezentációk Deep Neuralban



A mélytanulás az elmúlt években drámai javulást eredményezett a mesterséges intelligencia számos területén, például a képosztályozás, a beszéd felismerés és a természetes nyelv megértése terén.⁴²

A mélytanulás által elért nagy ugrások három fő oka a következő:

- Nagy adatgyűjtemények: a mélytanulási rendszerek betanításához hatalmas mennyiségű adatra van szükség, ami a

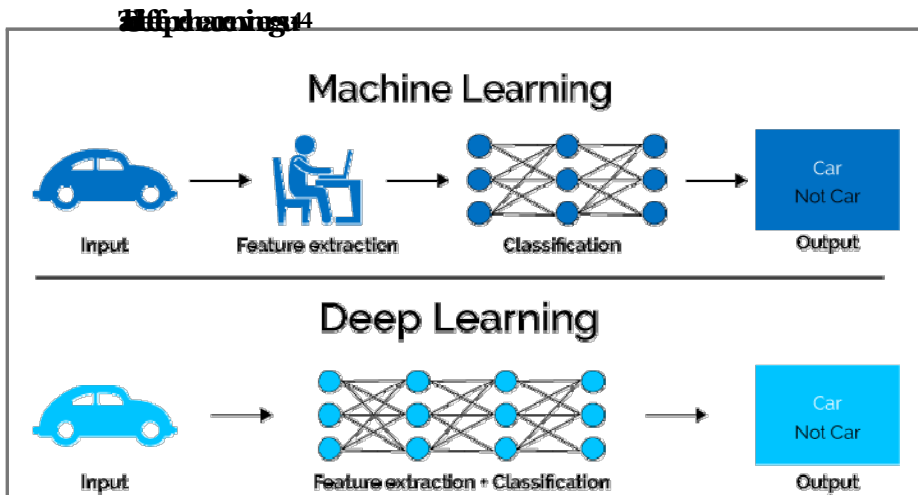
⁴¹ <https://arxiv.org/abs/1603.01511> "DeepFace: Closing the Gap to Human-Level Performance on Face Verification" by Jiankang Deng, Jiaxi Tan, Manjunath Matthew Beal, and Simon S. Liao, arXiv preprint arXiv:1603.01511, 2016.

⁴² LeCun, Bengio & Hinton, Supra note at 381.

a tárolókapacitás technikai fejlődésével és a több milliárd adatpontot tartalmazó adatbázisok létrehozásával megvalósítható;

- Nagyobb teljesítményű technológia: egy mély neurális háló képzése hatalmas mennyiségű számítást igényel. Egyes modellek betanítása napokig vagy akár hetekig is eltarthat. Kiderült azonban, hogy ez a számítás nagyon hatékonyan elvégezhető a számítógépes grafikus kártyákon. Ezáltal hihetetlenül összetett modellek is ésszerű idő alatt betaníthatóvá váltak;
- Jobb algoritmusok: a mélytanulási algoritmusok fejlődése az elmúlt években elképesztő volt. Olyan kutatók, mint Yoshua Bengio, Yann LeCun és Geoffrey Hinton olyan módszereket fejlesztettek ki és finomítottak, amelyek lehetővé tették a mélytanulás forradalmát.⁴³

Ábra - 3 s hagyományos gépi tanulás



⁴³ See Bengio, LeCun, and Hinton, "Deep Learning", in Bengio and LeCun (eds.), *Deep Learning* (Cambridge, MA: MIT Press, 2015), 141.

⁴⁴ Mahapatra, *Supra* note 41.

2.3. A gépi tanulás módszerei

Az ML megvalósításának két fő módja van: a felügyelt és a felügyelet nélküli tanulás.

2.3.1. Felügyelt tanulás

A felügyelt tanulás a gépi tanulás egy olyan formája, ahol a képzés során a gép a helyes választ kapja meg. Például egy képet egy címkével együtt adhatunk meg, amely megadja, hogy a kép egy kutyát vagy egy macskát ábrázol. Vagy egy ingatlanos alkalmazás esetében egy ház számos tulajdonságát lehet megadni, a ház árával együtt. Az algoritmus végül megpróbálná megjósolni ezt a címkét a rendelkezésre álló tulajdonságokkal.

Minden gépi tanulási algoritmus hasonló folyamatot követ:

- Adatok: A programozónak egy adatkészletet kell az algoritmus rendelkezésére bocsátania. Ez lehet például egy egymillió lakáshirdetést és azok árát tartalmazó halmaz. Ebben a példában az ár lenne az a célérték, amelyet az algoritmus megpróbál megjósolni. Minél több az adat, annál jobb lehet az algoritmus. Valójában a több adat felhasználása egy "hülye" algoritmussal általában legyőzi a kevesebb adatot használó jobb algoritmust.⁴⁵ A nagy cégek nagy előnye a gépi tanulásban a birtokukban lévő adatmennyiség. A Google például hatalmas adathalmazokkal rendelkezik, és ezeket használja fel a modelljeik képzéséhez.⁴⁶ A

⁴⁵ Pedro Domingos, "Néhány hasznos dolog, amit érdemes tudni a gépről learning" (2012) 55:10 Communications of the ACM, 786-7. o.

⁴⁶ Tom Simonite, "AI and 'Enormous Data' Could Make Tech Giants Like Google Harder to Topple", Wired (2017. július 13.), <https://www.wired.com/story/ai-and-enormous-data-could-make-tech-online>:

A Google például adatokat generál a különböző szolgáltatásaiba való bejelentkezési folyamatból. Annak ellenőrzésére, hogy nem botok-e, a felhasználókat arra kérik, hogy kattintsanak bizonyos elemeket tartalmazó képekre, például autókra vagy jelzőtáblákra. Ezek az ember által generált értelmezési adatok aztán felhasználhatók a mesterséges intelligencia rendszerek képzéséhez.⁴⁷ Ezen túlmenően a nagy technológiai vállalatok több ezer dolgozót alkalmaznak, akik kézzel nézik át és címkézik fel a képeket az önvezető autók számára;⁴⁸

- Jellemzők: a számítógép ebben a szakaszban nem tudja, hogyan kezelje ezeket az adatokat. Az adatokat egy sor jellemzővé, vagy az adatok numerikus ábrázolásává kell alakítani. Ezt hívják feature engineeringnek. Ez egy összetett feladat, amely sok időt és tudást igényel ezen a területen.⁴⁹ Az előző példánkban, egy ház árának előrejelzésénél a releváns jellemzők lehetnek a hálószobák száma, a ház teljes területe, a ház elhelyezkedése és az ablakok száma. A színnek viszont nagyon kevés hatása lehet az árra, és ezért rossz jellemző lehet. A mélytanulás egyik nagy előnye, hogy nem kell ilyen jellegű feature engineeringet végezni. A hálózat ehelyett maga tanulja meg az adatok szerkezetét több absztrakciós rétegben, ahogyan azt korábban már leírtuk. Ez azt jelenti, hogy ez a drága és időigényes folyamat gyakran kihagyható;

47 "Google's Anti-Robot reCAPTCHA Trains Their AI on Images of Street View Cars", <https://www.technologyinsider.com/google-research/2015/07/20/google-research-ai-robot-detection/>.

48 "Why Big Tech Companies Hire Humans to Label Images", <https://www.technologyinsider.com/google-research/2015/07/20/google-research-ai-robot-detection/>.

49 "Why Big Tech Companies Hire Humans to Label Images", <https://www.technologyinsider.com/google-research/2015/07/20/google-research-ai-robot-detection/>.

- **Algoritmus:** a jellemzőket ezután egy algoritmusba tápláljuk. Ennek az algoritmusnak különböző céljai lehetnek: Főleg regresszió vagy osztályozás. Regresszió esetén az algoritmus befogadja az adatokat, és megpróbál kitalálni egy számértéket. Példánkban megpróbálhatja megjósolni egy ház értékét számos jellemző alapján. Minél közelebb jut az algoritmus a ház tényleges árához, annál jobb. Az osztályozás megpróbálja a példát egy osztályba sorolni. Ez lehet például annak eldöntése, hogy egy képen macska vagy kutya látható. Itt a siker mércéje az, hogy az algoritmus hány képet osztályoz helyesen;
- **Kiértékelés:** az algoritmus kiértékelésére is kell lennie módnak. Ezt általában a számítógép belsőleg használja annak megállapítására, hogy az éppen futó algoritmus hogyan teljesít;
- **Tréning:** miután a számítógép megtanulja, hogyan teljesít jelenleg, finoman módosítja az algoritmust, hogy a következő próbálkozásnál jobban teljesítsen. Ezt a folyamatot nevezzük betanításnak. A betanítás után a mérnök gyakran visszatér, hogy megváltoztassa a használt jellemzőket vagy algoritmust, hogy tovább javítsa a modell teljesítményét.

2.3.2. Nem felügyelt tanulás

A felügyelet nélküli tanulás a gépi tanulás egy olyan osztálya, ahol nincsenek címkék. Ehelyett a számítógép maga próbálja kitalálni, hogy mi különbözteti meg az egyik adatot a másiktól. A macskákkal és kutyákkal kapcsolatos példánkban ez azt jelentené, hogy a mérnök macskák és kutyák képeit adja meg az algoritmusnak, és maga a számítógép rájön, hogy két különböző állat van az adathalmazban, és hogy mi különbözteti meg őket. Felügyelet nélküli

tanulás nem teljesít olyan jól, mint a felügyelt tanulás. Ez azonban aktív kutatási terület, és számos előnye van a felügyelt tanulással szemben. Nagy előnye, hogy az adatokat nem kell címkézni, így hatalmas mennyiségű strukturálatlan adat válik hozzáférhetővé az elemzés számára. Ezért sokan a felügyelet nélküli tanulást tekintik a jövő megközelítésének.

A felügyelet nélküli tanulás egyik fontos felhasználási területe az anomáliák észlelése. Itt egy hálózatot képeznek ki, hogy megtanulja egy adatfolyam szerkezetét és általános megjelenését. Ezután képes megmondani, ha egy adatpont eltér a többitől. Ez felhasználható például a gyártósorok problémáinak vagy a nagyszámú pénzügyi tranzakcióban elkövetett esetleges kibercsalási kísérleteknek a felismerésére.

2.3.3. Erősítéses tanulás

Van néhány más típusú ML, amely kezd felszínre kerülni. Az egyik a megerősítéses tanulás, amely egy ágenszt egy környezetbe enged, és megpróbál rávenni egy bizonyos cél elérésére, például egy autó vezetésére vagy egy játékra. Az algoritmus először véletlenszerűen indul. Ha azonban véletlenül elér egy győztes állapotot, akkor ez a viselkedés megerősödik. Ez mindaddig így megy, amíg az algoritmus megbízhatóan meg nem tanulja, hogyan érje el a kitűzött célt. A megerősítéses tanulás a társasjátékoktól kezdve a számítógépes játékokig mindenféle játék megtanulásában szerepet játszott.

2.3.4. Generáció

Viszonylag új keletű mesterséges intelligencia technika a generatív adverszális hálózatokhoz kapcsolódó technika. Ez egy olyan technika, amely a mesterséges intelligenciát nem csak az adatok osztályozására, hanem azok generálására is használja. Technikailag ez azt jelenti, hogy egy hálózat megpróbálja becsapni a

egy másikat, hogy elhiggye, hogy a képei valódiak, és nem hamisak. A két hálózat együtt fejlődik, amíg mindkettő nagyon jól végzi a dolgát. Ezen a ponton a generátor már képes olyan adatokat kiadni, amelyek szinte valódinak tűnnek. Vannak más architektúrák is, amelyek jól teljesítenek az adatok generálásában, például a rekurzív neurális hálózatok. A generatív adverzális hálózatokat és más típusokat már használták arcképek⁵⁰ létrehozására, zene komponálására és rendkívül valósághű hangzású beszéd előállítására. Vannak módszerek arra is, hogy egy generált (hamis) tartalmat átvigyünk egy másikba, amely a valóságot hűen tükrözi. Ezzel például bármilyen képet át lehet alakítani egy híres művész stílusává,⁵¹ vagy olyan hírességeket ábrázoló valósághű videókat lehet generálni, akik olyan dolgokat tesznek vagy mondanak, amelyeket soha nem mondtak vagy tettek.⁵²

⁵⁰ Sratasbieltitya I, " r og kofrokrinlgmpPraopveerd
 , a r r y a s i e G (2 0 1 8)
 :l 0. 10 19 6. NE], onlinea:
 ahrttXpiv: //arxi v. o g / a b s / 1 0 . 1 1 5
 26.

⁵¹ , k e & atathrXiaiv R M "
 LAelgoonriAthmGatyosf A n t e S t y l e c " (2 0 1 5 M) i n g a
 v: 0 5 7 6 , q b i o] , o n h D e :
 ahrttXpi: /arxi . o g / a b s / 1 5 0 6 5 7 6 ; " e e p D r e a m
 NPeauprearl,

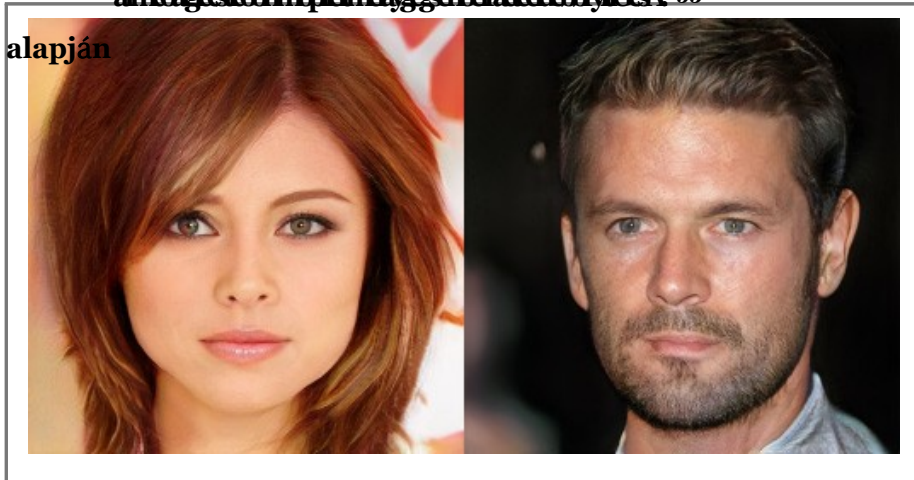
Generator", Deep ://dGeenpedtraetomr g e v l e h n :
 P e l e t u g e t o m A p r e h a c k i n
⁵² b o v h , (1 7 2 8) :
 : . i m a g e l a c n o m p e / t e d l e r - / b u z z / e e / d 2 0 1 8 4 7 / 1 / a i - f a k e - n e w s -
 heott-pbsa r / d v o w b
 vid7247334

ábra - 4

N, a következők

almodjstomplmággsmefatcdhryiCsA 53

alapján



2.4. A mesterséges intelligencia kockázatai

Bár a mesterséges intelligenciának számos előnye van, a mesterséges intelligencia használata számos lehetséges buktatót is rejt magában. Fontos, hogy ezekkel foglalkozunk, mielőtt a mesterséges intelligenciát a kormányok és a vállalatok nevében érzékeny döntések meghozatalára alkalmazzák.

2.4.1. Általános AI

Mint már említettük, az általános mesterséges intelligencia valószínűleg még messze van. Azonban a sci-fi szerzők és a tudományos kutatók egyaránt elmélkedtek már arról, hogy egy ilyen rendszer milyen hatással lehet a társadalomra. A nagy kérdés az, hogy nem lehetünk biztosak abban, hogy egy ilyen mesterséges intelligencia osztozni fog abban az etikában és az emberi jogok tiszteletben tartásában, amelyre a polgárok a demokratikus társadalomban törekszenek.

⁵³ Karras et al., Supra note 50.

társadalmak. Ha például kapnának egy feladatot, akkor ezt a feladatot céltudatosan végeznék, és semmilyen más szempont nem állna az útjukba. Nick Bostrom egy olyan mesterséges intelligencia példáját hozza fel, amelynek feladata az iratkapcsok létrehozása, és amely végül az egész világegyetemet felemészti, hogy még több iratkapcsot termeljen.⁵⁴ Számos kutató dolgozik ezen a területen annak meghatározásán, hogy miként biztosíthatjuk, hogy az AI jóindulatú maradjon, vagy egy olyan dobozba szoruljon, ahol nem árthat.⁵⁵

2.4.2. Szűk AI

Még a fejlett, szűk körű mesterséges intelligencia fejlődése is számos kockázatot rejt magában, amelyek közül néhányat az alábbiakban általánosságban ismertetünk, mielőtt e jelentés következő fejezeteiben megvizsgálánk, hogy ezek hogyan vonatkoznak a büntető igazságszolgáltatási intézményekre. E kockázatok többsége abból a tényből ered, hogy a mesterséges intelligencia nagyon hatékony eszköz lehet bizonyos célok eléréséhez. Előfordulhat azonban, hogy ezek a célok nem egyeznek meg az érintett személyek céljaival és érdekeivel, vagy azért, mert rosszul fogalmazták meg őket, vagy azért, mert a mesterséges intelligencia tervezőinek teljesen más érdekeik vannak, és nem vagy csak kevés jogi vagy piaci korlátozást tapasztalnak.

2.4.2.1. Adatvédelem

A magánéletet úgy lehet meghatározni, mint a jogot arra, hogy eldönthessük, mikor és kinek adunk ki személyes adatokat. A modern mesterséges intelligenciaeszközök és a személyes adatok tömeges gyűjtése komolyan veszélyeztetik ezt a jogot. Amint azt Kosinski et al. 2013,

⁵⁴ Nick Bostrom "Less than Perfect: A Guide to the Risks of Artificial Intelligence" (2013).
⁵⁵ Steven Weber, "The Risks of Artificial Intelligence" (Florida: University of Miami, 2013).

Chapman and Hall/CRC Press, 2015) a következő címen: Chapman and Hall/CRC Press, 2015. 5.

a látszólag egymástól teljesen független adatok összekapcsolhatók, hogy mélyreható képet alkossanak az adatmorzsák mögött álló személyről. Ebben a konkrét tanulmányban a 68Facebook-kedvelések elegendőek voltak ahhoz, hogy pontosan megjósoljanak számos személyes tulajdonságot, például a személyiségtípust, a szexualitást, a bőrszínt és a politikai meggyőződéseket.⁵⁶

Egy másik, nagy nyilvánosságot kapott példa a mesterséges intelligencia által támasztott hasonló adatvédelmi kihívásra a Target nagy kiskereskedelmi lánc által kiadott, terhességgel kapcsolatos termékekre vonatkozó kuponokat kapott egy 2012. fiatal tinédzser nő. A nő azonban nem közölte a terhesség tényét a Targetnek, de még a szüleinek sem. A Target nagy adatelemzési technikákat használt arra, hogy a vásárlói profilokat hozzon létre vásárlóiról azáltal, hogy a hűségkártya-rendszerükben rögzített vásárlásokat tényleges preferenciákhoz és jövőbeli igényekhez kötötte. A nő bizonyos bőrápolási termékek és étrend-kiegészítők vásárlási szokásai alapján képesek voltak megjósolni a terhességének intim részleteit.⁵⁷

2.4.2.2. Nudging

Ezeket a profilokat többnyire arra használják, hogy hirdetésekkel célozzanak meg az embereknek. Vannak azonban más szándékolt vagy nem szándékolt felhasználási módok is. Azáltal, hogy átfogó profilokat készítenek az emberekről, és felhasználják a felhalmozott tudást arról, hogy bizonyos személyes jellemzők hogyan hatnak egymásra vagy hogyan függnek össze, a vállalatok képesek célzottan megcélozni és befolyásolni az embereket saját céljaik elérése érdekében, még akkor is, ha ezek a célok eltérnek a következőkétől

56

„The Data Self” című előadás f. 19. oldalán

57 (2013) 11 015 ~~File~~ AAcTaedeenmGy WSciaesnPceresgnant52.
Kam irH ill," ~~igndd~~ iorf
~~B\H\wF sites\01,~~ (16 2012), :
: . . /sfitorsb/eksas ~~in February/2016~~ /honolwin-tea rget-f
igured-out-a-teen-girl-was-pregnant-before-her-father-did/.

ügyfeleik (és a társadalom) érdekeit. A szűrőbuborékokról már sokat írtak. Ezek annak az eredményei, hogy a nagy technológiai vállalatok, mint például a Google és a Facebook, optimalizálják algoritmusait, hogy az emberek minél tovább maradjanak az oldalaikon. Ez általában olyan tartalmakat részesít előnyben, amelyekkel az illető már egyetért. Ez viszont olyan buborékokat hoz létre, ahol a felhasználók csak a saját szemszögükből származó információkkal találkoznak, ami veszélyezteti a független véleményalkotási folyamatot, és ezáltal a demokráciát.⁵⁸

A Cambridge Analytica néven ismert 2018.céget azért vették tűz alá, mert állítólag nagyszámú Facebook-felhasználói profilt használt fel a 2016-os amerikai elnökválasztás befolyásolására. A Cambridge Analytica állítólag a Facebook-felhasználók személyiségjegyeiről gyűjtött információkat olyan mikrocélu hirdetésekhez használta fel, amelyek jelentős számú szavazatot befolyásoltak vagy elnyomtak.⁵⁹ A mesterséges intelligencia teljesen új lehetőségeket kínál a lakosság elemzésére és befolyásolására, ami nyilvánvalóan nagy kockázatot jelent a demokratikus kormányok stabilitására és legitimitására nézve.

2.4.2.3. Diszkrimináció

Egy másik kockázat, amely már megnyilvánult, a diszkrimináció veszélye. A mesterséges intelligencia nagyon jól tanul.

58 "The Guardian (18március 2018) 'Data war whistleblower', The Guardian (18március 2018) 'Data war whistleblower', The Guardian (18március 2018) 'Data war whistleblower'." (4. oldal)

59 "The Guardian (18március 2018) 'Data war whistleblower', The Guardian (18március 2018) 'Data war whistleblower', The Guardian (18március 2018) 'Data war whistleblower'." (4. oldal)

adatokból. Ha azonban ezek az adatok torzok, akkor ezeket a torzításokat a mesterséges intelligencia is reprodukálni fogja. Például a technológiai ágazatban az álláspályázatok automatikus elemző eszköze észreveheti azt a történelmi tendenciát, hogy a férfiakat előnyben részesítik a nőkkel szemben, és ezért a férfiakkal kapcsolatos tulajdonságokat magasabbra értékeli, mint a nőkkel kapcsolatosakat.⁶⁰ A szavak szemantikai jelentését megtanulni próbáló szóbeágyazások gyakran társítanak bizonyos kifejezéseket a nőkhöz, másokat pedig a férfiakhoz, így reprodukálva a nemi sztereotípiákat. Például az ápolót a nőkhöz, míg az orvost a férfiakhoz társíthatják.⁶¹ Továbbá az arcfelismerő szoftverek nem képesek felismerni bizonyos etnikai csoportokhoz tartozó embereket, ha a tanulási szakaszban használt adatok kizárólag egy másik csoportból származnak.⁶² A felhasználók közötti beszélgetéseket reprodukáló botokat megtaníthatják arra, hogy rasszista megjegyzéseket tegyenek, és diszkriminatív értékrendet fogadjanak el a többi felhasználóval való interakcióik során.⁶³ Férfiaknak olyan álláshirdetéseket mutathatnak, amelyek magasabb fizetést vonzanak, mint a nőknek mutatottak, ami tükrözi a számos szakmában tapasztalható bérszakadékot, és reprodukálja a szakmai lehetőségek egyenlőtlenségét.⁶⁴

60 "Amazon.com Recruiters Used Gender Data to Predict Which Candidates Would Be Most Successful", *Recruiting Industry News*, (10. február 2018), <https://www.recruitingindustrynews.com/article/us-amazon-com-allasok-automatizalasa-in-2018>.
61 "Amazon.com Recruiters Used Gender Data to Predict Which Candidates Would Be Most Successful", *Recruiting Industry News*, (10. február 2018).

62 "How Accurate is Facial Recognition Technology? It's Racist", *The Week UK* (július 27. 2018), <https://www.theweek.co.uk/5383-facial-recognition>.

63 "How Accurate is Facial Recognition Technology? It's Racist", *The Week UK* (július 27. 2018).

64 "Twitter Bot Called 'Tay' Mimicked User's Racist Asshole in Less Than a Day", *The Verge* (24. március 2016), <https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot>.

⁶⁴ Julia Carpenter, "A Google algoritmus a rangos álláshirdetéseket mutat a

2.4.2.4. Opacitás

Ezeket a kockázatokat fokozza, hogy gyakran lehetetlen megmagyarázni, hogyan jut egy mesterséges intelligencia rendszer következtetésre. Egyes esetekben az algoritmust a szellemi tulajdon titkosságának fátyla mögé rejtik. Előfordulhat, hogy a vállalatok nem hajlandók felfedni algoritmusuk részleteit, és csupán az eredményt adják át, ami lehetetlenné teszi az elemzést. Más esetekben, különösen a mélytanulási algoritmusok használata esetén, a folyamat összetettsége önmagában is megnehezítheti, hogy egy ember számára megmagyarázható legyen. A kutatók rengeteg erőfeszítést tesznek a megmagyarázható mesterséges intelligencia megalkotására, ami valószínűleg a mesterséges intelligencia széles körű társadalmi alkalmazásának feltétele lesz.⁶⁵ Ha a mesterséges intelligenciát fontos döntések meghozatalára használják anélkül, hogy azok megmagyarázhatóak, és ezért felülvizsgálhatóak lennének, a lakosság nem biztos, hogy képes lesz megérteni, hogyan születnek ezek a döntések, vagy nem lesz hajlandó azokat szisztematikusan megtámadni és megfellebbezni.

⁶⁵ Winney, H. (2015), "Why AI is scary", <http://www.technologyreview.com/2015/06/01/350766/why-ai-is-scary/>, accessed 2015-06-01.

⁶⁶ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁶⁷ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁶⁸ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁶⁹ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁷⁰ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁷¹ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁷² "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁷³ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁷⁴ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁷⁵ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁷⁶ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁷⁷ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁷⁸ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁷⁹ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁸⁰ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁸¹ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁸² "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁸³ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁸⁴ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁸⁵ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁸⁶ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁸⁷ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁸⁸ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁸⁹ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁹⁰ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁹¹ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁹² "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁹³ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁹⁴ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁹⁵ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁹⁶ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁹⁷ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁹⁸ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

⁹⁹ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

¹⁰⁰ "The Inexplicable AI: The data scientists' dilemma", *MIT Technology Review*, (1420), 2015, pp. 34-35.

2.5. Következtetés

Ez a fejezet megpróbált áttekintést adni a mesterséges intelligencia hihetetlenül hatalmas és virágzó területéről. Fontos megérteni a mesterséges intelligencia mögött álló technológiát ahhoz, hogy értékelnünk tudjuk, milyen hatással lehet a büntető igazságszolgáltatási rendszerre. E fejezet első tanulsága, hogy a mesterséges intelligencia jelenlegi tétele a szűk értelemben vett mesterséges intelligencia. Egy bizonyos feladat elvégzésére képzik ki. Miközben nagyon jó lehet ebben a feladatban, nem képes arra, hogy ezt a tudást más területekre is kiterjessze. Nem rendelkezik a világ működésének általános megértésével sem, amit a köznyelvben józan észnek nevezünk. Bár a jövőben valószínűleg fontosak lesznek azok az aggodalmak, hogy a mesterséges intelligencia felváltja az embert, mint a Föld legintelligensebb lényét, a mesterséges intelligencia jelenlegi használatában nem ezek a kérdések lesznek a meghatározóak.

A gépi tanulás az önfejlesztő algoritmusok építésének gyakorlata. Ezek az adatokat szitálják át, hogy mintákat azonosítsanak, és modellt építsenek az adatokból. Ez a modell lehet például az, hogy mi a közös a képek egy osztályában, és hogyan lehet megkülönböztetni őket (osztályozás), vagy hogy a tényezők hogyan hatnak egymásra, hogy egy számszerű következtetést kapjunk, például a hőmérséklet vagy az ár (regresszió). Ezen algoritmusok létrehozásához elengedhetetlenül fontos, hogy nagy mennyiségű, jó minőségű adat álljon rendelkezésre. Az adatok tehát az "új olaj" szerepét töltik be.

A hagyományos gépi tanuláshoz funkciótervezésre van szükség, amihez szakterületi ismeretekre és időre van szükség. A mélytanulás, amely az algoritmusok azon osztálya, amely a jelenlegi hype motorja, képes automatikusan kivonni az adatokból a jellemzők különböző absztrakciós szintjeit. Így képes hatalmas mennyiségű adatból nagyon kifinomult

modelleket létrehozni, minimális emberi beavatkozással.

A mélytanulás számos felhasználási területen, például az önvezető autókban, az adatok, például beszéd, videók és képek elemzésében, valamint a játékokban nagy előrelépést ért el.

A mesterséges intelligencia felhasználóinak számos kockázattal kell tisztában lenniük. Sok esetben hihetetlenül hatékony eszköz lehet. Azáltal, hogy az AI más adatok alapján következtet az emberekre, olyan tulajdonságokat is felfedhet az emberekről, amelyeket esetleg titokban akarnak tartani, vagy amelyekkel ők maguk sincsenek tisztában. Arra is felhasználható, hogy tömegesen bizonyos irányokba terelje az embereket, és ezáltal aláássa a demokratikus elveket, ha nem megfelelően használják. Mivel a mesterséges intelligencia adatoktól függ és azokból tanul, fennáll annak a veszélye, hogy az adatokban lévő elfogultságok állandósulnak. Ez megerősítheti a status quo-t és fenntarthatja a szisztematikus diszkriminációt. Ezt a megkülönböztetést nehéz lehet felismerni, mivel a mesterséges intelligencia által felépített modelleket nagyon nehéz megérteni.

3. AZ AI MINT A BŰNÖZÉS VEKTORA: A "BŰNÜGYIAI" MEGJELENÉSE

2018 elején a Reddit internetes platform egyik felhasználója egy "FakeApp" nevű, ingyenesen letölthető eszközt tett közzé. Ez az eszköz lehetővé tette a felhasználók számára, hogy egy (általában meglehetősen nagyszámú) kép segítségével "photoshopolják" vagy szerkesszék egy személy arcát egy másik videóba, beleértve az arckifejezések és viselkedési részletek valóság-hű ábrázolását. Ezt az eszközt több mint 100 000 alkalommal töltötték le.⁶⁶ A technikát filmmontázsok készítésére használták, például Nicolas Cage olyan filmekben jelent meg, amelyekben nem is szerepelt, komikus hatásra.⁶⁷ A létrehozott videók nagy része azonban pornográf videókra átültetett emberekről készült. A felhasználók a közösségi médiából szerzett adatok felhasználásával pornográf videókat hoztak létre hollywoodi sztárokkal⁶⁸, sőt barátaikkal vagy volt kapcsolataikkal.⁶⁹ A technológiát arra is használták, hogy hamis videót készítsenek az elnökről.

⁶⁶ Kohn, "Come the Fake Videos, Too", The NY Times (8/2018), <https://www.nytimes.com/technology/fake-videos-deepfakes20180304>.

⁶⁷ "How to Use DeepFakes in Movies", <https://www.fox.com/deep-fakes-in-movies/>.

⁶⁸ "Telereciprocity", <https://www.telereciprocity.com/>.

⁶⁹ "How to Use DeepFakes in Movies", <https://www.fox.com/deep-fakes-in-movies/>.

⁷⁰ "How to Use DeepFakes in Movies", <https://www.fox.com/deep-fakes-in-movies/>.

Trump gúnyolódik Belgium klímaválasztási döntései felett. Csak a szerzők tisztázása után jött rá a nyilvánosság, hogy a videó hamisítvány. ⁷⁰ Ez a példa jól szemlélteti, hogy a mesterséges intelligencia milyen erőteljes és bomlasztó hatással lehet az emberi tevékenység bármely területére. Amint azt az előző fejezetben tárgyaltuk, a mesterséges intelligencia nagyon előnyös lehet a társadalom nagy része számára, de óriási kockázatokkal is jár, ha a technológiát rosszindulatú célokra használják. Ez a fejezet ezért a mesterséges intelligencia bűnözést lehetővé tevő technológiaként való felhasználására összpontosít.

A jelentés többi részéhez képest ez a fejezet inkább spekulatívnak tűnik. Miközben a mesterséges intelligencia gyorsan elterjedt a büntető igazságszolgáltatásban, a bűnügyi szereplők általi alkalmazása szerencsére továbbra is ritka - vagy nem érte el azt a kritikus tömeget, amely kellő figyelmet vonzana. Sok kutató és megfigyelő azonban úgy véli, hogy ez hamarosan megváltozik.⁷¹ Ebben a fejezetben megvizsgáljuk, hogy jelenleg hogyan használható a mesterséges intelligencia a bűnözésben, és megvitatjuk a szakirodalomban felmerült jövőbeli lehetséges felhasználási módokat. Azokra az AI-képességekre összpontosítunk, amelyek ma már rendelkezésre állnak vagy a közeljövőben valószínűleg elérhetővé válnak, és nem a jövőbeli technológiák, például az "általános" AI spekulatív és nagyon távoli képességeire. Nem állítjuk, hogy képesek lennének megjósolni, hogyan fogják a bűnelkövetők kihasználni a mesterséges intelligenciát, és tartózkodunk a világvége-forgatókönyvektől, mivel mindig nagy a különbség a lehetséges és a valószínűsíthető között. Mindazonáltal

⁷⁰ "Deep Fakes: A New Threat to Trust", *MIT Technology Review*, (2018), <https://www.technologyreview.com/2018/11/12/deep-fakes-fake-news/>.

⁷¹ "The Future of Artificial Intelligence", *The Guardian*, (2018), <https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news>.

⁷¹ "The Future of Artificial Intelligence", *The Guardian*, (2018), <https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news>.

fontos, hogy tisztában legyünk azzal, hogy a büntető igazságszolgáltatási rendszer milyen új kihívásokkal nézhet szembe az új technológiák miatt.

Ez a szakasz nem foglalkozik a mesterséges intelligenciával kapcsolatos ügynöki kérdésekkel. Mint már említettük, a "szűk értelemben vett" mesterséges intelligenciára, azaz egy eszközre összpontosítva azt feltételezzük, hogy a felelős szereplő az a személy, aki a mesterséges intelligencia rendszert tervezte vagy működteti. Nem vesszük figyelembe a mesterséges intelligencia olyan felhasználását sem, amely véletlenül negatív eredményeket okoz, például autóbaleseteket, amelyek bizonyos joghatóságokban a mesterséges intelligencia üzemeltetőjének vagy tulajdonosának büntetőjogi felelősségét vonhatják maguk után. Ehelyett azokra a szereplőkre összpontosítunk, akik szándékosan használnak mesterséges intelligenciát, hogy kárt okozzanak.

3.1. A mesterséges intelligencia demokratizálása

A mesterséges intelligenciát övező közelmúltbeli izgalom és felhajtás következtében a nyilvánosság számos olyan kulcsfontosságú forráshoz jutott hozzá, amelyek szükségesek saját mesterséges intelligencia-eszközök használatához és fejlesztéséhez. Az élvonalbeli technológiákhoz való széles körű hozzáférés általában pozitív dolog, mivel felgyorsítja az innovatív gyakorlatok elfogadását. Ez azonban a rosszindulatú szereplők egy kis csoportját is képessé teheti arra, hogy a mesterséges intelligenciát aljas célokra használják. Egy mesterséges intelligencia eszköz létrehozásához számos erőforrásra van szükség, amint azt az előző fejezetben láttuk. A mesterséges intelligenciához adatokra, szakértelemre, eszközökre és hardverre van szükség. A következő fejezetek leírják, hogy ezek az erőforrások hogyan válnak egyre könnyebben hozzáférhetővé a nyilvánosság számára.

3.1.1. Adatok

A mesterséges intelligencia korában az adat az új olaj. A nagy

a gépi tanulási algoritmusok képzéséhez elengedhetetlenek a jó minőségű adatok.⁷² Az olyan technológiai óriások, mint a Google és a Facebook hatalmas mennyiségű adathoz férnek hozzá a felhasználóikról.⁷³ Amint arról korábban már szó volt, rendelkeznek olyan erőforrásokkal is, amelyekkel több ezer dolgozót tudnak alkalmazni, hogy adatokat címkézzenek számukra.⁷⁴ Bár jellemzően nagylelkűen megosztják algoritmusait, az adatokat általában szigorúan őrzik, ami azt jelenti, hogy a technológiai óriások jelentős előnnyel rendelkeznek a mesterséges intelligencia kutatásában és alkalmazásaiban.⁷⁵ Ez azonban nem jelenti azt, hogy a rosszindulatú szereplők számára lehetetlen lenne adatokat szerezni az algoritmusaik betanításához. Először is, az interneten számos nyilvános adathalmaz áll rendelkezésre, amelyek például anonimizált orvosi adatokat,⁷⁶ gazdasági mutatókat⁷⁷ vagy a tartalmukat leíró szavakkal megjelölt képek millióit⁷⁸ tartalmazzák.⁷⁹ Másodsor, az emberek által a nagy közösségi hálózatokra feltöltött adatok nagy része nyilvánosan hozzáférhető. Mint ilyenek, az

⁷² Domingos, supra note upra45. noet n 45.(Weboldal): 5b4>6.

⁷³ GDoyloagnleChuarvraeno, " ~~o~~ i sMarechdaF adla nArey', arTchis 80 (2018), : [tisfree//mar//all-the-data201828](https://www.tisfree//mar//all-the-data201828)

⁷⁴ " ~~y~~ TechNovpeamysbeprork e to programhoz g dWars", 83 (2018), [nytimes.com/2018/03/08/technology/google-ai-ethics.html](https://www.nytimes.com/2018/03/08/technology/google-ai-ethics.html)

⁷⁵ ~~Plenge~~ <https://www.nytimes.com/2018/03/08/technology/google-ai-ethics.html>. Óriások: Amazon, Facebook, and Google", TechEmergence (2018. november 24.), <https://www.techemergence.com/ai-ethics/>

⁷⁶ " ~~50~~ ~~Best~~ Machine Learning", ~~2~~ ~~Public~~ ~~Data~~ ~~2018~~, ~~lfionre~~: <https://www.kaggle.com/datasets>

⁷⁷ ~~hron~~ et al. " ~~Egy~~ szabadon hozzáférhető ~~AcalirsetadiratEaWbasJeo~~ " (2016)3 ~~e~~.

⁷⁸ ~~Quandl~~", Quandl (Weboldal), online: <https://www.quandl.com>.

⁷⁹ " ~~Image~~", ~~ogregN/inedt~~ (~~ebsite~~) online: <https://www.kaggle.com/datasets>

az adatokat gyakran egyszerűen úgy lehet megszerezni, hogy felkeresik a weboldalt, vagy olyan engedélyezett eszközökkel, amelyek adatokat gyűjtenek ezekről a weboldalokról. Egy rosszindulatú szereplő például a hivatalos twitter API-t (Application Program Interface) használhatja arra, hogy adatokat szerezzen arról, hogy egy felhasználó mit tweetelt.⁸⁰ Más esetekben az adatgyűjtésre vonatkozó hivatalos korlátozások megkerülésének módjai is létezhetnek. A Cambridge Analytica a "This Is Your Digital Life" kvízalkalmazás létrehozásával 87 millió Facebook-felhasználó személyes adataihoz jutott hozzá. Ha egy felhasználó, vagy bármelyik ismerőse használta ezt az alkalmazást, az ő adatait gyűjtötték össze, és később átadták a vállalatnak. Állítólag ezeket aztán arra használták fel, hogy politikai és pszichológiai profilokat készítsenek a felhasználókról.⁸¹ Az illegális piactereken több engedély nélküli adatgyűjtő eszköz és szolgáltatás is elérhető.

A nagy platformokon túlmenően más módjai is vannak az egyének személyes adatainak megszerzésére. Az úgynevezett adatbrókerek olyan nyomkövető hálózatokat működtetnek, amelyek figyelik a felhasználókat, miközben weboldalról weboldalra böngésznek. Ezeket az adatokat aztán összesítik és eladják a hirdetőknak vagy bárki másnak, aki hajlandó fizetni.⁸² Weboldalak és adatbázisok feltörése révén a hackerek felhasználók millióinak (és néha milliárdjainak) személyes adataihoz juthatnak hozzá. Ezeket az adatokat gyakran bűnözői online piactereken értékesítik.⁸³ "Have I been

⁸⁰ <https://datasciencepost.com/2018/04/04/twitter-api-referenc/>

⁸¹ <https://www.wired.com/2018/04/cambridge-analytica-how-they-got-your-data/>

⁸² <https://www.wired.com/2018/04/cambridge-analytica-how-they-got-your-data/>

⁸³ <https://www.wired.com/2018/04/cambridge-analytica-how-they-got-your-data/>

1. ~~projekt~~ /what-are-data-
as

A "pwned", egy weboldal, amely lehetővé teszi az emberek számára, hogy megtudják, hogy az adataik veszélybe kerültek-e, közel egymilliárd kiszivárgott fiókot sorol fel.⁸⁴

3.1.2. Szoftver és szakértelem

Miután az adatokat összegyűjtöttük, a következő lépés az, hogy felhasználjuk azokat egy algoritmus képzésére. Ehhez az szükséges, hogy a fejlesztő hozzáférjen a szoftverhez és a szoftver használatához szükséges szakértelemmel rendelkezzen. Mindkettő ma már elérhető a nyilvánosság számára. A gépi tanulás eleve nagyon nyitott terület. A legújabb kutatások azonnal nyílt hozzáférésű online formában jelennek meg, például az ArXiv e-Print szolgáltatáson.⁸⁵ Az iparágban használt vezető keretrendszerek szintén nyilvánosan elérhetőek.⁸⁶ Számos online oktatóanyag kínál gyors és egyszerű belépést az ML-be. ⁸⁷ Ez nem jelenti azt, hogy az ML tanulása könnyű - számos olyan kihívás van, amely még a képzett mérnökök számára is megnehezíti a tanulást.⁸⁸ A gépi tanulás azonban egyre inkább

⁸³ "Exploring a bad crypto", (2015) 4:2-socGialol3 55
nAdlisteruHctuutrehoinfsstoalhend

T m Holt, "The art of stealing", (2015) 53 AthcerimBreitsischripJtouanrnaalysiosf rthmmonlogy5 96 "M"
",
S 177Kvot ", (), #
htps : . nif onpplv/kras/Webs/sitpo reats
- 2017. afe2

⁸⁴ "How to check if your email is pwned", (2017) 1:1-secGialol3 10
htps://www.pwned.com/

⁸⁵ "The art of stealing", (2015) 53 AthcerimBreitsischripJtouanrnaalysiosf rthmmonlogy5 96 "M"
v. -oprgin/ t archive", arXiv.org (Weboldal), online:

⁸⁶ "The art of stealing", (2015) 53 AthcerimBreitsischripJtouanrnaalysiosf rthmmonlogy5 96 "M"
TPyeTnosorcrFhl ", yTensch (V), lme htps://www.pytorch.org
" o wP", (V) stn) ineh:
htaps : w wfvas e arioMlvs /.

⁸⁷ "The art of stealing", (2015) 53 AthcerimBreitsischripJtouanrnaalysiosf rthmmonlogy5 96 "M"
"Google LCaounpncuhteersFHreowCtoouTrseacohn",
Theplasioq

eoanchliinne
The CSF : ohntt-pd: .
e.com/2017/07/google-launches-free-course-
@pwa rping knt

91 "W Cleobusdite T P M l t p e / e a n t c o m s o / t p / w", Google
(), : : . s g o f o o g r l e T .

Cloud

GPU-k. Az Amazon, a Microsoft és a Google olyan szervereket kínál bérbeadásra, amelyek kifejezetten a mélytanuláshoz szükséges számítási típusok befogadására vannak konfigurálva. Ezek a vállalatok több GPU-val rendelkező gépek bérlésére is lehetőséget kínálnak, amelyek lehetővé teszik összetettebb modellek létrehozását és a Deep Learning feladatok támogatására tervezett rendszerekkel való integrációt.⁹²

3.2. A mesterséges intelligencia káros felhasználása

Mostanra bebizonyítottuk, hogy a mesterséges intelligencia már olyan szintre fejlődött, hogy bármely elkötelezett fejlesztő képes belépni a területre a nyilvánosan elérhető források felhasználásával. Mint említettük, ez a hozzáférhetőség általában véve pozitív dolog, ugyanakkor potenciálisan lehetővé teszi a rosszindulatú szereplők számára is, hogy kihasználják a technológiát. A mesterséges intelligenciának számos olyan tulajdonsága van, amely vonzónak teheti a rosszindulatú szereplők számára. Mint sok más technológia, ez is kettős célokat szolgálhat, és hasznos és káros célokra egyaránt felhasználható. A mesterséges intelligencia számos, ember által végrehajtott műveletet képes utánózni, sőt egyes esetekben hatékonyság és skálázhatóság tekintetében még az emberi teljesítményt is felülmúlja. Ez azt jelenti, hogy a korábban emberi képességeket és időt igénylő bűncselekményeket sokkal nagyobb léptékben, egyszerre több ezer áldozatot megcélozva lehet végrehajtani.⁹³ A mesterséges intelligencia az elkövető és az áldozatok közötti távolságot is növelheti. Ez megnehezítheti a bűnözők nyomon követését és csökkentheti a pszichológiai

⁹² <https://www.zdnet.com/article/google-amazon-microsoft-offer-gpu-cloud-computing/>; <https://www.hiAnme-laezaornniWngeb/amSeirsv/i>; () : "C"Mo"b"v"oCnllouined A Google : "SG:/o/colgoued. . d u"ka"; jonbeck7, "Azure Windows /p/z/edocs/Git, : . o sMofic. sh-Wu"bsite /voirntluinale-gépek/ablakok/

93 Site at 71 16-17.

38

gátlások.⁹⁴ Emellett a mesterséges intelligencia, mint minden technológiai rendszer, szükségszerűen számos technikai sebezhetőséggel rendelkezik, amelyeket a bűnös érdekek elkerülhetetlenül ki fognak használni.

A mesterséges intelligencia által jelentett kockázatokkal kapcsolatban tehát három fenyegető következmény van:

1. A meglévő fenyegetések bővíthetnek: a mesterséges intelligencia skálázhatósága miatt az elkövetők egyre több áldozatot vehetnek célba a technológia segítségével;
2. Teljesen új fenyegetések is megjelenhetnek: A mesterséges intelligencia képes adatokat, például valódi emberek hangját utánozó hangfájlokat generálni. Ezeket teljesen új típusú támadások végrehajtására és újszerű bűncselekményekre lehetne felhasználni;
3. A fenyegetések jellege megváltozhat: a mesterséges intelligencia képességeinek köszönhetően a bűncselekmények hatékonyabbá, célzottabbá és nehezebben beazonosíthatóvá válhatnak.⁹⁵

A mesterséges intelligencia tehát jelentősen megváltoztatja a számítógép-felhasználók ellen irányuló károkozás fajtáit és mértékét.

3.3. A rosszindulatú mesterséges intelligencia megközelítései

Ez a szakasz áttekintést nyújt a különböző bűnözési stratégiákról, amelyeket a mesterséges intelligencia rosszindulatú felhasználása elősegíthet. Ez a

⁹⁴ Ibid. 17.

⁹⁵ Ibid. 18-22.

nem a teljesség igényével készült, mivel a bűnügyi innováció természete mindig kiszámíthatatlan, de igyekszik kiemelni néhány olyan területet, amelyre hatással lehet a mesterséges intelligencia rendelkezésre állása.

3.3.1. Social Engineering

A social engineering meghatározása szerint "minden olyan cselekedet, amely egy személyt olyan cselekvésre befolyásol, amely lehet, hogy az ő érdekeit szolgálja, de lehet, hogy nem".⁹⁶ Ez egy hatékony támadási stratégia, amely inkább az emberi, mint a technikai sebezhetőségeket célozza meg, és amely ellen rendkívül nehéz védekezni, mind az egyének, mind a vállalatok számára. ⁹⁷ Ebben az alfejezetben a social engineering számos olyan megközelítését ismertetjük, amelyeket a mesterséges intelligencia jelentősen kibővíthet és megkönnyíthet.

3.3.1.1. Adathallászat

A hang használata helyett az emberek az "adathallászat" módszerét is alkalmazhatják, amelyet úgy határozhatunk meg, mint "a megbízható forrásból származónak tűnő e-mailek küldésének gyakorlatát, amelynek célja a személyes adatok befolyásolása vagy megszerzése".⁹⁸ Valószínűleg ez a social engineering legelterjedtebb típusa. ⁹⁹ Általában a támadó olyan e-mailt hoz létre, amely úgy tűnik, mintha megbízható forrásból származna, például egy pénzintézettől, technikai ügyfélszolgálatától vagy egy

⁹⁶ " a/EwgrwvngDifer ", (Stops . orgS/efrcaumriteywEordku/cgaetnioenral -

),ro/strid
Wdsustio g dding
⁹⁷ angMerri he human: Social engineering technikák és

sPehuisrhityngc oB (: ,0 08).
⁹⁸ " ", ugnhaRtionle(Use), online:

: w. social-engineer.org/framework/attack-vectors/phishing
hpa/62

⁹⁹ Ibid.

szolgálat vagy kormányzati intézmény. Ezeket az e-maileket ezután tömegesen fogják kiküldeni. A linkre kattintó személyt egy hamisított, de meggyőző weboldalra viszik, ahol arra kéri, hogy adja meg személyes adatait.¹⁰⁰ Az e-mail tartalmazhat egy mellékletet is, amelyre kattintva az áldozat számítógépe rosszindulatú szoftverrel fertőződik meg. A támadó számos módon próbálhatja meggyőzni a felhasználót arról, hogy az e-mail valódi, például úgy, hogy megváltoztatja az e-mail címet, hogy az legitimnek tűnjön, vagy olyan webdomaineket vásárol, amelyek nagyon hasonlítanak a célba vett intézmények hivatalos domainneveihez.

A személyre szabottabb változatot spear-phishingnek nevezik. Ahelyett, hogy tömegesen küldenének e-maileket a felhasználóknak, a spear-phishing műveletek konkrét felhasználókat céloznak meg aprólékosan kidolgozott e-mailekkel. Ezek az e-mailek alapulhatnak a közösségi médiából szerzett adatokon vagy bármilyen más nyílt forrásból származó információn, amelyet a támadó a célpontról gyűjteni tudott.¹⁰¹ Például egy önéletrajzra mutató linket tartalmazó e-maileket küldhetnek egy toborzónak. Az önéletrajz megtekintéséhez a felhasználót arra kéri, hogy jelentkezzen be a Microsoft-fiókjába egy olyan oldalon keresztül, amely pontosan tükrözi a valódi Microsoft portál kinézetét. Miután azonban a felhasználók megadták adataikat, a bejelentkezési adatokat a támadó begyűjti, és így képes veszélyeztetni áldozatai fiókját. Bár a spear-phishing nagyon hatékony, a támadóknak jelentős mennyiségű háttérkutatót kell végezniük, és hiteles üzeneteket kell létrehozniuk, ami a nagy értékű célpontokra korlátozza a használatát.¹⁰²

¹⁰⁰ ; "/" g v(), online:

<https://www.owk.com/it/>

¹⁰¹ ; " ", 4() online:

<https://www.owk.com/it/>

¹⁰² Supra note at 7119.

Nagy a kockázata annak, hogy a mesterséges intelligencia lehetővé teszi a bűnözők számára, hogy a hagyományos adathalász-támadások méretét a spear-phishing célzott jellegével és hatékonyságával kombinálják. Olyan rendszert lehetne tervezni, amely a célpontok nagyszámú online jelenlétét, például a közösségi médián belüli adatfolyamokat vizsgálná át. Ezután ezekről a felhasználókról profilokat lehetne készíteni, amelyek tartalmaznák, hogy milyen érdeklődési körük van, milyen vállalatokkal állnak kapcsolatban, és feltérképeznék az online tevékenységük mintáit. Ezen információk alapján a gép létrehozhatna vagy kiválaszthatna egy rendkívül meggyőző e-mailt. Ezt tömeges méretekben lehetne megtenni, anélkül, hogy emberi operátorokra lenne szükség. A mesterséges intelligencia rendszere emellett képes lenne megtanulni, hogy a válasz- vagy kattintási arányok alapján mi működik, és finoman megváltoztathatná az egyes üzeneteket, hogy megkerülje az áldozatok levelezőplatformjai által telepített adathalász-szűrőket. Egy nemrégiben készült tanulmány megmutatta, hogy az ilyen stratégiák mennyire hatékonyak lehetnek, és milyen könnyen megszervezhetőek. A kutatók egy csoportja egy gépi tanulási algoritmus segítségével képes volt azonosítani a célpontok egy csoportjának érdeklődési körét a Twitter-tevékenységük elemzésével. Ezután az algoritmus segítségével megszövegezték és személyre szabott üzeneteket küldtek nekik, amelyek egy potenciálisan rosszindulatú linket tartalmaztak, az áldozatok érdeklődési körének megfelelőnek ítélt üzenetek tartalmára támaszkodva. A hamis üzeneteket a nap azon időszakához időzítették, amikor az áldozatok a legaktívabbnak tűntek a közösségi platformon, hogy maximalizálják az elköteleződés esélyét. Ezután nyomon követték, hogy hány felhasználó kattintott a beágyazott linkekre, amelyek rosszindulatúak lehettek volna, ha a kutatók inkább bűnöző hackerek lettek volna. A célpontok 3366%-a kattintott a linkekre, ami felülmúlta a tömeges adathalászattal általában elért 514%-os arányt.¹⁰³

103 Jeonhgrine Seeryinmgo: u& , " ciePaefolboed
on&P& arWpehspingzongTwa" (

42

3.3.1.2. Vishing

Vishing (a "hang" és az "adathalászat" szavak összetétele) a "telefonon keresztül történő információszerzés vagy cselekvés befolyásolására tett kísérlet".¹⁰⁴ A támadó manipulálhatja a jelét azzal, hogy azt állítja, hogy az áldozat bankjának dolgozik, hogy a Microsoft ügyfélszolgálatának munkatársa, vagy hogy egy adóhivatalt képvisel.¹⁰⁵ Az átveréseknek pusztító következményei lehetnek - állítólag a telefonos átverések áldozatai átlagosan USD-t720 veszítettek a telefonhívásokban való bizalomra való hajlam miatt.¹⁰⁶ Ezek ellen a támadások ellen nehéz védekezni. ¹⁰⁷ Még a technikában jártas emberek is bedőlhetnek a fejlettebb módszereknek. ¹⁰⁸ Ezekhez a csalásokhoz azonban gyakran nagy előkészületekre és egy ügyes és meggyőző operátorra van szükség.¹⁰⁹ A támadások végrehajtása is időigényes lehet, ami korlátozza az áldozattá válás arányát.

104 <http://www.tulascakhat.com/2016/02/24/2016-also/unsli-ne-16> Seymour-Tully-W al-Mérnöki-Automata-EE-Spear-2 "in/wg"; <http://www.furcancrow.com/vecnolrins/evishing/>.

105 Radman Al-Minghish", (2007)3 :3 :
<http://www.rnraelcoefntLadwevaenlodpmPoelnictysfTohr ethtoep Soccoensymer59>

106 "Infraudms2017", Information, (1március2018),
 online:
<http://www.finnaguardnsd-2Smi07>.
 (Wmeabksie), lcinom: shing",
<http://www.seonf.com/tag/new-phishing-techniques-aware-hiNg/>

108 "Voice Phishing Scams Are Getting More Clever",
 (),
<http://www.SecurityMe.com/2018/08/voice-phishing-scams-are-getting-more-ting-more->

109 "Let's Go Vishing", (2014. december 22.), online: Security Through clever/ation.roughgetting-more-clev/<

107

109

Oktatás.

[https://www.social-](https://www.social-engineer.org/general-blog/lets-go-vishing)

[w.social-](https://www.social-engineer.org/general-blog/lets-go-vishing)

[engineer.o](https://www.social-engineer.org/general-blog/lets-go-vishing)

[rg/general-](https://www.social-engineer.org/general-blog/lets-go-vishing)

[blog/lets-](https://www.social-engineer.org/general-blog/lets-go-vishing)

[go-](https://www.social-engineer.org/general-blog/lets-go-vishing)

[vishing](https://www.social-engineer.org/general-blog/lets-go-vishing)>.

Ez a mesterséges intelligenciával megváltozhat. Ugyanazok a technikák, amelyeket egy segítőkész chatbot, például az Apple Siri¹¹⁰ vagy az Amazon Alexa¹¹¹ létrehozására használnak, felhasználhatók egy olyan számítógépes rendszer létrehozására is, amely képes egy embert utánozni. A Google már bebizonyította, hogy a mesterséges intelligencia segítségével olyan telefonos operátorokat lehet létrehozni, amelyek hangszínükben és kifejezőmódjukban gyakorlatilag megkülönböztethetetlenek a valódi emberektől. Ez a Duplex néven ismert rendszer képes éttermeket és fodrászokat felhívni, hogy asztalt foglaljanak vagy időpontot kérjenek anélkül, hogy a vonal másik végén lévő alkalmazottak észrevennék, hogy egy géppel érintkeznek.¹¹² Azáltal, hogy a lekérdezésekre való válaszadáshoz a reális hanggenerálás és a természetes nyelvi feldolgozás mesterséges intelligencia módszereit használják, a bűnöző hackerek¹¹³ így automatizált célzott műveleteket hozhatnak létre. Még ha nem is olyan hatékonyak, mint az emberi operátorok, ezek a rendszerek sokkal nagyobb léptékben, naponta több ezer személyt megcélözva bevethetők. Ez tehát egy olyan terület, ahol a mesterséges intelligencia növelheti a bűnözés mértékét. Brian Krebs leírja például, hogy már léteznek olyan rendszerek, amelyek mesterséges intelligenciát használnak a vishing stratégiát alkalmazó egyének megcélzására. Leírja egy személy tapasztalatait, akit egy hitelriasztó szolgálat munkatársa hívott fel. A hívó nagyon élethűen hangzott, és egyszerű kérdésekre is tudott válaszolni. Néhány bonyolultabb kérdés után azonban a hívó fél zökkenőmentesen

110 "Siri", Apple (Weboldal), online: <https://www.apple.com/siri/>.

111 "Ways to Build with Amazon Alexa", Amazon (Weboldal), online: <https://developer.amazon.com/alexa>.

112

© 2018

es-201805konver

2018. május 15. 14:00

gömb

2018. május 15.

ArCADoS

Am (B)Ac

hing

világbeli feladatok

p
n

di

g

gl

e

bl

o

g.

c

o

m

//

/

d

u

pl

e

x-

ai

-

re

n

d

sz

er

-

te

r

m

é

sz

et

kicserélték egy valódi emberre, aki megpróbálta véglegesíteni a csalárd cserét. Ez azt mutatja, hogy a hangfelismerés és -generálás hogyan használható a vishing műveletek automatizálására.¹¹⁴

A mesterséges intelligencia akár új támadási vektorok létrehozására is felhasználható a vishingben. A Lyrebird, egy 2017-ben indult montreali székhelyű AI startup lehetővé teszi a felhasználó számára, hogy néhány mondatnyi valódi hangjának rögzítésével betanítsa hangjának szintetikus változatát.¹¹⁵ A rosszindulatú szereplők ezt a technológiát arra használhatják, hogy olyan hangüzeneteket generáljanak, amelyek úgy hangzanak, mintha közeli rokonoktól vagy barátoktól származnának (a gépet nyilvánosan elérhető videókkal vagy olyan személyekkel folytatott hamis hívásokkal betanítva, akiknek a hangját hamisítani kell), és ezzel a felhasználót adatok kiadására csábíthatják.¹¹⁶ Ez az új képesség megváltoztathatja a hangba vetett bizalmat.¹¹⁷

3.3.1.3. Astroturfing

Egy másik gyakorlat, amelyet a mesterséges intelligencia súlyosbíthat, az asztroturfing. Ez abból áll, hogy hamis, alulról szerveződő mozgalmakat hoznak létre, amelyek valódiaknak és széles körben elterjedtnek tűnnek, de valójában csak nagyon kevés szereplőből indulnak ki.¹¹⁸ Számos cég kínál

¹¹⁴ Krebs, fenti megjegyzés 108.

¹¹⁵ es Vishi ni, "Hr AI megtalálni a (mesterséges) a wv .
 W (5 028) dUrsere //; " elid
 ComRealitVoc/OrbigarsEafosPita 200 1
), : Int " ,rds. .

¹¹⁶ Mital as (WArtifid i/Lyrebe, up a note at 7120.

¹¹⁷ Abhimanyu Ghoshal: "Betanítottam egy mesterséges intelligenciát, ijedtem meg", The Next Web (2018. január 22.), online: <https://thenextweb.coinsights/2018/01/22/i-trained-an-ai-to-copy-magam-rosszul/>.

¹¹⁸ Thomas P Lyon & J hn W Maxwell, "Astroturf: Interest Strategy Lobbizás és vállalati stratégia" (2004) 13:4 J Econ Manag 561; Kevin Grandia, "Bonner & Associates: A hosszú és

asztroturfing szolgáltatásként, és olyan szoftvereket biztosítanak, amelyek lehetővé teszik az alkalmazottak számára, hogy több online személyiséget kezeljenek.¹¹⁹ Az astroturfinget a vállalatok felhasználhatják termékeik felülvizsgálatára, hogy azokat kívánatosabbnak tüntessék fel. Egyesek azt állítják, hogy az online vélemények akár egyharmada is hamisítvány.¹²⁰ Az astroturfinget politikai manipulációra is fel lehet használni, például egy bizonyos nézet tweetelésével vagy megosztásával. Egy tanulmány például kimutatta, hogy az astroturfing technikák nagyon hatékonyak lehetnek a globális felmelegedés eredetével kapcsolatos kétségek felvetésében.¹²¹ Így a szélsőséges politikai nézetek mainstreamnek tűnhetnek, és megjelenhetnek a "trending" szekcióban az olyan közösségi oldalakon, mint a Twitter. Állítólag botokat használtak a 2016-os amerikai elnökválasztás előtt és után, hogy a közvéleményt a Trumpra való szavazás irányába tereljék, hogy a bázisát erősebbnek tüntessék fel, mint amilyen valójában volt, vagy hogy bizonyos szavazókat egyáltalán ne szavazzanak.¹²² Az Egyesült Államokban a Szövetségi Hírközlési Bizottság (FCC) által folytatott konzultáció során a hálózatsemlegesség eltörlését támogató beadványok millióit nyilvánvalóan hamis fiókok nyújtották be, sokszor halott emberek nevéen. Egy adattudós több millió 1.3hozzászólást fedezett fel

Ure c History of Astroturfing", Huffington Post (26augusztus 20 09)noté
<http://www.huffingtonpost.com/kevin-grandia/bonner-associates-the-lon-29-06-wht-in-119>, 118
 118 Rades, "The
 0 12), : Mental De ", e 25
<https://www.nytimes.com/2012/08/26/business/book-reviewers-for->

¹²⁰ Shtrei-tmfeedt-as-udperma annot-efor-on line-raves. html.

¹²¹ CGhreaernler Cde rASsidtreoutoufrtthinegFeGnlcoeb " (20) 1044 J B
 alW a rmin g:



¹²² 20 16RSp, (1 72018, cto



h . ethteedg-uaafrridciaann-ammerruanswe/edion/ 2017/russian-propa
stac 06 .

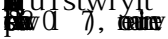
46





amelyek rendkívül hasonló nyelvi szerkezeteket követtek, és így valószínűleg hamisítványok voltak.¹²³

A mesterséges intelligencia potenciálisan drasztikusan növelheti az asztroturfing hatékonyságát. A Twitter például botellenes mechanizmusokat használ a hamis fiókok felismerésére és letiltására.¹²⁴ Ez azt jelenti, hogy a támadóknak "terelgetniük" kell a fiókokat azáltal, hogy regisztrálják őket, képeket adnak hozzá, időnként tweetelnek és követnek más felhasználókat.¹²⁵ A mesterséges intelligencia segítségével ezt a folyamatot automatizálni lehetne. Arra is felhasználható lenne, hogy automatikusan olyan üzeneteket generáljon, amelyek ugyanazt az információt terjesztik, de elég egyediek ahhoz, hogy ne lehessen hasonlóknak felismerni őket. Végül a mesterséges intelligencia felhasználható lenne az üzenetek jobb célzására, hogy azok bizonyos emberek számára meggyőzőbbek legyenek szociodemográfiai jellemzőik vagy pszichológiai tulajdonságaik alapján.¹²⁶ Az astroturfing gyakorlatát soha nem látott mértékű rágalmazásra vagy zaklatásra lehetne felhasználni.

¹²³ aLoi, " aHMaicklieorn pealNnoevemNebuetralityC 
 k eMofatradh',  217), :
 bn/ehatswercorik. n-pro-repeal-net-
 neutralitás ceolym-f/amkeodre-e-thfaen-ead-milialio36

¹²⁴ , " in the War on Twitter Spam", Krebs :
 (Vid)Pak 
 nsecurity.com/3//buying-battles-in-the-war-on-20108

¹²⁵ ", tethus e
 tuTstwrvit", BAmppicalionestigatethJurneOm(7
 (2017), 
 : . tu estigates. com/stories/--/twitterbots20171207.


¹²⁶ , "Ctdme :
 MWaitt Cenhehsasnece pMactiomEhla 
 ltuTrhee,  nocSreapctye. ... Vit Done About
 Citu", (1 m and20 17), 
 ://www. scribd. com/document//The-MADCOM-Future359972969


3.3.2. Generáció

Mint korábban említettük, a mesterséges intelligencia segítségével rendkívül valóságúnak tűnő adatokat lehet létrehozni. Ez felhasználható social engineering célokra, de új támadási vektorokra is. Az emberek megtanulták, hogy a képek könnyen manipulálhatók olyan eszközökkel, mint az Adobe Photoshop. A mesterséges intelligenciával azonban még az olyan médiumok, mint a hang és a videó is meggyőző módon és tömegesen hamisíthatók. Mint már említettük, ezt a lehetőséget a vadonban aktívan kihasználják. Ez lehet tehát a mesterséges intelligencia leglátványosabb rosszindulatú felhasználása. A tendencia a korai időszakban kezdődött, amikor a Reddit internetes fórum 2018, egyik felhasználója létrehozta és nyilvánosan közzétette az általa FakeAppnak nevezett eszközt, amelyet több mint letöltöttek 100,000.¹²⁷ Ez lehetővé teszi bármely, kellően erős grafikus kártyával rendelkező felhasználó számára, hogy hamis videókat hozzon létre az úgynevezett autoencoderek néven ismert technológiára épülő mélytanulási hálózatok segítségével.¹²⁸ A felhasználó egyszerűen csak kevés számú képet vagy videót szolgáltat egy célszemélyről. A neurális hálózat ezután "megtanulja" az adott személy arcát. Ezután a felhasználó egy másik videót szolgáltat, és kijelöli a célzott arcot. A neurális hálózat ekkor egy új videót generál, és a célszemély arcát a célvideón szereplő személy arcára rendereli. Ez magában foglalja az arckifejezések adaptálását, és nagyon valóságúnak nézhet ki.¹²⁹

¹²⁷ Roose, Supra note 66.

¹²⁸ Gar a i, "Exploring DeepFakes", Hacker Noon (5március h 20 8), 

: . 201729 ; Alan ,  2
 "Exploring DeepFakes", Zuccoonii
 (8), :
 alanzuoccnolini.com////understanding-the-technology-20180314

¹²⁹ nd-deepfakes/.

Ábra - 5. A Deepfake technológia alkalmazása



A programot széles körben használták, főként humoros célokra, mint például Obama elnök közszolgálati közleménye, amelyben azt tanácsolta a nyilvánosságnak, hogy ne bízson a videókban,¹³¹ vagy olyan videókban, amelyekben Nicolas Cage színész egy filmben minden szerepet eljátszott.¹³² A DeepFakes technológiájának számos hasznos felhasználási módja van, például az oktatás, a művészet és az autonómia segítése.¹³³ A legnagyobb nyilvánosságot kapott és legrosszindulatúbb felhasználása azonban felnőtteknek szóló anyagok készítésére irányult. Számos híres film- és zenei sztárokat bemutató videót tettek közzé a közösségi oldalakon és a felnőtteknek szóló weboldalakon, majd később betiltották őket. Úgy tűnt, hogy a felhasználók is

¹³⁰ [https://www.youtube.com/watch?v=...](#) "Obama Is Not What You Think He Is" (2018).

It is a deepfake video of Barack Obama. [https://www.youtube.com/watch?v=...](#)

¹³¹ [https://www.youtube.com/watch?v=...](#)

¹³² Usersub, Supra note 67.

¹³³ R. Chobale, "The Ethics of Deepfakes: A Call for Regulation," 107 California Law Review (megjelenés előtt), 15-17.

oo nig
", (00)

hogyan próbáljanak olyan videókat készíteni, amelyekben barátaikat vagy korábbi szerelmi kapcsolataikat mutatják be.¹³⁴

A DeepFake eszköz rávilágít számos olyan problémára, amely a mesterséges intelligencia alkalmazásával kapcsolatban felmerülhet. Az első a technológia könnyű elterjedése.¹³⁵ A mesterséges intelligencia megjelenése előtt egy hamis pornográf videó létrehozása, amelyben bármely személy szerepelhetett, lehetséges lehetett volna speciális effektusokkal, de ez továbbra is rendkívül költséges maradt, és sok szakértelmet igényelt. A mesterséges intelligencia azonban lehetővé teszi, hogy egy kellően képzett egyén létrehozzon egy ilyen feladatot ellátó eszközt, majd azt szinte bárki számára elérhetővé tegye, aki csak nagyon mérsékelt technikai tudással rendelkezik.¹³⁶ Továbbá az eszköz rávilágít a társadalomban a bizalom számos vektorának lehetséges összeomlására. A DeepFake eszköz által készített videók közül sok már nagyon is valóságúnak tűnik. Azonban gyakran vannak olyan műalkotások, amelyek a közönségnek azt az érzetet keltik, hogy valami nem stimmel. Feltételezhető, hogy egy napon lehetőség lesz hamis, nagyon valóságú videók létrehozására, ami aláássa a videóanyagokba, mint valaminek az igazságtartalmának bizonyítékába vetett bizalmat.

A pornográf anyagokon túl a DeepFake eszközt tehát bárki használhatja arra, hogy videót készítsen egy olyan személyről, aki bármilyen cselekedetet hajtott végre vagy mond bármit. Egy német humorista hamis videót készített egy görög miniszterről, amint ujjal mutogat a tömegre, aminek hatására a 2016. média napokig találgatta, hogy a videó valódi vagy hamis, és valószínűleg a közvéleményt is formálta. A közszereplőkről készült videókat politikusok vagy vállalkozók is felhasználhatják ellenfeleik vagy versenytársaik lejáratására,

¹³⁴ Cole & Maiberg, *Supra note*. 69.

¹³⁵ A mesterséges intelligencia rosszindulatú felhasználása, lásd a következőt.

¹³⁶ Chesney & Citron, *Supra note*, 1338-9. o.

hivatkozást 17.

vagy nemzetállamok által a demokratikus folyamatok megtámadása vagy ellenfelek destabilizálása érdekében. E jól végrehajtott támadások kis száma potenciálisan a tömegmédiába vetett közbizalom megingását idézheti elő. Hogyan lehetne megbízni bármelyik videofelvételben, ha mindegyik hamisítvány lehet? Ez nem csak azt jelentheti, hogy egyes közszereplőknek folyamatosan védekezniük kell a felvételeken rögzített vádakkal szemben, amelyek szerint helytelenül cselekedtek vagy korrupciót követtek el, hanem azt is, hogy a személyiségek számára hihető védekezési lehetőséget biztosítanak olyan dolgok ellen, amelyeket valóban mondtak vagy tettek.

Nem csak a közszereplők vannak kitéve ilyen támadásoknak. Manapság a legtöbb emberről számos kép nyilvánosan elérhető az interneten. Egy rosszindulatú személy a DeepFake eszközzel videókat vagy hangfelvételeket készíthet ezekről az emberekről azzal a céllal, hogy tönkretegyje a hírnevüket. Ez lehet akár egy elégedetlen volt partner, egy dühös alkalmazott vagy egyszerűen csak valaki, aki kárt akar okozni. Sok minden okozhat helyrehozhatatlan kárt egy személynek, például pornográf tartalmak főszereplése vagy rasszista megjegyzések hangoztatása. Még ha az illető tagadja is a videó valóságtartalmát, ez nem biztos, hogy elég - a pletykák gyorsan terjednek - különösen a közösségi médiában -, és ha egyszer kialakult a vélemény, azt időnként nagyon nehéz megváltoztatni. Ráadásul az egyének azonnali internetes keresésének megjelenésével egy negatív történet azt eredményezheti, hogy az illetőnek egész életében nehéz lesz munkát találnia vagy helyreállítania a hírnevét.

3.3.3. Kiberbiztonság

Nagymértékben összekapcsolt társadalmunkban a mesterséges intelligenciából eredő nagy támadási vektor a kiberbiztonság. A biztonságos szoftverek és platformok megírása és karbantartása olyan feladat, amely magasan képzett

szakértők, akikből nagyon kevés van. Továbbá sok vállalatnak nem biztos, hogy van elég erőforrása vagy ösztönzője arra, hogy biztosítsa rendszereit, ami az elkerülhető sebezhetőségek igen magas arányát eredményezi. Az utóbbi időben a kibertámadások kifinomultsága egyre nő, ami részben a hírszerző ügynökségek által kifejlesztett, igen kifinomult eszközkészletek kiszivárgásának köszönhető. A kiberbűnözők is számba vették a digitális technológiáktól és adatoktól való növekvő függőségünket, és válaszul új üzleti modelleket fejlesztettek ki, mint például a zsarolóvírusok. A zsarolóvírus üzleti modell felhagy a személyes adatok ellopásával, amelyeket korábban az online bűnözői piacereken harmadik feleknek továbbértékesítettek. Ehelyett az értéket magából az áldozatból vonják ki, aki fizet az elkövetőknek, hogy visszaszerezze a hozzáférést értékes személyes adataihoz.¹³⁷ Ez a szakasz azt vizsgálja, hogy a bűnöző hackerek miként használhatják a mesterséges intelligenciát támadásaik mértékének és hatékonyságának további javítására.

3.3.3.1. Sebezhetőség felfedezése

Számos számítógépes vírus a rendszer sebezhetőségének kihasználásán alapul. Ez lehet egy operációs rendszer (például a Windows) vagy egy szoftver (például az Adobe Reader), de akár egy webes technológia (például a WordPress, az online publikáláshoz használt eszköz) hibája is, amely lehetővé teszi a hacker számára, hogy hozzáférjen a rendszerhez, és információkat lopjon el, vagy saját kódot hajtson végre. A sebezhetőségeket, ha egyszer felfedezik őket, a szoftvergyártóknak gyorsan javítaniuk kell, hogy minél kevesebb kárt okozhassanak. Olyan sebezhetőségek, amelyeket egy vírus használ fel a gép megfertőzéséhez

137 ¹³⁷ Nicholas D. Clark, "The Economics of Information Security", (Baltimore: Johns Hopkins University Press, 2004), p. 180.
 17th Annual Workshop on the Economics of Information Security, (2004), p. 180.
 abs/1804.0080.

mielőtt a vállalat befolytozta volna őket, nulladik napi kihasználásoknak nevezik. A StuxNet-vírus négy ilyen sebezhetőséget használt ki. Ezek rendkívül értékesek lehetnek a feketepiacon, ami miatt sok vállalat hibajutalmat ajánl fel azoknak a kutatóknak, akik elsőként tárják fel a sebezhetőségeket.

Számos módszer létezik e sebezhetőségek felfedezésére. A statikus elemzéshez a kutatónak manuálisan vagy félautomatikusan elemeznie kell a program kódját. A Fuzzing több milliárd véletlenszerű permutációval táplálja a programot, hogy lássa, mikor hibázik. A behatolásvizsgálat során a kutató hackernek adja ki magát, és a rendszerbe való belépési kísérletekkel fedezi fel a sebezhetőséget.¹³⁸ Ezeket a technikákat a kutatók saját szoftvereik sebezhetőségének felfedezésére és javítására használhatják, de a sebezhetőségeket megtalálni és kihasználni kívánó támadók is alkalmazhatják. ¹³⁹ A sebezhetőségek felfedezéséhez képzett elemzőre van szükség.¹⁴⁰

A mesterséges intelligencia alkalmazása a támadások minőségének és mennyiségének növekedéséhez vezethet. A kutatók ígéretes megközelítéseket mutattak be a sebezhetőségek felfedezésének további automatizálására mesterséges intelligencia segítségével. ¹⁴¹ Amíg

138 B. SurLievuy " (et Papl, " Vi DnvevTTCofas Software Health ncAe onlinMeu: lhtitmtpsd urity, 2012), :/infomaticone Nyvdrkicog/6456

139 A mesterséges intelligencia rosszindulatú felhasználása, fenti jegyzet. 7116. DVuanlnieelraVboitliptkyaDeitscalo veHyPrces Et stePa

HE iuhmttps://arGdnomlipvaerriesdonaot ftShoefwac208 2018), Sympo : . . uSmaentF/rancisco8184

141 GDuissctoaveorG , " o w PrdapSemr nUccoin& Attilahng.T. (lly y g

most, a fuzzingot nehéz volt beállítani a használatban. A mesterséges intelligencia segítségével meg lehetne tanulni azokat az adatstruktúrákat, amelyekre egy program támaszkodik, majd automatikusan hamis adatokat lehetne beadni. Ez növelhetné az ilyen támadásokat végrehajtani képes emberek számát, és így a felfedezett sebezhetőségek számát is.¹⁴² A Microsoft kutatói²⁰¹⁷, bemutatták, hogy a neurális hálózatok segítségével hogyan lehetne egyszerűbbé, hatékonyabbá és általánosabbá tenni a fuzzingot.¹⁴³

A gyenge jelszó is egyfajta sebezhetőséget jelenthet, mivel lehetővé teszi a hacker számára, hogy hozzáférjen a felhasználó fiókjához.¹⁴⁴ A kutatások bebizonyították, hogy a mesterséges intelligencia nagyon erős lehet a jelszavak kitalálásában. A kiszivárgott jelszavak millióin betanítható, hogy mintákat ismerjen fel, majd ezeket alkalmazva kitalálja az egyes felhasználók jelszavait.¹⁴⁵

Vulnerabilities in Windows System Update Agent (WSUS) and Windows Update Agent (WU) (CPA),
 per elio vnerliendeat a [https://www.microsoft.com/en-us/security/default?search=windows%20update%20agent%20vulnerability](#) (2018),
 22125_0445_Automated_...
 ingt_/ApIu_bPlliacnatnioinng/at 8.
 m
¹⁴² FLoeartrinGiunagr dPoiSsEoniTnega", „Fo
 " : AINoFvuezmzibnegr és
 rPtimeedtiBilong(15...), [Mandiant](#) hintgtp-asn:/d/w-
 mwawc. . [https://www.mandiant.com/resources/predictions-ai-fuzzing](#)
¹⁴³ MNeucad : [https://www.microsoft.com/en-us/security/default?search=windows%20update%20agent%20vulnerability](#)
 ftfuRzezsienagr d(1... 2017),
 tesztelés",
 n-uRsis/hreasbeharScihn/gbhlg;
 : N raby tes seveforifu zhs. (2017) [https://www.microsoft.com/en-us/security/default?search=windows%20update%20agent%20vulnerability](#)
 a[171.0.496].], : ://a.v.o 7105 960
¹⁴⁴ . . " Computer hackers "bejutnak" egy számítógépbe?",
 SudenJiCiH aH
¹⁴⁵ : . [https://www.microsoft.com/en-us/security/default?search=windows%20update%20agent%20vulnerability](#)
 a[171.0.496].], : ://a.v.o 7105 960

P. B. Ghosh (2017) ~~875~~ Papír, arXiv:1709.00440
[cs], : ~~http://~~ xaiivr. 1709.00 .

3.3.3.2. Kihasználás

Még a sebezhetőség felfedezése után sem ér véget a támadó munkája. Megpróbálja megtalálni a módját annak, hogy a kihasználást felhasználva hozzáférjen egy vagy több célgéphez. Ezt megteheti például egy olyan számítógépes vírus létrehozásával, amely a kihasználtságot felhasználva megpróbál önállóan minél több számítógépet megtámadni. Használható egy szerver elleni rendszeres kibertámadás végrehajtására is. Itt a támadó maga futtat parancsokat, hogy oldalirányban más gépek felé mozogjon.

A védelmi oldalon a gépi tanulást használják az ilyen típusú támadások megfigyelésére. A vírusirtó programok gyakran kétféle módon azonosítják a rosszindulatú programokat: A szignatúra-alapú technológiákat és a viselkedéselemzést. A szignatúra-alapú elemzés a vírus kódjának digitális ujjlenyomata alapján próbálja azonosítani a vírust. Ez arra támaszkodik, hogy a vírusirtó gyártó azonosítja a rosszindulatú szoftvereket, és hozzáadja azokat a rosszindulatú aláírásokat tartalmazó adatbázishoz.¹⁴⁶ A viselkedéselemzés azt azonosítja, hogy egy program mit próbál tenni, nem pedig azt, hogy milyen kódon alapul.¹⁴⁷ Gyakran használ ML technológiákat.¹⁴⁸ A mesterséges intelligencia felhasználható e rendszerek kijátszására. Kutatók kimutatták, hogy lehetséges olyan mesterséges intelligencia-rendszereket létrehozni, amelyek automatikusan olyan rosszindulatú szoftvereket hoznak létre, amelyek kikerülnek a szokásos vírusirtó programokat.¹⁴⁹ A támadók a mesterséges intelligenciát arra használhatnák, hogy egy-egy programot egészen addig módosítsanak, amíg

146 " " dvInanfocseedcuMritaylwMaaregazDineteec tionAp-riIlsignat u
sisA", (1 1017),

rethes

p .tiunrfeos/e curity-magazine.com:443/opinions/malware-de
kaga

147 Ibid.

¹⁴⁸ A mesterséges intelligencia rosszindulatú felhasználása, lásd a következőt

¹⁴⁹ Hyun S. Anderson et al, "Learning to Evade Static PE

Machine" (Statikus PE gép tanulása),
Learning Malware Models via Reinforcement Learning" (2018)
arXiv Working Paper, arXiv:180108917 [cs], online:
<http://arxiv.org/abs/1801.08917>.

a vírusirtó szűrők számára jóindulatúnak tűnik.

Hasonlóképpen, a szerverrendszereken gyakran futnak behatolásérzékelő rendszerek néven ismert védelmi szoftverek, amelyek ellenőrzik a szerverek vagy a forgalom furcsa viselkedését, és jelentik ezt a rendszergazdáknak. Ezek gyakran használnak gépi tanulási technológiákat.¹⁵⁰ Ha például egy szerver hirtelen hatalmas mennyiségű adatot kezd el továbbítani egy oroszországi IP-címre, az jelezheti, hogy hackelés van folyamatban. Ugyanakkor az is lehet, hogy ez csak annak a jele, hogy az orosz felhasználók egy népszerű linket követve jutnak el a weboldalra. Egy hacker a mesterséges intelligencia segítségével megpróbálhatja kijátszani ezeket a rendszereket, és tevékenységét emberi viselkedésnek látszó viselkedés álcája mögé rejtve próbálja meg kijátszani. A mimikai támadások, amelyek megpróbálnak a radar alá bújni, bizonyítottan hatékonyak.¹⁵¹ A gépi tanulás alkalmazása ezek automatizálására természetes fejlődésnek tűnik.

3.3.3.3. Post-Exploitation & adatlopás

A kihasználás után a támadó gyakran a létrehozott hozzáférést használja arra, hogy saját hátsó ajtót telepítsen, amellyel újra beléphet a szerverre, mélyebb hozzáférést szerezve a rendszerhez, és körülnézhet a szerveren potenciálisan érzékeny információk után, és letöltheti ezeket az információkat.¹⁵² Más hekkerek felhasználhatják a

¹⁵⁰: "Theodhonoriquets", "st eAnsomandy-bcahsaddennngestw"

orki ntrus io-n
(2009 28:1 2

elms 18;
CAoyemsphu, "SiSgeecnutriitnytrus
,
ioAnlexdeSthecetniofineldsysteamvids anddri

(2018) S42 CMEmpircersys9 .
¹⁵¹ "Ab otol," Attacks on Host-Based
"InfenceDatChompSystems" (VWMA
p 200), ing onFI
s://d .com /citation.cfm?id=586145 at10 .

¹⁵² Ivan Novikov, "How AI Can Be Applied To Cyberattacks", Forbes (2018. március 22.), <https://www.forbes.com/sites/forbestechcouncil/2018/03/22/how-ai-online>:

56

hozzáférés, hogy további hozzáférést szerezzenek a vállalat működéséhez, vagy hogy pénzügyi károkat okozó szolgáltatásokat semmisítsenek meg. E folyamat során a hackernek ügyelnie kell arra, hogy rejtve maradjon, és eltöröljön minden olyan nyomot, amely elárulhatja az üzemeltetőnek, hogy a szerveren járt, és ami ahhoz vezethet, hogy lebukik. Ez egy bonyolult folyamat, amely sok türelmet, ügyességet és a számítógépes rendszer ismeretét igényli. A támadásoknak gyakran az emberi reakció gyorsasága szab határt - aszerint, hogy a hacker milyen információkat lát a szerveren, más-más módon kell reagálnia.

Bár ez sokkal erőltetettebb, mint a többi alkalmazás, a hackerek számára potenciálisan lehetséges lehet, hogy egy mesterséges intelligencia rendszert képezzenek ki arra, hogy automatizálják e lépések egy részét. Már léteznek olyan, a számítógépes rendszerek biztonsági auditálására létrehozott keretrendszerek, amelyek lehetővé teszik, hogy az emberek támadások egész sorát zúdítsák egy számítógépes rendszerre.¹⁵³ A mesterséges intelligencia növelheti ezeknek a rendszereknek a képességét, hogy automatikusan következtetni tudjanak arra, hogy mely támadások megfelelőek, vagy hogy mely adatok lehetnek érzékenyek, és ezért prioritást kell élvezniük. Egy ilyen rendszert párhuzamosan lehetne használni arra, hogy egyszerre több rendszert is intelligensen kihasználjon, emberi beavatkozás nélkül. Bár ez bizonyos mértékig már most is lehetséges, a mesterséges intelligencia képes lehet fokozni ezeket a képességeket.

3.3.4. A telepített mesterséges intelligencia kihasználása

A legtöbb elemző úgy látja, hogy a mesterséges intelligencia nagy hatással lesz a társadalom legtöbb, ha nem minden szektorára. Ez egy újabb

¹⁵³ [https://www.cisa.gov/secure/2018/08/22/pen-testing-security/](https://www.cisa.gov/secure/2018/08/22/pen-testing-security).

¹⁵³ "Pen Testing Security", Metasploit

(Weboldal), online:

<https://www.metasploit.com/>.

a rosszindulatú felhasználók számára megnyíló támadási vektor. Mint már említettük, a mesterséges intelligencia rendszerek jelenlegi termése számos gyengeségtől szenved. Ha a társadalom széles körében alkalmazták őket, akkor fennáll a veszélye, hogy olyan új támadásokat tesznek lehetővé, amelyek kihasználják ezt a gyengeséget. Attól függően, hogy a mesterséges intelligenciát milyen módon hajtják végre, és hogy milyen mértékű ellenőrzést kap az emberek és a folyamatok felett, ez óriási károkat okozhat a társadalomnak.

3.3.4.1. Ellenséges támadások

Az ellenséges támadások olyan támadások, amelyek kihasználják azt a tényt, hogy a mesterséges intelligencia nem úgy működik, mint az emberi intelligencia. A mesterséges intelligencia általában, és különösen a konvolúciós neurális hálózatok olyan jellemzők alapján azonosítják a mintákat, amelyek az emberek számára nagyon kevésbé intuitívak lehetnek. A bemenet kismértékű megváltoztatásával teljesen megváltoztatható, ahogyan a mesterséges intelligencia rendszer értelmezi a mintát. Kimutatták, hogy egy kiskutya képe olyan módon módosítható, amely az ember számára észrevehetetlen. Ezek a hatások valós forgatókönyvekben is megvalósíthatók - egy kutatócsoport megmutatta, hogy egy módosított 3d-nyomatású teknőt egy videófelvételen pisztolyként lehetett besorolni, függetlenül a teknős tájolásától. A kutatók még azt is kimutatták, hogy a közlekedési táblák csíkokkal való ellátása megváltoztathatja a tábla jelentését az autonóm járműveken futó mesterséges intelligencia számára.

Fontos megjegyezni, hogy egy támadónak általában hozzáférésre van szüksége egy neurális hálózathoz ahhoz, hogy ellenséges példákat tudjon generálni. Gyakran azonban előzetesen betanított hálózatokat használnak, ami azt jelenti, hogy a modellek könnyen elérhetők az interneten.¹⁵⁴ A legújabb kutatások

154 DAREELPIS IGAARING "PART 0" TO AGNEAT
(1 - COMPUTER VIOSDIOENLS)",
2018. JÜLIUS),
LYOTIUCSVAIRDEHYAW@17
58 online:

azt is megmutatja, hogy ellenséges példák hozhatók létre úgy, hogy először egy másik neurális hálózatot képezünk ki a célhálózat utánzására.¹⁵⁵

Ezt a gyengéséget kihasználva számos lehetséges támadás hajtható végre. A forgalomban katasztrófát okozhat, ha egy yield jelzést rosszindulatúan go jellé alakítanak át. Hasonlóképpen, egy fegyverek felismerésére létrehozott rendszert megzavarhat egy olyan fegyver, amelyet úgy terveztek, hogy egy ártalmatlanabb tárgyra hasonlítson, és a neurális hálózat annak értelmezze. A vírusirtó szoftverek észlelésére tervezett neurális hálózatok szintén sebezhetőek a támadói technikákkal készített rosszindulatú szoftverekkel szemben.¹⁵⁶ Ha egy autonóm fegyverrendszereket irányító modellt vesznek célba, az eredmény lehet, hogy civilek is megsérülnek.¹⁵⁷ Az ellenséges támadásokkal szemben ellenálló neurális hálózatok létrehozása aktív kutatási terület, ¹⁵⁸azonban amíg megbízható ellenintézkedések nem kerülnek bevezetésre, a mesterséges intelligencia egyre szélesebb körű alkalmazása új támadási vektorok előtt nyitja meg a társadalmat.

3.3.4.2. A mesterséges intelligencia rendszerek mérgezése

A mesterséges intelligencia rendszerek elleni másik támadás a mérgezéses megközelítésre épül. Ahelyett, hogy magát az algoritmust aláásnák azáltal.

¹⁵⁵ [1], [https://arxiv.org/abs/1606.02925](#).
 "Machine Hacking" (2016) arXiv Working Paper arXiv:1606.02925.
 aBpoexr, :602 027

¹⁵⁶ [1], [https://arxiv.org/abs/1606.02925](#).
 "Defenses Against Deep

Learning for Malicious Classification" (2016) arXiv Working Paper arXiv:1606.02925.

¹⁵⁷ [1], [https://arxiv.org/abs/1606.02925](#).
 Intelligence, supra note at 7120.

¹⁵⁸ [1], [https://arxiv.org/abs/1606.02925](#).
 "Adversarial Machine Learning" (2017)

Phattppe:f ,axxi : 1707 [cs, a t], online:
.vorga/ 1712.0 10

adatok vagy objektumok manipulálása a modellje szélsőértékén, a mérgezés a mesterséges intelligencia rendszer létrehozásához használt képzési adatok támadására támaszkodik. Ha ezek az adatok rossz minőségűek, az így kapott gépi tanulási rendszer nem fog megfelelően működni. Már néhány mérgezett példa hozzáadása is elegendő lehet ahhoz, hogy súlyosan károsítsa egy mesterséges intelligencia rendszer teljesítményét.¹⁵⁹ A mérgezéses támadások arra épülnek, hogy a támadóknak ellenőrzésük alatt kell tartaniuk a mesterséges intelligencia képzéséhez használt adatok egy részét. Ez sok esetben megvalósíthatatlanná teszi a támadást. A gépi tanulás nagy adatigénye miatt azonban az adatok gyakran tömegesen kerülnek átadásra. Egy másik probléma az online tanulással kapcsolatos. Ez egy gyakori megközelítés az anomália-érzékelésben. Itt a rendszert folyamatosan betanítják egy rendszerben zajló alaptevékenység elemzésére. Csak akkor veszi észre a detektor az anomáliát, ha egy esemény kívül esik ezen az alapvonalon. Ezt a támadók kihasználhatják. Idővel olyan mintákat juttathatnak be, amelyek még mindig a megengedett paramétereken belül vannak, de közel vannak a megengedett határértékekhez. Ez kiterjeszti az alapvonalat, hogy több helyzetet fedjen le. Miután egy ideig így kiterjesztették az alapvonalat, a támadók észrevétlenül indíthatják el a támadásukat.¹⁶⁰

159 <https://arxiv.org/abs/1607.07488>, "Poisoning Attacks Against Deep Learning Models", arXiv:1607.07488 [cs], hHé: 07.07.2016. URL: <https://arxiv.org/abs/1607.07488>

160 [https://www.esonline.com/articles/150719/security/hackers-get-online:](https://www.esonline.com/articles/150719/security/hackers-get-online) "A támadóknak ellenőrzésük alatt kell tartaniuk a mesterséges intelligencia képzéséhez használt adatok egy részét. Ez sok esetben megvalósíthatatlanná teszi a támadást. A gépi tanulás nagy adatigénye miatt azonban az adatok gyakran tömegesen kerülnek átadásra. Egy másik probléma az online tanulással kapcsolatos. Ez egy gyakori megközelítés az anomália-érzékelésben. Itt a rendszert folyamatosan betanítják egy rendszerben zajló alaptevékenység elemzésére. Csak akkor veszi észre a detektor az anomáliát, ha egy esemény kívül esik ezen az alapvonalon. Ezt a támadók kihasználhatják. Idővel olyan mintákat juttathatnak be, amelyek még mindig a megengedett paramétereken belül vannak, de közel vannak a megengedett határértékekhez. Ez kiterjeszti az alapvonalat, hogy több helyzetet fedjen le. Miután egy ideig így kiterjesztették az alapvonalat, a támadók észrevétlenül indíthatják el a támadásukat."

3.4. Következtetés

Ez a szakasz azt vizsgálta, hogy a rosszindulatú szereplők milyen lehetőségekkel élhetnek, ha a mesterséges intelligenciát bűnözési eszközként vagy célpontként használják. Míg a mesterséges intelligencia aktív kutatási terület, és jellemzően a kutatói közösségre korlátozódott, a demokratizálódás legújabb hulláma azt jelenti, hogy a fejlett mesterséges intelligencia-eszközök széles körben elérhetővé váltak. Ez pozitív fejlemény, amely sajnos egyben megnyitja az ajtót a bűnelkövetők előtt a mesterséges intelligencia kihasználására. Az adatokat számos online forrásból lehet megszerezni, például weboldalak feltörésével vagy a közösségi médiaplatformok személyes adatainak tömeges gyűjtésével. Az ML-közösség nyitottságának köszönhetően mind a szükséges algoritmusok, mind a szükséges készségek megtalálhatók az interneten. Az egyre nagyobb teljesítményű hardverek létrehozása grafikus kártyák formájában, valamint ezen erőforrások egyszerű online bérlésének lehetősége a rosszindulatú szereplők számára is elérhetővé teszi a mesterséges intelligencia ezen szükséges infrastruktúráit.

Sok technológiai fejlesztéshez hasonlóan a mesterséges intelligenciát is kettős felhasználás jellemzi - mind társadalmilag hasznos, mind pedig rosszindulatú célokra alkalmazható. Használható a bűncselekmények hatékonyabbá tételére. Ezt láthatjuk a social engineering és a kiberbiztonság esetében. Ezeket a támadásokat jellemzően erőforrás-igényes végrehajtani, ezért általában csak nagy értékű célpontokra vagy olyan áldozatokra korlátozódnak, amelyek vonzó nyereséget termelhetnek. Ezen szempontok némelyikének automatizálása utat nyithat a bűnöző hackerek számára, hogy egyszerre iparosíthassák és személyre szabhassák támadásaikat - ami a kapacitás aggasztó növekedését jelenti. A mesterséges intelligencia például ahhoz vezethet, hogy az adathalászatot ugyanolyan mértékben, de célzottabb módon hajtják végre, olyan e-mailek automatikus létrehozásával, amelyek

a felhasználók nagyobb valószínűséggel reagálnak. Végül pedig a kibertámadásokat automatizált módon lehet végrehajtani, a mesterséges intelligencia megjósolhatja, hogyan lehet a leghatékonyabban és a legmeghittebb módon hozzáférni egy szerverhez, és hogyan lehet a leghatékonyabban és legrejtettebben eljárni.

A mesterséges intelligencia a támadások teljesen új formáinak kifejlesztésére is lehetőséget teremt. A mesterséges intelligencia például felhasználható a felhasználó hangjának pontos szimulációjának létrehozására. Ehhez az emberek nem szoktak hozzá, ezért még mindig azt feltételezzük, hogy barátaink és rokonaink hangja valóban az övék. Ez a jövőben nem biztos, hogy így lesz. Továbbá, valóság-hűnek tűnő videókat lehet generálni egyszerűen néhány kép felhasználásával egy személy arcáról. Ezek felhasználhatók egy személy hírnevének aláírására vagy akár zsarolásra is. A mesterséges intelligencia felhasználható olyan botnetek létrehozására is, amelyek becsapják a felhasználókat, vagy félrevezetik a lakosság bizonyos nézeteinek valós mértékét. A bűnöző hackerek a mesterséges intelligenciát olyan új képességek kifejlesztésére is felhasználják majd, mint a kritikus sebezhetőségek automatikus felfedezése és a meglévő behatolásjelző rendszerek kijátszása.

Végül, a mesterséges intelligencia széles körű elterjedésével a támadások egy új osztálya jöhet létre. A mesterséges intelligencia valószínűsíti, hogy életünk egyre nagyobb része automatizálódik a közeljövőben. A mesterséges intelligencia rendszerek jelenlegi változatai továbbra is érzékenyek a mérgező támadásokra. Ez pusztító hatású lehet, például az önvezető járművek bevezetésével kapcsolatban.

Ez az értékelés továbbra is nagyrészt spekulatív, és még mindig bizonytalan, hogy az elkövetők hogyan és mikor fogják ezeket az eszközöket használni. A bűnözői csoportok azonban megbizonyították, hogy hajlandóak gyorsan átvenni az alábbiakat

az új technológiákat, ha azok új jövedelmező lehetőségeket biztosítottak számukra. Ebben az összefüggésben hogyan kellene a társadalomnak átalakítania ellenőrzési mechanizmusait, hogy minimalizálja az ebben a fejezetben felvázolt kockázatokat? A social engineering és a generációs támadások esetében ez két fő cselekvési iránynak tűnik: Ellenintézkedések és oktatás. Meg kell jegyezni, hogy ugyanazok a technológiák, amelyeket az elkövetők használhatnak, felhasználhatók e támadások felderítésére is, például mesterséges intelligencia-rendszerek képzése révén, amelyek képesek felismerni a generált hangokban vagy videóknál az enyhe akcentust. Az oktatás valószínűleg ugyanilyen fontos intézkedés lesz. A közvéleményt tudatosítani kell, hogy a régi feltételezések közül sok már nem állja meg a helyét. Például a videók hamisítottak lehetnek, és az adatokat kérő e-maileket és telefonhívásokat gépek generálhatják, hogy elválasszák őket a pénzüktől. A közelgő támadások jellegétől és mértékétől függően ez sok ember számára fájdalmas alkalmazkodási időszak lehet. Ez az alkalmazkodási folyamat a kiberbiztonság esetében még potenciálisan még fáradságosabb lesz. Már egyetlen sebezhetőség vagy támadás is több milliárd dolláros kárt okozhat. Ha a mesterséges intelligencia segítségével gyorsan sok ilyen támadás generálható, az adatszivárgások száma exponenciálisan fog növekedni.

4. MESTERSÉGES INTELLIGENCIA A BŰNÜLDÖZÉS BEN



Képzeld el, hogy 2054-et írunk. Az érintőképernyős technológia mindennapos. A hirdetések személyre szabottak és testre szabottak az ember élete, döntései, tartózkodási helye és felhasználói előzményei alapján. Az autók képesek önállóan vezetni. A háztartási gépek hanggal vezérelhetők. A biometrikus felismerés, mint például a tenyérlellyomtatás és az azonosító arcszkennelés, mindennapos. A rendőrség képes megjósolni, hogy ki az, aki valószínűleg bűncselekményt fog elkövetni, és még azelőtt elfogni az illetőt, mielőtt az elkövetné. Nem véletlen, hogy a leírás minden eleme a 2002-es *Minority Report* című amerikai sci-fi film cselekményére utal. Valójában az előző bekezdés minden leíró eleme igaz a cikk megírásának időpontjában, kivéve az évszámot és azt a kijelentést, hogy a rendőrség rendszerint elfog egy személyt, mielőtt az bűncselekményt követne el.

Amint azt az alábbiakban látni fogjuk, a bűnözők szervek világszerte elkezdtek használni a mesterséges intelligenciával működő technológiát a bűncselekmények felderítésére, sőt időnként még a bűncselekmények előrejelzésére is. Bár a technológia bünyügyi nyomozásban való felhasználásának már hosszú története van, a mesterséges intelligencia használata képes átalakítani a rendőrök és az állampolgárok közötti kapcsolatot, valamint elősegíteni a példátlan felügyeletet és társadalmi ellenőrzést. Számba vesszük a jelenleg használatos eszközöket, amelyek segítik a rendőrséget a bűncselekmények felderítésében és kivizsgálásában, és az ilyen technológiák mesterséges intelligencia-képességük alapján történő osztályozását kínáljuk. Emellett áttekintjük azokat az újonnan megjelenő eszközöket, amelyek a bűnözés előrejelzését ígérik a bűnözési gócpontok és a bűnelkövetésben valószínűleg részt

vevő személyek meghatározásával.

fegyveres erőszak. Áttekintést nyújtunk a mesterséges intelligencia által felvetett etikai kérdésekről, valamint a kormányok és a bűnüldöző szervek számára, amelyek a mesterséges intelligenciát a bűnüldözési eszköztárunkba kívánják beilleszteni. Célunk, hogy kritikusan értékeljük a mesterséges intelligenciáról gyakran feltételezett erkölcsi és technikai tekintélyt, és emberközpontú megközelítést javasolunk a mesterséges intelligencia eszközeinek a bűnüldözés általi alkalmazására.

Itt egy megjegyzés a hatókörrel kapcsolatban. Amikor a "bűnüldözés" kifejezést használjuk, akkor a belföldi rendőri szolgálatokra utalunk (amelyek egy adott joghatóságon belül elkövetett bűncselekményekre reagálnak), és e jelentés alkalmazásában ez a kifejezés külön értendő a nemzetbiztonsági, a külföldi hírszerzési vagy a közigazgatási rendészeti szervek (például a bevándorlással foglalkozó szervek) területén működő kormányzati szervektől.

4.1. AI és bűnfelderítés

A mesterséges intelligenciát a világ minden országában használják a bűncselekmények felderítésére és kivizsgálására. A bűnfelderítést úgy határozzuk meg, mint azt a tevékenységet, amelynek során megpróbáljuk megállapítani, hogy bizonyos bűncselekményeket elkövetnek-e vagy követtek-e el. A bűnfelderítés ebben a kontextusban múlt- vagy jelenorientált, míg a bűnözés előrejelzése, amelyet a fejezetben részletesebben tárgyalunk, 4.2.jövőorientált.

4.1.1. A technológia és a bűnfelderítés története

A technológia alkalmazása a megtörtént - vagy valós időben zajló - bűncselekmények észlelésére valójában megelőzi a "mesterségesen intelligens" technológia létezését. A

Vegyük például az olyan eszközök használatát, mint a videokamerák, a fizikai tereket észlelő vagy figyelő biztonsági rendszerek, a hazugságvizsgálat, a radardetektorok és a törvényszéki elemzés, beleértve a DNS-elemzésre vagy bármely más fizikai vagy fiziológiai nyomra alkalmas technológiát, amelyek mind felhasználhatók a bűncselekmény elkövetésére vonatkozó megállapítások megerősítésére. Maguk a bűnügyi helyszínek olyan fizikai terekként értelmezhetők, ahol bűncselekmény történt, és ahol a bűncselekmény bizonyítékai megtalálhatók. A bűnügyi helyszínek nem fizikai terekre is utalhatnak, ahol a bűncselekményre utaló digitális nyomok megfigyelhetők, összegyűjthetők és elemezhetők, hogy alátámasszák a bűncselekmény megtörténtének megállapítását. A digitális bűncselekmények nyomaira példaként említhetők az emberek megtévesztésére irányuló adathalász programokról szóló e-mailek, az online fórumokon folytatott viták, ahol az emberek bűncselekmény útján szerzett tárgyakat adhatnak el vagy vehetnek, vagy bűncselekmény elkövetésére irányuló szándékuk részleteit vitatják meg, a számítógépes rendszerbe betörni próbáló géphez kapcsolódó IP-cím, vagy az egér vagy a billentyűzet használati mintája. Ezek a példák természetesen korántsem teljes körűek.

A bűnügyi helyszínek - akár fizikai, akár digitális természetűek - ma már technológiában gazdag környezetként határozhatók meg,¹⁶¹ még mielőtt megvizsgálnánk, hogy a mesterséges intelligenciát milyen módon használják a bűncselekmények felderítésére. Ahogy Julie Mennell törvényszéki szakértő írja, a bűnügyi helyszíneken minden bizonnyal "rengeteg technológia" található, beleértve a technológia alábbi altípusait, amelyek:

1. A bűncselekmény elkövetésétől való elrettentés és/vagy a bűncselekmény bekövetkeztére való figyelmeztetés, például betörés esetén.

riasztások;

161 II, "The Myth of Supremacy" : An
"The Myth of Supremacy" (2012) 45
"The Myth of Supremacy" 304.

66

2. A bűncselekmény elkövetésének rögzítése, például zárt láncú televíziós rendszerek;
3. Magával a helyszínnel együtt található, és további (digitális) bizonyítékokat tartalmazhat, amelyek a bűncselekménnyel, az áldozattal vagy az elkövetővel kapcsolatosak, például mobiltelefonok vagy számítógépek;
4. A helyszínre a helyszínelő (beleértve a törvényszéki tudósokat is) által hozott eszközök, amelyek megkönnyítik a bizonyítékok felfedezését, visszaszerzését, rögzítését, elemzését és továbbítását, például digitális kamerák, lézerszkennerek, lab on a chip (LOC) technológia;
5. Segíti az áldozatok és az elkövetők azonosítását, például ujjlenyomat-felismerő és -rögzítő technológia, sőt automatikus rendszámfelismerés.¹⁶²

Ezt az információt szem előtt tartva tehát egyértelmű, hogy a mesterséges intelligencia alkalmazása a bűnüldözés által a bűncselekmények felderítésében nem feltétlenül olyan technológiai szempontból zavaró, mint amilyennek elsőre tűnhet. Más szóval, a technológiát már most is használják a bűncselekmények felderítésére. A mesterséges intelligencia egyszerűen csak egy új kiegészítése a bűnüldöző szervek által használt technológiák repertoárjának, amelyekkel megállapítható, hogy mikor történik vagy történt már meg egy bűncselekmény. A mesterséges intelligencia csupán új információfeldolgozási és elemzési kapacitásokat hoz létre más, a bűnüldözésben már rutinná vált technológiák számára.

¹⁶² Ibid.

4.1.2. A mesterséges intelligencia képességeinek taxonómiája

A bűnüldöző szervek számára a felderítési feladatokhoz rendelkezésre álló mesterséges intelligencia különböző típusait a szoftver képességei alapján lehet kategorizálni. A jelentés megírása során azonosított mesterséges intelligencia-képességtípusok a következők:

6. Tárgyak osztályozása
7. Tárgyfelismerés (beleértve az arcfelismerést is)
8. Beszédfelismerés
9. Lövésérzékelés
10. DNS-elemzés
11. Digitális kriminalisztika

A következő szakaszban a bűncselekmények felderítésére használt ilyen típusú eszközök mindegyikét ismertetjük abból a szempontból, hogy általában hogyan működnek, hogyan sorolhatók be a fenti bűnfelderítési technológiák már létező altípusaiba, valamint a bűnüldözési felhasználási forogatókönyvek szempontjából.

4.1.2.1. Tárgyak osztályozása

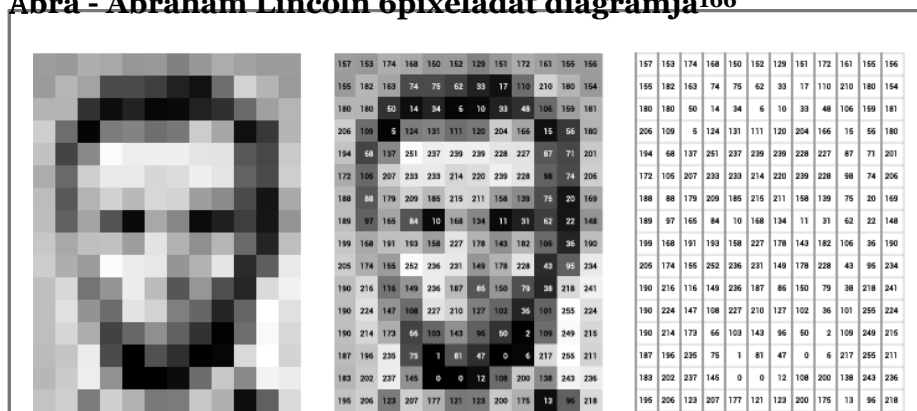
Az objektumosztályozó szoftverek célja, hogy önállóan azonosítsanak bizonyos elemeket a képeken és videókon, és az emberekhez hasonlóan címkézzék vagy kategorizálják ezeket az elemeket.¹⁶³ A tárgyak osztályozása a számítógépes látás egyik részterülete, amely a mesterséges intelligencia és az objektumosztályozás alkalmazásaként értelmezhető.

¹⁶³ UNKils CJ., *Forensic Artificial Intelligence* (Cambridge, Massachusetts: MIT Press, 2018).

intelligencia. A képi objektumokat osztályozó rendszerek azután képesek működni, hogy a kutatók egy számítógépes programot vagy algoritmikus modellt számos képből álló adathalmazon betanítanak. Ahogy ez a gépi tanulásban általában is történik, a képi elemeket kisebb részekre, például pixelekre és pixelcsoportokra rakják össze, amelyeket (gyakran kézzel) címkéznek olyan leírók alapján, mint a szín vagy a textúra.

e.¹⁶⁴ A program vagy a modell tanulási folyamata ezután egy olyan döntési fát épít fel, amely képes a régiók osztályozására a képzési készlet képein, valamint a jövőbeli képeken. A program ezt követően képes lesz a pixelcsoportok és így az objektumok osztályozására a képzési kategóriák részeként.¹⁶⁵

Ábra - Abraham Lincoln 6pixeladat diagramja¹⁶⁶



164 n, 30; "No Computer Vision", Algorithmia [b/b . . .](#)
 NBlolsqso(2 A1018), "Enga

et:
 gmaif Computer Vision p OpenFrame, ohnttpins: /openframeworks.
 ",
 cc/ofBook/chapters/image_processing_com
 puter_vision.html.

165 Ibid.

166 Levin, *ibid.*

Számtalan oka van annak, hogy a bűnüldöző szervek a bűncselekmények felderítése során miért akarják és miért használják a tárgyak osztályozását. Például:

12. A bűnüldöző szervek hozzáférhetnek egy bűncselekmény elkövetéséről készült képhez, és a gépi tanulásra támaszkodva próbálhatják azonosítani a kép készítésének vagy rögzítésének helyét. A Google PlaNet nevű programja pontosan ezt teszi, és a geolokációs képességek tekintetében a konvolúciós neurális hálózatokra támaszkodik;¹⁶⁷
13. A rendőrök a képen ábrázolt bűncselekmények esetleges meglétét is fel akarják fedezni. A kép tartalma bűncselekményt bizonyíthat (pl. a kép esetleges lopást ábrázol) és/vagy maga a kép létezése bűncselekményt valósíthat meg (pl. a kép gyermekpornográfiát ábrázol). Ez utóbbira jól ismert példa a Microsoft és Hany Farid, a Dartmouth College munkatársa által kifejlesztett PhotoDNA szoftver, amelynek elsődleges célja a gyermekpornográfia felderítése, és amely úgy működik, hogy a) létrehoz egy digitális aláírást (úgynevezett "hash"-t) a képhez kapcsolódóan, hogy megakadályozza a kép módosítását, és b) a képet fekete-fehérre konvertálja, átméretezi, rácsra bontja és számszerűsíti az árnyékolását.¹⁶⁸ Ezután összehasonlítja a kép hash értékét egy

167 <https://www.technologyreview.com/2018/04/26/414444/google-unveils-neural-network-for-geolocation/>

168 <https://www.microsoft.com/en-us/ai/photo-dna>

online exploitation", Microsoft On the Issues (12 szeptember 2018), <https://www.microsoft.com/en-us/ai/photo-dna>

a jogellenesnek minősített képek adatbázisa, és az egyezéseket emberekkel manuálisan lehet ellenőrizni.¹⁶⁹ A Microsoft azt állítja, hogy a PhotoDNA nem használható sem arcok, sem személyek vagy tárgyak felismerésére a képen belül.¹⁷⁰ A PhotoDNA-t leginkább olyan szoftveróriások használják, mint a Facebook,¹⁷¹ a Google,¹⁷² a Twitter,¹⁷³ valamint az amerikai székhelyű National Center for Missing & Exploited Children.¹⁷⁴ További példák olyan technológiákra, amelyek a bűncselekmény elkövetését igyekeznek felismerni a képeken belül, az európai P-REACT projekt,¹⁷⁵ az amerikai StopLift vállalat által kínált veszteségmegelőző termék,¹⁷⁶ valamint a kínai SenseTime szoftver.¹⁷⁷

https://www.microsoft.com/en-us/ai/photo-dna

photo-dna

¹⁶⁹ Ibid.

¹⁷⁰ Ibid.

¹⁷¹ "Microsoft's AI-powered PhotoDNA system is used by Facebook, Google, and Twitter to detect and remove child sexual abuse material (CSAM) from their platforms." (2020), <https://www.microsoft.com/en-us/ai/photo-dna>.

¹⁷² "Google removes CSAM from its services, including Gmail, YouTube, and Google Photos." (2020), <https://www.google.com/about/press/2020/04/20200420-google-removes-child-sexual-abuse-material-from-its-services/>.

¹⁷³ "Twitter uses PhotoDNA to detect and remove CSAM." (2020), <https://www.twitter.com/photo-dna>.

¹⁷⁴ "National Center for Missing & Exploited Children (NCMEC) uses PhotoDNA to detect and remove CSAM." (2020), <https://www.ncmec.org/press-releases/2020/04/20200420-ncmec-uses-photo-dna-to-detect-and-remove-child-sexual-abuse-material-from-its-services/>.

photo-dna

"National Center for Missing & Exploited Kids (Webste), <https://www.missingkids.org/supportus/partners>.

¹⁷⁵ "P-REACT: A European Union initiative to combat child sexual abuse material." (2020), <https://www.p-react.eu/>.

¹⁷⁶ "StopLift: A company that provides a cloud-based solution for detecting and removing CSAM." (2020), <https://www.stoplift.com/>.

¹⁷⁷ "SenseTime: A Chinese AI company that provides a cloud-based solution for detecting and removing CSAM." (2020), <https://www.sensetime.com/>.

SenseTime

14. A bűnüldöző szervek képfelismerő szoftvert használhatnak a bűncselekmények megállapításainak megerősítésére. Az Electronic Frontier Foundation például megállapította, hogy 2016 az amerikai Szövetségi Nyomozó Iroda olyan kutatásba fektetett be, amely képes tömegesen azonosítani és szemantikailag elemezni a tetoválásokat, hogy ne csak "segítse a bűnüldöző szerveket a bűnözők és áldozatok azonosításában"¹⁷⁸, hanem az emberek kapcsolatainak feltérképezésében és meggyőződésük azonosításában is.¹⁷⁹ Ez egy olyan feladat, amelyet emberi elemzők egyértelműen el tudnak végezni, de az ilyen automatizálás új hatékonysági szintet vezethet be a bűnügyi információk tömeges és nyilvánosan elérhető adathalmazokból történő kinyerésében.

4.1.2.2. Tárgyfelismerés (beleértve az arcfelismerést is)

A tárgyfelismerés a számítógépes látás egyik részterületének tekinthető. Ahelyett, hogy a képi elemeket egy bizonyos kategóriába sorolnánk, a tárgyfelismerés a képen belüli egyedi példányok azonosítására összpontosít.¹⁸⁰ Ilyenek például a kézzel írt betűk vagy számjegyek, rendszámok, meghatározott járművek, ujjlenyomatok és egy adott személy arca. A tárgyfelismerés ugyanúgy működik, mint az objektumosztályozás, de a legfontosabb különbség az, hogy minden egyes felismert objektumot lehet

¹⁷⁸ <https://www.fbi.gov/geoproxy/jnewsweek-tattoo>

¹⁷⁹ David Mas, "Wish List: Egy alkalmazás, amely képes felismerni a", <http://www.fbi.gov/geoproxy/jnewsweek-tattoo>, (1. 08. 2016), : 1. <http://www.fbi.gov/geoproxy/jnewsweek-tattoo>, Yeoffu. n. 1. 08. 2016. <http://www.fbi.gov/geoproxy/jnewsweek-tattoo>,

¹⁸⁰ "Detection with lines 10 of code", Towards Data Science, 2016. 08. 08. <https://towardsdatascience.com/object-detection-with-lines-of-code-10>

egyedileg azonosítható, mint saját egyedi példány, nem pedig mint objektumok osztálya. Az arcfelismerő szoftverek például a technológiától függően különböző módon működnek, de általában a következőkből állnak: (i) az arc kulcsfontosságú tájékozódási pontjainak azonosítása, mint például a személy szemei közötti távolság és a homlok és az áll közötti távolság; (ii) e geometriai méretek azonosítása egyfajta arcjelzéssé vagy arclenyomattá alakul; amelyet aztán (iii) összehasonlítanak az ismert arcok adatbázisával; és végül (iv) összevetnek egy, a szoftver adatbázisában található képpel.¹⁸¹

Számos példa van a tárgyfelismerő szoftverekre, amelyeket a bűnüldöző szervek világszerte használnak. Az egyik figyelemre méltó példa a Faception, egy izraeli székhelyű cég és szoftver névadója, amely "képes elemezni az arcokat (rögzített és élő) videofolyamokból, kamerákból vagy online/offline adatbázisokból, az arcokat saját képi leírókba kódolja, és nagy pontossággal párosítja az egyént különböző személyiségjegyekkel és típusokkal".¹⁸² A szoftvert kritika érte, mert állítólag megkönnyíti az "arcprofilozást" vagy a biológiai jellemzők alapján történő profilalkotást¹⁸³, és mert merészen azt állítja, hogy képes besorolni egy személyt "magas IQ-val" rendelkezőnek, "tudományos kutatónak", "profi pókerjátékosnak", "fehérgalléros bűnözőnek", "pedofilnak"

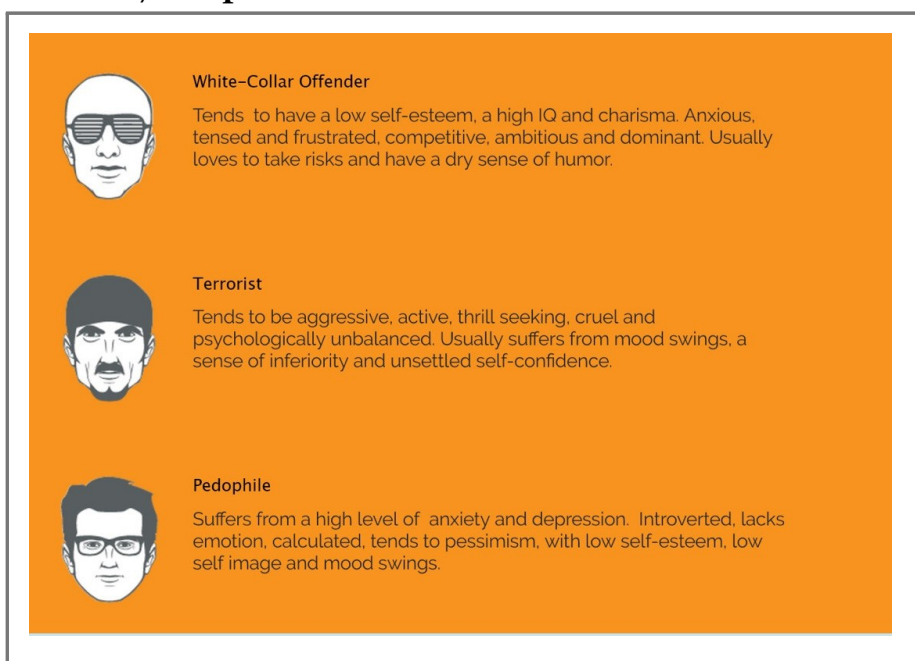
¹⁸¹ "Hogyan működnek az arcfelismerő szoftverek?", <http://www.technet.hu/arcfelismeres>, utoljára megtekintve 2016. március 10-én.

¹⁸² "Faception: a szoftver, amely képes elemezni az arcokat", <http://www.technet.hu/arcfelismeres> honlap), utoljára megtekintve 2016. március 10-én.

¹⁸³ "Faception: a szoftver, amely képes elemezni az arcokat", <http://www.technet.hu/arcfelismeres> honlap), utoljára megtekintve 2016. március 10-én.

és még "terrorista" is.¹⁸⁴ Egy olyan eszköz, mint a Faception, egyértelműen felveti a diszkrimináció lehetőségét, és egy ponton a vállalat honlapja számítógépes rajzokat tartalmazott olyan emberekről, akik az osztályozóikba tartoznak, és sztereotipikus ábrázolásokat mutatott napszemüveges fehérgalléros bűnözőkről és terroristákról, akiknek arcszörzete és fejfedője utalhat a muszlimként azonosított emberek által viselt ruhadarabokra:

Ábra - A 7Faception korábbi bűnözői ábrázolása¹⁸⁵



Az arcfelismerés nyilvános helyeken történő alkalmazásában élenjáró ország Kína. Úgy tűnik, mintha az ország szinte minden nap

184 " <https://www.7faception.com/> website, online: <https://www.7faception.com/>

185 <https://www.7faception.com/>, "It's Worse Than You Think: Robo-Profiling", Free Press, (16 March 2017), <https://www.7faception.com/stderr/7//6/its-worse-than-you201031>

az arcfelismerő technológia alkalmazását dokumentáló híradás tárgya, legyen szó akár az intelligens zárakról,¹⁸⁶ a készpénzmentes társadalom¹⁸⁷ felé való elmozdulásról vagy az arcfelismerés használatáról a fürdőszobákban.¹⁸⁸ Az ország területén szétszórtan elhelyezett mintegy egymillió 200kamerával és a 2020-ban üzembe helyezendő 400 millió további kamerával az¹⁸⁹ ország részben mesterséges intelligenciával működő CCTV megfigyelőrendszere csak egy eleme a kormánynak a társadalmi ellenőrzésre irányuló törekvésének, amelyet a szociális hitelrendszerén keresztül valósít meg.¹⁹⁰ A kínai kormány által használt számos mesterséges intelligencia-eszköz alapos ismertetése nem tartozik e jelentés tárgykörébe. Ezen eszközök megjelenését azonban érdemes megemlíteni, mivel úgy tekinthető, hogy olyan igazságszolgáltatás feletti rendszert hoznak létre, amely összevonja az illegális és az "antiszociális" viselkedést, és potenciálisan automatizálja a meghatározott deviáns viselkedés olyan mértékű felderítését és elítélését, amelyet nehéz lenne felügyelni.

186 <http://www.technology.com/2019/05/21/ai-locks/>, accessed 2019.05.21.

187 <http://www.reuters.com/article/technology-cashless/home-sfhaacriianlgr-escioteg-nxiitaioonzhthue-rfoultlu-oreuto-faccaisahl-187>

188 <http://www.asiatraveltips.com/2019/05/21/asia-times-cashless-facial-recognition/>, accessed 2019.05.21.

189 <http://www.bbc.com/news/technology-50712321>, accessed 2019.05.21.

190 <http://www.bbc.com/news/technology-50712321>, accessed 2019.05.21.

answers to

(9)

China

Shutterstock: <https://www.shutterstock.com/technologia/online/big-brother-chinas-control-ever>

Különösen a "szabálytalan járás, a számlák vagy adók késedelmes kifizetése, a túl sok alkohol vásárlása vagy a kormány ellen való felszólalások kerülnek pontokba" a polgárok társadalmi hitelpontszámából. ¹⁹¹ A magasabb pontszám olyan előnyökkel jár, mint a szállodák és bérautók kauciójának elengedése, VIP-kezelés a repülőtereken, kedvezményes hitelek, elsőbbségi álláspályázatok és a legrangosabb egyetemekre való gyorsabb bejutás. ¹⁹² A büntetések közé tartozik a repülő- vagy vonatutazás jogának elvesztése, a közösségi médiából való kizárás és a kormányzati állásokból való kizárás. ¹⁹³

Kína arcfelismerő rendszerét a Közbiztonsági Minisztérium indította el a Sanghaji székhelyű biztonsági céggel közösen fejlesztett rendszerrel 2015. ¹⁹⁴ A Forbes szerint a kínai kormány a világ egyik legnagyobb arcfelismerő adatbázisának kiépítésére törekszik. ¹⁹⁵ Egyébként a nemzeti projekt tervezett terjedelme és nagyságrendje nem volt egyértelmű. Úgy tűnik, hogy az ország arcfelismerő rendszerének átfogó célja a bűncselekményeket vagy kisebb szabálysértéseket (például szabálytalankodást vagy vécepapírlopást) elkövetett személyek azonosítása, valamint a gazdasági tranzakciók és a mindennapi életben való érintkezés hiperhatékony megkönnyítése. ¹⁹⁶ A technológiát már most is használják

¹⁹¹ J. L. ... (2018) ...

203), ... : ...
Wen ...

¹⁹² Ibid.

¹⁹³ Ibid.

¹⁹⁴ StoteipdheenntifCy henny ciCihzeinnawtiothbinusldegoindst",
(2 ... T),
httpOs: scmp .

...
... news/china/society/article/2115094/china-
TI-hreecoFganscitiinoant-idnagtaWbayses-

¹⁹⁵ ...

iFdaecniatilfyR-eacnoyg.

h h

nitioN AIs Are :/hw0ti. b eFs.

odms(1218), :

tsDecandnear/ 2018/12/17 he-amazing-amazing-

letartóztatni körözött személyeket, akik egy koncerten vettek részt, ¹⁹⁷ tévesen azonosítani és nyilvánosan megszégyeníteni egy szabálytalanul közlekedő személyt, akinek a képe valójában egy mozgó busz oldalán elhelyezett hirdetésen jelent meg, ¹⁹⁸ és elemezni az iskolások arckifejezését, hogy kiderüljön, figyelnek-e az órán. ¹⁹⁹

A kínai arcfelismerési keretrendszer jelentős vizsgálatot váltott ki az észak-amerikai és európai politikai döntéshozók és a magánélet védelmezői részéről, akik szerint a technológia sérti az egyéni polgári szabadságjogokat és az alapvető jogokat, és akik attól tartanak, hogy az ilyen mindenre kiterjedő technológia használatának normája más joghatóságokra is áttérjed. ²⁰⁰ Valóban, a

¹⁹⁶ Ibid.

¹⁹⁷ "Use of facial recognition technology to identify protesters", NHK World (2018), <https://www3.nhk.or.jp/world/story/2018/08/180828-use-facial-recognition-to-identify-protesters/>

¹⁹⁸ "China's facial recognition technology", BBC News (2018), <https://www.bbc.com/news/technology-45828128>

¹⁹⁹ "China's facial recognition technology", BBC News (2018), <https://www.bbc.com/news/technology-45828128>

²⁰⁰ "China's facial recognition technology", BBC News (2018), <https://www.bbc.com/news/technology-45828128>

¹⁹⁹ "China's facial recognition technology", BBC News (2018), <https://www.bbc.com/news/technology-45828128>

²⁰⁰ "China's facial recognition technology", BBC News (2018), <https://www.bbc.com/news/technology-45828128>

²⁰⁰ "China's facial recognition technology", BBC News (2018), <https://www.bbc.com/news/technology-45828128>

<https://www.lemonde.fr/economie/article/2017/12/09/en-chine-la-re>".

77

Decemberben az 2018 Egyesült Államok Belbiztonsági Minisztériuma nyilvánosságra hozta, hogy a titkosszolgálat az arcfelismerés használatát tervezi tesztelni a Fehér Házban és annak környékén.²⁰¹ A mesterséges intelligencia használata a tárgy- és arcfelismeréshez különösen hatékony eszköz, ha a modern utcaképeken mindenütt jelenlévő kamerahálózattal²⁰² vagy a rendőrök egyenruhájára egyre gyakrabban felvett "testkamerákkal" kombinálják, amelyek minden egyes rendőr-polgár interakciót rögzítenek.²⁰³ Ez a technológia azonban továbbra is hibaérzékeny az operatív környezetben, ahol a képeket alacsony felbontással rögzítik, és ahol az elemek és az utcabútorok is rontják az adatok minőségét.

Ezenfelül az emberek mozgása miatt a képek sokféle szögből készülnek, ami rontja az elemzés minőségét. Az Egyesült Királyságban végzett néhány valós kísérlet, amelynek eredményeit nyilvánosságra hozták, rendkívül magas téves pozitív eredményekre utal: A South

0 17), :
 erDz22760 No 3234entle hps ://www.zeit.
 ia " (2 9
 de/217/49/china-datenspeicherung-gesichtserken0
 a
 201 "Secret Surveillance" Announces Az arcfelismerés tesztje
 § m d White House", ACLU Free Future (4december
 20), da
 b
 /swecwrewt -aseclruv iocerg-a/bnlnoogu/pnrcievsa-cteyss-tte-fcahcneo-
 llance-techno
 rleocgoyg/snuitrivoeni.
 " 202 DBraivtaidinB, asarryesttC C
 illTanhceeTcealemgeraraphfo reJvuelryy 11 peoopnllienien
 ", (10 2013), :
 hps . teyghp . 2017/298 thvemillanc
 y/vfrove llcop
 203 DAianto ", TSproectbrulemW(ithNTorvuemstibnegr2
 0 18), :
 hps ://www.ieee.org/computing/software/the-trouble-with-tr
 usting-ai-to-interpret-police-bodycam-video

A walesi rendőrség az UEFA Bajnokok Ligája júniusi döntője alatt végzett arcfelismerő rendszerrel végzett kísérlete lehetséges mérkőzésekre vonatkozó figyelmeztetéseket 2,470 generált 2017, amelyek 92%-a téves volt. A londoni fővárosi rendőrség 2016-ban és 2017-ben szintén hasonló technológiát tesztelt egy utcai karnevál kezeléséhez, és 98%-os hibaarányt mértek a lehetséges gyanúsítottak azonosítása során.²⁰⁴ A fejezet utolsó alfejezetében megvizsgáljuk az arcfelismerő technológiával kapcsolatos egyéb kiemelkedő kritikákat.

4.1.2.3. Rendőrségi testkamerák

A rendőrségnek a mesterséges intelligenciával működő testkamerák használatáról szóló döntése egy másik olyan eszköz, amely előnyöket ígér, ugyanakkor számos kihívást is rejt magában. Ebben az iparágban vezető szerepet tölt be az Axon nevű amerikai vállalat, a korábban Taser International nevű, a Taser kábítófegyverről is ismert Taser International.²⁰⁵ Az Axon a márkanév váltásról és az üzletág bővítéséről szóló döntése részeként felajánlotta, hogy ingyenes testkamerákat biztosít minden érdeklődő rendőrkapitányságnak.²⁰⁶ A vállalat júniusban kijelentette, 2018 hogy a mesterséges intelligencia segítségével automatizálni kívánja a rendőrségi testkamerás videók értékelését és megjegyzéseinek elkészítését, és végül a mesterséges intelligenciának köszönhetően segíteni kívánja a rendőrök és állampolgárok közötti találkozások rögzített videóiból rendőrségi jelentések készítését.²⁰⁷ A cél az adatok automatizálása volt

²⁰⁴ u rWesse, "A Spandag UKp obrinebauu keves bizonyiték van arra, ~~---~~ d (21 - 20 - 18,

²⁰⁵ hogy ://www.s swired . dn uk/articl e/opnollicnee-ar gress hrettepns (201 8 : 20B), : : H H .

²⁰⁶ uesjudpicat.
 1
 érvelés, hogy e. Weresumed hatóság, hogy r bűncselekmény
 Patterson, Supra note
 Greene &
 Devin Coldewey, "Taser ebrands as Axo and offers free body

²⁰⁷ kamerák bármelyik rendőrkapitányságra", Tech Crunch (2017. április
 https://techcrunch.com/2017/04/05/taser-rebrands-as-axon-and-offers-free-body-cameras-to-any-police-department/
 5) online

N advances in policing", [https://www.policeone.com/police-](https://www.policeone.com/police-products/body-cameras/articles)
a products/body-cameras/articles

n
y
P
e
rr
y,
"
H
o
w
A
x
o
n
is
a
c
c
el
e
r
at
in
g
te
c
h

gyűjtés és iratkezelés, hogy a rendőrök több időt tölthessenek más feladatok elvégzésével.²⁰⁸ A vállalat azt hirdette, hogy több mint 200 000 rendőr veszi igénybe a szolgáltatásaikat, és hogy 30 petabájtnyi adatot halmoztak fel ("10-szer nagyobb, mint a Netflix adatbázisa")²⁰⁹, amelyet a többfunkciós mesterséges intelligencia rendszere elemezni fog.²¹⁰ A vállalat szabadalmat nyújtott be a valós idejű arcfelismerésre is, hogy lépést tartson versenytársaival.²¹¹

2018 áprilisában az Axon elindította az AI and Policing Technology Ethics Boardot, amely különböző területekről érkező külső erőfeszítésekből áll, és amelynek célja, hogy "szakértői iránymutatást nyújtson az Axon számára az AI-termékek és -szolgáltatások fejlesztésével kapcsolatban, különös figyelmet fordítva a közösségekre gyakorolt hatásokra".²¹² A hírek szerint a csoport évente kétszer fog összeülni, hogy megvitassa a vállalat termékeinek etikai vonatkozásait,²¹³ és a testület szerepe az, hogy őszinte, őszinte tanácsokat adjon.²¹⁴ Nem világos, hogy a testületnek milyen hatása volt, ha volt egyáltalán, az Axon termékeinek etikai fejlesztésére. De az a döntés, hogy az etika iránti elkötelezettség által fémjelzett utat választja

²⁰⁸ "The New York Times", "Axon's AI Police Software Is Being Used by 200,000 Officers", <https://www.nytimes.com/2016/04/26/us/politics/axon-ai-police-software.html>, accessed 2018-04-26.

²⁰⁹ Perry, fenti

²¹⁰ Greene & Patterson, fenti megjegyzés. 203.

²¹¹ Perry, fenti megjegyzés 207.

²¹² "Axon AI and Policing Technology Ethics Board", Axon (Weboldal), <https://www.axon.com/ai-ethics-board>.

²¹³ "Axon AI and Policing Technology Ethics Board", Axon (Weboldal), <https://www.axon.com/ai-ethics-board>.

²¹⁴ "Axon AI and Policing Technology Ethics Board", The Verge, <https://www.theverge.com/2018/4/26/17285034/axon-ai-ethics-board-arcfelismero-faji-elfogultsag>, accessed 2018-04-26. (április 26.)

<https://www.theverge.com/2018/4/26/17285034/axon-ai-ethics-board-arcfelismero-faji-elfogultsag>.

dicséretes, és néhányan azt mondták, hogy azt kívánják, hogy az olyan vállalatok, mint a Google (a DeepMind nevű mesterséges és emberi intelligencia laboratóriumának fényében) kövessék a példát, és hozzák nyilvánosságra, hogy kik ülnek az igazgatótanácsban, mit vitatnak meg, és milyen gyakran üléseznek.²¹⁵

4.1.2.4. Beszédfelismerés

A beszédfelismerés annyiban hasonlít a tárgyfelismeréshez, hogy a technológia a beszédminták sajátos elemeinek azonosítására törekszik, gyakran azzal a céllal, hogy azonosítsa a beszélő személyt és automatikusan átírja az elhangzott szavakat. Függetlenül attól, hogy pontosan milyen algoritmusokat lehet használni ebben a folyamatban, a beszédfelismerő szoftverek érzékelik és mérik a hanghullámokat és a beszédjel frekvenciamintáit. ²¹⁶ E folyamat során számos akadályt kell leküzdeni, például a háttérzajok meglétét és a beszédsebesség változásainak figyelembevételét. ²¹⁷ A szoftver ezután a beszéd kivont blokkjait vagy szakaszait különböző - és időnként többféle - technikák, például statisztikai modellek vagy mesterséges neurális hálózatok segítségével osztályozza.²¹⁸ A cél a kis szegmensek osztályozása a hangok típusa szerint, majd az egyes hangok nagyobb szegmenseinek osztályozása annak meghatározására, hogy melyik szót mondják.

²¹⁵ Liskov, G. "The Turing Test is Dead, Long Live the Turing Test." *AI Magazine* 27(2), Spring 2006. <http://www.scribd.com/doc/128091/128091-1>

²¹⁶ N. Reith, "The Turing Test is Dead, Long Live the Turing Test." *AI Magazine* 27(2), Spring 2006. <http://www.scribd.com/doc/128091/128091-1>

²¹⁷ Ibid. <http://www.scribd.com/doc/128091/128091-1>

²¹⁸ Ibid. <http://www.scribd.com/doc/128091/128091-1>

218 Ibid.

A hangfelismerés operatív felhasználására az Interpol - a Nemzetközi Bűnügyi Rendőrségi Szervezet - szolgáltató példát. A szervezet 2018 közepén részt vett a Speaker Identification Integrated Project nevű projekt végső felülvizsgálatában.²¹⁹ A technológia kibővíti a hangfelismerő szoftverek képességeit azáltal, hogy hangmintákból gyűjtést végez, azokat bizonyos viselkedési jellemzők szempontjából elemzi, és "hanglenyomatokat" hoz létre annak érdekében, hogy a rendszerébe feltöltött új hangadatok (például rendőrségi lehallgatásokból) összevethesse a gyanúsított bűnözőkről már nyilvántartott hangadatokkal.²²⁰ A technológia a hangmintákat nem, kor, nyelv és akcentus szerint is képes szűrni.²²¹ A Speaker Identification Integrated Project lehetővé teszi a minták feltöltését és letöltését a világ 192 bűnüldöző szerveitől.²²² Az adatbázis állítólag nemcsak a bűnüldöző szervektől származó mintákat tartalmaz majd, hanem "a YouTube-ról, a Facebookról, nyilvánosan rögzített beszélgetésekből, hangfelvételekből az internetprotokollban, és más olyan forrásokból is, ahol az egyének esetleg nem veszik észre, hogy a hangjukat biometrikus hangnyomatokká alakítják".²²³

4.1.2.5. Lövésérzékelés

A lövésérzékelő szoftver a lövések előfordulását igyekszik felismerni.

219 <https://www.interpol.int/Newsroom/2018/06/20/interpol-speech-recognition-technology>

220 <https://www.interpol.int/Newsroom/2018/06/20/interpol-speech-recognition-technology>

221 <https://www.interpol.int/Newsroom/2018/06/20/interpol-speech-recognition-technology>

222 <https://www.interpol.int/Newsroom/2018/06/20/interpol-speech-recognition-technology>, supra note 219.

223 Ibid.

a lövés pontos helyének meghatározására. Az akusztikus lövésérzékelő rendszerek jellemzően nagy lakott területeken elosztott mikrofonokat használnak, amelyek érzékelik és elkülönítik a lövések staccato hangjait, amelyeket aztán emberek megerősíthetnek, akik értesíthetik a bűnüldöző szerveket arról, hogy hol dördült el a lövés.²²⁴ A lövésérzékelés a mesterséges intelligencia körébe sorolható, mivel a szoftverek tervezői gépi tanulásra támaszkodnak annak érdekében, hogy betanítsák rendszereiket a lövés hangjának azonosítására és a lövés hangjának elkülönítésére a városi környezetben gyakran előforduló egyéb hangzavaroktól.²²⁵

A ShotSpotter egy amerikai székhelyű vállalat, amely az Egyesült Államokban több mint 90 városban²²⁶ kínál lövésérzékelési szolgáltatásokat, és a kanadai Toronto nagyvárosban is engedélyezték a használatát.²²⁷ A bűnüldöző szervek többször is indokolták, hogy ezt a szoftvert közterületeken használják a fegyveres erőszak visszaszorítása érdekében, különösen a környékeken.

²²⁴ "ShotSpotter, a 'Silicon Valley' gun violence detector", *Wired* (27. 2017): <http://www.wired.com/story/how-shotspotter-works-microphones/>.

²²⁵ "How ShotSpotter works: artificial intelligence-based gun video", *Phys.org* (7. 2017): <http://phys.org/news/2017-07-artificial-intelligence-based-gun-video.html>.

²²⁶ "ShotSpotter, a 'Silicon Valley' gun violence detector", *Wired* (27. 2017): <http://www.wired.com/story/how-shotspotter-works-microphones/>.

²²⁷ "ShotSpotter, a 'Silicon Valley' gun violence detector", *Wired* (27. 2017): <http://www.wired.com/story/how-shotspotter-works-microphones/>.

ahol a lövések gyakran előfordulnak (és nem feltétlenül hívják ki a rendőrséget), vagy ahol a polgárok megfélemlítettnek érezhetik magukat, és inkább elkerülik a rendőrséggel való interakciót.²²⁸

Egy másik példa a lövésérzékelő szoftverre - bár ez nem tartozik e jelentés tárgykörébe - a Boomerang III, az Egyesült Államok Védelmi Minisztériuma által a hadseregben való használatra kifejlesztett rendszer. Az online leírása szerint "a Boomerang pontosan meghatározza a lövész helyét a bejövő kézfegyveres lövéseknél. A Boomerang passzív akusztikus érzékelést és számítógépes jelfeldolgozást használ, hogy kevesebb mint egy másodperc alatt lokalizálja a lövést".²²⁹ Még ha ezt a technológiát eddig csak háborús környezetben alkalmazták is, a rendőrség militarizálódásának számos nyugati demokráciában megfigyelhető tendenciája ahhoz vezethet, hogy a magas gyilkossági rátával szembesülő rendvédelmi szervek gyorsan átveszik.²³⁰

4.1.1.2.6. DNS-elemzés

A DNS-elemzés a legtágabb értelemben a genetikai vizsgálatok bűnügyi és jogi célú alkalmazását jelenti.²³¹

228

"ShorootSnptotpteorl? orGbeNvgun shoJut
 iedRgpp rWovhead iE, (Ø)
 e:
 r ohnttpins: /globalnews.ca/news/4/controversial-gunshot-
 detector344093
 AgnsporttWtoithrShooptopicte/r; " 23DmMö
 ", (Ø) 5 (Ø),
 ImpN/e/wxtwDwe. csahdoets p 6 contpVdes es/Scehpicteamgob-esirgns- 23-
 :
 monilliinoen
 hotspotter-to
 exndeginsygechreningdetecionxte-ndte-cwaidthe-/s.
 229 " nognliInI: State-of-the-Art Shooter Detection", Raytheon
 (Ø) e:
 230 Phetttpesr: Bw KkayhM
 . "

ctIsts/broeolemvearnacneg.
tamiza/diaprabandeps/plondu to 21st
Gen tury police", (2007)1 : 4Policing: A Journal of Policy and
50 . Practice

A DNS törvényszéki anyagként való felhasználása a törvényszéki tudomány egyik ága, amely a genetikai anyagot vizsgálja a bűnügyi nyomozás során. A legkézenfekvőbb ok, amiért a bűnöző szervek genetikai anyagot akarnak gyűjteni és elemezni egy bűncselekmény helyszínén, az az, hogy meg akarják határozni, ki volt jelen az állítólagos bűncselekmény elkövetésekor, mi lehetett a szerepük az összetűzésben, hol történt a bűncselekmény, és hogy az eset szereplői (áldozat, tanú vagy gyanúsított) kapcsolatba hozhatók-e korábbi megoldott vagy megoldatlan bűncselekményekkel.

A mesterséges intelligencia azért játszik szerepet a DNS-elemzésben, mert az általa kínált új képességek jelentősen felgyorsítják a DNS-szekvencia egyeztetési folyamatot, amelynek során a begyűjtött DNS-t összevetik az adott adatbázisban található DNS-sel. Vegyük például a kaliforniai rendőrség 2018-as döntését, miszerint a kereskedelmi genealógiai weboldalak által tárolt DNS-adatokat használta.²³² Ebben az esetben a bűnöző szervek megtaláltak és letartóztattak egy személyt, akit többrendbeli nemi erőszakkal és gyilkossággal vádoltak, és a jelek szerint feltöltötték a vádlott DNS-adatait a GEDMatch weboldalra.²³³ A DNS-t egy bűncselekmény helyszínéről nyerték, és a rendőrség állítólag arra használta fel, hogy megtalálja az egyik rokonát.²³⁴ Nem volt egyértelmű, hogy a rendőrség engedélyt kapott-e a cégtől arra, hogy feltöltse a vádlott DNS-ét, és összehasonlítsa azt a

231 "We cannot find a genetic testing company that is willing to provide a DNA test to a law enforcement agency." <https://www.foxnews.com/tech/2018/04/27/california-police-use-genealogy-dna-database-identify-suspect/>

232 "The police used a genealogy website to find a suspect in a case involving a woman's DNA." <https://www.foxnews.com/tech/2018/04/27/california-police-use-genealogy-dna-database-identify-suspect/>

2018, "Genealogy: A State-Sponsored 'Genealogy' Project", MIT Technology Review (április 27.)

<https://www.foxnews.com/tech/2018/04/27/california-police-use-genealogy-dna-database-identify-suspect/>

233 Ibid.

searched

234 Ibid.

és kérdéses, hogy a bűncselekmény elkövetője által elhagyott DNS alkotmányos védelemben részesül-e az Egyesült Államokban.²³⁵ Az ehhez hasonló esetek megkérdőjelezzik, hogy a bűnüldöző szerveknek bírósági engedélyt kellene-e kérniük arra, hogy feltöltsék az elkövetők genetikai anyagát a genealógiai és DNS-elemző honlapra. Továbbá nem világos, hogy a bűnüldözésnek szabad-e olyan algoritmusokra támaszkodnia, amelyek magáncégek tulajdonát képezik, és amelyek nem szabadok és nyílt forráskódúak, és így nem mentesülnek a technikai és jogi ellenőrzés alól. Míg az elkövető által a tetthelyen elhagyott DNS magánéletével kapcsolatban kevés jogi védelem állhat fenn, addig azoknak a rendőri szervezeteknek, amelyek esetleg érdekeltek a mesterséges intelligencia alapú DNS-illesztési és -elemzési eszközök használatában, mérlegelniük kellene, hogy nem sértik-e az összes többi olyan ember magánélethez való jogát, akiknek a DNS-ét az adott adatbázisban tárolják.

4.1.2.7. Digitális kriminallisztika

A digitális helyszínelés, más néven számítógépes helyszínelés az elektronikus eszközökben található digitális anyagok kinyerése és elemzése, hogy azokból bizonyítékot nyerjenek. Számos olyan eszköz létezik, amely átfésüli a számítógépeket, mobilkészülékeket és szoftvereket, és olyan adatokat keres, amelyek terhelő bizonyítékokat tartalmazhatnak. A mesterséges intelligencia azért lényeges ebben a kérdésben, mert növeli a digitális törvényszéki elemző eszközök képességeit, amelyek hatalmas mennyiségű adatot generáltak, amelyek feldolgozására az embernek nincs meg a kognitív képessége ésszerű idő alatt.

Az egyik legfontosabb példa erre a Magnet AXIOM nevű szoftver, amelyet a kanadai Waterloo-i székhelyű Magnet Forensics készített. Az eszköz neve

²³⁵ Ibid.

"egy olyan digitális nyomozati platform, amely lehetővé teszi a vizsgáló számára, hogy okostelefonokról és számítógépekről szerezze be és vizsgálja meg a releváns adatokat, és a jobb elemzés érdekében vizualizálja azokat."²³⁶ A szoftver egyik fő jellemzője a Magnet.AI használata, amely gépi tanulást használ az okostelefonokon, számítógépeken és csevegőalkalmazásokon folytatott beszélgetések szemantikai vagy kontextuális tartalomelemzésére.²³⁷ A vállalat állítása szerint az eszközt a gyermekek kizsákmányolásának eseteire optimalizálták, és arra törekszik, hogy kategorizálja és megjelölje a beszélgetésekben szereplő olyan nyelvezetet, amely gyermekcsábításnak minősülhet.²³⁸ A vállalat külön kiemeli, hogy ez az eszköz meg fogja változtatni a rendőrség kihallgatásainak és letartóztatási eljárásainak módját.²³⁹

4.2. AI a bűnözés előrejelzéséhez és megelőzéséhez

A mesterséges intelligenciát azzal a céllal is fejlesztik, hogy előre jelezzék és megelőzzék a bűncselekményeket, és ne csak azt észleljék, ami már megtörtént vagy kibontakozóban van. Érdekes módon a technológia alkalmazása a bűncselekmények jövőbeli előfordulásának előrejelzésére nem újdonság. Gondoljunk csak az erőszak kockázatának felmérésére szolgáló eszközök használatára a büntető igazságszolgáltatásban és az igazságügyi pszichiátriában. Egy tanulmány kimutatta, hogy számos joghatóságban több mint 200 eszköz áll rendelkezésre a kezdeti ítélethozatal, a feltételes szabadlábra helyezés, valamint a szabadulás utáni megfigyeléssel és rehabilitációval kapcsolatos döntések megalapozására, de még ott is nagyon kevés 2017 volt a

236

" aBgneteatkiFtorWenesbicsstelandMesaMag et. fight
 Análízis rM, () (1) (2017), d

h .com/magnet-forensics-indít-mágnes-ai-tai-harcra-
 d

237 Ibid.

238 Fontemoluccs n Magnet : n eLlan ing to Work for
 ; A nPist (M), :

239 Ibid.

releváns, megbízható és elfogulatlan adatok, amelyek bizonyíthatják az ilyen igazságügyi pszichiátriai adatok előrejelzési pontosságát.²⁴⁰

Ezen eszközök közül sok még fejlesztés alatt áll, és úgy tekinthetjük, hogy ezek olyan technológiák, amelyek ígéretesek, de még nem elég érettek ahhoz, hogy kereskedelmi forgalomba kerüljenek. Az egyik jelentős, ezen a területen szolgáltatásokat kínáló vállalat a PredPol, egy amerikai székhelyű cég, amely "a Los Angeles-i Rendőrség és az UCLA közötti kutatási projektből nőtt ki".²⁴¹ A vállalat azt állítja magáról, hogy "piacvezető a prediktív rendfenntartás területén", és arra törekszik, hogy azonosítsa azokat az időpontokat és helyszíneket, ahol bizonyos bűncselekmények a legnagyobb valószínűséggel történnek, hogy ezeken a területeken járőrözve megelőzze a bűncselekmények bekövetkezését.²⁴² A vállalat azt állítja, hogy szabadalmaztatta algoritmusát, amely az elkövetők viselkedésének három aspektusának statisztikai elemzésén alapul: 1) Ismétlődő áldozattá válás (röviden, a vállalat feltételezi, hogy ahol egy bűncselekmény történt, ott nagyobb a valószínűsége, hogy nem sokkal később egy másik bűncselekmény is megtörténik), 2) Közeli ismétlődő áldozattá válás (amely feltételezi, hogy a bűncselekmények egymáshoz közel történnek), 3) Helyi keresés (amely ismét feltételezi, hogy a bűncselekmények hajlamosak csoportosulni). Ezt az algoritmust részben azok a statisztikai modellek ihlették, amelyeket a földrengések utóregéseinek előrejelzésére használnak.²⁴³

240 .
 sDesosumgelanst tjo oPlsuginh i nSju tiScaevaunledscfour eannscic Sp jly:

"

Rllrke

p enttcebri " (2 017) 42 134, online:

:fwb . rdn n h. g/ p548162.

" ic , p (M) online:

241 Htper: ww . . c t/.

242 Ibid.

243 AlelaerxnaingearlgBoarbituhtmas MapDevalio& n-

eLReginailk , "
Cmharkisintign: , et al.

e gundiny kihívások" (2018) Whitehall Reports (21szeptember), at
5,
: <https://rusi.org/publication/whitehall-reports/machine-learning->

A technológia különbözik attól, amit más amerikai városokban fejlesztettek ki, például Chicagóban, ahol a stratégiai alanylista algoritmikus vagy valószínűségi alapon igyekszik meghatározni, hogy ki a legvalószínűbb elkövető vagy áldozat a jövőbeni lövöldözésekben.²⁴⁴ A PredPol nem értékeli, hogy ki fogja valószínűleg elkövetni a bűncselekményt, de ennek ellenére kritika érte, hogy a gépi tanulást, a Los Angeles-i rendőrség bűnügyi adatait és egy elavult bandaterületi térképet használ a "bandákkal kapcsolatos" bűncselekmények osztályozásának automatizálására.²⁴⁵ Ez a kombináció olyan visszacsatolási hurkot hozhat létre, amelyben bizonyos környékeket vagy embercsoportokat bűnözőnek bélyegeznek.²⁴⁶ Emellett egy francia folyóiratban megjelent cikkben a PredPol algoritmust befolyásoló szeizmográfiai algoritmus eredeti tervezőjét felkérték, hogy tesztelje modelljének alkalmazhatóságát a chicagói bűnügyi adatokon, és komolyan megkérdőjelezte az eszköznek a bűnözési minták előrejelzésére való átvihetőségét. Az ilyen megközelítés által generált kimenet nem tűnik sokkal hatékonyabbnak a jövőbeli bűncselekmények helyének előrejelzésében, mint a hagyományos hotspot-térképek.²⁴⁷

²⁴⁴ <https://www.nytimes.com/2015/06/13/us/politics/predictive-policing-chicago.html>, "Predictive Policing in Chicago", The New York Times (13 június 2015).

hat Tries to Predict Violence in Chicago", The New York Times (13 június 2015).

²⁴⁵ <https://www.nytimes.com/2015/06/13/us/politics/predictive-policing-chicago.html>, "Predictive Policing in Chicago", The New York Times (13 június 2015).

²⁴⁶ <https://www.nytimes.com/2015/06/13/us/politics/predictive-policing-chicago.html>, "Predictive Policing in Chicago", The New York Times (13 június 2015).

²⁴⁷ <https://www.nytimes.com/2015/06/13/us/politics/predictive-policing-chicago.html>, "Predictive Policing in Chicago", The New York Times (13 június 2015).

<https://www.nytimes.com/2015/06/13/us/politics/predictive-policing-chicago.html>, "Predictive Policing in Chicago", The New York Times (13 június 2015).

²⁴⁷ Bilel Benbouzid, "À qui profite le crime? Le marché de la prediction du crime aux États-Unis" (2016) La Vie des Idées, online a <https://laviedesidees.fr/A-qui-profite-le-crime.html>.
következő címen: La Vie des Idées.

Amint azt a PredPolhoz hasonló vállalatok munkája is mutatja, egyre növekvő és nagyrészt szabályozatlan piac van a bűnüldöző szerveket a bűncselekmények előrejelzésében segíteni kívánó szoftverek számára. A bűncselekmények elkövetését előrejelző eszközöket alkalmazni kívánó rendőri szervezeteknek óvatosan kell eljárniuk, és a lehető legtöbb információt kell beszerezniük a használni kívánt eszközök pontosságáról, mielőtt erőforrásokat fordítanak rájuk.

4.3. Következtetés: A szakirodalom hiányosságai és etikai aggályok

Ez a szakasz a mesterséges intelligencia bűnüldöző szervek általi felhasználását igyekezett megvilágítani. Bemutatjuk, hogy a bűnügyi elemzésben a segédtechnológiának van történelmi analógiája. Hasznos felismerni a jelenleg alkalmazott taktikák taxonómiáját, például a hangokat, tárgyakat, arcokat és DNS-t elemző szoftverek bevetését, valamint a bűncselekmények digitális nyomainak feltárását, amelyek magukban a technológiai eszközökben találhatóak. Továbbra is kialakulóban van az olyan eszközök szabályozatlan piaca, amelyek gépi tanulást használnak a bűnözés "gócpontjainak" és a bűnözés egyéb elemeinek előrejelzésére.

Mégis számos megválaszolatlan kérdés maradt azzal kapcsolatban, hogy a mesterséges intelligencia milyen hatással lehet a bűnüldözés bűnüldözésre adott válaszára. Hannah és Fry matematikus, valamint Alexander Babuta, Marion Oswald és Christine Rinik kutatók munkájára támaszkodunk, hogy útmutatást adjunk a mesterséges intelligencia alkalmazását fontolgató bűnüldöző szervek döntéseinek meghozatalához. Számos olyan kérdést is felvetünk, amelyek rámutatnak arra, hogy a mesterséges intelligencia túl széles körű alkalmazását gondosan meg kell vizsgálni, megmutatva, hogy vannak olyan esetek, amikor a mesterséges intelligencia előnyei látszólag meghaladják a költségeit, és fordítva, a mesterséges intelligencia alkalmazása más helyzetekben valójában jelentős

kihívásokat jelent.

90

amelyeket még le kell küzdeni. Arra ösztönözzük a bűnüldöző szerveket és a kormányokat, hogy határozzák meg és egyértelműen jelentsék ki a mesterséges intelligencia alkalmazását alátámasztó prioritásokat. Számos megoldás áll azon kormányok rendelkezésére, amelyek bűnüldöző szervei mesterséges intelligenciát kívánnak alkalmazni, és ezekhez proaktív szabályozásra van szükség, amelyet az átláthatóságra, a felügyeleti rendszerekre és az interdiszciplináris együttműködésre vonatkozó minimumszabályok iránti elkötelezettséggel kell kiegészíteni.

4.3.1. A mesterséges intelligenciával kapcsolatos kérdések feltérképezése a bűnüldözésben

Hannah Fry brit matematikus, a számítástechnika és az emberi viselkedés szakértője számos etikai problémát azonosított, amelyeket a mesterséges intelligencia bűnügyi elemzésre való felhasználása vet fel. Szakértői véleménye szerint a mesterségesen intelligens algoritmusok szükségszerűen hibáznak, és vannak olyan esetek, amikor igazságtalanok lesznek.²⁴⁸ A mesterséges intelligenciának a büntető igazságszolgáltatási rendszerre gyakorolt minden pozitív hatása mellett is mindig lesznek végtelen példák az algoritmusok által okozott igazságtalanságokra. Gondoljunk csak arra a tényre, hogy a stratégiai célpontlistát eredetileg a fegyveres bűncselekmények áldozatainak segítésére szánták, de végül a rendőrség "halállistaként" használta a fegyveres erőszakot elkövetők üldözésére.²⁴⁹ Azzal, hogy felismerjük a tervezők elkerülhetetlen tökéletlenségét és tudattalan elfogultságának megismétlődését, csökkentjük azt a feltételezést, hogy egy algoritmikus eszköz veleszületett, szenvedélytelen tekintéllyel rendelkezik.

Az algoritmikus eszközök számos módon lehetnek szükségtelenek vagy tisztességtelenek, amikor a bűnüldözés alkalmazza őket, ami megkérdőjelezi, hogy hogyan és mikor kell használni a mesterséges intelligenciát. A mesterséges intelligencia bűnüldözési célú alkalmazása mellett szóló érvek

feltételezhetik, hogy a mesterséges intelligencia alkalmazása és a bűnözés csökkenése között okozati összefüggés áll fenn.

248 ~~Harvard Law Review~~, ~~116~~ ~~1209~~ ~~1211~~ ~~1213~~ ~~1215~~ ~~1217~~ ~~1219~~ ~~1221~~ ~~1223~~ ~~1225~~ ~~1227~~ ~~1229~~ ~~1231~~ ~~1233~~ ~~1235~~ ~~1237~~ ~~1239~~ ~~1241~~ ~~1243~~ ~~1245~~ ~~1247~~ ~~1249~~ ~~1251~~ ~~1253~~ ~~1255~~ ~~1257~~ ~~1259~~ ~~1261~~ ~~1263~~ ~~1265~~ ~~1267~~ ~~1269~~ ~~1271~~ ~~1273~~ ~~1275~~ ~~1277~~ ~~1279~~ ~~1281~~ ~~1283~~ ~~1285~~ ~~1287~~ ~~1289~~ ~~1291~~ ~~1293~~ ~~1295~~ ~~1297~~ ~~1299~~ ~~1301~~ ~~1303~~ ~~1305~~ ~~1307~~ ~~1309~~ ~~1311~~ ~~1313~~ ~~1315~~ ~~1317~~ ~~1319~~ ~~1321~~ ~~1323~~ ~~1325~~ ~~1327~~ ~~1329~~ ~~1331~~ ~~1333~~ ~~1335~~ ~~1337~~ ~~1339~~ ~~1341~~ ~~1343~~ ~~1345~~ ~~1347~~ ~~1349~~ ~~1351~~ ~~1353~~ ~~1355~~ ~~1357~~ ~~1359~~ ~~1361~~ ~~1363~~ ~~1365~~ ~~1367~~ ~~1369~~ ~~1371~~ ~~1373~~ ~~1375~~ ~~1377~~ ~~1379~~ ~~1381~~ ~~1383~~ ~~1385~~ ~~1387~~ ~~1389~~ ~~1391~~ ~~1393~~ ~~1395~~ ~~1397~~ ~~1399~~ ~~1401~~ ~~1403~~ ~~1405~~ ~~1407~~ ~~1409~~ ~~1411~~ ~~1413~~ ~~1415~~ ~~1417~~ ~~1419~~ ~~1421~~ ~~1423~~ ~~1425~~ ~~1427~~ ~~1429~~ ~~1431~~ ~~1433~~ ~~1435~~ ~~1437~~ ~~1439~~ ~~1441~~ ~~1443~~ ~~1445~~ ~~1447~~ ~~1449~~ ~~1451~~ ~~1453~~ ~~1455~~ ~~1457~~ ~~1459~~ ~~1461~~ ~~1463~~ ~~1465~~ ~~1467~~ ~~1469~~ ~~1471~~ ~~1473~~ ~~1475~~ ~~1477~~ ~~1479~~ ~~1481~~ ~~1483~~ ~~1485~~ ~~1487~~ ~~1489~~ ~~1491~~ ~~1493~~ ~~1495~~ ~~1497~~ ~~1499~~ ~~1501~~ ~~1503~~ ~~1505~~ ~~1507~~ ~~1509~~ ~~1511~~ ~~1513~~ ~~1515~~ ~~1517~~ ~~1519~~ ~~1521~~ ~~1523~~ ~~1525~~ ~~1527~~ ~~1529~~ ~~1531~~ ~~1533~~ ~~1535~~ ~~1537~~ ~~1539~~ ~~1541~~ ~~1543~~ ~~1545~~ ~~1547~~ ~~1549~~ ~~1551~~ ~~1553~~ ~~1555~~ ~~1557~~ ~~1559~~ ~~1561~~ ~~1563~~ ~~1565~~ ~~1567~~ ~~1569~~ ~~1571~~ ~~1573~~ ~~1575~~ ~~1577~~ ~~1579~~ ~~1581~~ ~~1583~~ ~~1585~~ ~~1587~~ ~~1589~~ ~~1591~~ ~~1593~~ ~~1595~~ ~~1597~~ ~~1599~~ ~~1601~~ ~~1603~~ ~~1605~~ ~~1607~~ ~~1609~~ ~~1611~~ ~~1613~~ ~~1615~~ ~~1617~~ ~~1619~~ ~~1621~~ ~~1623~~ ~~1625~~ ~~1627~~ ~~1629~~ ~~1631~~ ~~1633~~ ~~1635~~ ~~1637~~ ~~1639~~ ~~1641~~ ~~1643~~ ~~1645~~ ~~1647~~ ~~1649~~ ~~1651~~ ~~1653~~ ~~1655~~ ~~1657~~ ~~1659~~ ~~1661~~ ~~1663~~ ~~1665~~ ~~1667~~ ~~1669~~ ~~1671~~ ~~1673~~ ~~1675~~ ~~1677~~ ~~1679~~ ~~1681~~ ~~1683~~ ~~1685~~ ~~1687~~ ~~1689~~ ~~1691~~ ~~1693~~ ~~1695~~ ~~1697~~ ~~1699~~ ~~1701~~ ~~1703~~ ~~1705~~ ~~1707~~ ~~1709~~ ~~1711~~ ~~1713~~ ~~1715~~ ~~1717~~ ~~1719~~ ~~1721~~ ~~1723~~ ~~1725~~ ~~1727~~ ~~1729~~ ~~1731~~ ~~1733~~ ~~1735~~ ~~1737~~ ~~1739~~ ~~1741~~ ~~1743~~ ~~1745~~ ~~1747~~ ~~1749~~ ~~1751~~ ~~1753~~ ~~1755~~ ~~1757~~ ~~1759~~ ~~1761~~ ~~1763~~ ~~1765~~ ~~1767~~ ~~1769~~ ~~1771~~ ~~1773~~ ~~1775~~ ~~1777~~ ~~1779~~ ~~1781~~ ~~1783~~ ~~1785~~ ~~1787~~ ~~1789~~ ~~1791~~ ~~1793~~ ~~1795~~ ~~1797~~ ~~1799~~ ~~1801~~ ~~1803~~ ~~1805~~ ~~1807~~ ~~1809~~ ~~1811~~ ~~1813~~ ~~1815~~ ~~1817~~ ~~1819~~ ~~1821~~ ~~1823~~ ~~1825~~ ~~1827~~ ~~1829~~ ~~1831~~ ~~1833~~ ~~1835~~ ~~1837~~ ~~1839~~ ~~1841~~ ~~1843~~ ~~1845~~ ~~1847~~ ~~1849~~ ~~1851~~ ~~1853~~ ~~1855~~ ~~1857~~ ~~1859~~ ~~1861~~ ~~1863~~ ~~1865~~ ~~1867~~ ~~1869~~ ~~1871~~ ~~1873~~ ~~1875~~ ~~1877~~ ~~1879~~ ~~1881~~ ~~1883~~ ~~1885~~ ~~1887~~ ~~1889~~ ~~1891~~ ~~1893~~ ~~1895~~ ~~1897~~ ~~1899~~ ~~1901~~ ~~1903~~ ~~1905~~ ~~1907~~ ~~1909~~ ~~1911~~ ~~1913~~ ~~1915~~ ~~1917~~ ~~1919~~ ~~1921~~ ~~1923~~ ~~1925~~ ~~1927~~ ~~1929~~ ~~1931~~ ~~1933~~ ~~1935~~ ~~1937~~ ~~1939~~ ~~1941~~ ~~1943~~ ~~1945~~ ~~1947~~ ~~1949~~ ~~1951~~ ~~1953~~ ~~1955~~ ~~1957~~ ~~1959~~ ~~1961~~ ~~1963~~ ~~1965~~ ~~1967~~ ~~1969~~ ~~1971~~ ~~1973~~ ~~1975~~ ~~1977~~ ~~1979~~ ~~1981~~ ~~1983~~ ~~1985~~ ~~1987~~ ~~1989~~ ~~1991~~ ~~1993~~ ~~1995~~ ~~1997~~ ~~1999~~ ~~2001~~ ~~2003~~ ~~2005~~ ~~2007~~ ~~2009~~ ~~2011~~ ~~2013~~ ~~2015~~ ~~2017~~ ~~2019~~ ~~2021~~ ~~2023~~ ~~2025~~ ~~2027~~ ~~2029~~ ~~2031~~ ~~2033~~ ~~2035~~ ~~2037~~ ~~2039~~ ~~2041~~ ~~2043~~ ~~2045~~ ~~2047~~ ~~2049~~ ~~2051~~ ~~2053~~ ~~2055~~ ~~2057~~ ~~2059~~ ~~2061~~ ~~2063~~ ~~2065~~ ~~2067~~ ~~2069~~ ~~2071~~ ~~2073~~ ~~2075~~ ~~2077~~ ~~2079~~ ~~2081~~ ~~2083~~ ~~2085~~ ~~2087~~ ~~2089~~ ~~2091~~ ~~2093~~ ~~2095~~ ~~2097~~ ~~2099~~ ~~2101~~ ~~2103~~ ~~2105~~ ~~2107~~ ~~2109~~ ~~2111~~ ~~2113~~ ~~2115~~ ~~2117~~ ~~2119~~ ~~2121~~ ~~2123~~ ~~2125~~ ~~2127~~ ~~2129~~ ~~2131~~ ~~2133~~ ~~2135~~ ~~2137~~ ~~2139~~ ~~2141~~ ~~2143~~ ~~2145~~ ~~2147~~ ~~2149~~ ~~2151~~ ~~2153~~ ~~2155~~ ~~2157~~ ~~2159~~ ~~2161~~ ~~2163~~ ~~2165~~ ~~2167~~ ~~2169~~ ~~2171~~ ~~2173~~ ~~2175~~ ~~2177~~ ~~2179~~ ~~2181~~ ~~2183~~ ~~2185~~ ~~2187~~ ~~2189~~ ~~2191~~ ~~2193~~ ~~2195~~ ~~2197~~ ~~2199~~ ~~2201~~ ~~2203~~ ~~2205~~ ~~2207~~ ~~2209~~ ~~2211~~ ~~2213~~ ~~2215~~ ~~2217~~ ~~2219~~ ~~2221~~ ~~2223~~ ~~2225~~ ~~2227~~ ~~2229~~ ~~2231~~ ~~2233~~ ~~2235~~ ~~2237~~ ~~2239~~ ~~2241~~ ~~2243~~ ~~2245~~ ~~2247~~ ~~2249~~ ~~2251~~ ~~2253~~ ~~2255~~ ~~2257~~ ~~2259~~ ~~2261~~ ~~2263~~ ~~2265~~ ~~2267~~ ~~2269~~ ~~2271~~ ~~2273~~ ~~2275~~ ~~2277~~ ~~2279~~ ~~2281~~ ~~2283~~ ~~2285~~ ~~2287~~ ~~2289~~ ~~2291~~ ~~2293~~ ~~2295~~ ~~2297~~ ~~2299~~ ~~2301~~ ~~2303~~ ~~2305~~ ~~2307~~ ~~2309~~ ~~2311~~ ~~2313~~ ~~2315~~ ~~2317~~ ~~2319~~ ~~2321~~ ~~2323~~ ~~2325~~ ~~2327~~ ~~2329~~ ~~2331~~ ~~2333~~ ~~2335~~ ~~2337~~ ~~2339~~ ~~2341~~ ~~2343~~ ~~2345~~ ~~2347~~ ~~2349~~ ~~2351~~ ~~2353~~ ~~2355~~ ~~2357~~ ~~2359~~ ~~2361~~ ~~2363~~ ~~2365~~ ~~2367~~ ~~2369~~ ~~2371~~ ~~2373~~ ~~2375~~ ~~2377~~ ~~2379~~ ~~2381~~ ~~2383~~ ~~2385~~ ~~2387~~ ~~2389~~ ~~2391~~ ~~2393~~ ~~2395~~ ~~2397~~ ~~2399~~ ~~2401~~ ~~2403~~ ~~2405~~ ~~2407~~ ~~2409~~ ~~2411~~ ~~2413~~ ~~2415~~ ~~2417~~ ~~2419~~ ~~2421~~ ~~2423~~ ~~2425~~ ~~2427~~ ~~2429~~ ~~2431~~ ~~2433~~ ~~2435~~ ~~2437~~ ~~2439~~ ~~2441~~ ~~2443~~ ~~2445~~ ~~2447~~ ~~2449~~ ~~2451~~ ~~2453~~ ~~2455~~ ~~2457~~ ~~2459~~ ~~2461~~ ~~2463~~ ~~2465~~ ~~2467~~ ~~2469~~ ~~2471~~ ~~2473~~ ~~2475~~ ~~2477~~ ~~2479~~ ~~2481~~ ~~2483~~ ~~2485~~ ~~2487~~ ~~2489~~ ~~2491~~ ~~2493~~ ~~2495~~ ~~2497~~ ~~2499~~ ~~2501~~ ~~2503~~ ~~2505~~ ~~2507~~ ~~2509~~ ~~2511~~ ~~2513~~ ~~2515~~ ~~2517~~ ~~2519~~ ~~2521~~ ~~2523~~ ~~2525~~ ~~2527~~ ~~2529~~ ~~2531~~ ~~2533~~ ~~2535~~ ~~2537~~ ~~2539~~ ~~2541~~ ~~2543~~ ~~2545~~ ~~2547~~ ~~2549~~ ~~2551~~ ~~2553~~ ~~2555~~ ~~2557~~ ~~2559~~ ~~2561~~ ~~2563~~ ~~2565~~ ~~2567~~ ~~2569~~ ~~2571~~ ~~2573~~ ~~2575~~ ~~2577~~ ~~2579~~ ~~2581~~ ~~2583~~ ~~2585~~ ~~2587~~ ~~2589~~ ~~2591~~ ~~2593~~ ~~2595~~ ~~2597~~ ~~2599~~ ~~2601~~ ~~2603~~ ~~2605~~ ~~2607~~ ~~2609~~ ~~2611~~ ~~2613~~ ~~2615~~ ~~2617~~ ~~2619~~ ~~2621~~ ~~2623~~ ~~2625~~ ~~2627~~ ~~2629~~ ~~2631~~ ~~2633~~ ~~2635~~ ~~2637~~ ~~2639~~ ~~2641~~ ~~2643~~ ~~2645~~ ~~2647~~ ~~2649~~ ~~2651~~ ~~2653~~ ~~2655~~ ~~2657~~ ~~2659~~ ~~2661~~ ~~2663~~ ~~2665~~ ~~2667~~ ~~2669~~ ~~2671~~ ~~2673~~ ~~2675~~ ~~2677~~ ~~2679~~ ~~2681~~ ~~2683~~ ~~2685~~ ~~2687~~ ~~2689~~ ~~2691~~ ~~2693~~ ~~2695~~ ~~2697~~ ~~2699~~ ~~2701~~ ~~2703~~ ~~2705~~ ~~2707~~ ~~2709~~ ~~2711~~ ~~2713~~ ~~2715~~ ~~2717~~ ~~2719~~ ~~2721~~ ~~2723~~ ~~2725~~ ~~2727~~ ~~2729~~ ~~2731~~ ~~2733~~ ~~2735~~ ~~2737~~ ~~2739~~ ~~2741~~ ~~2743~~ ~~2745~~ ~~2747~~ ~~2749~~ ~~2751~~ ~~2753~~ ~~2755~~ ~~2757~~ ~~2759~~ ~~2761~~ ~~2763~~ ~~2765~~ ~~2767~~ ~~2769~~ ~~2771~~ ~~2773~~ ~~2775~~ ~~2777~~ ~~2779~~ ~~2781~~ ~~2783~~ ~~2785~~ ~~2787~~ ~~2789~~ ~~2791~~ ~~2793~~ ~~2795~~ ~~2797~~ ~~2799~~ ~~2801~~ ~~2803~~ ~~2805~~ ~~2807~~ ~~2809~~ ~~2811~~ ~~2813~~ ~~2815~~ ~~2817~~ ~~2819~~ ~~2821~~ ~~2823~~ ~~2825~~ ~~2827~~ ~~2829~~ ~~2831~~ ~~2833~~ ~~2835~~ ~~2837~~ ~~2839~~ ~~2841~~ ~~2843~~ ~~2845~~ ~~2847~~ ~~2849~~ ~~2851~~ ~~2853~~ ~~2855~~ ~~2857~~ ~~2859~~ ~~2861~~ ~~2863~~ ~~2865~~ ~~2867~~ ~~2869~~ ~~2871~~ ~~2873~~ ~~2875~~ ~~2877~~ ~~2879~~ ~~2881~~ ~~2883~~ ~~2885~~ ~~2887~~ ~~2889~~ ~~2891~~ ~~2893~~ ~~2895~~ ~~2897~~ ~~2899~~ ~~2901~~ ~~2903~~ ~~2905~~ ~~2907~~ ~~2909~~ ~~2911~~ ~~2913~~ ~~2915~~ ~~2917~~ ~~2919~~ ~~2921~~ ~~2923~~ ~~2925~~ ~~2927~~ ~~2929~~ ~~2931~~ ~~2933~~ ~~2935~~ ~~2937~~ ~~2939~~ ~~2941~~ ~~2943~~ ~~2945~~ ~~2947~~ ~~2949~~ ~~2951~~ ~~2953~~ ~~2955~~ ~~2957~~ ~~2959~~ ~~2961~~ ~~2963~~ ~~2965~~ ~~2967~~ ~~2969~~ ~~2971~~ ~~2973~~ ~~2975~~ ~~2977~~ ~~2979~~ ~~2981~~ ~~2983~~ ~~2985~~ ~~2987~~ ~~2989~~ ~~2991~~ ~~2993~~ ~~2995~~ ~~2997~~ ~~2999~~ ~~3001~~ ~~3003~~ ~~3005~~ ~~3007~~ ~~3009~~ ~~3011~~ ~~3013~~ ~~3015~~ ~~3017~~ ~~3019~~ ~~3021~~ ~~3023~~ ~~3025~~ ~~3027~~ ~~3029~~ ~~3031~~ ~~3033~~ ~~3035~~ ~~3037~~ ~~3039~~ ~~3041~~ ~~3043~~ ~~3045~~ ~~3047~~ ~~3049~~ ~~3051~~ ~~3053~~ ~~3055~~ ~~3057~~ ~~3059~~ ~~3061~~ ~~3063~~ ~~3065~~ ~~3067~~ ~~3069~~ ~~3071~~ ~~3073~~ ~~3075~~ ~~3077~~ ~~3079~~ ~~3081~~ ~~3083~~ ~~3085~~ ~~3087~~ ~~3089~~ ~~3091~~ ~~3093~~ ~~3095~~ ~~3097~~ ~~3099~~ ~~3101~~ ~~3103~~ ~~3105~~ ~~3107~~ ~~3109~~ ~~3111~~ ~~3113~~ ~~3115~~ ~~3117~~ ~~3119~~ ~~3121~~ ~~3123~~ ~~3125~~ ~~3127~~ ~~3129~~ ~~3131~~ ~~3133~~ ~~3135~~ ~~3137~~ ~~3139~~ ~~3141~~ ~~3143~~ ~~3145~~ ~~3147~~ ~~3149~~ ~~3151~~ ~~3153~~ ~~3155~~ ~~3157~~ ~~3159~~ ~~3161~~ ~~3163~~ ~~3165~~ ~~3167~~ ~~3169~~ ~~3171~~ ~~3173~~ ~~3175~~ ~~3177~~ ~~3179~~ ~~3181~~ ~~3183~~ ~~3185~~ ~~3187~~ ~~3189~~ ~~3191~~ ~~3193~~ ~~3195~~ ~~3197~~ ~~3199~~ ~~3201~~ ~~3203~~ ~~3205~~ ~~3207~~ ~~3209~~ ~~3211~~ ~~3213~~ ~~3215~~ ~~3217~~ ~~3219~~ ~~3221~~ ~~3223~~ ~~3225~~ ~~3227~~ ~~3229~~ ~~3231~~ ~~3233~~ ~~3235~~ ~~3237~~ ~~3239~~ ~~3241~~ ~~3243~~ ~~3245~~ ~~3247~~ ~~3249~~ ~~3251~~ ~~3253~~ ~~3255~~ ~~3257~~ ~~3259~~ ~~3261~~ ~~3263~~ ~~3265~~ ~~3267~~ ~~3269~~ ~~3271~~ ~~3273~~ ~~3275~~ ~~3277~~ ~~3279~~ ~~3281~~ ~~3283~~ ~~3285~~ ~~3287~~ ~~3289~~ ~~3291~~ ~~3293~~ ~~3295~~ ~~3297~~ ~~3299~~ ~~3301~~ ~~3303~~ ~~3305~~ ~~3307~~ ~~3309~~ ~~3311~~ ~~3313~~ ~~3315~~ ~~3317~~ ~~3319~~ ~~3321~~ ~~3323~~ ~~3325~~ ~~3327~~ ~~3329~~ ~~3331~~ ~~3333~~ ~~3335~~ ~~3337~~ ~~3339~~ ~~3341~~ ~~3343~~ ~~3345~~ ~~3347~~ ~~3349~~ ~~3351~~ ~~3353~~ ~~3355~~ ~~3357~~ ~~3359~~ ~~3361~~ ~~3363~~ ~~3365~~ ~~3367~~ ~~3369~~ ~~3371~~ ~~3373~~ ~~3375~~ ~~3377~~ ~~3379~~ ~~3381~~ ~~3383~~ ~~3385~~ ~~3387~~ ~~3389~~ ~~3391~~ ~~3393~~ ~~3395~~ ~~3397~~ ~~3399~~ ~~3401~~ ~~3403~~ ~~3405~~ ~~3407~~ ~~3409~~ ~~3411~~ ~~3413~~ ~~3415~~ ~~3417~~ ~~3419~~ ~~3421~~ ~~3423~~ ~~3425~~ ~~3427~~ ~~3429~~ ~~3431~~ ~~3433~~ ~~3435~~ ~~3437~~ ~~3439~~ ~~3441~~ ~~3443~~ ~~3445~~ ~~3447~~ ~~3449~~ ~~3451~~ ~~3453~~ ~~3455~~ ~~3457~~ ~~3459~~ ~~3461~~ ~~3463~~ ~~3465~~ ~~3467~~ ~~3469~~ ~~3471~~ ~~3473~~ ~~3475~~ ~~3477~~ ~~3479~~ ~~3481~~ ~~3483~~ ~~3485~~ ~~3487~~ ~~3489~~ ~~3491~~ ~~3493~~ ~~3495~~ ~~3497~~ ~~3499~~ ~~3501~~ ~~3503~~ ~~3505~~ ~~3507~~ ~~3509~~ ~~3511~~ ~~3513~~ ~~3515~~ ~~3517~~ ~~3519~~ ~~3521~~ ~~3523~~ ~~3525~~ ~~3527~~ ~~3529~~ ~~3531~~ ~~3533~~ ~~3535~~ ~~3537~~ ~~3539~~ ~~3541~~ ~~3543~~ ~~3545~~ ~~3547~~ ~~3549~~ ~~3551~~ ~~3553~~ ~~3555~~ ~~3557~~ ~~3559~~ ~~3561~~ ~~3563~~ ~~3565~~ ~~3567~~ ~~3569~~ ~~3571~~ ~~3573~~ ~~3575~~ ~~3577~~ ~~3579~~ ~~3581~~ ~~3583~~ ~~3585~~ ~~3587~~ ~~3589~~ ~~3591~~ ~~3593~~ ~~3595~~ ~~3597~~ ~~3599~~ ~~3601~~ ~~3603~~ ~~3605~~ ~~3607~~ ~~3609~~ ~~3611~~ ~~3613~~ ~~3615~~ ~~3617~~ ~~3619~~ ~~3621~~ ~~3623~~ ~~3625~~ ~~3627~~ ~~3629~~ ~~3631~~ ~~3633~~ ~~3635~~ ~~3637~~ ~~3639~~ ~~3641~~ ~~3643~~ ~~3645~~ ~~3647~~ ~~3649~~ ~~3651~~ ~~3653~~ ~~3655~~ ~~36~~

árak. Olyan városokban, mint Kent (Egyesült Királyság) és Los Angeles, valamint Alhambra (Kalifornia, USA), a PredPol kipróbálását követően a bűnözés csökkenését figyelték meg bizonyos városrészekben, ami összefüggésbe hozható azzal, hogy a rendőröket közvetlenül a bűncselekmények elkövetése után küldték ki az adott területekre.²⁵⁰ De ahogy Fry megjegyzi, nehéz eldönteni, hogy a technológiának a bűncselekmények felderítéséért vagy előrejelzéséért jár-e az érdem. A PredPol minden bizonnyal szeretné magáénak tudni a bűnözés csökkentését, ugyanakkor a rendőrök bizonyos földrajzi területekre történő kiküldése - algoritmusok használatával vagy anélkül - okozati tényező lehet a bűnözés csökkentésében ezekben a városrészekben.²⁵¹

A mesterséges intelligencia bűnüldöző szervek általi használata a bűnözést kereső rendőrökben megerősítési torzítást eredményezhet, ami valójában megváltoztathatja a bűnözési arányokat. Toby Davies matematikus és bűnügyi kutató szerint a rendőrök több bűncselekményt fognak észlelni, ha egy bizonyos helyen járnak, mint amennyit egyébként észlelnének.²⁵² Más szóval, ha két helyen ugyanannyi bűncselekmény történik, a rendőrök több bűncselekményt fognak észlelni azon a helyen, ahol voltak, mint a másik helyen, ahol nem voltak. Az eredmény egy visszacsatolási hurok lehet, ahol egy algoritmus azt jósolja, hogy például egy szegény környéken több bűncselekmény fog történni. A rendőröket arra a környékre küldenék, ahol bűncselekményeket észlelnek. Mivel az algoritmus továbbra is azt jósolja, hogy a környék bűnözési gócpont, több rendőrt küldenek oda, és több bűncselekményt észlelnek az adott területeken. Amint fentebb említettük, az ilyen visszacsatolási ciklusok akkor fordulnak elő, amikor a mesterséges intelligencia rendszereket nem kérdőjelezzik meg a megerősítés vagy a tudattalan előítéletesség miatt, amely

²⁵⁰ Ibid. 260-262.

251 Ibid. 262.

252 Ibid. 262.

a kialakításukra jellemzőek, és valószínűleg problémát jelentenek azok számára, akik már eleve bizonytalan gazdasági vagy bevándorlási helyzetben vannak. További aggodalomra ad okot az a tény, hogy a bűnfelderítési és előrejelzési technológiák és az azokban alkalmazott algoritmusok nagy része védett. Az olyan szakértők számára, mint Fry, nem is beszélve az átlagos bíróról vagy emberről, nem világos, hogyan működik a PredPolhoz hasonló technológia. Anélkül, hogy képesek lennének értékelni, hogyan jutnak az algoritmusok a megállapításaikhoz, a bűncselekményekkel vádolt embereket megfoszthatják az eljárási méltányosságtól vagy a tisztességes eljáráshoz való jogtól.²⁵³ Ezt a kérdést a záró fejezetben újra megvizsgáljuk.

Az arcfelismerésnél az egyik fő probléma a hamis azonosítás lehetősége. A mesterséges intelligenciával működő rendszerek esetében a téves azonosítás matematikailag elkerülhetetlen, ami súlyos következményekkel járhat a tévesen gyanúsítottként azonosított személyek számára. Ezzel szemben az igazságügyi DNS-elemzés az egyének nagymértékben változó genetikai információinak értékelésén és a DNS-szekvenciák egyezésének valószínűségén alapul, és a téves egyezés esélye csökken, ha nagyobb mintaméretet és nagyobb számú genetikai markert használnak.²⁵⁴ Mégis a

253 David Koehn, "The Role of DNA in Forensic Science" (2008), 6
 85. "The Role of DNA in Forensic Science" (2008), 6
 s: MDiigetaskt
 er-Magurly aonndliAntetribution in State v. Loomis" Jolt
 (3120, :
 -d
 CDoeucristiCour-rMenatkiSntgr", [Installing C24](#) (2018),
 //mffcecdiu rñ /@PaAsIqNuowalel sStzlggofTherone/wwedMdyTechev
 792 9 rcaomk
 (1 2017), :
 -the-rule-of- 681 sJreh mosn-thinreea ten
 law/.

az arcfelismerő technológia esetében jelenleg ennek fordítottja igaz. A Google FaceNet 99,6 százalékos pontosságot ért el, amikor ötezer híresség arcképének azonosítását kellett elvégeznie, ²⁵⁵de amikor 2015-ben részt vett a Washingtoni Egyetem "Megaface challenge" elnevezésű kihívásán, csak 75 százalékos azonosítási arányt ért el. ²⁵⁶ Ennek oka, hogy az arcok félreazonosításának esélye drámaian megsokszorozódik, ha több arcot kell összehasonlítani (a jelenlegi technikai lehetőségek mellett). Minél több arcot keres át az algoritmus, annál nagyobb az esélye annak, hogy két hasonlóknak tűnő arcot talál. Fry szavaival élve: "a hasonlóság a szemlélő szemében van". ²⁵⁷ Ezt szem előtt tartva "az arcfelismerés, mint azonosítási módszer, nem olyan, mint a DNS, amely büszkén áll egy robusztus statisztikai platformon". ²⁵⁸ Továbbá az arcfelismerő technológiát megtéveszthetik az ikrek, ²⁵⁹ testvérek, ²⁶⁰ maszkok, ²⁶¹ és a kifejezetten erre a célra tervezett hamis szemüvegkeretek. ²⁶²

254 [Culhane, "Simple face recognition of DeepFakes" \(1992\) 61:2](#)
[14; \[Harris, "Simple face recognition of DeepFakes" \\(1992\\) 61:2\]\(#\)](#)

255 [f, Dm itry7 K&B M H C G e m s](#) es Philbin, "FaceNet:
[a deep learning architecture for face recognition", arXiv](#)
[1706.07694v1 \[cs.LG\], 2017. március 16. 2017. március 16. 2017. március 16.](#)

256 " ["DeepFakes" \(W \)](#), online:
[https://www.wired.com/story/deep-fakes-are-real/](#)

257 ["Megaface challenge" \(2015\) 11:1](#)
[https://www.wired.com/story/megaface-challenge/](#)

258 Fry, *Supra* note at 248275.
["The 'Megaface Challenge' \(2015\) 11:1](#)

259 ["The 'Megaface Challenge' \(2015\) 11:1](#)
[https://www.wired.com/story/megaface-challenge/](#)

260 " ["The 'Megaface Challenge' \(2015\) 11:1](#)
[https://www.wired.com/story/megaface-challenge/](#)

261 ["The 'Megaface Challenge' \(2015\) 11:1](#)
[https://www.wired.com/story/megaface-challenge/](#)

262 ["The 'Megaface Challenge' \(2015\) 11:1](#)
[https://www.wired.com/story/megaface-challenge/](#)

Vannak azonban olyan helyzetek, amikor az arcfelismerő technológia használatának előnyei meghaladják a fenti költségeket. Ilyen például a kanadai Ontario tartomány döntése, miszerint arcfelismerő technológiát alkalmaznak a szerencsejáték-függőségben szenvedő emberek esetében, akik önként felkerültek egy önkizáró listára, és lehetővé teszik, hogy a kaszinóba belépve algoritmusok felismerjék őket, és udvariasan megkérjék őket, hogy hagyják el az épületet.²⁶³

Ábra - 8Carcinoma Ringo Wiggins és Russell

264



Nehéz kompromisszumok állnak a kormányok és a bűnüldöző szervezetek előtt, amelyek algoritmikus bűnügyi elemzést kívánnak bevezetni.

261 [1], " ppFleorFbaecse D'Nfoovleemd ' e By
 Da sAk", 27 (2017),
 p fulliseme/sins/mhokabrewhex/#/vape2017 e
 t/fvicwawl oo AdccSehsasroifr, 78077

262 MReaitRae, " izSerutoti
 anva allujndSrety MATitcahcakesl
 Sa-ditAr Face Recognition", Konferenciadokumentum (Október
 206) : . cs . du -OsbnhtargiaovLa/opttaepreysa/nfadcGe-armeci-
 " Ekvsvio Bg ",
 ncgcsCor16.
 (s(t), porfation
 olinge :
 HMs ouotn. . ca/self-exclusion/arcfelismerés/.

264 gi, "ReCede n", (:/i/ngoald. 1/a 2 ; WEviathReirnsaplodoi, R uskGWoweeb
 online: <https://goo.gl/AO7QYu>.

stř, Wineeb:
", ickorn(site),

eszközök: az algoritmikus döntéshozatal méltányosságának biztosítása érdekében gondosan egyensúlyt kell teremteniük az egyéni magánélet és a nyilvánosság egészének védelme közötti versengő érdekek között. Visszatérve a Fry által azonosított kérdések térképéhez, bármely szervnek, amely úgy dönt, hogy az algoritmusokat a bűnözés szabályozási eszközeként használja, végső soron el kell döntenie, hogy mik a prioritásai. "A bűnözést a lehető legalacsonyabb szinten tartani? Vagy mindenekelőtt az ártatlanok szabadságának megőrzése? Mennyit áldozna fel az egyikből a másikért?"²⁶⁵ És Fry emlékeztet minket: "Gary Marx, az MIT szociológiai professzora jól fogalmazta meg a dilemmát a Guardiannek adott interjújában: 'A Szovjetunióban figyelemre méltóan kevés volt az utcai bűnözés, amikor totalitárius, tekintélyelvű irányításuk a legrosszabbkor volt. De, Istenem, milyen áron?'²⁶⁶ Fryhoz és számos más szakértőhöz hasonlóan mi is azt tanácsoljuk, hogy az algoritmikus döntéshozatal hatókörét óvatosan hajtsák végre és kifejezetten korlátozzák a bűnözés felderítésében és előrejelzésében. A bűnüldöző szervek döntése a mesterséges intelligencia alkalmazásáról, valamint az, hogy a szervek hogyan használják azt, fontos része annak a szabályozási ökoszisztémának, amely lehetővé teszi vagy korlátozza a technológia hatalmát.

4.3.2. Előremutató utak

Számos megoldás áll azon kormányok rendelkezésére, amelyek bűnüldöző szervei mesterséges intelligenciát kívánnak alkalmazni, és ezekhez proaktív szabályozásra van szükség, amelyet az átláthatóságra, a felügyeleti rendszerekre és az interdiszciplináris együttműködésre vonatkozó minimumszabályok iránti elkötelezettség jellemez. A bűnüldöző szervek

²⁶⁵ Fry, *Supra* note at 248290.

LFrAyP, nTothee248 0, dngNB eg' diktáló
Disputé, Gaardian (2 34), line
bünözés, : . thesguakidcha 425 e-
happóóg . . .

a mesterséges intelligencia felhasználását vizsgálják, és az ezen ügynökségek mögött álló kormánzatnak egyre több munka áll rendelkezésére az algoritmikus döntéshozatal legjobb gyakorlataival kapcsolatban. Különösen Alexander Babuta, Marion Oswald és Christine Rinik kutatók megállapításaihoz fordulunk, akik a brit Royal United Services Institute védelmi és biztonsági agytrösztnek írtak.²⁶⁷ A gépi tanulási algoritmusok rendőrségi döntésekhez való alkalmazása által támasztott jogi, etikai és szabályozási kihívásokat igyekeztek megvizsgálni.²⁶⁸ Megállapításaikat érdemes itt felsorolni, és azok joghatóságtól függetlenül minden bűnüldöző szervre vonatkoznak:²⁶⁹

15. Sürgősen egyértelmű iránymutatást és gyakorlati kódexeket kell kidolgozni, amelyek korlátozzák, hogy a bűnüldözésnek hogyan kell kipróbálnia és használnia az algoritmikus eszközöket;
16. Szabályozási keretre van szükség az algoritmikus eszközök rendőri szervek általi használatára vonatkozó minimumszabályok megállapításához, különösen a vonatkozó adatvédelmi jogszabályok, az AI-rendszer átláthatósága és érthetősége, valamint az emberi jogok és a közigazgatási jog elveinek tiszteletben tartása tekintetében;
17. Az algoritmus visszamenőleges visszafejtésének minden közbeszerzési szerződés kötelező elemévé kellene válnia, hogy értékelni lehessen a modell előrejelzéseit befolyásoló tényezőket;

²⁶⁷ Babuta, Oswald és Rinik: (2018), *Artificial Intelligence and the Law: A Practical Guide to the Use of AI in the Criminal Justice System*, London: Routledge.

²⁶⁸ Babuta, Oswald és Rinik: (2018), *Artificial Intelligence and the Law: A Practical Guide to the Use of AI in the Criminal Justice System*, London: Routledge, 243.

²⁶⁹ Babuta, Oswald és Rinik: (2018), *Artificial Intelligence and the Law: A Practical Guide to the Use of AI in the Criminal Justice System*, London: Routledge, 243.

18. A szabályozási keret betartásának biztosításához formalizált ellenőrzési és felügyeleti rendszerre van szükség (legyen az bizottság, munkacsoport, bizottság, testület stb.). Ezeknek az etikai testületeknek multidiszciplinárisnak kell lenniük, és szakemberek, műszaki szakértők, akadémikusok, esetleg átlagemberek vagy laikusok kombinációjából kell állniuk;
19. A megközelítésnek együttműködésen alapulónak és szakterületeket átfogónak kell lennie, hogy a különböző szakértők és érdekeltek képviselése biztosított legyen. A testületnek ajánlásokat kell megfogalmaznia az egyes bűnüldöző szervek számára az algoritmusok alkalmazásával kapcsolatos gyakorlati, stratégiai és szakpolitikai döntésekhez.

A mesterséges intelligenciával kapcsolatban számos más általános irányadó elv is olvasható, többek között a "Principles for Accountable Algorithms and a Social Impact Statement for Algorithms" című dokumentum, amelyet a Fairness, Accountability, and Transparency in Machine Learning (FAT/ML) közösség tagjai állítottak össze.²⁷⁰ AI Now Institute legújabb jelentése és publikációi, amelyeket a Data & Society Research Institute által 2018,²⁷¹ nemrégiben kiadott jelentésben tettek közzé,²⁷²

270 [Principles for Accountable Algorithms and a Social Impact Statement for Algorithms](#), (), [https://arxiv.org/abs/1906.00036](#).

271

[AI Now Institute, "AI Now 2018 Report", \[https://ai.nowinstitute.org/ai-now-2018-report\]\(#\), \(2018\), \[https://ai.nowinstitute.org/ai-now-2018-report\]\(#\).](#)

[Data & Society Research Institute, "Algorithmic Justice League", \[https://www.dataproject.com/algorithmic-justice-league\]\(#\), \(2018\), \[https://www.dataproject.com/algorithmic-justice-league\]\(#\).](#)

272 [AI Now Institute, "AI Now 2018 Report", \[https://ai.nowinstitute.org/ai-now-2018-report\]\(#\), \(2018\), \[https://ai.nowinstitute.org/ai-now-2018-report\]\(#\).](#)

és a legutóbb decemberben frissített Montréali Nyilatkozat a mesterséges intelligencia felelős fejlesztéséről néhány példa 2018az ezeket az elveket felvázoló magas szintű dokumentumokra, amelyeket a záró fejezetben újra áttekintünk.²⁷³

Röviden, tekintettel a mesterséges intelligencia bűnüldözési célú alkalmazása során kockáztatott nagy tételekre (magánélet, ártatlanság vélelme, büntetésmentesség), támogatjuk azt, amit egyes tudósok a technológia emberi jogok általi tervezéssel történő megközelítésének neveznek,²⁷⁴ ahol az algoritmusokat úgy tervezik, hogy a tervezés, a bevezetés és az iteratív fejlesztés²⁷⁵ minden szakaszában az ember (és nem a gép feltételezett tekintélye) legyen az első helyen, amikor a bűnüldözésről van szó.

273

https://www.montrealdeclaration.ca/en/2018/12/04/declaration-of-principles-on-responsible-development-of-artificial-intelligence

https://www.montrealdeclaration.ca/en/2018/12/04/declaration-of-principles-on-responsible-development-of-artificial-intelligence

274

https://www.montrealdeclaration.ca/en/2018/12/04/declaration-of-principles-on-responsible-development-of-artificial-intelligence

https://www.montrealdeclaration.ca/en/2018/12/04/declaration-of-principles-on-responsible-development-of-artificial-intelligence

https://www.montrealdeclaration.ca/en/2018/12/04/declaration-of-principles-on-responsible-development-of-artificial-intelligence

https://www.montrealdeclaration.ca/en/2018/12/04/declaration-of-principles-on-responsible-development-of-artificial-intelligence

https://www.montrealdeclaration.ca/en/2018/12/04/declaration-of-principles-on-responsible-development-of-artificial-intelligence

275

https://www.montrealdeclaration.ca/en/2018/12/04/declaration-of-principles-on-responsible-development-of-artificial-intelligence

10 0 **Táblázat - A bűnüldözési és büntető igazságszolgálati szolgáltatásokban használt mesterséges intelligencia szoftverek**

Név	Alkotó	Cél és képességek	Csoport	Funkció(s)
PhotoDNA ²⁷⁶	Microsoft ; Fairchild Hany	" (an" si diogiftaalninst) si h aiohdeatsaabmadseentciofinetdainWie nggal , rexpnoitifaciant .	Műs elimerés	Naftoior r anCdhEilxdprleo nit ed ,
Optimalizálás	University of	. b An jenboet areveinsig , használ	Videó és	University of

²⁷⁶ National Institute of Standards and Technology támogatással a


Technológia	te f u t e	a rendőrség megfigyelési és elemzési módszere		Országos Részleg,
-------------	---------------	--	--	----------------------

				Shreveport
Sept 27 9		illegible pilot rtheacet 1-20	előrejelzés	12000 (\$)

Szám	Alkotó	Cél és képességek	Családnevelési	Intézmény(ek)
ediktív	Chicagoói rendőrség	<p>hópep dion gowdils tre vats lou ante inghein "lannTe v& amydaoef rad tutistnhge apnrookpeenrvawtioi halte includi res uthdieogryussicu ch aspriolna ctRivAitNyD, , of m uthrse winille parta rerdot bycfhutoasbsrheoakottingos, bbery, " a " visszanyert és a a megvalósításhoz. CPDeward</p>	<p>his</p>	Chicagoói rendőrség
PRoelsiecinrcg Chicago280	Technológia	<p>pefafftitearcnys oift</p>	előrejelzés	DepaUSm et ()

		aws://aws-logs-917251231111-us-east-1		
--	--	---------------------------------------	--	--

Kor	Alkotó	Cél és képességek	Családi háttér	Intézmény(ek)
HAnotrii- zCornimoer 282	HAnotrii- zCornimoer 282	Cél és képességek	Családi háttér	Intézmény(ek)
PredPol ²⁸³	saacampusy	ain al 6 0 acrim es are adott időszakban."	előrejelzés	az USA-ban)

	Alkotó	Cél és képességek	Családnevelő	Intézmény(ek)
W (auAtRoarMn AatNteTd service 284	RTreisaenagrleeh Intézet	" <p> Japán AI-ethics Hírdetés a hewviocerktinregatruncoroelate Rózsánál film sNtloJ aanaoet sivch unsiothor ,0 rdoaeasme. 300 iTh thevnritvilslthaenanepxrts etivmrfeosopfans ocutthenmcsom vafifabnstedh deTdnheisofmeondreiksw(a fcaudngauv). if aplhsenbiteiogeorlograsphicatl lsyureefceornecnecnetdrastoionthslaot f activ warr " </p>	; prediction	RepWosaitrorray nt(US)

	Alkotó	Cél és képességek	Család	Integráció
<p>V I A s a következő esetében SiteClrigme nce Elemzés) 285</p>	<p>M European Bizottság</p>	<p>" a pa ho sminidssti nWg haen le sitrectianntg aliynsstisghttos nTshrgoeunghrate andbsuocvsiuad anhtoulnmoamnoutesaamwo a rrVkaOLrCRcolllcarbeoartnaivteiolyn d evixspulanlnigsaatitoatitoininths, agaisotr higsaofesagum rVotAeLctCinRgl ap imob jecrtrivoe inge speed "</p>	<p>f ; tion; ; ts l konstrukciók Arc</p>	<p>Különböző</p>
<p>Analitika</p>	<p>Cellebrite</p>	<p>"Tranprecisio w, széttagolt da a digitálisba sform r</p>		<p>Brit erők:</p>

Vállalat ²⁸⁶		1001	Definíció; Eg.	Mezőgazdaság
-------------------------	--	------	-------------------	--------------

Alkotó	Cél és képességek	Család	Intézmény(ek)
<p>ADnesaklyt otipcs⁸⁷</p>	<p>rsa, andnors és n nyestartus dlnncatetrally huatubfminscenfect autnmaait sli ge. midle Fococmuspromterdancadfitreolmdiozdsroource sroources rgenesrieicsewlmibfralyrya. ecroemd plex Schiiscotexint, wredtthstthkthetnssitab e gerteadauceügye es." " AtDneaslygtnnicesdDsaevsskataospta neyldiioaloinnaetrenaspplication greawalddata</p>	<p>Működés d ion; felismerés;</p>	<p>drainel (USCrededSaeVfCB I, égnmicspl) Poltuekyr ctehse inUAE, hrain,</p>

El
ek
tr
on
ik
us
an
el
ér
he
tő
a
kö
ve
tk
ez
ő
cí
m
en
:
htt
ps
://
ss
rn
.c
o
m/

	Alkotó	Cél és képességek	Családnevelő	Intézmény(ek)
HART (Harm	Unive sity of	<p>times.</p> <p>mitnhovaeresytilgeaatdiosneincyelcelses</p> <p>Asobibularinfutdelylligveenrcsetg a</p> <p>ud s</p> <p>fsilstedrbaoindedriga digital</p> <p>yaor</p> <p>tif act acrodeveisparate sources</p> <p>az egyetetté t tatarságokat</p>	Visszaesés	Durham
ARisskesTs moeln) ²⁸⁸	Palantir	<p>onfrencadsint</p> <p>garmdoantabisktosbaregibes</p> <p>SChuckposiClisakpit</p> <p>forrogtrhaemCmoen.</p> <p>itnhteerCvoenstitoanbuclurryreantldy</p> <p>dofisfepnocseal notan</p> <p>l'rosing'atfartnek célja' a jövőbeli</p> <p>bróság'Palantir'atell</p> <p>l'ünsekmények megelőzése</p>	előrejelzés	Costa () Korábban új
Palantir Intelligencia ²⁸⁹		széttagolt adatok összekapcsolt adatokból származó széttagolt adatok	előrejelzés	Orleans-i rendőrség

El
ek
tr
on
ik
us
an
el
ér
he
tő
a
kö
ve
tk
ez
ő
cí
m
en
:
htt
ps
://
ss
rn
.c
o
m/

10
9


Kód	Alkotó	Cél és képességek	Capabilities f	Infirmit(s)
Faception ²⁹⁰	Faception	<p>Sítesadnmasvítóga</p> <p>esneaterphraisneroduagtah</p> <p>fidhot</p> <p>nmáidre ,</p> <p>iocnoadl</p> <p>imigtvuniatfive</p> <p>ercns</p> <p>to</p> <p>auendertreunude</p> <p>deEnnppearlptertirsaes,</p> <p>diantseocucrtuceres,</p> <p>d</p> <p>rkteflferpafhos</p> <p>edbrantspanfadyazeed</p> <p>thoydargugm dlmtooullngeancedi</p> <p>q</p> <p>dfias</p> <p>nginthae</p> <p>lineesidghatnshvvinassokdi,</p> <p>hugfumegeérik."</p> <p>Arcepcion az-első - a technológia és a</p>	Arc	<p>Dep</p> <p>()</p> <p>Ismeretlen</p>

		személyre szabottan az emberek profilozására és felfedésére	elismerés	
--	--	---	-----------	--

	Alkotó	Cél és képességek	Családnevelési f	Ismereti(s)
Entrup 291	Entrup	<p>fabcaespedtmioonnlcyaenonardnth</p> <p>aleyizrenfafacciaelse</p> <p>), eoersotrnlaisneis/o(</p> <p>ceanomedrvaids</p> <p>afancde</p> <p>aprhiogrhistlepyvelsoolnfalaicfieurrsa,</p> <p>dWred a</p> <p>caenrotpaxinteopareerrsocnaaslsiteyrstoypnee</p> <p>aoirhtrdaistg</p> <p>alt,</p> <p>lansetwtl. vgaer</p> <p>pscaoyewr</p> <p>perceples</p> <p>toof</p> <p>im n f</p>	Kép	Ismeretlen

		<p>ntro h dev their came Eem py elo ped g ms hogy</p>		
		<p>allanwinigt foralyregioibmteib dhTehled rw,</p>	<p>from az aunthseunmtiec of rity</p>	

	Alkotó	Cél és képességek	Család	Infinit(s)
Axon test	Axon	mariecarsosopcfopaeinc iptEhmotoagnrdaprhushsoftdeifmfertehtrot thacnomupt98 cennttroufptyheis másodpercek 30 alatt eredményt kapunk." A rendőrség új kamerákat keres	termékek Gunsh t	Különböző rendőrök
2, 3292		, 'so 's vainddeo lfrowmhetrhee, "Kifüggetlen maskvizitációk számára kínésztett	a Mg	Compl e
Identif 293	Veritone (USA)	gethnecsiees cspriemedinalndjusetfificieiepnrcoycesfs aApnliactautricanl	; the Video ; ;	(ecDomiscp y oavneyr)

	Alkotó	Cél és képességek	Capabiltások	Ismeret(s)
Internet	erly Magnet	<p>to</p> <p>magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p>	<p>Digitális</p>	Ismeretlen
AI ²⁹⁴	erly Magnet	<p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p> <p>Magintelligens, amely képes a felhasználókat azonosítani, és a káros tartalmakat eltávolítani.</p>	<p>törvényszéki szakértő</p>	

Kód	Alkotó	Cél és képességek	Család	Integráció
		<p>midiesnstinigy</p> <p>ltirkaeckcinrigmainnadt</p> <p>igiosnea,</p> <p>' racnhd. "</p>		

276 "PhotoDNA", Microsoft (Weboldal), online: <https://www.microsoft.com/en-us/photodna>.

277 "Florida Adopts Crime Scene Video Analysis Goes High-Tech With \$1.3 Million Grant to UCF" (2015), <http://www.floridapublicaccess.com/2015/04/08/mrleatnrdoop-ocrlimtaen-sPceonlic-evid-Weoe-absaitlyes-is-ognoleisn-he>

278 "Police Uses Predictive Policing to Prevent Crime" (2015), <http://www.policemag.com/news/predictive-policing-13>, <http://www.policemag.com/news/predictive-policing-13>, <http://www.policemag.com/news/predictive-policing-13>

279 "Predictive Policing", <http://www.policemag.com/news/predictive-policing-13>, <http://www.policemag.com/news/predictive-policing-13>, <http://www.policemag.com/news/predictive-policing-13>

280 <http://www.nij.gov/topics/law-enforcement/strategies/predictive-policing/Pages/research.aspx>.

281 "Predictive Policing: The Future of Crime Prevention", <http://www.policemag.com/news/predictive-policing-13>, <http://www.policemag.com/news/predictive-policing-13>, <http://www.policemag.com/news/predictive-policing-13>

282 "Police prédictive : la tentation de "dire quel sera le crime de demain", <http://www.policemag.com/news/predictive-policing-13>, <http://www.policemag.com/news/predictive-policing-13>, <http://www.policemag.com/news/predictive-policing-13>

283 "Predictive Policing: The Future of Crime Prevention", <http://www.policemag.com/news/predictive-policing-13>, <http://www.policemag.com/news/predictive-policing-13>, <http://www.policemag.com/news/predictive-policing-13>

284 "Predictive Policing Research" (Előrejelző rendőrségi kutatás), fenti lábjegyzet. 280.

285 "VALCRI", VALCRI (honlap), online: <http://www.valcri.org/>.

286 "Analytics Enterprise", Cellebrite (Weboldal), online: <https://www.cellebrite.com/en/products/analytics-enterprise/>.

287 "Analytics Desktop", Cellebrite (Weboldal), online: <https://www.cellebrite.com/en/products/analytics-desktop/>.

- 288 [Enos, S. W.](#), " [Algorithmic Decision-Making: A Durham HART Model](#)", *Algorithmic Decision-Making* (2018) 2: 72. [Online: <http://www.algorithmicdecisionmaking.com/>](#)
- 289 [Hart, S.](#), " [Algorithmic Decision-Making: A Durham HART Model](#)", *Algorithmic Decision-Making* (2018) 2: 72. [Online: <http://www.algorithmicdecisionmaking.com/>](#)
- 290 " [Algorithmic Decision-Making: A Durham HART Model](#)", *Algorithmic Decision-Making* (2018) 2: 72. [Online: <http://www.algorithmicdecisionmaking.com/>](#)
- 291 [Hart, S.](#), " [Algorithmic Decision-Making: A Durham HART Model](#)", *Algorithmic Decision-Making* (2018) 2: 72. [Online: <http://www.algorithmicdecisionmaking.com/>](#)
- 292 [Hart, S.](#), " [Algorithmic Decision-Making: A Durham HART Model](#)", *Algorithmic Decision-Making* (2018) 2: 72. [Online: <http://www.algorithmicdecisionmaking.com/>](#)
- 293 [Hart, S.](#), " [Algorithmic Decision-Making: A Durham HART Model](#)", *Algorithmic Decision-Making* (2018) 2: 72. [Online: <http://www.algorithmicdecisionmaking.com/>](#)
- 294 " [Algorithmic Decision-Making: A Durham HART Model](#)", *Algorithmic Decision-Making* (2018) 2: 72. [Online: <http://www.algorithmicdecisionmaking.com/>](#)
- 295 [Hart, S.](#), " [Algorithmic Decision-Making: A Durham HART Model](#)", *Algorithmic Decision-Making* (2018) 2: 72. [Online: <http://www.algorithmicdecisionmaking.com/>](#)
- 296 [Hart, S.](#), " [Algorithmic Decision-Making: A Durham HART Model](#)", *Algorithmic Decision-Making* (2018) 2: 72. [Online: <http://www.algorithmicdecisionmaking.com/>](#)

5. MESTERSÉGES INTELLIGENCIA A BÜNTETŐELJÁRÁSBAN



A világ különböző joghatóságainak bíróságai egyre inkább beépítik a mesterséges intelligenciát a döntéshozatali folyamatokba. Kutatásunk azonosít néhány olyan területet, ahol a mesterséges intelligenciát már alkalmazzák a büntetőeljárásokban: nevezetesen az óvadékkal és az ítélethozatalokkal kapcsolatos kockázatértékelési döntéseket. Megállapítottuk, hogy a stratégiaileg mesterséges intelligenciaként forgalmazott vagy mesterséges intelligenciaként működő technológiák kínálata egyre bővül. Ez a technológia általában a bűncselekménnyel vádolt vagy börtönben lévő, bűncselekmény elkövetésében bűnösnek talált személyhez kapcsolódó kockázati szintet értékeli. Ismétlem, bölcs lenne, ha a döntéshozók minden joghatóságban nagy körültekintéssel és előrelátással alkalmaznák az ilyen kockázatértékelő eszközöket, tekintettel arra, hogy azok negatív hatással lehetnek a büntető igazságszolgáltatás olyan alapelveire, mint az ártatlanság vélelméhez való jog, az eljárási méltányosság és a megkülönböztetés nélküli döntéshozatal szükségességére.

5.1. Hogyan használják már a mesterséges intelligenciát a büntetőeljárásokban

Számos példa van arra, hogy az igazságszolgáltatási rendszerek már alkalmaznak mesterséges intelligenciaeszközöket a büntetőeljárásokban. Eddigi megállapításaink azt mutatják, hogy a jelenleg használt mesterséges intelligencia a vádlott jövőbeli nem kívánt viselkedésének kockázatát értékeli - ahelyett, hogy a kockázat más lehetséges helyeit vizsgálná, például annak valószínűségét, hogy a bíró

vagy az esküdtszék az előttük lévő tények függvényében egy adott módon fog reagálni. Az igazságszolgáltatási rendszerek, különösen az Egyesült Államokban, elsősorban az óvadékkal és a bíróság előtti első megjelenéssel (ha az adott joghatóságban alkalmazható), valamint az ítélethozatallal kapcsolatos döntések kapcsán támaszkodnak a mesterséges intelligenciára.

5.1.1. A mesterséges intelligencia alkalmazása az óvadékkal kapcsolatos döntésekben

Itt hasznos leírni, hogy mit értünk óvadék alatt. Az óvadék, más néven előzetes letartóztatás, olyan megelőző biztosítékként értelmezhető, amelyet a bíróságok annak biztosítására használnak, hogy a vádlott megfeleljen a büntetőjogi eljárásnak. A fogalom azon a félelmen alapul, hogy egy személy, ha egyszer már megvádolták egy bűncselekménnyel, elmulasztja a bírósági tárgyalásokat, vagy továbbra is bűncselekményeket követ el, illetve kárt okoz. Az óvadék vagy az előzetes letartóztatás fogalma a világ számos országában létezik. Egyes joghatóságok, például az Egyesült Államok egyes államai olyan óvadéki rendszert alkalmaznak, amely lehetővé teszi, hogy a vádlott az előzetes letartóztatásból való szabadulás feltételeként számos biztosítékot nyújtson, mint például készpénz, harmadik félre támaszkodó kezességvállalás, vagyon elzálogosítása, ígéret arra, hogy nem vesz részt illegális magatartásban, távoltartási végzés, a fentiek kombinációja és más, itt nem felsoroltak.²⁹⁷

Az óvadékkal kapcsolatos döntések meghozatalának egyik jelenleg alkalmazott módszere az óvadékkal kapcsolatos menetrendek használata. Az óvadéklisták számos joghatóságban az óvadék megállapításának egyszerűsítésére szolgálnak: ezek az óvadékkal kapcsolatos döntések során az óvadék összegének listáját tartalmazzák.

²⁹⁷ "Mi az a Bail? Megértése, hogy mi az óvadék és a különböző Bail Bonds", Bail USA (Weboldal), típusú <http://www.bailusa.net/what-is-bail.php>.
online:

a vádlott köteles fizetni. Ezek a vádlottat terhelő bűncselekmény jellegén alapulnak.²⁹⁸ Például Alabama állam óvadéktáblázata az alábbiak szerint határozza meg a bírák által a vád súlyossága és minősítése alapján megkövetelt óvadék ajánlott összegének tartományát:

Ábra -9 Alabama állam óvadéki menetrendje²⁹⁹

BAIL SCHEDULE			
Recommended Range			
Felonies:			
Capital felony	\$50,000	to	No Bail Allowed
Murder	\$15,000	to	\$ 150,000
Class A felony	\$10,000	to	\$ 60,000
Class B felony	\$ 5,000	to	\$ 30,000
Class C felony	\$ 2,500	to	\$ 15,000
Drug manufacturing and trafficking	\$ 5,000	to	\$1,500,000
Class D felony	\$1,000	to	\$ 10,000
Misdemeanors (not included elsewhere in the schedule):			
Class A misdemeanor	\$ 300	to	\$ 6,000
Class B misdemeanor	\$ 300*	to	\$ 3,000
Class C misdemeanor	\$ 300	to	\$ 1,000
Violation	\$ 300	to	\$ 500
Municipal Ordinance Violations	\$ 300	to	\$ 1,000
Traffic-Related Offenses:			
DUI	\$ 1,000	to	\$ 7,500

Az Egyesült Államok számos 2018, államában reformokat vezettek be a készpénzes óvadék és az óvadék rendszerében, és ezek helyett néhány államban olyan törvények bevezetésébe kezdtek, amelyek előírják a kockázatértékelési eszközök használatát az óvadék befolyásolásához.

298 "Bail Schedules", (Website),
 h: . us/cga/ h/ 2 crs/

volume , ": 2 §, Intersec. dicial érvelés,
 r e . Was under auth o rity net riemeju.
 72(b), dñ

299 : . gionva/ldoPcrso/cliebduarey/ruRluese/cr 7_2. p .

vonat:

döntések. New Jersey és Kalifornia két példa arra, hogy az államok a készpénzes óvadékról és a rögzített óvadéktervekről áttértek a kockázatértékelési rendszerekre.³⁰⁰ Kalifornia esetében a közelmúltbeli változás alapelve "2018az, hogy a gyanúsítottat a közbiztonságra jelentett kockázat és annak valószínűsége alapján értékeli, hogy nem jelenik meg a bíróságon, nem pedig aszerint, hogy képes-e letenni egy bizonyos óvadékösszeget".³⁰¹ A remény az, hogy ahelyett, hogy egy bizonyos összegű készpénzt fizetnének egyfajta biztosítékként, hogy meggyőzzék a bíróságot arról, hogy a vádlott meg fog jelenni a tárgyaláson, a bírák ehelyett részben empirikus rendszerek alapján hozzák meg az előzetes letartóztatásról vagy szabadlábra helyezéssel szülő döntéseiket, amelyek meghatározzák, hogy az illető valószínűleg elszökik-e vagy elkövet-e egy másik állítólagos bűncselekményt.

New Jersey az egyik olyan állam, amely eddig a legtöbb tapasztalattal rendelkezik a statisztikákon és algoritmusokon alapuló automatikus kockázatértékelő eszköz használatában. Az állam a Laura és John Arnold Alapítvány által kifejlesztett Public Safety Assessment (PSA), a tárgyalás előtti kockázatértékelési eszközt használja. Ez az alapítvány azt reméli, hogy javítani tudja a büntető igazságszolgáltatási rendszert az Egyesült Államokban. Az alapítvány például kijelentette, hogy csapata csak azután hozta létre a PSA-t, hogy "vezető büntető igazságszolgáltatási kutatókkal" együttműködve meghatározta, hogy hol van a legnagyobb szükség a büntető igazságszolgáltatási rendszer javítására, és hogy a statisztikai kockázatértékelést

³⁰⁰ [California's New First Scrap Cash Bail Program](#), [https://www.courts.ca.gov/first-scrap-cash-bail-program](#); [New Jersey's New Bail Program](#), [https://www.nj.gov/agencies/indiv/dep/cas/2018/08/28/20180828-nj-new-bail-program.htm](#); [New York's New Bail Program](#), [https://www.nyc.gov/html/doh/html/prd/20180828-ny-new-bail-program.htm](#); [New York's New Bail Program](#), [https://www.nyc.gov/html/doh/html/prd/20180828-ny-new-bail-program.htm](#).

³⁰¹ [ibid.](#)

eszközök életképes megoldást jelentenek a túlzott elzárás és az adófizetők pénzének a tárgyalást megelőző szakaszhoz kapcsolódó túlzott mértékű elköltése korlátozására. ³⁰² Az alapítvány kezdetben Kentucky, Észak-Karolina, Kalifornia és Arizona egyes megyéiben kísérleti jelleggel alkalmazta a PSA-t.³⁰³ Az Alapítvány szerint 2018 áprilisában mintegy 40 joghatóságban indult el vagy van folyamatban a PSA bevezetése, ³⁰⁴ ami azt mutatja, hogy az Egyesült Államokban és valószínűleg azon túl is elképesztő hatókörrel rendelkezik ez a modell a kockázatértékelésre a tárgyalás előtti szakaszban.

5.1.2. New Jersey közbiztonsági értékelő eszköze

Hogyan működik valójában a közbiztonsági értékelő eszköz? Amint azt New Jersey állam által kiadott dokumentumok leírják, a PSA kilenc kockázati tényezőt használ annak meghatározására, hogy a vádlott milyen valószínűséggel fog új bűncselekményt elkövetni vagy

(b) erőszakos bűncselekmény a tárgyalást megelőző időszakban, vagy c) annak valószínűsége, hogy nem jelenik meg a tárgyaláson.³⁰⁵ A kilenc tényezőt, beleértve az esetleges magyarázó információkat is, az alábbiakban soroljuk fel, az "igen" válasz állítólag növeli a vádlottal kapcsolatos nem kívánt kockázat valószínűségét:

³⁰² <https://www.pardocfoundation.org/wp-content/uploads/PSA-2018-01-01.pdf>, 5.

³⁰³ <https://www.pardocfoundation.org/wp-content/uploads/PSA-2018-01-01.pdf>, 5.

³⁰⁴ <https://www.pardocfoundation.org/wp-content/uploads/PSA-2018-01-01.pdf>, 5.

305 Ibid. 1.

120

Táblázat - 2New Jersey közbiztonsági értékelő eszköz³⁰⁶

A factor	magyarázat	válaszok
<p>1. Jelenlegi</p> <p>currgeen tat</p> <p>letartóztá tás</p> <p>Jelenlegi</p>	<p>PS kora</p> <p>"age tfehntdimane aa</p> <p>tfehntdimane</p> <p>jelenlegi tarrest. A PSA ca egorize s an</p>	<p>"AgPossible nusef ttr</p> <p>defteernmisi tis 2 0</p> <p>youngta, 21or, vagy 22, 23 vagyagy .</p> <p>"Ha yolder "</p>
<p>2a. Jelenlegi</p> <p>voifofaelennste</p>	<p>o anepnesresoans nen</p> <p>apthteymsicpats injnyshougfyne h</p> <p>," of</p> <p>trick A PSA a</p>	<p>Onoh erwise, s ."</p> <p>"Ha egy vagy több</p>
<p>3. Pending</p> <p>voifofaelennst eold&2 yournsger</p>	<p>msidmreatinoen cfp mmitted a</p> <p>A PSA vizsgálja, hogy azt</p>	<p>2 and tatsdeffimneedofn 1 , the Onoh erwise, "Ha az alperes"</p>
<p>Great of the offense</p>	<p>aitndyofinheer itage cownhteicxht NewtJheartsehyasasa "fustuare</p>	<p>ns ns z fenealltegeedalnyswer</p>

³⁰⁶ Ibid. 1-4.

Kérdés	Explanation	válaszok
<p>4. Előző</p>	<p>re-dis ed positione langhe jursyp, ifa u g o d i s d o t h e s p d o r d i s h g r o u d f o r a l statuhsar(. g . , p c r o e p t r i a t i o n a l d i s a t o g r a m) ." Ez is emítés se kérdés,</p>	<p>igepozitív hOisthreiskwisac ,totr hea válasz nem." "Ha az alperes</p>
<p>DPeisrosordn esrly elítélés</p>	<p>choangeudct woitrh h y m f e a n o r egy másik államban. vizsgálja, hogy azt</p>	<p>prábeadagis h h r m a r k e m e a m o n g o f e m o s r p r o d f e s e h a t u g , a z a f a n c s t w o r e r i s t o y e t s h . i O t h e w i e "Ha az alperes"</p>
<p>5. B individualien</p>	<p>a leudndgug i k k o r a b e u f e o m n e y fenntartásokkal.</p>	<p>pfoleudndgugultiultiylty orasbeann h d i l l i o f r e l o m n o y r e h a l d e t a g e s e a n t u s m o i n g p a d a y e t y o e t . hOisthreiskwifsaec ,totrheis a válasz nem."</p>

Tényező	Magyarázat	Válaszol
6. Előző	<p>„A PSA a következőket veszi figyelembe</p>	<p>„A válasz szám igen.” Bűnös</p>
7. Előző	<p>szálja, hogy Aztis megviz</p>	<p>„A válasz szám a</p>
8. Előző	<p>a hasonló 2 Aztis megviz</p>	<p>„A válasz szám a</p>
9. Előző	<p>a jelenlegi letartóztatás.</p>	<p>„A válasz nem.”</p>

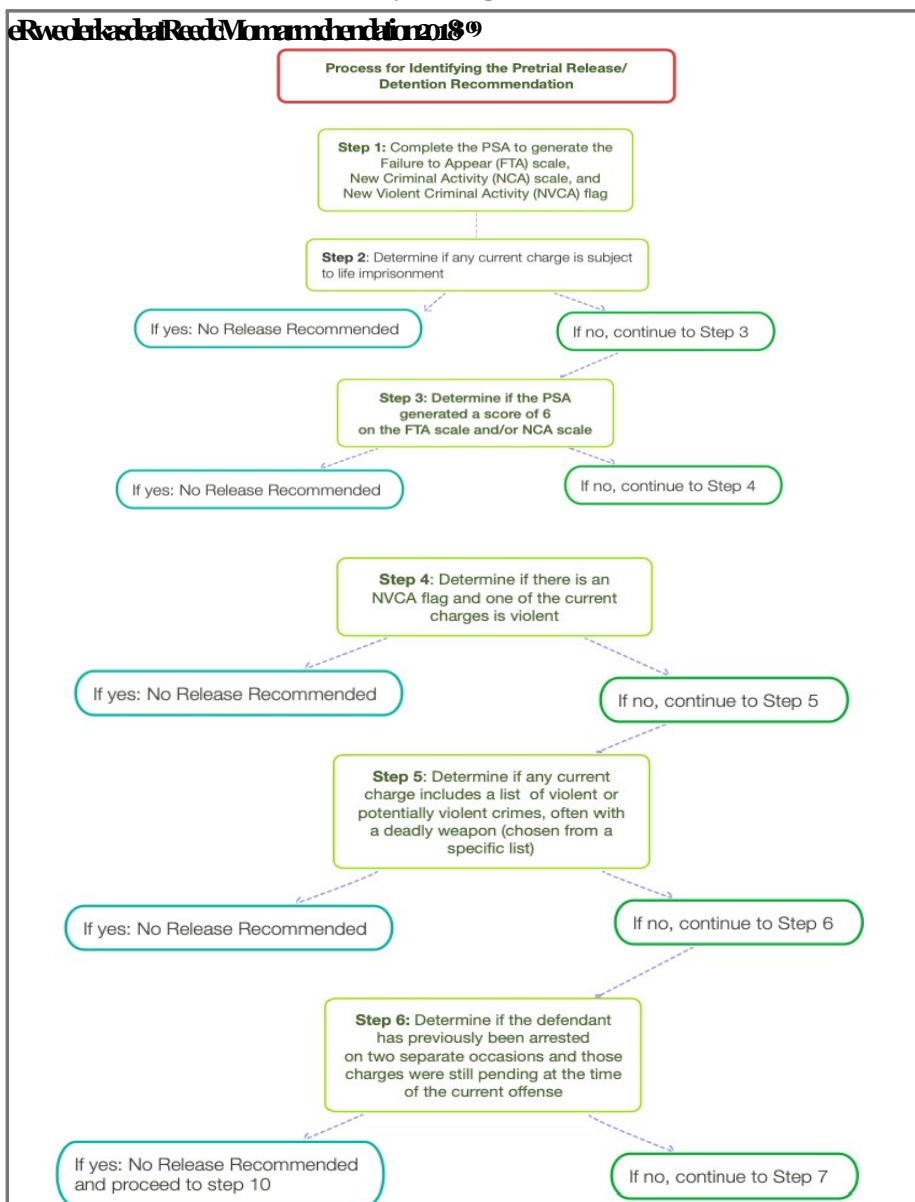
Factor 9.	A végeredmény megfogalmazása	A lehetséges válaszok
	<p>A végeredmény megfogalmazása</p> <p>caocnussideedrl</p> <p>efyofatcys</p> <p>ca jilolpud' yjg</p> <p>itainpocscfd</p> <p>e üreg</p> <p>kondicionálók.</p>	<p>"Ha neveztho eucs dleyfere a p... n</p> <p>dceainvted</p> <p>1 4</p> <p>caj jhd... nswr</p> <p>cajlo a a</p> <p>wisef, thoe answer</p> <p>" n</p>

A Laura és John Arnold Alapítvány szerint a fenti kockázati tényezőket "súlyozzák, és külön FTA-skálára [megjelenési kötelezettség elmulasztása] és új bűncselekmény skálára alakítják át, amelyek 1-től 6-ig terjednek, valamint egy új erőszakos bűncselekményre vonatkozó jelzőt (azaz az igen/nem bináris mutatóját)".³⁰⁷ Amint az egyik jelentés jelzi, a keretrendszer feltételezi, hogy ha az illetőt erőszakos bűncselekménnyel vádolták, akkor a bírák számára "megjelölik", hogy "nagy az erőszakos cselekmények lehetősége, és ezt az esetet alaposabban meg kell vizsgálni, mielőtt a szabadlábra helyezésről szóló döntést meghozzák".³⁰⁸ Ez egy logikus következtetés, amely kapcsolatot feltételez a korábban állítólagosan megtörtént és a jövőben megismétlődni vélt cselekmények között. New Jersey és a PSA-t alkalmazó más államok ezután a fenti kockázati tényezőket arra használják, hogy a bírót az alábbi 10 lépéses folyamat segítségével arra ösztönözzék, hogy óvadék ellenében engedje szabadon a személyt, amelyet az alábbiakban vizualizációként ábrázoltunk New Jersey márciusban kelt, előzetes letartóztatásban lévő szabadlábra helyezésre vonatkozó ajánlási döntéshozatali keretrendszerének alapján. 2018.

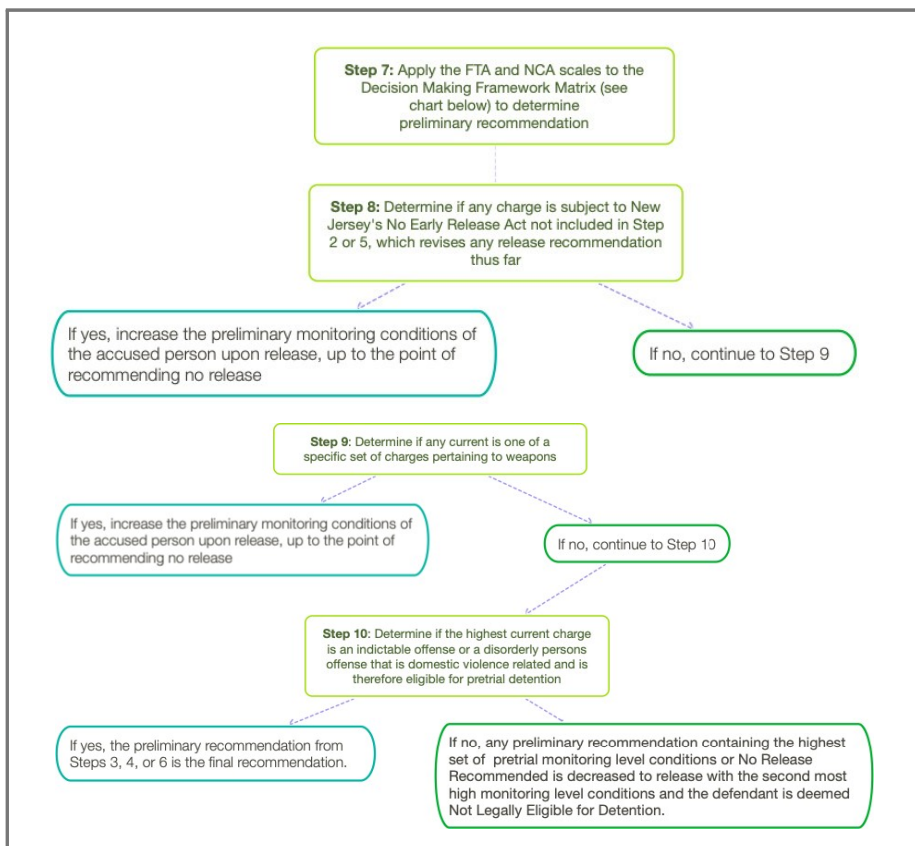
308 Ibid. 13.

124

ábra - 10 **ks**
NDecwisiJoernsMeya **ig**



309 "DP rMetFri al NRee wleJseersReyeCoomuntesndMinh D iding keret fi ()", (20 18), : ?
 : . g
 sca/wed= 2 8.
 ov/bírószágok/bírószágok/bűnügyi/decmakframework.



A fenti táblázatban és a vizualizációban több dologra is érdemes odafigyelni. Nagyon dicséretes, hogy New Jersey állam úgy döntött, hogy nyilvánosságra hozza ezeket a dokumentumokat. Azt is fontos megjegyezni, hogy vannak kizárási kritériumok arra vonatkozóan, hogy milyen információkat használnak fel ebben az aktuáriusi meghatározásban, például a fiatakorúak nyilvántartását, a családon belüli erőszakkal kapcsolatos távoltartási végzéseket, a "Petty Disorderly Persons" bűncselekményeket, valamint a helyi rendeletek vagy önkormányzati rendeletek megsértését.³¹⁰ A PSA-eszközt úgy alakították ki, hogy az

310 MPaurbach, Safety Assessment, New Jersey, Risk Factor Definitions - 2018 ", , :

http://www.courts.gov/courts/assets/criminal/psariskfactor.pdf?



legalábbis papíron csak ajánlásokat kíván adni a bírának az előzetes letartóztatásról vagy szabadlábra helyezésről szóló döntéseikhez. Azt is fontos megjegyezni, hogy az amerikai jogban már van precedens arra, hogy az óvadékot a fent felsorolt tényezők közül több alapján határozzák meg. Vegyük például az alabamai büntetőeljárás szabályokat, amelyek kimondják, hogy a vádlottnak vélelmezhetően joga van a szabadlábra helyezéshez óvadék ellenében vagy óvadék ellenében.³¹¹ Ahhoz, hogy a bíró a vádlottal szemben egyéb feltételeket szabhasson, olyan körülményeket "vehet" figyelembe, mint például a következők:

1. "A vádlott életkora, háttere és családi kötődései, kapcsolatai és körülményei;
2. A vádlott korábbi büntetett előélete, beleértve a korábbi szabadlábra helyezéseket szabadlábra helyezés ellenében, illetve óvadék ellenében, valamint egyéb folyamatban lévő ügyeket;
3. Erőszak vagy erőszak hiánya a bűncselekmény állítólagos elkövetése során."³¹²

Mindazonáltal számos olyan etikai kérdés van, amelyet a jogalkotóknak és a politikai döntéshozóknak figyelembe kellene venniük az algoritmikus eszközök használata során, mint amilyen ez az algoritmikus eszköz az előzetes letartóztatással vagy szabadlábra helyezéssel kapcsolatos döntésekben. Ezeket az alábbiakban ismertetjük, miután megvitattunk egy hasonló, mesterséges intelligenciával működő eszközt, amelyet az Egyesült Államokban az ítélelhozatali döntésekhez használnak.

5.1.3. A mesterséges intelligencia alkalmazása az ítélelhozatalban

A bíróságok a statisztikai és biztosításmatematikai eszközöket is egyre gyakrabban használják az ítélelhozatal során. Az ítélelhozatal a bíró

³¹¹ Alabama büntetőeljárás szabályai, fenti megjegyzés. 3.

döntés arról, hogy az elítélt személyt hogyan kell büntetni. A joghatóságtól függetlenül az ítéletek a kisebb pénzbírság megfizetésétől az életfogytiglani börtönbüntetésig, egyes joghatóságoknál pedig a halálbüntetés alkalmazásáig terjedhetnek. Az egyes joghatóságok eltérő módon határozzák meg az ítélethozatalt, de általában olyan tényezőkön alapulnak, mint az elkövetett bűncselekmény súlyossága vagy minősítése, az, hogy az adott személyt korábban már elítélték-e bűncselekményért, valamint a már meglévő irányelvek, amelyek alapján a politikai döntéshozók bizonyos bűncselekményeket meghatározott büntetést érdemlőnek ítélnék. Számos joghatóság már alkalmazza az olyan jelentéseket, mint az ítélethozatalt megelőző jelentés vagy az áldozatokra gyakorolt hatásról szóló nyilatkozatok, amelyek információkat nyújtanak a bíráknak, amikor arról döntenek, hogyan ítéljenek el egy személyt.

5.1.4. A COMPAS használata az ítélethozatal során

Az ítélethozatalban alkalmazott mesterséges intelligencia egyik kiemelkedő példája, amely nemrégiben került előtérbe, a COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) nevű szoftverrel kapcsolatos. A COMPAS jelentős figyelmet kapott, miután 2016-ban a hírmédia bemutatta, és a riporterek azt állították, hogy a szoftvert be nem vallott elfogultság jellemzi, különösen a feketékkel és más színesbőrűekkel szemben az Egyesült Államokban.³¹³A szoftver később újabb figyelemhullámot kapott, miután 2017 az Egyesült Államok Legfelsőbb Bírósága elutasította egy wisconsini férfi fellebbezését, akit hat év börtönbüntetésre ítélték, miután egy bíró a COMPAS kockázatértékelésének eredményeit vette figyelembe. A COMPAS mögött álló vállalat az Equivant (korábbi nevén

ents-in

~~Am~~

~~B~~

bJli

ecfa

f

~~LaMa~~

(2

,

3

~~ya0~~

M

~~6),~~

~~ant&~~

La

e:

ure

n

Kirc

hne

r,

"M

ach

ine h

~~is~~

i/n/

val

w-

swe

.

n

~~repi~~

~~ng~~

.

ca.

org

/art

icle

/ma

chin

e-

bias

-

risk

-

asse

ssm

Northpointe). A vállalatnak az Egyesült Államok számos államában vannak telephelyei: "Büntetőjogi szakemberként Ön felelős olyan politikák és gyakorlatok végrehajtásáért, amelyek csökkentik a visszaesést és őrzik a közbiztonságot. Mi biztosítjuk, tudományosan validált értékelési eszközöket, jelentős gyakorlati tapasztalatot és technikai ismereteket, amelyek szükségesek ahhoz, hogy segítsük Önt céljai elérésében."³¹⁴ A COMPAS a Northpointe által kínált egyik kockázatértékelési eszköz volt, amely a visszaesési arány csökkentésére és a "közbiztonság őrzésére" irányult.³¹⁵

A COMPAS-t 1998-ban fejlesztették ki, és a Northpointe fejlesztői 1998-ban vezették be a visszaesési kockázatértékelési komponenst. A szoftver többek között kifejezetten arra törekszik, hogy a vádlott által megválaszolt 137 kérdés vagy a bűnügyi nyilvántartásból származó információk alapján megjósolja, hogy a vádlott az értékeléstől számított két éven belül újabb bűncselekményt követ el.³¹⁷ A COMPAS-ról író újságírók a COMPAS adataira vonatkozó információkhoz közérdekű adatigénylés útján jutottak hozzá.³¹⁸ Az alábbiakban a kérdőív egy részének pillanatképét mutatjuk be, különös tekintettel arra, hogy a vádlottal folytatott interjút végző személy szerint a vádlott "feltételezett vagy bevallottan bandatag"-e vagy sem.

³¹⁴ "Sünetlen támogatás", Northpointe Inc. (Northpointe Inc.), <http://www.northpointe.com> archive.org/web/h20160307002839

³¹⁵ Ibid.

³¹⁶ "Sünetlen támogatás", Northpointe Inc. (Northpointe Inc.), <http://advances.sciencemag.org/content/4/1/eao5580.full>.

³¹⁷ Ibid.

³¹⁸ Angwin, Supra note 319.

ábra - COMPAS rendszerben használt kérdések 11

A

319

Current Charges

<input type="checkbox"/> Homicide	<input checked="" type="checkbox"/> Weapons	<input checked="" type="checkbox"/> Assault	<input type="checkbox"/> Arson
<input type="checkbox"/> Robbery	<input type="checkbox"/> Burglary	<input type="checkbox"/> Property/Larceny	<input type="checkbox"/> Fraud
<input type="checkbox"/> Drug Trafficking/Sales	<input type="checkbox"/> Drug Possession/Use	<input type="checkbox"/> DUI/OUIL	<input checked="" type="checkbox"/> Other
<input type="checkbox"/> Sex Offense with Force	<input type="checkbox"/> Sex Offense w/o Force		

1. Do any current offenses involve family violence?
 No Yes
2. Which offense category represents the most serious current offense?
 Misdemeanor Non-violent Felony Violent Felony
3. Was this person on probation or parole at the time of the current offense?
 Probation Parole Both Neither
4. Based on the screener's observations, is this person a suspected or admitted gang member?
 No Yes
5. Number of pending charges or holds?
 0 1 2 3 4+
6. Is the current top charge felony property or fraud?
 No Yes

Nem teljesen világos, hogy a COMPAS pontosan hogyan készíti előrejelzéseit. Az Equivant úgy döntött, hogy nem hozza nyilvánosságra, hogy algoritmusai hogyan jut el a döntésekhez, bár időnként elmagyarázta a munkája alapjául szolgáló elméleti logikát.³²⁰ Annyit tudunk, hogy a COMPAS szoftver a fent említett kérdőívben szereplő körülbelül jellemzőkre¹³⁷ támaszkodik, hogy előrejelzéseket készítsen a következőkre vonatkozóan: (i) a személy kockázata annak, hogy az értékeléstől számított két éven belül ugyanazzal a bűncselekménnyel vádolják meg, (ii) a bíróság előtti megjelenés elmulasztása, vagy (iii) annak valószínűsége, hogy a személy erőszakos bűncselekményt követ el.

319 "HSaomstpinleg-CsOerMviPcAeS-Roinslki-nAes sessment-COMPAS- ()",

'CORE"', DocumentCloud

702103

320 <http://www.compasscore.com/otmrgl/documents/2-Sample-Risk->

I WPreabcsitcee M sessment tp/wth ad/vie q/nd/E
" id (, in/nting/16), PoAnSinAes
En-oirmthppleominetnetiirncg.
centoi RACTE

nCeO

:

MPA

S

Soft
ware

",

Nort
hpoi

nte

(honl

ap,

via

p

:

:

ond

.

osr/ _COMPAS.pdf

cgo

/w

me

pba

/s/P

racti

tion

ers-

Gu/i

hdt

et-

Ø

pC

100

0229

.

MS

BS

.

Sy

sped

;

nf

"

Azt is tudjuk, hogy válaszul azokra az állításokra, amelyek szerint a COMPAS faji alapon elfogult a feketékkel szemben, az Equivant megpróbálta bizonyítani, hogy szoftverének általános előrejelzési pontossága minden etnikumra vonatkozóan átlagosan 68%, és azt állítja, hogy ez megfelel a kriminológiai tanulmányokban a megbízhatóságra vonatkozó, 70%-os vagy annál magasabb küszöbértéknek. ³²¹ Azt is kijelentette, hogy a COMPAS csak egy eszköz, amely a büntető igazságszolgáltatás keretében hozott döntések egy részét alkothatja, és ezért az általa kínált eredmények értelmezését indokolja.³²²

A Julia Dressel és Hany Farid tudósok által januárban közzétett tanulmány a COMPAS pontosságát igyekezett 2018 felmérni, és ennek során kimutatta, hogy a szoftver az esetek átlagosan 65%-ában pontos.³²³ Ez a tanulmány azt is kimutatta, hogy a COMPAS által készített visszaesési előrejelzések két jellemző alapján nem pontosabbak, mint a büntetőjogi szakértelemmel alig vagy egyáltalán nem rendelkező emberek által készített előrejelzések vagy az egyszerű statisztikai elemzés.³²⁴ Dressler és Farid tanulmánya megerősíti azt a megállapítást, amelyet az Equivant megpróbált megcáfolni, nevezetesen a ProPublica következtetését, miszerint a COMPAS általános visszaesési előrejelzései átlagosan 65,1%-ban pontosak voltak.³²⁵

³²¹ W. Isikoff & S. Meese, "Predicting Recidivism: The COMPAS Algorithm", *ProPublica*, 2016. <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>.

³²² "COMPAS: A Risk Assessment Tool Used in the Criminal Justice System", *ProPublica*, 2016. <https://www.propublica.org/article/compas-risk-assessment>.

³²³ Dressel & Farid, *Supra note*. 322.

³²⁴ Ibid.

³²⁵ J. L. Naraslojz, "The COMPAS Algorithm: A Risk Assessment Tool Used in the Criminal Justice System", *ProPublica*, 2016. <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>.

Ábra - 12 Egy kép a Northpointe korábbi weboldaláról³²⁶



Az amerikai kontextuson kívül olyan joghatóságok jogi kutatói, mint például Ausztrália, szintén elkezdtek vizsgálni a mesterséges intelligencia alkalmazását az ítélelhozatalban, abban a reményben, hogy az ítélelhozatal folyamata nemcsak "átláthatóbbá és gyorsabbá", hanem "igazságosabbá" és "pontosabbá" is válik.³²⁷

5.2. Hiányosságok a szakirodalomban és etikai aggályok

Számos olyan kutatási kérdés van, amelyet még fel kell tární, amikor az automatizált kockázatlértékelő eszközök büntető igazságszolgáltatási rendszerben történő használatáról van szó. A politikai döntéshozóknak tisztában kellene lenniük ezekkel a kevésbé vizsgált területekkel, amelyek etikai aggályokat vetnek fel a közbiztonság "örzését" célzó eszközök használata során. Először is, nem világos, hogy a kockázatlértékelési eszközök

³²⁶ <http://www.northpointe.com/Products/Tools/BarChartReport.aspx>, accessed 2018.01.15.

³²⁷ "The Australian Justice System", [http://www.austlii.edu.au/other/dfat/special/australia/justice.html](http://www.austlii.edu.au/au/other/dfat/special/australia/justice.html), accessed 2018.01.15.

Shwrtip: [http://www.austlii.edu.au/other/dfat/special/australia/justice.html](http://www.austlii.edu.au/au/other/dfat/special/australia/justice.html), accessed 2018.01.15.

meghaladja a büntetőjogi szakértelemmel rendelkező bírák átlagos pontosságát. Másodszor, nem világos, hogy az Egyesült Államokon kívüli joghatóságoknak kellene-e használniuk ezeket az eszközöket, hacsak az óvadéki és büntetés kiszabási eljárásaik nem mutatnak kimutatható hiányosságokat. Harmadszor, és végül, feltételezve, hogy ezeket az eszközöket egyes joghatóságokban még használhatják, Kelly Hannah-Moffat munkájára támaszkodunk, akinek a bűnügyi eljárásokban alkalmazott visszaesési és kockázatértékelési eszközök elemzése világossá teszi, hogy legalább három elsődleges aggály merül fel az ilyen vállalkozásokkal kapcsolatban: (i) az információk és eljárások pontossága és átláthatósága, (ii) az ítéletekre és az egyenlőtlenségekre gyakorolt hatás, valamint (iii) a kockázat beépítésének szükségessége az ilyen technológia alkalmazását szabályozó iránymutatásokba, a büntetőeljárás egyes elemeiben.³²⁸ A következő alfejezetek csak néhány olyan kérdést vázolnak fel, amelyeket az automatizált kockázatértékelő szoftverek beszerzésére törekvő politikai döntéshozóknak fel kell tenniük.

5.2.1. Van bizonyíték arra, hogy ezek az eszközök pontosabbak, mint a már meglévő rendszerek? Van-e bizonyíték arra, hogy a mesterséges intelligencia alkalmazása a jogi eljárásokban beváltja az ígéreteket?

Először is, Dressler és Farid 2018-as tanulmánya hiteles súlyt ad annak az érvelésnek, hogy nem egyértelmű, hogy a kockázatértékelő szoftverek növekvő (és gyakran szabályozatlan) piaca valóban kielégíti-e a büntető igazságszolgáltatási rendszerben felmerülő igényeket, és hogy az ilyen szoftverek valóban képesek-e teljesíteni az ígéreteiket. További információ:

— "Proposition" (2013) 30:2 Justice Quarterly 270-296, DOI:

³²⁸ Kelly Hannah-Moffat, "Aktuárius ítélethozatal: An 'Unsettled' Kern, "Nézet a terepről: A gyakorlati szakemberek válasza az 10.1080/07418825.2012.682603; Mark H. Bergstrom & Richard P. Sutton

Report of Audi ' (23) 25: 3 Bg n n
§ 4. state Propose? Insign (aud.), 18),
o ryle .

uřy . udicial reasoning, ther e Weres med autho it
hřir cřn e.

hasznos lehet a bírói döntések pontosságának meghatározása: például milyen gyakran korrelál a bíró azon döntése, hogy nem vesz őrizetbe valakit, azzal, hogy a vádlott nem jelenik meg a tárgyaláson? Milyen gyakran korrelál egy bíró őrizetbe vételre vagy elítélésre vonatkozó döntése azzal, hogy az adott személy a tárgyalást megelőző vagy követő időszakban ugyanazt vagy súlyosabb bűncselekményt követ el? Más szóval, szükség van-e olyan technológiára, amely az emberi döntéshozatal pontatlansága miatt, amely bizonyíthatóan kárt okoz az igazságszolgáltatási rendszernek vagy a közvéleménynek, segíti a bírákat az óvadékkal és az ítéletekkel kapcsolatos döntések meghozatalában?

Az ilyen kérdésekre adott konkrét és mérhető válaszok nélkül nehéz indokolni a mesterséges intelligencia sürgős alkalmazását a büntető igazságszolgáltatási rendszerben. Egyébként a mesterséges intelligencia továbbra is vonzó eszköz marad, amely lenyűgözheti a politikai döntéshozók, valamint a számítógépes és az adattudósok intellektuális kíváncsiságát, de ez a technológiai beavatkozás és az igazságügyi ösztönzés megbízhatatlan adatok felhasználásával kárt okozhat a büntető igazságszolgáltatási rendszerrel szembenézőknek, anélkül, hogy konkrétan bizonyítható lenne, hogy egyáltalán szükség van ilyen erős statisztikai technikákra és algoritmusokra. Ha a COMPAS-hoz hasonló eszközök valóban a szükségesnél jóval több változót használnak olyan értékelésekhez, amelyeket sokkal kevesebb tényezővel is el lehetne végezni, és ha az olyan algoritmikus eszközök, mint a PSA vagy a COMPAS, nem bizonyíthatóan felülmúlják az emberek kockázatértékelési pontosságát, akkor minden felelős, közérdekből eljáró politikai döntéshozónak vissza kellene fognia az ilyen eszközök használatát mindaddig, amíg egy világosan meghatározott próbaidőszak során meg nem bizonyosodik arról, hogy a hatékonyság és pontosság terén elért nyereség meghaladja a lehetséges károkat.

5.2.2. Egy adott kontextusban létrehozott és/vagy használt mesterséges intelligencia eszközt kell-e használni egy másik kontextus eltérő igényeinek kielégítésére?

Másodszor, az Egyesült Államokon kívüli politikai döntéshozóknak tudatosítaniuk kellene magukban azt a rendkívül sajátos kontextust, amelyben az olyan eszközök, mint a PSA és a COMPAS létrejöttek, és kritikusan meg kellene vizsgálniuk, hogy a saját joghatóságuknak ugyanezekre az igényekre van-e szüksége. Vegyük figyelembe, hogy az Egyesült Államokban számos államban jelentős reformok zajlanak az óvadék- és büntetés kiszabási rendszerekben, előbbi bíralták a szegény vagy alacsony jövedelmű emberekkel szembeni rendszerszintű megkülönböztetés fenntartása miatt, utóbbiban ³²⁹pedig legalább az elmúlt tíz évben mind állami³³⁰, mind szövetségi szinten jelentős változások történtek.³³¹ Az amerikai büntető igazságszolgáltatási rendszer egyben a világ egyik leginkább privatizált rendszere is, ahol egy egész iparág tervezi és forgalmazza a termékek és szolgáltatások széles skáláját a növekvő igények kielégítésére.³³² Ezeket a tényeket szem előtt tartva érthető, hogy a bűnügyi igazságszolgáltatási rendszeren belül a mesterséges intelligencia néhány kiemelkedő esete

329 [M. H. ...](#), "The Wired ...", (1)

0 18), :
<https://www.wired.co.uk/article/police-ai-uk-durham-hart-check>

330 [M. Wolff](#), "Bizonyítékalapú bírói mérlegelés:

Pr on Nat'ny Puk U Safety Th Lawg Re Seve Sent R Reform" (2008)
 83 5
<http://www.view.org/wp-content/uploads//NYULaw201808>

331 [...](#), "ral Criminal Justice Reform in 2018" (2018) 26:10
 , oferte

332 <http://www.view.org/te h/civil-and-criminal-justice/federal-criminal>
 i/c/ew-rwewfo me ZRanc

[Oxford U ...](#)
[Oxford U ...](#)
 Tochieetcyul(: , ,
 2001)

Az is logikus, hogy az ezeket az eszközöket létrehozó vállalatok és szervezetek - legyen szó a Laura és Arnold Johnson Alapítványról vagy az Equivantról - az Egyesült Államokban székhellyel rendelkeznek, és saját kulturális valóságuk és joghatóságuk sajátos igényeire reagálnak.

Másrészt az Egyesült Államokban a kockázatértékelési eszközöket a készpénzes óvadékrendszerről való elmozdulás nyomán kezdték el használni; az olyan eszközöket, mint a PSA, egy kirívóan igazságtalan paradigma ellenszereként vagy megoldásaként állították be. Egyáltalán nem egyértelmű, hogy más országok előzetes szabadlábra helyezési rendszere ugyanazokat a hiányosságokat vagy problémákat mutatja, mint az Egyesült Államokban. Ebben az értelemben a PSA-hoz hasonló eszközök alkalmazása az Egyesült Államokon kívül inkább problémákat okozhat, mintsem hogy enyhítené a már létező problémákat. Az egyes joghatóságok technológusainak, jogászainak és döntéshozóinak ezért hihetetlenül óvatosan kell eljárniuk, amikor az amerikai büntető igazságszolgáltatási rendszerre létrehozott és optimalizált mesterséges intelligencia technológiát átadják vagy alkalmazzák.

5.2.3. A technológia tervezése és alkalmazása bizonyítottan átlátható, a veszélyeztetett népességcsoportokat érintő károk enyhítése, valamint az általa jelentett kockázatokkal kapcsolatos tájékozott beleegyezés lehetővé tételének követelménye mellett történik-e?

Minden kormánynak és politikai döntéshozónak, amely fontolgatja a mesterséges intelligencia alkalmazását a büntető igazságszolgáltatási rendszerében, érdekében áll, hogy a legmagasabb etikai normákat állítsa fel az ilyen eszközök tényleges alkalmazásához. Hannah-Moffat kriminológus munkájára támaszkodva azonosítunk néhányat ezen ideális etikai célok közül, és a munkáját kritikusan értékelő gyakorlati szakemberek megállapításaira támaszkodva azonosítunk

néhányat e célok eléréséhez szükséges eszközök közül. Egészen egyszerűen,

136

Hannah-Moffat amellett érvel, hogy a büntető igazságszolgáltatási rendszerben használt kockázatértékelési eszközöknek nemcsak indokoltnak kell lenniük, hanem elő kell segíteniük a tisztességes eljárást (vagy eljárási méltányosságot), és tájékoztatniuk kell a bírákat az ilyen technológia alkalmazásával járó fenntartásokról és kockázatokról, különös elkötelezettséggel a rendszerszintű megkülönböztetés újratermelődésének lehetősége ellen. Ez nem kis feladat. Két amerikai gyakorlati szakember, mindketten Pennsylvania és Virginia állam büntetéskiszabási bizottságának igazgatói, betekintést nyújtottak abba, hogy más joghatóságok hogyan próbálhatják meg elérni ezeket a célokat.

Virginia állam például hosszú folyamatot indított el a kockázatértékelési eszköz kifejlesztése érdekében, amely kísérleti teszteléssel, független értékeléssel és számos érdekelt fél - bírák, állami tisztviselők, törvényhozók, büntetés-végrehajtási tisztviselők, ügyészek, kirendelt védők, védőügyvédek, kriminológusok és az áldozatok szervezeteinek képviselői - részvételével végzett újraértékelési tanulmányt tartalmazott.³³³ Más joghatóságoknak is meg kellene vizsgálniuk annak lehetőségét, hogy a kockázatértékelési jelentéseket nyílt tárgyaláson mutassák be a bírák előtt, hogy a pártfogó felügyelők megállapításait és általában a jelentést keresztkérdések tárgyává tehesék mind a védőügyvédek, mind az ügyészek, akik Virginiában legalább egy hétig hozzáférhetnek a jelentéshez.³³⁴ Amint az elképzelhető, a virginiai Büntetőjogi Büntetéskiszabási Bizottság igazgatója kijelenti, hogy bőséges bizonyíték van arra, hogy a bírák jelentősen támaszkodnak a kockázati eszközökre, amelyek bizonyítottan megváltoztatták az állam egész területén az ítélezési gyakorlatot, olyannyira, hogy a kockázatértékelési eszközök "megváltoztatták a bűnelkövetők áramlásának

³³⁴ Ibid.

³³³ Bergstrom, supra note at 3344.

börtönbe, börtönbe és közösségi alapú szankciókba."³³⁵ Azok a döntéshozók, akik meg vannak győződve arról, hogy a kockázatértékelési eszközöket be kell vezetniük, két dolgot tehetnek annak érdekében, hogy felmérjék, tudatában legyenek és enyhítsék a károkat:

1. Biztosítani kell, hogy a kockázatértékelés megállapításai csak egy részét képezzék a tanácsadói döntéshozatali iránymutatásoknak. Ez csökkentené az ilyen jelentésekre való túlzott bírósági támaszkodást;
2. Minden kockázatértékelési jelentésben szerepeljenek konkrét, megbízható empirikus adatok, például statisztikák, amelyek bizonyítják, hogy a vádlott jellemzőivel rendelkező személyek túlreprezentáltak a büntető igazságszolgáltatási rendszerben. A kockázatértékelési eszköz kockázatainak kezelésével a politikai döntéshozók ellensúlyozzák azt a valóságot, hogy bizonyos marginalizált csoportok a kockázatértékelési eszközökkel magasabb pontszámot érnek el, mivel ki vannak téve a megkülönböztetésnek és az egyenlőtlenségnek, és nem azért, mert nagyobb valószínűséggel lesznek visszaesők;³³⁶
3. A büntető igazságszolgáltatási rendszerben használt automatizált technológiákkal kapcsolatos szilárd és alapos képzés biztosítása minden fontos szereplő (védőügyvédek, ügyészek, bírák, pártfogó felügyelők) számára. Hogy ismét Virginia kontextusából tanuljunk, ez a képzés olyan alapos, hogy magában foglalja "az eszköz keletkezését, a tanulmányt és annak eredményeit, valamint a kockázati eszközt és azt, hogy annak minden tényezőjét hogyan kell helyesen pontozni".³³⁷ Ennél is több, "szükségszerűen magában foglalja az aktuáriusi kockázati eszközök korlátainak és erősségeinek lefedését is".

³³⁵ Ibid.

336 Ibid. 6.

337 Ibid. 4.

hogyan helyesen tudják értelmezni és alkalmazni az eredményeiket." 338

Számos más, itt fel nem vetett kérdés is van - például az, hogy a kockázatértékelésnek statikus, történelmi vagy meghatározatlan, kortárs tényezőket kell-e használnia a kockázat értékeléséhez. Ebben a szakaszban megkíséreltük azonosítani azokat a helyeket a büntetőeljáráson belül, ahol a mesterséges intelligenciát alkalmazzák. Kutatásunk azt mutatja, hogy a mesterséges intelligenciát eddig különösen az óvadékkal és az ítélethozatallal kapcsolatos döntéseknél alkalmazták az elkövetői kockázatértékelés során.

Számos további vizsgálatot igénylő kérdést is azonosítottunk, amelyek azt firtatják, hogy szükség van-e egyáltalán mesterséges intelligenciára a bírói érvelés fokozásához vagy javításához, hogy helyénvaló-e az egyik joghatóságra optimalizált mesterséges intelligencia technológiát más területekre átültetni, és hogy a bíróságok mindazonáltal azonosították és mérsékelték-e az általuk választott mesterséges intelligencia rendszerrel kapcsolatos kockázatokat.

Táblázat 3 - A mesterséges intelligencia alkalmazása a büntetőeljárásokban

Ország	Alkotó	Cél és képességek
<p>USA</p> <p>Parole Commission</p> <p>COMPAS³³⁹</p>	<p>Northpointe,</p>	<p>algorithm-based</p> <p>bármilyen</p> <p>U.S. Supreme Court</p> <p>and</p> <p>COMPAS</p> <p>reduces the risk of</p> <p>recidivism/harm to the</p> <p>community</p> <p>asc al exclusio</p>

bid.

	Alkotó	Cél és képességek
<p>PAussbelsicsmSeanf etty (PSA)³⁴⁰</p> <p>Pretrial kockázat</p>	<p>Alapítvány</p> <p>US Office of</p>	<p>of</p> <p>Use of</p> <p>ec</p> <p>Pretrial</p> <p>of</p> <p>Pre-s</p> <p>ncedefendss sment</p> <p>enteriska e</p>
<p>Virginia Pretrial</p>	<p>Preotbraiatil onand</p> <p>Luminozítás,</p>	<p>Pretrial</p> <p>elő</p> <p>eszköz</p>
<p>(VPRAI)³⁴² PREDICTICE</p>	<p>Predictice</p>	<p>misokt</p>
<p>343</p> <p>Matematikai</p>		<p>tersrso,</p> <p>psoiarawumteer</p> <p>acopurognosis</p> <p>Fstatisztikák alapján.</p> <p>romaslaw</p> <p>lásis a</p>
<p>dicial arinsdkju³⁴⁴</p>		<p>a kockázat számszerűsítése négy</p>

	Alkotó	Cél és képességek
Analitikai	Doctrine.fr	cél : a rendszer (withongfuleadisamnidssal); ceodmnutpriebnuostaiotonrytcobemn ; d aeifnittse tealmofalyol)reof(abrucpat alapítva kereskedelmi kapcsolatok. intelligencia mesterséges
		, with , vagy sthime h m deecthiseimones. utalások

339 " AS kockázat- és szükségletértékelő rendszer", Northpointe
 cGoIMeP:

(honlap), http://www.northpointeinc.com/files/downloads/FAQ_Document.

340 " ty Assoct Ferni tőh a p r m o t e s b i z t o n s á g ,
 a P n u d b j u c s t S i a c f e e ",
 p . a f e r t o y d e f u i n y d a u s t i n e . o r g / p u b l i c - s a f e t y - a s s e s s m e n t - r i s k - t o o l

341 " h : // A w s w s e w s s . .

342 orPg/rMetriciarlosJuitsetsic/PeJCeCn/Hteormfoer/TCoopuircts/R
 Van Nostand & Kenneth Rosen "Practical Risk Assessment In
 : / a w (w w w i .) . i c a v i d / g e l p r i n a t a . i r g / l i s t
 ge/Mequb1

343 /cLoarjcuicttiocnes/pvriregdiincitai-vpere t r / a l - r k ot-urveeprotrut.
 " (1 § : ' e n g s u s c h e i
 M t t a g t u (B o l o n g d ,
 : / o / i n t e r n I n e t a e c r n t u e . e .
 pedd es données",

9 frS/epte/mb/er9/la-jus2109 ticoen-lpinreedi ctive
 -LI-nlétneljleigue-dnéc-eloaurvtiefriictulerlele-daeus-

344 " dsoernvnicesd/&
 ' e la quantification du risque
 juri ",
 Weboldal), online:
 : # C a r e l l a w s a c a l n

345 " ~~Le~~ ~~droit~~ e juridique", Doctrine (honlap), online:
<https://www. . .>

6. KÖVETKEZTETÉS ÉS AJÁNLÁSOK

Ebben a jelentésben megpróbáltunk áttekintést nyújtani a mesterséges intelligencia technológiák számos meglévő és jövőbeli alkalmazásáról a büntető igazságszolgáltatási rendszerben, kezdve a rosszindulatú mesterséges intelligencia online elkövetők általi felhasználásától a bűnüldöző szervezetek által a bűncselekmények felderítésére, előrejelzésére és kivizsgálására történő alkalmazásáig. A bírósági tisztviselők és a büntetés-végrehajtási szolgálatok is egyre inkább a mesterséges intelligenciára támaszkodnak a bűnelkövetők kockázati szintjéről, bűnösségéről, elítéléséről és szabadon bocsátásáról szóló döntések meghozatalában. Mint megállapítottuk, egyre több eszköz ígéri, hogy lehetővé teszi az adatáradat feldolgozását a komplex döntéshozatal támogatása érdekében, a modern társadalmak biztonságának fokozása céljából. Ezek az AI-eszközök azonban négy fő kihíváskategóriát is felvetnek, amelyek az egyéni szabadságjogokra gyakorolt potenciális hatásuk miatt különösen kritikusak a büntető igazságszolgáltatás területén: etika, hatékonyság, beszerzés és kisajátítás. E négy kérdéscsoport szorosan összefügg egymással, befolyásolják és felerősítik egymást, és alaposan meg kell őket vizsgálni, mielőtt a mesterséges intelligenciát széles körben elfogadnák és rutinszerűen beépítenék a büntető igazságszolgáltatási eljárásokba.

6.1. Etikai kihívások

A mesterséges intelligencia eszközeinek büntetőjogi környezetben történő fejlesztése és alkalmazása által teremtett központi kihívás etikai jellegű. Ha a mesterséges intelligencia kétségtelenül számos vitathatatlan társadalmi

Az olyan előnyök, mint a megbízhatóbb orvosi diagnózis, a kevésbé zsúfolt (és ezért szennyezett) utak, vagy a jobb mezőgazdasági eredmények a fejlődő országokban, hogy csak néhányat említsünk, a bűnüldözési vagy igazságszolgáltatási kontextusban való alkalmazása számos erkölcsi dilemmát vet fel, amelyek az olyan alapelvekkel való ütközéshez kapcsolódnak, mint a méltányosság és az igazságosság. Virginia Eubanks alapvető jelentőségű könyvében például bemutatta, hogy a társadalmi ellenőrzés ezen új algoritmikus eszközei hogyan zárhatják ki és izolálhatják társadalmaink legkiszolgáltatottabb tagjait, behatolva életükbe, megtagadva tőlük az alapvető szolgáltatásokat, vagy kiemelve őket a beavatkozás fokozott formái számára.³⁴⁶

Az előző fejezetekben már felvázoltuk ezen etikai dilemmák gyakorlati megnyilvánulásait a bűnüldözési és büntetőeljárásokban, ezért itt nem ismételjük meg ezeket az aggályokat. Ehelyett azokra az etikai keretekre összpontosítunk, amelyeket a mesterséges intelligencia negatív társadalmi hatásainak minimalizálása érdekében dolgoznak ki. Mivel magasabb szintű általánosságban fogalmazták meg őket, hogy a helyzetek lehető legszélesebb körére alkalmazhatóak legyenek, ezek az etikai keretek jó kiindulópontot jelentenek azon büntetőjogi szervek számára, amelyek átlátható megközelítést kívánnak alkalmazni a mesterséges intelligencia technológiák alkalmazása során. Bár több is rendelkezésre áll, mi öt olyan keretrendszerre összpontosítunk, amelyeket a legkülönbözőbb megközelítések révén alakítottak ki, beleértve a szabályozó hatóság (Franciaország), a jogalkotók (Egyesült Királyság), a tudósok és mérnökök (Japán és az IEEE) vagy egy akadémiai intézmény (Kanada) által vezetett erőfeszítéseket.

³⁴⁶ Passoglu, D. (2017). *Automated Justice*. New York: NYU Press.

14
4

Táblázat - A meglévő mesterséges intelligencia etikai keretek áttekintése³⁴⁷

Keretrendszer	IEEE (AIATóság)	AI Ethics Center iránymutatók	House of Lords hírszerzéssel foglalkozók	AI Engineering V. 2 (IEEE)	AI Principles
Country	Franciaország	Japán	UK	Nemzetközi	Kanada
Kiadott év	2017	2017	2018	2018	2018
Érdekeltek	3000+ személy	Etikai bizottság	57 szakértő a	Több száz	Több mint 500
konzultált	5-6 szervezet (public link, utannikns, vállalatok)	10-12 szervezet (IAS, STS kutató)	AI szakértők	AI, industry, kormányzat	AI, industry

³⁴⁷ O'Hare, M. & S. J. (2018). *AI Ethics: A Framework for the Development of AI Systems*. London: Springer.

³⁴⁸ Association for Computing Machinery (ACM). (2018). *AI Ethics Principles*. Available at: <https://www.acm.org/publications/ethics>

El
ek
tr
on
ik
us
an
el
ér
he
tő
a
kö
ve
tk
ez
ő
cí
m
en
:
htt
ps
://
ss
rn
.c
o
m/

Keretrendszer	IEEENormatóság	Intelligenciairánymutatók	Housesectorfordíróhírszerzéssel foglalkozó	AligEntehdicaDelysign V. 2 (IEEE)	DataManagementPlatform
Alapelvek	F (és éberség	Integritás Responsibility g AI	Ha a táplálkozás originhuttserosr magánélet Alighanem az egészet a emberi lények	M T S	V S P R S nasibblielity

14
6

szövegek:

vive cmligile

TFraablnee: , Hogyan tarthatja meg az ember a fölényét? Az algoritmusok és a hrttipsic:wt .
(: 27)

fron/Palagroisrit hCmosm-amndis-sairotinfNialt-ionnteeleigJennfcoer-mcnaitlisq-urep&ortLebheitas- issues által
online a következő címen

felvetett etikai kérdések.

Japán : T <http://www.iaai.or.jp/eng/SAH/Guide>

(<http://www.iaai.or.jp/eng/SAH/Guide> 2017. pdf)

és a oldalon.

(<http://www.iaai.or.jp/eng/SAH/Guide> 2017/AI/09

Koreai
-willinga

EGYESÜLT KIRÁLYSÁG: Se www.iaai.or.jp/eng/SAH/Guide , az Egyesült Királyságban: Kész,

nKdoNabBeP200303.pdf.

? (ndon: Ház www.iaai.or.jp/eng/SAH/Guide, 2018), : <https://ethicsinaction.ieee.org/>
v2, (Piscataway : IEEE 2018), online a <https://ethicsinaction.ieee.org/>

Kanada: Déclaration de Montréal IA responsable, Rapport de la Déclaration de Montréal pour un
design

développement responsable de l'intelligence artificielle (Montréal: Université de Montréal 2018).

Ezt az öt keretrendszert olyan alapelvek kötik össze, amelyek az átláthatóságot (és ezáltal a demokratikus vita és részvétel elősegítését e technológia felhasználásáról), az egyének és a társadalom számára nyújtott előnyöket, a magánélet tiszteletben tartását és az elszámoltathatóságot hangsúlyozzák. Még ha ezen elvek többsége túlságosan elvontnak is tűnik, a fent felsorolt keretrendszerek közül néhány részletesebb politikai és tervezési ajánlásokat tartalmaz, amelyeket be lehet építeni a tényleges mesterséges intelligencia rendszerekbe. Emellett még nem került megvitatásra az a kényes kérdés, hogy megakadályozzuk, hogy az innovatív bűnözői szereplők kihasználják a nyitottság és a tisztességesség ezen elveit a jogszerű megfigyelési és végrehajtási tevékenységek elkerülése érdekében. Az elkövetők és áldozataik egymásnak ellentmondó jogai közötti elkerülhetetlen feszültséggel sem foglalkoztak. Talán ezek az aggodalmak kissé elhamarkodottak, mivel néhány kutató kezdi megkérdőjelezni a mesterséges intelligencia állítólagos hatékonyságát a megbízható előrejelzések készítésében a rendkívül strukturálatlan alkalmazási területeken.

6.2. Hatékonysági kihívások

A mesterséges intelligencia általánosságban, és különösen a mélytanulás terén több évtizedes szünet után az elmúlt néhány évben lenyűgöző előrelépések történtek. Ezek azonban eddig csak néhány olyan területre korlátozódtak, ahol az adatok bőségesek és már meglehetősen jól strukturáltak és címkézettek, mint például a beszédfelismerés és fordítás, a képfelismerés vagy a játék.³⁴⁸ Gary Marcus, a NYU pszichológiai professzora, aki egy gépi tanulással foglalkozó céget is alapított, a legátfogóbban fejtette ki, hogy miért nem tűnnek a DL-megközelítések túlságosan alkalmasnak a következőkre

³⁴⁸ Marcus, *Supra* note at 221.

instabil területekre, ahol korlátozott adatokból kell általánosításokat tenni. Felsorolja azokat a kihívásokat¹⁰, amelyeket már az 1. fejezetben említettünk, de úgy véljük, hogy itt is részleteznünk kell, hogy szemléltessük, hogy a mesterséges intelligencia által bizonyos területeken elért lenyűgöző eredmények miért nem feltétlenül vihetők át zökkenőmentesen a büntetőjogi alkalmazásokra:

- Míg az emberek gyorsan tanulnak néhány szabályból és példából, a gépi tanulási modelleknek hatalmas mennyiségű adatot kell feldolgozniuk ahhoz, hogy megbízható döntéseket hozzanak. Az a használható adatmennyiség, amelyet a bűnügyi szervek a ritka bűncselekmények ritka formáira vonatkozó mesterséges intelligenciamodellekbe betáplálhatnak, nem biztos, hogy elegendő ahhoz, hogy megbízható előrejelzéseket hozzanak létre;
- A számos mesterséges intelligencia eszköz alapjául szolgáló tanulási folyamat is sekélyesebb vagy szűkebb, mint azt a Deep Learning terminológia alapján gondolnánk, ami azt jelenti, hogy az egyik területen (nyelvi fordítás) elért lenyűgöző teljesítményt nem lehet könnyen átültetni egy másik területre (például a visszaesés esélyének előrejelzésére);
- A mélytanulásnak nincs természetes módja a hierarchikus struktúra kezelésére, ami azt jelenti, hogy az összes rendelkezésre álló változót ugyanazon a szinten, "laposnak" vagy nem hierarchikusnak tekintik. Ez komoly akadályt jelent, amikor a döntéseknek nagy erkölcsi vagy jogi súlya van, amelynek felül kell írnia más jellemzőket;
- A mélytanulási eszközök küzdenek a nyílt végű következtetésekkel, amelyeket egy nyomozó, egy bíró vagy egy felügyelőtiszte intuitív módon és könnyedén fel tudna venni;
- Az AI-eszközök "fekete doboz" jellege lehetővé teszi számukra, hogy

több ezer vagy akár több millió változóra épülő előrejelzések, amelyek kölcsönhatása emberi elemzéssel nem vizsgálható. Ez a rendkívüli összetettségi szint azt a reflexív folyamatot is nagyon nehéz megmagyarázni, amely ezekhez a jóslatokhoz vezetett. Ha ez az átláthatatlanság nem is lenne túl ellentmondásos a macskaképek címkézésekor vagy a YouTube-videók feliratozásakor, sokkal aggasztóbb, amikor a mesterséges intelligencia eszközeit arra használják, hogy felmérjék egy elítélt bűnöző visszaesési kockázatát, vagy akár megelőző járőrözést folytassanak kisebbségi negyedekben, amelynek eredményei és hibalehetőségei sokak életét és szabadságát befolyásolhatják;

- Ezt súlyosbítja az a tény, hogy a mesterséges intelligencia rendszerek alig tudják megkülönböztetni az ok-okozati összefüggést a korrelációtól, ami problematikus azon intézmények számára, amelyeknek magas szintű elszámoltathatóságot kell fenntartaniuk;
- A fent említett "lapos" és "fekete doboz" megközelítések miatt a mélytanulás ellenáll az előzetes tudás integrálásának. Nagyon árulkodó például, hogy a PredPol algoritmus magját a szeizmológiából kölcsönözték, ahelyett, hogy a kriminológiában elterjedt, a bűnözés és a hely többféle elméletéből fejlesztették volna ki.³⁴⁹ Az előzetes tudás elismerésének elutasítása szándékosnak tűnik, mind ismeretelméleti szempontból, egyrészt egy olyan kutatási terület története miatt, amely a megoldandó, önálló problémákat részesítette előnyben, másrészt technikailag, mert ez azt jelentené, hogy a mesterséges intelligencia eszközei kevésbé lennének hatékonyak. Tehát azokon a területeken, ahol a tudást nagyon különböző területeken kell integrálni (mint például a büntető igazságszolgáltatásban), az ember továbbra is az ember marad.

sokkal hatékonyabb, mint a mesterséges intelligencia, még akkor is, ha a kutatók vizsgálják a "tanulószerződéses tanulás" lehetőségeit, hogy a gépek tanulhassanak a szakértők munkájának megfigyeléséből;³⁵⁰

- A fentiekben kiemelt technikai jellemzők azt jelentik, hogy a mesterséges intelligencia rendszerek a leghatékonyabbak olyan stabil környezetben, ahol a mögöttes változók és az eredmények közötti kölcsönhatások időben állandóak maradnak, és az adatok növekvő hozzáférhetősége csak fokozhatja a rendszer teljesítményét. Sajnos a bűnözők nagyon innovatívak, akik fáradhatatlanul új módszereket találnak ki arra, hogy manipulálják környezetüket, és kikerüljék a társadalmi ellenőrzési mechanizmusokat és a végrehajtási stratégiákat;
- A mesterséges intelligencia rendszerek egyik fő jellemzője továbbra is a törekenység: a legtöbbször nagyon szűk körű feladatokban képesek az embereket felülmúlni, de látványosan kudarcot vallhatnak, ha az általuk elemzett adatok látszólag apró részletei megzavarják belső logikájukat. Jiawei Su és kollégái egy nagy nyilvánosságot kapott tanulmányban kimutatták, hogy egy képfelismerési feladatokat végző mélytanuló algoritmust egyetlen pixel megváltoztatásával is át lehet verni egy egyébként teljesen normális képen. Ennek eredményeképpen egy lovat békaként, egy szarvast repülőgépként vagy egy macskát kutyaként azonosított tévesen.³⁵¹ Elképzelhető, hogy a büntető igazságszolgáltatási szerveknek sokkal robusztusabb és megbízhatóbb eszközökre van szükségük, amelyek nagyon korlátozott hibaarányal rendelkeznek;

³⁵⁰ [https://arxiv.org/abs/1706.03826](#), A., "fooling deep neural networks", (Paper) [https://arxiv.org/abs/1706.03826](#)

³⁵¹ [https://arxiv.org/abs/1706.03826](#), 4-July 2014), online:

[https://arxiv.org/abs/1706.03826](#) 01 543.

J. Su, D. Vasco cellos Vargas, & K. Sakurai, "One pixel attack for
arXiv:1710.08864 [cs.LG], online: <https://arxiv.org/abs/1710.08864v4>.
150

- Végezetül, mérnöki szempontból úgy tűnik, hogy még a nagy teljesítményű mesterséges intelligencia rendszereket is nehéz beágyazni a néhány évtizede működő örökölt rendszerekbe, különösen a büntető igazságszolgáltatási szervek esetében, amelyek más szervezeteknél lassabban alkalmaznak új technológiákat, és ezért olyan örökölt rendszerekkel működnek, amelyek jelentős súrlódásokat okoznak a kortárs technológiákkal.³⁵²

Ezért nagyon óvatosnak kell lennünk a mesterséges intelligencia rendszereket és azok valós életbeli alkalmazásait övező marketing-felhajtással kapcsolatban, amelyet bürokratikus szervezetek folytatnak, amelyek nem mindig rendelkeznek az ilyen paradigmaváltáshoz szükséges készségekkel, infrastruktúrával és kultúrával. A Gartner tanácsadó cég által népszerűsített koncepciót idézve, az AI talán elérte a "felfújt elvárások csúcsát", de a "termelékenység csúcspontja" még évek múlva következhet be.³⁵³ A mesterséges intelligenciával kapcsolatos ígéreték és a valóság közötti szakadékra példa a The Guardian nemrégiben megjelent oknyomozó cikke, amely az "ál-intelligenciák" esetét vizsgálta, ahol az ilyen rendszereket értékesítő vállalatok fejlődő országokban embereket alkalmaznak, hogy kézzel végezzék el a technológiájuk által automatizálnak vélt munkát.³⁵⁴ Ez a

³⁵² . . . & . . . " [The rise of 'pseudo-AI': how tech firms quietly use](#)

[https://www.ft.com/content/2018/06/27/pseudo-ai-tech-firms](#)

" [Management](#)," (1996)9 : 4International Journal of Public Sector

" [Journal of Public Administration](#)," (1996)11 : 1

³⁵³ [https://www.gartner.com/en/newsroom/press-releases/2018-06-27-gartner-hype-cycle-for-artificial-intelligence-2018](#)

[https://www.gartner.com/en/newsroom/press-releases/2018-06-27-gartner-hype-cycle-for-artificial-intelligence-2018](#)

³⁵⁴ . . . on. "The rise of 'pseudo-AI': how tech firms quietly use [https://www.ft.com/content/2018/06/27/pseudo-ai-tech-firms](#)

[https://www.ft.com/content/2018/06/27/pseudo-ai-tech-firms](#)

elligence-ai-emberek-robotok-tech-

vállalatok.

"addig hamisítsd, amíg nem sikerül" megközelítés figyelmeztetésként kell szolgálnia a bűnügyi igazságügyi ügynökségeknek, amelyek mesterséges intelligencia eszköz beszerzését fontolgatják, ami kihívásokkal teli feladat, amint azt a következő szakaszban látni fogjuk.

6.3. Közbeszerzési kihívások

A fent vázolt etikai és technikai megfontolások a bűnügyi igazságügyi szervezetek által a mesterséges intelligencia rendszerek beszerzési folyamataiban is visszaköszönek, számos eljárási kérdést vetve fel, amelyek viszont maguk is etikai és teljesítménybeli következményeket eredményezhetnek, ha nem megfelelően kezelik őket. Más szóval, a mesterséges intelligencia technológiákat tervező és forgalmazó vállalatok versenyképes üzleti gyakorlata, és különösen a szellemi tulajdonuk védelme érdekében termékeikhez fűzött titoktartási követelmények gyakran ütköznek a nyilvános átláthatóság és elszámoltathatóság igényével, amely a kormányzati szervek munkáját jellemzi. E feszültség egyik legjobb példája a Northpointe Inc. elutasító magatartása. (ma Equivant), a jelentésben korábban tárgyalt COMPAS rendszert értékesítő vállalat, hogy a vádlottak és az újságírók betekinthesse a szoftver titkos algoritmusába és megkérdőjelezhessék azt.³⁵⁵ Gretchen Greene átfogó elemzést készített arról, hogy a kormányzati felhasználóknak milyen bevált gyakorlatokat kellene alkalmazniuk a mesterséges intelligencia megoldások megvásárlásakor és bevezetésekor, hogy jobban kezeljék az ezzel az összetett technológiával kapcsolatos etikai és teljesítménybeli kockázatokat.³⁵⁶

algorithm", The New York Times (2017. május 1.),
³⁵⁵ Adam Liptak, "Börtönbe küldött egy szoftverprogram titkos online:
<https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-szoftverprogramok-titkos->

³⁵⁶ K. Gretchen Greene, "Az első AI megvásárlása vagy "soha ne bízz a használtban".
 algoritmusok.html.

Kiemel hat olyan kérdést, amelyet a kormányzati ügynökségeknek részletesen meg kellene vitatniuk az új rendszereket értékesítő AI-vállalatokkal.

A mesterséges intelligencia megoldásokat fejlesztő vállalatok ellenállása ellenére az ilyen típusú terméket beszerző kormányzati ügynökségnek képesnek kell lennie arra, hogy hozzáférjen a forráskódhoz és elemezze az azt működtető algoritmusokat. A "fekete dobozos algoritmusok" megvásárlásának gyakorlatát gyakran azzal indokolják támogatói, hogy az eladó technológiai előnyét (a "titkos szósz") a könyörtelen versennyel szemben is meg kell őrizni, de a neurális hálózatok rosszindulatú szereplők általi manipulációjának elkerülése érdekében is, amint azt a 2. fejezetben láttuk.³⁵⁷ Bár nem minden állami szervezetnek lesz meg az érettsége és erőforrása ahhoz, hogy saját nyílt forráskódú eszközöket és algoritmusokat fejlesszen ki, legalább arra képesnek kell lenniük (egyesekek szerint kénytelenek), hogy megvizsgálják, hogyan épül fel az általuk megvásárolni tervezett technológia, és hogyan hozza meg azokat a döntéseket, amelyek hatással lesznek a polgáraikra. A mélytanulási algoritmusok egyik fő jellemzője, hogy a számításaikba beépíthető változók nagy száma és összetettsége miatt nem teljesen megmagyarázható eredményeket produkálhatnak, de a mögöttes kódjuk alapos megértésének mindazonáltal a büntető igazságszolgáltatási intézmények által történő alkalmazásukban is szerepet kell játszania, hogy csökkentsék a torzítások előre nem látható eseteit.

³⁵⁷ See, e.g., An Introduction to the Law of AI & Society, 75 Cal. W.I.T. 1 (2019), available at <https://www.williamsinstitute.com/berkman-klein-center/buying-your-first-ai-13626-2>.
 See also, e.g., "The Case for Open Source Algorithms in AI", *Open Source* 8 (2019), available at <https://opensource.com/article/8/1/open-source-classifiers-ai-algo10>.

1
5
3

A forráskód és az algoritmusok átláthatóságára vonatkozó, fentebb vázolt minimumkövetelményeknek ki kell terjedniük azokra az adatokra is, amelyeket a szóban forgó algoritmusok képzéséhez használtak, vagy amelyeket előrejelzések készítéséhez fognak használni. A gépi tanulási modelleknek általában hatalmas mennyiségű adatra van szükségük ahhoz, hogy optimális eredményeket érjenek el és megbízható előrejelzéseket készítsenek, de a képzési szakaszban e rendszerekbe táplált adatok jellege meghatározza a működésbe lépésükkor hozott döntések minőségét. Az elfogult adatok - például a diszkriminatív végrehajtási vagy ítélkezési gyakorlatból eredő faji egyenlőtlenségeket tükröző adatok - felhasználása egy mesterséges intelligencia modell képzéséhez ugyanilyen elfogult eredményt fog generálni, amely hajlamos lesz egy nemkívánatos helyzetet reprodukálni, csak tudományos lakkozással bevonva. Ezért alapvető fontosságú, hogy minden használatra kész mesterséges intelligencia-eszközt ne csak az algoritmus minősége, hanem a képzéséhez használt adatok minősége szempontjából is megvizsgáljunk. Ha a mesterséges intelligencia-eszközöket belső fejlesztésű, helyi adatok felhasználásával fejlesztik ki, ezt az értékelést sokkal könnyebb elvégezni, mint amikor egy rendőrségi szervezet vagy bírósági rendszer vásárol egy készen kapható mesterséges intelligenciát, amelyet bizonytalan eredetű adatokkal képeztek ki.

Végezetül alaposan meg kell vizsgálni azokat a független változókat is, amelyeket az algoritmusok az egyes eredményekre vonatkozó előrejelzésekhez használnak. Ezek a változók azok a karok, amelyeket az algoritmusok az adatok osztályozásához és a jóslatok elkészítéséhez meghúznak. A büntetőjogi alkalmazásokban a statisztikai elemzésekben hagyományosan használt változók közé tartozik a gyanúsítottak kora, neme, faji hovatartozása, jövedelme, képzettsége, egészségi állapota, társadalmi hálózata vagy korábbi elítélései. A gépi tanulási algoritmusok és az őket futtató számítógépes rendszerek analitikus ereje azonban azt jelenti, hogy több ezer

változót képesek feldolgozni egy-egy döntés meghozatalához. A feltételes szabadlábba helyezésre való jogosultság elbírálására használt mesterséges intelligenciával összefüggésben a

algoritmus például felhasználhatna látszólag nem kapcsolódó jellemzőket, például a szemszínt, a zenei ízlést vagy a letöltött alkalmazásokat, feltéve, hogy ezek kivonhatók az adatokból. E változók némelyike korrelálhat a faji hovatartozással vagy a társadalmi-gazdasági státusszal, és különösen hajlamos lehet a torzításra. Ennélfogva alapvető fontosságúvá válik annak felülvizsgálata, hogy mely változóknak van a legnagyobb hatása, és hogy az ok-okozati összefüggés jól érthető legyen, és összhangban legyen az igazságosság és a méltányosság elveivel.

Egyes vállalatok, például az IBM, olyan eszközöket fejlesztenek, amelyek segítenek a szervezeteknek a kód, az adatok és a változó átláthatóság elveinek gyakorlati megvalósításában. Az AI OpenScale technológiája, amelyet a vállalat az állítása 2018, szerint a gépi tanulási termékek széles skálájánál képes automatizálni az elfogultságok felismerését és mérséklését, magyarázatot adva arra, hogyan születnek a döntések, és megerősítve a kimenetelükbe vetett bizalmat.³⁵⁸ A DARPA, az amerikai védelmi kutatási ügynökség szintén elindított egy Explainable AI programot, amelynek célja olyan gépi tanulási technikák előállítása, amelyek lehetővé teszik az emberi felhasználók számára, hogy könnyebben megértsék, hogyan születnek a jóslatok, és mennyire megbízhatóak.³⁵⁹ Ezek az új alkalmazások különösen hasznosak lesznek a büntető igazságszolgáltatásban.

A tisztán technikai megfontolásokon túlmenően számos vádlottat, áldozatot és büntetőjogi szakembert érint majd a mesterséges intelligenciával működő rendszerek által hozott döntések növekvő száma. Az esélyek

³⁵⁸ "AI OpenScale", IBM (Weboldal), o sor:
<https://www.ibm.com/cloud/ai-openscale/>

³⁵⁹ David Gunni g, "Explainable Artificial Intelligence (XAI)", DARPA (Weboldal),
<https://www.darpa.mil/program/explainable-artificial-intelligence>.
 online:

egy vádlott számára a vádemelés, az elítélés, az ítélelhozatal és a feltételes szabadlábra helyezés jelentősen megváltozhat az új rendszerben. A büntető igazságszolgáltatás igazgatásának ilyen radikális átalakítása nem hajtható végre annak megfelelő megértése nélkül, hogy az eredmények mennyiben fognak különbözni a jelenlegi rendszerektől, ahol a döntéseket kizárólag emberek hozzák meg. A döntéshozatali folyamatba különösen be kell építeni azokat a károkat, amelyeket a mesterséges intelligencia hibás működése okozhat (például téves pozitív vagy téves negatív eredmények). Eközben a rendőrök, ügyészek, védőügyvédek, bírák, büntetés-végrehajtási és feltételes szabadlábra helyezési tisztviselők szakértelmének átképzése jelentős erőfeszítéseket igényel majd. A mesterséges intelligencia eszközeit olyan hatékonyságnövelésre is fel lehet használni, amely munkahelyek megszűnésével jár. Ezért egy új mesterséges intelligencia-rendszer bevezetésekor átfogó algoritmikus hatásvizsgálatot kell végezni, hogy fel lehessen mérni egy ilyen döntés többszörös szervezeti és szolgáltatásnyújtási következményeit.³⁶⁰

Akár az új mesterséges intelligencia eszközt bevezető bűnügyi igazságügyi szervezet dönt úgy, hogy közvetlenül az ilyen technológia bevezetéséhez szükséges digitális infrastruktúrába fektet be, akár éppen ellenkezőleg, inkább egy felhőszolgáltatóra támaszkodik a gyártási háttérrendszer elhelyezésében, az adatbiztonságot és a magánélet védelmét garantálni kell. Amint azt e jelentésben már többször jeleztük, egy mesterséges intelligenciamodell előrejelző hatékonysága nagymértékben függ attól, hogy milyen mennyiségű adatot képes felvenni és feldolgozni, minél többet, annál jobb. A nagy adatbázisok azonban ki vannak téve a rosszindulatú támadásoknak.

360

(, "Algorithm assessment report" P//ww . . g vt.
m m , 28) : 20 & pdfdata33.
G nz/assets/Uploads/Algorithm-Assessment-Report

W
h
,
g
t
s
o
u
n
p
:
r
a
N
e
n
w
o
t
e
Z
e
a
l
a
3
6
5
;

n
S
d
t
a
G
t
s
o
v
N
e
Z

pénzügyi haszonszerzés, ideológia, bosszú vagy kormányzati szervek által támogatott hackerek. A Gemalto kezdeményezésére létrehozott Breach Level Index által fenntartott 2013.adatvédelmi incidens-adatbázis több mint 9700 adatvédelmi incidenst azonosított, amelyek több mint 13 milliárd adatot veszélyeztettek.³⁶¹ A büntető igazságszolgáltatási szervek sem mentesülnek ettől a tendenciától, és számos rendőrségi szolgálatot, bírósági adatbázisokat, sőt büntetés-végrehajtási számítógépes rendszereket is feltörték már. Egy biztonsági incidens során előfordulhat, hogy egy rosszindulatú szereplő hozzáfér a mesterséges intelligencia rendszer által központosított hatalmas mennyiségű személyes adathoz, hogy megjósoljon egy büntetőjogi kimenetet, vagy megpróbálja megmérgezni a mesterséges intelligencia rendszert, hogy megváltoztasson egy előrejelzést, és ezáltal befolyásolja azt a kimenetet, amelyre az előrejelzés irányul. Az ilyen felhasználási eseteket nem szabad sci-fi forgatókönyvként elvetni, és a bűnügyi igazságszolgáltatási szervek nem vásárolhatnak meg semmilyen mesterséges intelligencia-rendszert, mielőtt a szerződésért versengő szolgáltatók és informatikai vállalkozóik szigorú biztonsági ellenőrzésére nem kerül sor annak biztosítása érdekében, hogy a technológiájuk és az általa feldolgozott adatok magas szintű védelemben részesüljenek a lopás és a manipuláció ellen.

Végül pedig a szerződési feltételeket is alaposan meg kell vizsgálni, hogy a felkínált licencmodell teljes körű megértését biztosítsuk. Különösen fontos annak megállapítása, hogy a szellemi tulajdonjogok idővel hogyan kerülnek felosztásra, különösen egy olyan technológia esetében, amely folyamatosan tanul az új adatokból, és ennek megfelelően módosítja modelljeit. A mesterséges intelligencia bevezetésének élettartama során felmerülő költségeket is világosan meg kell értenie minden félnek. A képzési stratégiák és az infrastruktúra kiválasztása nagymértékben eltérő pénzügyi hatással lesz az ilyen projektek sikerére vagy kudarcára. A tesztelés

361 " ; Level Index (honlap), online:
hDapsa//BbrreeaacchhlSetvaetliisntidcesx . cBomre/ach

időszakot Gretchen Greene ajánlja, aki azt is tanácsolja, hogy határozzunk meg egyértelmű teljesítménykritériumokat és célokat, amelyekkel a sikert mérni fogjuk.³⁶² Végezetül, egy ilyen összetett terméket vagy szolgáltatást vásárló büntetőjogi ügynökségnek nem szabad haboznia, hogy megkérdezze, milyen garancia jár hozzá, mind a hatékonyság, mind a hibákért való felelősség tekintetében.

Az új-zélandi kormány által a közelmúltban az ügynökségek¹⁴ körében végzett értékelés szerint a legtöbb ügynökség (10) vegyes beszerzési modellt alkalmaz, szemben a belső fejlesztési vagy a "tisztá" külső beszerzési modellel, amelyre a fent említett kihívások többsége vonatkozik. Az Új-Zélandon előnyben részesített vegyes megközelítés külső szakértelmet von be a belső fejlesztési folyamatba, hogy enyhítse a két másik alternatívával kapcsolatos lehetséges kockázatokat (szakértelem hiánya vagy a külső szakértelem feletti ellenőrzés hiánya).³⁶³ Ezen az első országos értékelésen kívül még mindig nagyon kevés ismeret áll rendelkezésre azokról a módozatokról, amelyeken keresztül a mesterséges intelligenciát bevezetik a kormányzati szerveknél.

Még akkor is, ha a beszerzési kihívásokat ügyesen kezelik, a technológia közvetlen felhasználói is központi szerepet játszanak a sikeres elfogadásban, függetlenül attól, hogy a technológia mennyire kifinomultnak és erősnek bizonyul.

6.4. Kihívások az előirányzathoz

Eddig azt feltételeztük, hogy a mesterséges intelligencia rendszerek megtalálják az útjukat.

³⁶² Greene, fenti lábjegyzet

365.

³⁶³ Stats NZ, fenti megjegyzés 370.

a büntető igazságszolgáltatási szervezetekbe semleges környezetben, ahol a szakemberek passzívan alkalmazzák azokat a hierarchia és a tervezők szándékainak megfelelően. Ez természetesen egy szociológiai fikció, amely figyelmen kívül hagyja az első vonalbeli rendőrök, bűnügyi elemzők, bírák, felügyelőtisztok és sok más büntetőjogi szakember erőteljes kisajátítási gyakorlatát. A rendőri és biztonsági szakirodalom megállapította, hogy ha a biztonsági technológiák és eszközök minden bizonnyal kötelezővé váltak és alakítják emberi felhasználóik mindennapi gyakorlatát, az utóbbiak mindig nagyfokú cselekvőképességet tartanak fenn, amely különböző formákat ölthet, és a domesztikációtól az ellenálláson át a szabotázsig terjedhet.³⁶⁴ A kisajátítás fogalma tükrözi a komplex szervezeteken belül az egyes szereplők kreativitását, akik a rájuk bízott technológiát olyan gyakorlatokká alakítják át, amelyek lehetnek rutinszerűek vagy innovatívak, ami azt jelenti, hogy egy technológiát a meglévő kulturális értékekbe olvasztanak be, és hatástalanítják annak reformpotenciálját, vagy épp ellenkezőleg, egy technológiát váratlan módon újrahaznosítanak, hogy az operatív igényeikhez illeszkedjen. A bűnüldözési kontextusban nyersen fogalmazva: "bármilyen technológia növeli a tisztviselő hatékonyságérzetét, azt használni és módosítani fogják, ami pedig nem hasznos, azt megsemmisítik, szabotálják, elkerülik vagy rosszul használják".³⁶⁵ A mesterséges intelligencia tehát a legújabb technológia a bűnügyi igazságszolgáltatási innovációk hosszú sorában, amelyek az igazságszolgáltatás és intézményei hatékonyságának javítására törekedtek, de amelyek végül a vártnál sokkal kevésbé lesznek zavaróak.

³⁶⁴ RCI (Ricks & Erickson, 1977); ...

"Questioning Reformátivitas, ellenállás, politika," (2015) ...

³⁶⁵ ...

Így a jelentés utolsó ajánlása az, hogy kezdjük el tervezni azokat a kutatási erőfeszítéseket, amelyek szükségesek lesznek annak megértéséhez, hogy az emberek és a mesterséges intelligenciával működő gépek új összetétele, amely hamarosan áthatja majd a büntetőjogi intézményeket, hogyan fog működni, nem elméletben vagy disztópikus konfigurációban, hanem a mindennapi gyakorlatban, és milyen szándékolt és nem szándékolt következményekkel jár majd ez. Az Ericson és Haggerty "Policing the risk society" vagy Manning "The technology of policing" című munkájához hasonló megközelítést alkalmazó etnográfiai tanulmányokat kellene finanszírozni annak megragadására, hogy az AI-rendszereket hogyan fogják ""utólagosan" beilleszteni a [büntető igazságszolgáltatási] szervezetek gyakorlatába, struktúráiba és rutinjaiba".³⁶⁶ Csak így leszünk képesek túllépni az algoritmusok jelenlegi fetiszmusán, hogy felmérjük a beígért mesterséges intelligencia forradalom teljes hatókörét a biztonság és az igazságszolgáltatás terén.

³⁶⁶ Ibid. 276.

Hivatkozások listája

- "Nem vagyok robot": AI Business, (2017. október 25.), online:
<https://aibusiness.com/recaptcha-trains-google-robots/>.
- "8 vállalat, amelyek a mesterséges intelligenciát a bűnüldözésre használják", Nanalyze (honlap), online:
<https://www.nanalyze.com/2017/11/8-companies-ai-law-enforcement/>.
- "AI OpenScale", IBM (Weboldal), online:
<https://www.ibm.com/cloud/ai-openscale/>.
- "AI vs. Lawyers", LawGeex Blog (2018. február 26.), online:
<https://blog.lawgeex.com/ai-more-accurate-than-lawyers/>.
- "Algoritmusok a büntető igazságszolgáltatási rendszerben",
Elektronikus Adatvédelmi Információs Központ (honlap),
online: <https://epic.org/algorithmic-transparency/crim-justice/>.
- "Amazon Deep Learning AMI-k", Amazon Web Service
(Weboldal) online: <https://aws.amazon.com/machine-learning/amis/>.
- "Analytics Desktop", Cellebrite (Weboldal), online:
<https://www.cellebrite.com/en/products/analytics-desktop/>.
- "Analytics Enterprise", Cellebrite (Weboldal), online:
<https://www.cellebrite.com/en/products/analytics-enterprise/>.
- "Mesterséges intelligencia az ausztrál igazságszolgáltatási rendszer javítására", Swineburn University of Technology
(Blog) (január 29.)

2018), online:

<http://www.swinburne.edu.au/news/latest-news/2018/01/artificial-intelligence-to-enhance-australian-justiciary-system.php>.

"arXiv.org e-Print archive", arXiv.org (Weboldal), online:

<https://arxiv.org/>.

"Astroturfing, Twitterbots, Amplification - Inside the Online Influence Industry", The Bureau of Investigative Journalism (2017. december 7.), online:

<https://www.thebureauinvestigates.com/stories/2017-12-07./twitterbotok>.

"Axon AI and Policing Technology Ethics Board", Axon (Weboldal), online: <https://ca.axon.com/info/ai-ethics>.

"Óvadékkal kapcsolatos törvény és jogi definíció", USLegal (honlap), online: <https://definitions.uslegal.com/b/bail-schedule/>.

"Boomerang III: State-of-the-Art Shooter Detection", Raytheon (Weboldal), online:

<https://www.raytheon.com/capabilities/products/boomerang>.

"Kína arcfelismerést használ szökevények letartóztatására", NHK World - Japán (2018. december 26.), online:

https://www3.nhk.or.jp/nhkworld/en/news/20181227_10/.

"Cloud AI | Cloud AI", Google Cloud (Weboldal), online:

<https://cloud.google.com/products/ai/>; jonbeck7, "Azure Windows VM sizes - GPU", Microsoft (Weboldal), online: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-gpu>.

"Cloud TPUs - ML accelerators for TensorFlow", Google Cloud (Weboldal), online: <https://cloud.google.com/tpu/>.

- "COMPAS osztályozás", Equivant (honlap), online:
<http://www.equivant.com/solutions/inmate-classification>.
- "COMPAS Risk & Need Assessment System", Northpointe (honlap), online:
http://www.northpointeinc.com/files/downloads/FAQ_Document.pdf
- "COMPAS", Northpointe (honlap, az Internet Archive-on keresztül), online:
<https://web.archive.org/web/20160315175056/http://www.northpointeinc.com:80/risk-needs-assessment>.
- "Data Breach Statistics", Breach Level Index (honlap), online:
<https://breachlevelindex.com/>.
- "DeepMind", DeepMind (weboldal) online:
<https://deepmind.com>. "DNS-szakértői vizsgálatok: A genetikai vizsgálatok alkalmazása jogi célok", GeneEd (honlap), online:
https://geneed.nlm.nih.gov/topic_subtopic.php?tid=37.
- "Evidence-Based Practice Implementing the COMPAS Assessment System", Northpointe (honlap, az Internet Archive-on keresztül), online:
https://web.archive.org/web/20160506140944/http://www.northpointeinc.com/downloads/whitepapers/EVIDENCE-BASED_PRACTICE-implementing_COMPAS.pdf.
- "Faception : Facial Personality Analytics", Faception (Weboldal), online : <https://www.faception.com/>.
- "Faception: Faception honlapja, online:
<https://www.faception.com/our-technology>.
- "Faception", Faception (honlap), online:
<https://www.faception.com/>.

"Az arcfelismerés a készpénzmentes fizetés jövője Kínában",
Asia Times (2018. december 20.), online:
<http://www.atimes.com/article/facial-recognition-the-future-of-cashless-payment-in-china/>.

"fast.ai", fast.ai (Weboldal), online: <https://www.fast.ai/>; "Google Launches Free Course on Deep Learning: The Science of Teaching Computers How to Teaching Themselves", Open Cult (Weboldal), online:
<http://www.openculture.com/2017/07/google-launches-free-course-on-deep-learning.html>.

"FGNet eredmények", MegaFace (Weboldal),
online: "Gartner Hype Cycle", Gartner
(Weboldal), online:
<https://www.gartner.com/en/research/methodologies/gartner-hype-ciklus>.

"GET statuses/user_timeline", Twitter (Weboldal) online:
https://developer.twitter.com/en/docs/tweets/timelines/api-reference/get-statuses-user_timeline.html

"Google Duplex: Google AI (Blog), online:
<http://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html>.

"Google Unveils Neural Network with 'Superhuman' Ability to Determine the Location of Almost Any Image", MIT Technology Review (2016. február 24.), online:
<https://www.technologyreview.com/s/600889/google-unveils-neural-network-with-superhuman-ability-to-determine-the-location-of-almost/>.

"Have I Been Pwned: Ellenőrizze, hogy az e-mailje veszélybe került-e

- in a data breach", Have I Been Pwned (Weboldal) online:
<https://haveibeenpwned.com/>.
- "Hogyan működik az arcfelismerés?", Norton Security Center, online:
<https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html>
- "ImageNet", Image-Net (Weboldal) online: <http://imagenet.org/index>. "Intelligence", Palantir (honlap), online:
<https://www.palantir.com/solutions/intelligence/>.
- "Introducing Magnet.AI: Putting Machine Learning to Work for Forensics", Magnet Forensics (Weboldal), online:
<https://www.magnetforensics.com/blog/introducing-magnet-ai-putting-machine-learning-work-forensics/>
- "Introduction to Computer Vision", Algorithmia Blog (2018. április 2.), online.
<https://blog.algorithmia.com/introduction-to-computer-vision/>
 ; Golan Levin, "Image Processing and Computer Vision", OpenFrameworks, online:
https://openframeworks.cc/ofBook/chapters/image_processing_computer_vision.html.
- "Az arcfelismerő technológia rasszista?", The Week UK (2018. július 27.), online:
<https://www.theweek.co.uk/95383/is-facial-recognition-racist>.
- "L'Intelligence artificielle au service de la quantification du risque juridique", Case Law Analytics (Website), online:
<http://caselawanalytics.com>.
- "La justice prédictive (1/3) : l'enjeu de l'ouverture des données", Le Monde Internet Actu (Blog, szeptember 9 2017), online:
<http://internetactu.blog.lemonde.fr/2017/09/09/la-justice->

- predictive-13-lenjeu-de-louverture-des-donnees/.
- "Le moteur de recherche juridique", Doctrine (honlap), online:
<https://www.doctrine.fr>.
- "Let's Go Vishing", (2014. december 22.), online: Biztonság az oktatáson keresztül.
<https://www.social-engineer.org/general-blog/lets-go-vishing>.
- "Life Facial Recognition Trial", Metropolitan Police (honlap),
online: <https://www.met.police.uk/live-facial-recognition-trial/>.
- "LSI-R: Level of Service Inventory-Revised", MH Assessments
(honlap), online:
<https://www.mhs.com/MHS-Publicsafety?prodname=lsi-r>
- "Lyrebird: Lyrebird.a (honlap), online: <https://lyrebird.ai/>.
- "MagnetForensicsLaunchesMagnet.AItoFightChildExploitation", StartUp Toronto (Weboldal), online:
<https://startupheretoronto.com/sectors/technology/magnet.-forensics-launches-magnet-ai-to-fight-child-exploitation/>.
- "Measuring the Filter Bubble: How Google is influencing what you click", DuckDuckGo Blog (2018. december 4.), online:
<https://spreadprivacy.com/google-filter-bubble-study/>.
- "Meet the Safety Team", Facebook Safety (2011. augusztus 9.),
online: <https://www.facebook.com/notes/facebook-safety/meet-the.-safety-team/248332788520844/>
- "Neural fuzzing: applying DNN to software security testing",
Microsoft Research (2017. november 13.), online:
<https://www.microsoft.com/en-us/research/blog/neural-fuzzing/>; Mohit Rajpal, William Blum & Rishabh Singh, "Not

minden bájtt egyenlő: Neural byte sieve for fuzzing", (2017) arXiv Working Paper, arXiv:1711.04596 [cs.SE], online: <https://arxiv.org/abs/1711.04596>.

"Új adathalász technikák, amelyekkel tisztában kell lenni: Vishing and Smishing", MakeUseOf (Weboldal), online: <https://www.makeuseof.com/tag/new-phishing-techniques-aware-vishing-smishing/>.

"Northpointe lakosztály: Northpointe (Weboldal, az Internet Archive-on keresztül), online: <https://web.archive.org/web/20160307002839/http://www.northpointeinc.com/>.

"Official Launch Of The Montréal Declaration For Responsible Development Of Artificial Intelligence", Montréal Declaration for Responsible Development of Artificial Intelligence (honlap) (2018. december 4.), online: <https://www.declarationmontreal-iaresponsable.com/blogue/d%C3%A9voilement-de-la-d%C3%A9claration-de-montr%C3%A9al-pour-un-d%C3%A9veloppement-responsable-de-l-ia>

"OpenFace: OpenFace (Weboldal), online: <https://cmusatyalab.github.io/openface/>.

"Áttekintés", PredPol (honlap), online: <https://www.predpol.com/about/>.

"Partners", National Center for Missing & Exploited Kids (Webste), online: <http://www.missingkids.org/supportus/partners>.

"Penetrációs tesztelés szoftver, Pen tesztelés biztonság", Metasploit

(Weboldal), online:

<https://www.metasploit.com/>. "Phishing", Know4Be

(honlap), online:

<https://www.knowbe4.com/phishing>.

"Phishing", Security Through Education (honlap), online:

<https://www.social-engineer.org/framework/attack-vectors/phishing-attacks-2/>.

"PhotoDNA", Microsoft (Weboldal), online:

<https://www.microsoft.com/en-us/photodna>.

"A pittsburghi székhelyű technológiai vállalat bemutatja az első arcfelismerő technológiát, amelynek célja a globális emberkereskedelem megállítása", Marinus Analytics (Weboldal), online:

"Practitioner's Guide to COMPAS Software", Northpointe (honlap, az Internet Archive-on keresztül), online:

https://web.archive.org/web/20160507022911/http://www.northpointeinc.com/downloads/compas/Practitioners-Guide-COMPAS-Core-_031915.pdf.

"Predictive Policing Research", National Institute of Justice (honlap), online:

<https://www.nij.gov/topics/law-enforcement/strategies/predictive-policing/Pages/research.aspx>.

"Pretrial Release Recommendation Decision Making

Framework (DMF)", New Jersey Courts (2018. március), online:

<https://www.njcourts.gov/courts/assets/criminal/decmakframework.pdf?cacheID=JOvH2H8>.

"Principles for Accountable Algorithms and a Social Impact Statement for Algorithms", FAT/ML (honlap), online:

<http://www.fatml.org/resources/principles-for-accountable-algoritmusok>.

"Public Safety Assessment New Jersey Risk Factor Definitions-
March 2018", New Jersey Courts, online:
<https://www.njcourts.gov/courts/assets/criminal/psariskfactor.pdf?cacheID=IDYJVkr>.

"Közbiztonsági értékelés: Arnold Foundation (Blog), online:
<http://www.arnoldfoundation.org/public-safety-assessment-risk-tool-promotes-safety-equity-justice/>.

"PyTorch", PyTorch (Weboldal), online:
<https://www.pytorch.org>; "TensorFlow", TensorFlow
(Weboldal) online: <https://www.tensorflow.org/>.

"Quandl", Quandl (Weboldal), online: <https://www.quandl.com>.

"RFP: Nemzeti képzési és technikai segítségnyújtási
szolgáltató",

Arnold Alapítvány (honlap), online:
<https://www.arnoldfoundation.org/wp-content/uploads/PSA-National-Provider-RFP.pdf>.

"Risk Assessment", Pretrial Justice Center for Courts (weboldal),
online:
<http://www.ncsc.org/Microsites/PJCC/Home/Topics/Risk-Assessment.aspx>.

"Sample-COMPAS-Risk-Assessment- COMPAS-'
CORE'", DocumentCloud (Hosting service), online:
<https://www.documentcloud.org/documents/2702103-Sample-Kockázatértékelés-COMPAS-CORE.html>

"Self-
ExclusionProgram", Ontario Lottery and
GamingCorporation (honlap), online:
<https://about.olg.ca/self-exclusion/facial-recognition/>.

"SenseTime: SenseTime (honlap), online:

- <https://www.sensetime.com/ourCompany>.
- "Siri", Apple (Weboldal), online: <https://www.apple.com/siri/>.
- "Social Engineering Defined", Security Education (Weboldal),
online:
<https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/>.
- "Spear Phishing", Know4Be (honlap) online:
<https://www.knowbe4.com/spear-phishing/>.
- "StopLift", Stoplift (Weboldal), online:
<https://www.stoplift.com/>. "A TASER International (TASR)
vezérigazgatója, Rick Smith a negyedik negyedéves
eredmények2016ról.
- Earnings Call Transcript", Seeking Alpha (február 28.
2017), online:
<https://seekingalpha.com/article/4050796-taser-internationals-tasr-ceo-rick-smith-q4-2016-results-earnings-call-transcript?page=3>.
- "Tattoo Recognition", FBI.gov, (2015. június 25.), online:
<https://www.fbi.gov/audio-repository/news-podcasts-thisweek-tattoo-recognition.mp3/view>.
- "The Future of Firearm Forensics is 3D", Cadre Forensics
(Weboldal), online: <https://www.cadreforensics.com/>.
- "A mesterséges intelligencia rosszindulatú felhasználása", A
mesterséges intelligencia rosszindulatú felhasználása:
(honlap) online: <https://maliciousaireport.com/>.
- "A 2017-es év legnagyobb csalásai", Fogasztói információk,
(2018. március 1.), online:
<https://www.consumer.ftc.gov/blog/2018/03/top-frauds-2017>.
- "Ez a PSA a hamis hírekről Barack Obamától nem az, amit

Úgy tűnik", BuzzFeed News (2018. április 17.), online:
<https://www.buzzfeednews.com/article/davidmack/obama>.

-fake-news-jordan-peepe-psycho-video-buzzfeed.

"UFED Ultimate", Celebrite (Weboldal), online:

<https://www.celebrite.com/en/products/ufed-ultimate/>.

"VALCRI", VALCRI (honlap), online: <http://www.valcri.org/>. "A

Veritone® bejelentette az új, mesterséges intelligenciával

működő bűnüldözési

Alkalmazáscsomag a nyomozások kollektív felgyorsítására
 and Evidence Disclosure", Business Wire (2018.

szepember 20.), online:

<https://www.businesswire.com/news/home/20180920005160/en/Veritone%20AE-Announces-New-AI-Powered-Law-Enforcement-Application>.

"Vishing", Security Through Education (honlap), online:

<https://www.social-engineer.org/framework/attack-vectors/vishing/>.

"Ways to Build with Amazon Alexa", Amazon (Weboldal),

online: <https://developer.amazon.com/alexa>.

"Mi az AGI?", (2013. augusztus 11.), online: Gépi Intelligencia

Kutatóintézet:

<https://intelligence.org/2013/08/11/what-is-agi/>.

"Mi az a Bail? Mi az óvadék és a különböző óvadéktípusok

megértése", Bail USA (honlap), online:

<http://www.bailusa.net/what-is-bail.php>.

Abdeel, P. & A.Y. Ng, A., "Apprenticeship learning via inverse

reinforcement learning", (előadás a 21st International

Conference on Machine Learning konferencián, 2004. július

4-8.), online: <https://dl.acm.org/citation.cfm?id=1015430>.

- Aggarwal, Alok, "The Current Hype Cycle in Artificial Intelligence", Scry Analytics (2018. január 20.) online: <https://scryanalytics.ai/the-current-hype-cycle-in-artificial-intelligencia>.
- Alabama büntetőeljárás szabályai, 7.2(b) szabály, online: http://judicial.alabama.gov/docs/library/rules/cr7_2.pdf.
- AlMarhoos, Rasha, "Phishing for the answer: (2007) 3:3 I/S: A Journal of Law and Policy for the Information Society (Az információs társadalom joga és politikája című folyóirat). 595.
- Anderson, Hyrum S et al, "Learning to Evade Static PE Machine Learning Malware Models via Reinforcement Learning" (2018) arXiv Working Paper, arXiv:180108917 [cs], online: <http://arxiv.org/abs/1801.08917>.
- Angwin, Julia, Jeff Larson, Surya Mattu & Lauren Kirchner, "Machine Bias", ProPublica (2016. május 23.), online: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.
- Arthur, Charles, "Twitter to introduce PhotoDNA system to block child abuse images", The Guardian (2013. július 22.), online: <https://www.theguardian.com/technology/2013/jul/22/twitter-photodna-child-abuse>.
- Mesterséges intelligencián alapuló rendszer figyelmeztet, ha fegyver jelenik meg egy videóban", PhysOrg (Weboldal) (2017. július 7.), online: <https://phys.org/news/2017-07-artificial-intelligence-based-gun-video.html>
- Asher, Jeff & Rob Arthur, "Inside the Algorithm That Tries to Predict Gun Violence in Chicago", The New York Times (2017. június 13.), online:

<https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html>

Assheuer, Thomas, "Die Big-Data-Diktatur", Die Zeit (2017. november 29.), online:
<https://www.zeit.de/2017/49/china-datenspeicherung-gesichtserkennung-big-data-ueberwachung>.

Atkinson, Robert, "'Meg fog ölni minket!' és más mítoszok a mesterséges intelligencia jövőjéről" (2016) Information Technology 50.

Babuta, Alexander, Marion Oswald és Christine Rinik, "Gépi tanulási algoritmusok és rendőrségi döntéshozatal: Jogi, etikai és szabályozási kihívások" (2018) Whitehall Reports (szeptember 21.), online:
[5,https://rusi.org/publication/whitehall-reports/machine-learning](https://rusi.org/publication/whitehall-reports/machine-learning).

-algoritmusok-és-rendőrségi-döntéshozatal-jogi-etikai.

Banks, Alec, "What Are Deepfakes & Why the Future of Porn is Terrifying", Highsnobiety (2018. december 20.), online:
<https://www.highsnobiety.com/p/what-are-deepfakes-ai-porn>.

Barker, Colin, "How the GPU became the heart of AI and machine learning", ZDNet (2018. augusztus 13.), online:
<https://www.zdnet.com/article/how-the-gpu-became-the-heart-of-ai-and-machine-learning/>; Bernard Fraenkel, "For Machine Learning, It's All About GPUs", Forbes (2017. december 1.), online:
<https://www.forbes.com/sites/forbestechcouncil/2017/12/01/for-machine-learning-its-all-about-gpus/>.

Barrett, David, "Egy megfigyelő kamera minden egyes brit lakosra 11, állítja a CCTV felmérés", The Telegraph (július 10.).

2013), online:

<https://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britannia-says-CCTV-survey.html>

Bellamy, C. & J. Taylor, "Új információs és kommunikációs technológiák és intézményi változások: (1996) 9:4. International Journal of Public Sector Management (A közsféra menedzsmentjének nemzetközi folyóirata): "The case of the UK criminal justice system: The case of the UK criminal justice system" (1996). 51.

Benbouzid, Bilel, "À qui profite le crime? Le marché de la prediction du crime aux États-Unis" (2016) La Vie des Idées, online: <https://laviedesidees.fr/A-qui-profite-le-crime.html>.

Benbouzid, Bilel, "Des crimes et des séismes: La police prédictive entre science, technique et divination", 6: Réseaux 20695.

Benedikt, Carl Frey & Michael A Osborne, "A foglalkoztatás jövője: Mennyire érzékenyek a munkahelyek a számítógépesítésre?" (2017) Technológiai 114 előrejelzés és társadalmi változások. 254.

Berg, Nate, "Predicting crime, LAPD-style", The Guardian (2014. június 25.), online: <https://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority>.
-jelentés.

Best, Jo, "IBM Watson: The inside story of how the Jeopardy-winning supercomputer was born, and what it wants to do next", TechRepublic (2013. szeptember 9.), online: <https://www.techrepublic.com/article/ibm-watson-the-inside-történet-ahogyan-született-az-Jeopardy-győztes-szuperszámítógép-és-mit-akar-következtetni>.

Bhushan, Kul, "Meet Staqu, a startup, amely segít az indiai jogban

174

- enforcement agencies with advanced AI", Live Mint (2018. június 26.), online:
<https://www.livemint.com/AI/DIh6fmR6croUJps6x7JW5K/Meet-Staqu-a-startup-helping-Indian-law-enforcement-agencie.html>.
- Biggio, Battista, Blaine Nelson & Pavel Laskov, "Poisoning Attacks against Support Vector Machines" (2012) arXiv Working Paper, arXiv:12066389 [cs, stat], online:
<http://arxiv.org/abs/1206.6389>.
- Bolukbasi, Tolga, et al, "Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings" (2016) arXiv Working Paper, arXiv:160706520 [cs, stat], online: <http://arxiv.org/abs/1607.06520>.
- Borak, Masha, "China's public toilets now have facial recognition, thanks to Xi Jinping", Tech in Asia (2018. december 21.), online:
<https://www.techinasia.com/chinas-public-toilets-facial-felismerés-xi-jinping>.
- Bostrom, Nick, "Ethical Issues in Advanced Artificial Intelligence" (2003) Science Fiction and Philosophy: Az időutazástól a szuperintelligenciáig.
- Bragg, Lucia, "Federal Criminal Justice Reform in 2018" (2018) 26:10 LegisBrief, online:
<http://www.ncsl.org/research/civil-and-criminal-justice/federal-criminal-justice-reform-in-2018.aspx>.
- Breslin, Susannah, "Meet The Terrifying New Robot Cop That's Patrolling Dubai" Forbes (2017. június 3.), online:
<https://www.forbes.com/sites/susannahbreslin/2017/06/03/>.

robot-cop-dubai/#287b11c96872.

Brewster, Thomas, "Apple Face ID 'Fooled Again' -- This Time By \$200 Evil Twin Mask", Forbes (2017. november 27.), online: <https://www.forbes.com/sites/thomasbrewster/2017/11/27/apple-face-id-artificial-intelligence-twin-mask-tacks-iphone-x/#7df1a8052775>.

Buchanan, Bruce, "A mesterséges intelligencia (nagyon) rövid története" 26AI Magazine (2005).

Bughin, Jacques et al., "Mesterséges intelligencia: The Next Digital Frontier?", McKinsey Global Institute (2017. június) online: <https://www.mckinsey.com/~media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx>.

Burgess, Matt, "AI is invading UK policing, but there is little proof it's useful", Wired (2018. szeptember 21.), online a <https://www.wired.co.uk/article/police-artificial-intelligence-rusi-report> oldalon.

Burgess, Matt, "UK police are using AI to inform custodial decisions - but it could be discriminating against the poor", WIRED (2018. március 1.), online: <https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit>.

Cadwalladr, Carole, "'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower", The Guardian (2018. március 18.), online: <http://www.theguardian.com/news/2018/mar/17/data-war->.

- whistleblower-christopher-wylie-faceook-nix-bannon-trump.
- Camille Polloni, "Police prédictive : la tentation de " dire quel sera le crime de demain", L'Obs (2015. május 27.), online: <https://www.nouvelobs.com/rue89/rue89-police-justice/2015-0527.RUE9213/police-predictive-la-tentation-de-dire-quel-sera-le-crime-de-demain.html>.
- Carpenter, Julia, "A Google algoritmus a férfiaknak a tekintélyes álláshirdetéseket mutatja, de a nőknek nem. Here's why that should worry you.", Washington Post (2015. július 6.), online: <https://www.washingtonpost.com/news/the-intersect/wp/2015/07/06/googles-algorithm-shows-prestigious-job-ads-to-men-but-nem-nőknek-miért-mert-ez-önkellene-aggódnia/>.
- Chakraborty, R., "A DNS-típusosítás törvényszéki felhasználásának populációgenetikai kérdéseinek kezeléséhez szükséges mintanagyság követelményei" (1992) 64:2 Human Biology 141
- Chen, Stephen, "China to build giant facial recognition database to identify any citizen within seconds", South China Morning Post (2017. október 12.), online: <https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any>.
- Chesney, Robert & Danielle Keats Citron, "Mély hamisítványok: (2019) California 107 Law Review (megjelenés alatt): "A Looming Challenge for Privacy, Democracy, and National Security".
- Chessen, Matt, "A Madcom jövője: The Atlantic Council (2017. szeptember 1.), online: <https://www.scribd.com/document/359972969/The-MADCOM>.

-Jövő.

Cho, Charles et al, "Astroturfing Global Warming: (2011) 104:4 J Bus Ethics: It Isn't Always Greener on the Other Side of the Fence (2011) 104:4 J Bus Ethics 571.

Chui, Michael, James Manyika & Mehdi Miremadi, "Where machines could replace humans--and where they can't (yet)", McKinsey Quarterly (July 2016), online: <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/where-machines-could-replace-humans-and-where-they-cant-yet>.

Citron, Danielle Keats, "Technological Due Process" (2008), 85:6 Washington University Law Review online 1249,: https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1166&context=law_lawreview.

Cloonan, John, "Advanced Malware Detection - Signatures vs. Behavior Analysis", Infosecurity Magazine (2017. április 11.), online: <https://www.infosecurity-magazine.com:443/opinions/malware-detection-signatures/>.

Coldewey, Devin, "Taser rebrands as Axon and offers free body cameras to any police department", Tech Crunch (2017. április 5.), online: <https://techcrunch.com/2017/04/05/taser-rebrands-as-axon-and-offers-free-body-cameras-to-any-police-department/>.

Cole, Samantha & Emanuel Maiberg, "People Are Using AI to Create Fake Porn of Their Friends and Classmates", Motherboard (2018. január 26.), online: https://motherboard.vice.com/en_us/article/ev5eba/ai-fake.

- porn-of-friends-deepfakes; Ruiz, Rebecca, "Deepfakes are about to make revenge porn so much worse" Mashable (2018. június 24.), online:
<https://mashable.com/article/deepfakes-revenge-porn-domestic-violence/>.
- Copel, Michael, "The Difference Between AI, Machine Learning, and Deep Learning?", The Official NVIDIA Blog (2016. július 29.), online:
<https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/>.
- Cristiani, Francesca, "How Lyrebird Uses AI to Find Its (Artificial) Voice", Wired (2018. október 15.), online:
<https://www.wired.com/brandlab/2018/10/lyrebird-uses-ai-find-artificial-voice/>
- Curran, Dylan, "Készen állsz? This is all the data Facebook and Google have on you", The Guardian (2018. március 30.), online:
<http://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy>.
- Dastin, Jeffrey, "Amazon scraps secret AI recruiting tool that showed bias against women", Reuters (2018. október 10.), online:
<https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>.
- David Gunning, "Explainable Artificial Intelligence (XAI)", DARPA (honlap), online:
<https://www.darpa.mil/program/explainable-artificial-intelligence>.

Daws, Ryan, "Chinese facial recognition flags bus advert woman for jaywalking", IoT News (2018. november 28.), online: <https://www.iottechnews.com/news/2018/nov/28/chinese-facial-recognition-ad-jaywalking/>.

Dettmers, Tim, "Which GPU(s) to Get for Deep Learning", Tim Dettmers (2018. november 5.), online: <http://timdettmers.com/2018/11/05/which-gpu-for-deep-learning/>.

Dietrich, William, Christina Mendoza & Tim Brennan "COMPAS kockázati skálák: Demonstrating Accuracy Equity and Predictive Parity", Volaris Groupe (honlap), online: http://go.volarisgroup.com/rs/430-MBX-989/images/ProPublica_Commentary_Final_070616.pdf.

Diop, Mouhamadou-Lamine, "Explainable AI: The data scientists' new challenge", Towards Data Science (2018. június 14.), online: <https://towardsdatascience.com/explainable-ai-the-data-scientists-new-challenge-f7cac935a5b4>

Domingos, Pedro, "Néhány hasznos dolog, amit a gépi tanulásról tudni kell" (2012) 55:10 Communications of the ACM 78.

Douglas, T., J. Pugh, I. Singh, J. Savulescu, and S. Fazelb, "Risk assessment tools in criminal justice and forensic psychiatry: The need for better data" (2017) Eur42 Psychiatry online134,; <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5408162/>.

Dowd, Maureen, "Elon Musk milliárd dolláros keresztes hadjárata, hogy megállítsa a A.I. Apocalypse", Hive - Vanity Fair (2017. március 26.), online: <https://www.vanityfair.com/news/2017/03/elon-musk-billion-dollar-crusade-to-stop-ai-space-x>.

Drange, Matt, "Milliókat költünk erre a high-tech rendszerre, amelyet a fegyveres erőszak csökkentésére terveztek. Is It Making A Difference?", Forbes (2016. november 17.), online:
<https://www.forbes.com/sites/mattdrange/2016/11/17/shotspotter-struggles-to-prove-impact-as-silicon-valley-answer-to-gun-violence/#11ee763731cb>.

Dressel, Julia & Hany Farid, "The accuracy, fairness, and limits of predicting recidivism" Science Advances (2018. január 17.), online:
<http://advances.sciencemag.org/content/4/1/eaao5580.full>.

Dumiak, Michael, "Interpol's New Software Will Recognize Criminals by Their Voices", IEEE Spectrum (2018. május 16.), online:
<https://spectrum.ieee.org/tech-talk/consumer-electronics/audiovideo/interpols-új-automata-platform-felismeri-az-új-automatizált-platformot-bűnözők-a-hangjuk-által>.

Eisenstein, Paul A., "Millions of jobs are on the line when autonomous cars take over", NBC News (2017. november 5.), online:
<https://www.nbcnews.com/business/autos/millions-professional-drivers-will-be-replaced-self-driving-vehicles-n817356>.

Ericson, R., & K. Haggerty, Policing the risk society (Oxford: Clarendon Press, 1997); A. Amicelle, C. Aradau, & J. Jeandesboz, "Questioning security devices: (2015) 46:4 Security Dialogue. 293.

Eubanks, Virginia, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (New York: NY, St Martin's Press, 2017).

Eykholt, Kevin et al, "Robust Physical-World Attacks on Deep Learning Models" (2017) arXiv Working Paper, arXiv:1707.08945 [cs.CR] online: <http://arxiv.org/abs/1707.08945>.

Faggella, Daniel, "A technológiai óriások mesterséges intelligencia-előnye: Amazon, Facebook, and Google", TechEmergence (2018. november 24.), online: <https://www.techemergence.com/the-ai-advantage-of-the-tech-giants-amazon-facebook-and-google-etc/>.

FortiGuard SE Team, "Előrejelzések: Fortinet Blog (2018. november 15.), online: <https://www.fortinet.com/blog/industry-trends/predictions-ai-fuzzing-and-machine-learning-poisoning-.html>.

Fry, Hannah, Hello World: Being Human in the Age of the Machine (New York, NY: W.W. Norton, 2018).

Fuller, Thomas, "California Is the First State to Scrap Cash Bail", The New York Times (2018. augusztus 28.), online: <https://www.nytimes.com/2018/08/28/us/california-cash-bail.html>; Rebecca Ibarra, "New Jersey's Bail Reform Law Gets Court Victory", WNYC (2018. július 9.), online: <https://www.wnyc.org/story/new-jerseys-bail-reform-law-gets-court-victory/>.

García-Teodoro, P. et al, "Anomalia-alapú hálózati behatolásérzékelés: (2009) 28:1.
-2 Számítógépek és biztonság 18

Garland, David, Az ellenőrzés kultúrája: Oxford: Oxford University Press, Oxford, 2001).

- Gatys, Leon A, Alexander S Ecker & Matthias Bethge, "A Neural Algorithm of Artistic Style" (2015) arXiv Working Paper, arXiv:150806576 [cs, q-bio], online: <http://arxiv.org/abs/1508.06576>; "Deep Dream Generator", Deep Dream Generator (honlap), online: <https://deepdreamgenerator.com/>.
- Ghoshal, Abhimanyu, "I trained an AI to copy my voice and it scared me silly", The Next Web (2018. január 22.), online: <https://thenextweb.com/insights/2018/01/22/i-trained-an-ai-to-copy-my-voice-and-scared-myself-silly/>.
- Gibbs, Samuel "AlphaZero AI verte a sakkbajnok programot, miután négy óra alatt megtanította magát", The Guardian (2017. december 7.), online: <https://www.theguardian.com/technology/2017/dec/07/alpha-zero-google-deepmind-ai-beats-champion-program-teaching-self-to-play-four-hours>.
- Goertzel, Ben, Matt Iklé & Jared Wigmore, "The Architecture of Human-Like General Intelligence" in Pei Wang & Ben Goertzel, eds, Theoretical Foundations of Artificial General Intelligence (Paris: Atlantis Press, 2012).
- Grauer, Yael & Emanuel Maiberg, "What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?", VICE Motherboard (2018. március 27.), online: https://motherboard.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection.
- Greene, Dan & Genevieve Patterson, "The Trouble With Trusting AI to Interpret Police Body-Cam Video", IEEE Spectrum (2018. november 21.), online: <https://spectrum.ieee.org/computing/software/the-troubl>.

e-bízva-az-ai-interpretálni-rendőrségi-bodycam-vidéo

Gretchen Greene, K., "Az első AI megvásárlása vagy "soha ne bízz egy használt

algorithm salesman", Berkman Klein Center for Internet & Society - AI Ethics & Governance (2018. november 7.), online: <https://medium.com/berkman-klein-center/buying-your-first-ai-136cd2e6dd2>.

Grieco, Gustavo & Artem Dinaburg, "Toward Smarter Vulnerability Discovery Using Machine Learning". (Előadás a Proceedings of the 11th ACM Workshop on Artificial Intelligence and Security, Toronto, Canada, 2018)

Grosse, Kathrin et al, "Adversarial Perturbations Against Deep Neural Networks for Malware Classification" (2016) arXiv Working Paper, arXiv:160604435 [cs], online: <http://arxiv.org/abs/1606.04435>.

Gunning, David, "Megmagyarázható mesterséges intelligencia (XAI): (2016) Defense Advanced Research Projects Agency DARPA-BAA-16-53; Sandra Wachter,

Mittelstadt, Brent & Chris Russell, "Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR", (2017) arXiv Working Paper, arXiv:1711.00399 [cs.AI], online: <https://arxiv.org/abs/1711.00399>.

Guzmán, Arelis, "Top Pretrained 10 Models to get you Started With Deep Learning (Part -1 Computer Vision)", Analytics Vidhya (2018. július 27.), online: <https://www.analyticsvidhya.com/blog/2018/07/top-10-pretrained-models-get-started-deep-learning-part-1-computer-vision/>.

- Hannah-Moffat, Kelly, "Aktuárius ítélethozatal: (2013) 30:2 Justice Quarterly 270-296, DOI: 10.1080/07418825.2012.682603;
- Mark H. Bergstrom & Kern, Richard P., "A View from the Field: Practitioners' Response to Actuarial Sentencing: An 'Unsettled' Proposition" (2013) 25:3 Federal Sentencing Reporter. 185.
- Harp, Steven et al, "Automated Vulnerability Analysis Using AI Planning" (Az AAI2005 Spring Symposiumon, Stanford, CA, 2018) elhangzott előadás, online:
https://www.researchgate.net/publication/221250445_Automated_Vulnerability_Analysis_Using_AI_Planning.
- Hawkins, Andrew J. ≤ "Waymo is first to put fully self-driving cars on US roads without a safety driver", The Verge (2017. november 7.), online:
<https://www.theverge.com/2017/11/7/16615290/waymo-self-driving-safety-driver-chandler-autonomous>.
- Hern, Alex, "Apple: ne használd a Face ID-t az iPhone X-en, ha kiskorú vagy ikertestvéred 13van", The Guardian (2017. szeptember 27.), online:
<https://www.theguardian.com/technology/2017/sep/27/apple-face-id-iphone-x-under-13-twin-facial-recognition-system-more-secure-touch-id>.
- Hill, Kashmir, "How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did", Forbes (2012. február 16.), online:
<https://www.forbes.com/sites/kashmirhill/2/02/1/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>.
- Hitaj, Briland et al, "PassGAN: A Deep Learning Approach for

PasswordGuessing"(2017)arXivWorkingPaper,a
rXiv:170900440 [cs, stat], online:
<http://arxiv.org/abs/1709.00440>.

Holt, Tom, "Exploring the social organization and structure of stolen data markets", (2013) 14:2-3 Global Crime 155; Alice Hutchings és Tom Holt, "A crime script analysis of the online stolen data market", (2015) 55:3 The British Journal of Criminology 596; "McAfee Labs Threats2017 Predictions Report", McAfee (Website), online:
<https://www.mcafee.com/enterprise/en-us/assets/reports/rp-threats-predictions-2017.pdf>.
<http://www.marinusanalytics.com/articles/2017/6/27/face-search-debut>.
<https://megaface.cs.washington.edu/results/fgnetresults.html>.
<https://www.shotspotter.com/press-releases/chicago-signs-23-million-multi-year-agreement-with-shotspotter-to-extend-gunshot-detection-coverage-into-next-decade/>.

Information & Communications Technology Law 223, online:
<https://www.tandfonline.com/doi/pdf/10.1080/13600834.2018.1458455>.

Israni, Ellora, "Algoritmikus eljárás: Jolt Digest (2017. augusztus 31.), online:
<https://jolt.law.harvard.edu/digest/algorithmic-due-process-mistaken-accountability-and-attribution-in-state-v-loomis-1>,
"Taking Algorithms To Court Current Strategies for Litigating Government Use of Algorithmic Decision-Making", AI Now Institute (2018. szeptember 24.), online:
<https://medium.com/@AINowInstitute/taking-algorithms-to-court-7b90f82ffcc9>.

- Jing, Meng, "Chinese home sharing site Xiaozhu to roll out facial recognition-enabled smart locks in Chengdu pilot scheme", South China Morning Post (2018. december 26.), online: <https://www.scmp.com/tech/start-ups/article/2179495/chinese-home-sharing-site-xiaozhu-roll-out-facial-recognition-enabled>.
- Johnson, Alistair, et al, "MIMIC-III, a szabadon hozzáférhető intenzív ellátási adatbázis" (2016) Scientific3 Data.
- Kao, Jeff, "More than a Million Pro-Repeal Net Neutrality Comments Were Likely Faked", Hacker Noon (2017. november 23.), online: <https://hackernoon.com/more-than-a-million-pro-repeal-net-semlegesség-kommentek-valószínűleg-hamisítottak-e9f0e3ed36a6>.
- Karras, Tero, et al, "Progressive Growing of Gans for Improved Quality, Stability, and Variation" (2018) arXiv Working Paper, arXiv:1710.10196 [cs.NE], online: <https://arxiv.org/abs/1710.10196>.
- Khurana, Nitika, Sudip Mittal & Anupam Joshi, "Preventing Poisoning Attacks on AI based Threat Intelligence Systems" (2018), arXiv Working Paper, arXiv:1807.07418 [cs.SI], online: <https://arxiv.org/abs/1807.07418v1>.
- Kofman, Ava, "Interpol Rolls Out International Voice Identification Database Using Samples From Law Enforcement Agencies", The Intercept (2018. június 25.), online: <https://theintercept.com/2018/06/25/interpol-voice-identification-database/>
- Korolov, Maria, "Hackers get around AI with flooding, poisoning and social engineering", CSO Online (2016. december 16.), online:

<https://www.csoonline.com/article/3150745/security/hackers-get-around-ai-with-flooding-poisoning-and-social-engineering.html>.

Kosinski, Michal, David Stillwell & Thore Graepel, "Private traits and attributes are predictable from digital records of human behaviour" (2013) 110:15 Proceedings of the National Academy of Sciences 5802.

Kraska, Peter B., "Militarizáció és rendfenntartás: (2007) 1:4 Policing: A Journal of Policy and Practice 501.

Krebs, Brian, "Buying Battles in the War on Twitter Spam", Krebs on Security (Weboldal) online:
<https://krebsonsecurity.com/2013/08/buying-battles-in-the-war-on-twitter-spam/>.

Krebs, Brian, "Voice Phishing Scams Are Getting More Clever", Krebs on Security (Weboldal), online:
<https://krebsonsecurity.com/2018/10/voice-phishing-scams-are-getting-more-clever/>.

Langston, Jennifer, "How PhotoDNA for Video is being used to fight-online-child-ex ploitation", Microsoft On the Issues (2018. szeptember 12.), online:
<https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight-online-child-ex-ploitation/>.

Larson, Jeff, Surya Mattu, Lauren Kirchner & Julia Angwin, "How We Analyzed the COMPAS Recidivism Algorithm", ProPublica (2016. május 23.), online:
<https://www.propublica.org/article/how-we-analyzed-the->.

compas-recidivizmus-
 algoritmus.

- Latonero, Mark, "A mesterséges intelligencia kormányzása: Upholding Human Rights & Dignity", Data & Society Research Institute (2018. október 10.), online: <https://datasociety.net/output/governing-artificial-intelligence/>.
- LeCun, Yann, Yoshua Bengio és Geoffrey Hinton, "Deep learning" (2015) 521:7553 Nature 436
- Lee, Dave, "Why Big Tech pays poor Kenyans to programozás önzetű autók", BBC (2018. november 3.), online: <https://www.bbc.com/news/technology-460.55595>.
- Lee, Dave, "Why Big Tech pays poor Kenyans to programozás önzetű autók", BBC (2018. november 3.), online: <https://www.bbc.com/news/technology-460.55595>.
- Lee, Kai-Fu, szerk., AI Superpowers: China, Silicon Valley, and the New World Order, (New York, NY: Houghton Mifflin Harcourt, 2018).
- Leplâtre, Simon, "En Chine, la reconnaissance faciale envahit le quotidien", Le Monde (2017. december 9.), online: https://www.lemonde.fr/economie/article/2017/12/09/en-chine-la-reconnaissance-faciale-envahit-le-quotidien_5227160_3234.html.
- Liptak, Adam, "Sent to prison by a software program's secret algorithm", The New York Times (2017. május 1.), online: <https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html>.
- Liu, B. et al, "Software Vulnerability Discovery Techniques: International Conference on Multimedia Information Networking and

- Security, 2012), online:
<https://ieeexplore.ieee.org/document/6405650>.
- Liu, Joyce, "In Your Face: Kína mindent látó állama", BBC News (2017. december 10.), online:
<https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state>.
- Lubin, Gus, "'Facial-profiling' could be dangerously inaccurate and biased, experts warn", Business Insider (2016. október 12.), online:
<https://www.businessinsider.com/does-faception-work-2016-10>
- Lunden, Ingrid, "Element AI, a vállalatok számára AI-megoldásokat fejlesztő platform, 102 millió dollárt gyűjt", TechCrunch (2016. november), online:
<http://social.techcrunch.com/2017/06/14/element-ai-a-platform-for-companies-to-build-ai-solutions-raises-102m>.
- Lyon, Thomas P & John W Maxwell, "Astroturf: Interest Group Lobbying and Corporate Strategy" (2004) 13:4 J Econ Manag Strategy 561; Kevin Grandia, "Bonner & Associates: Huffington Post (2009. augusztus 26.), online:
https://www.huffingtonpost.com/kevin-grandia/bonner-associates-the-lon_b_269976.html.
- Maas, Dave, "FBI kívánságlista: EFF Deep Links (2018. július 16.), online:
<https://www.eff.org/deeplinks/2018/07/fbi-wants-app-cancelism-az-jelentést-tetoválásodat>

- Maffeo, L., "The case for open source classifiers in AI algorithms", *opensource.com* (2018. október 18.), online: <https://opensource.com/article/18/10/open-source-classifiers-ai-algorithms>.
- Mahapatra, Sambit, "Why Deep Learning over Traditional Machine Learning?", *Towards Data Science* (2018. március 21.), online: <https://towardsdatascience.com/why-deep-learning-is-needed-over-traditional-machine-learning-1b6a99177063>.
- Mann, Ian, *Hacking the human: Social engineering techniques and security countermeasures*, (London: Routledge, 2008).
- Manning, P. K., *A rendfenntartás technológiája*: New York: NY, New York University Press, 2008).
- Marcus, Gary, "Mélytanulás: A Critical Appraisal" (2018) arXiv Working Paper, arXiv:1801.00631 [cs.AI], online: <https://arxiv.org/abs/1801.00631>.
- Marr, Bernard, "The Fascinating Ways Facial Recognition AIs Are Used In China", *Forbes* (2018. december 17.), online: <https://www.forbes.com/sites/bernardmarr/2018/12/17/the-amazing-ways-facial-recognition-ais-ais-are-used-in-china/#5842e21c5fa5>.
- McCormick, Rich, "Google scans everyone's email for child porn, and it just got a man arrested", *The Verge* (2014. augusztus 5.), online: <https://www.theverge.com/2014/8/5/5970141/how-google-scans-your-gmail-for-child-porn>.
- Mennell, Julie, "A bünfelderítést támogató technológia: An

Bevezetés" (2012) 45:12 Mérés + ellenőrzés 304.

Mercer, Christina & Thomas Macaulay, "How tech giants are

investinginartificialintelligence", Techworld
(2018. november 27.), online:

<https://www.techworld.com/picture-gallery/data/tech-giants-investing-in-artificial-intelligence-3629737>.

Meyer, Robinson, "A Facebookomat a Cambridge Analytica megsértette. Was Yours?", The Atlantic (2018. április 10.), online:

<https://www.theatlantic.com/technology/archive/2018/04/facebook-cambridge-analytica-victims/557648/>.

Mitchell, Tom, Machine Learning, (New York: McGraw-Hill Education, 1997).

Moon, Louise: "FigyeljeteK háTul: Chinese school installs facial recognition cameras to keep an eye on pupils "South China Morning Post (2018. március 16.), online:
<https://www.scmp.com/news/china/society/article/2146387/pay-attention-back-chinese-school-installs-facial-recognition>.

Mozur, Paul, "Kína disztópikus álmainak belsejében: The New York Times (2018. július 8.), online:
<https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>.

MSV, Janakiram, "Why Do Developers Find It Hard To Learn Machine Learning?", Forbes (2018. január 1.), online:
<https://www.forbes.com/sites/janakirammsv/2018/01/01/why-do-developers-find-it-hard-to-learn-machine-learning/>.

Müller, Vincent, szerk., Risks of Artificial Intelligence (Florida: Chapman and Hall/CRC Press, 2015).

Murphy, Finn: "A hozzám hasonló teherautó-vezetőket hamarosan automatizálással fogják helyettesíteni. You're next", The Guardian (2017. november 17.), online: <https://www.theguardian.com/commentisfree/2017/nov/17/truck-drivers-automation-tesla-elon-musk>.

Newton, Casey, "Microsoft sounds an alarm over facial recognition technology", The Verge (2018. december 7.), online: <https://www.theverge.com/2018/12/7/18129858/microsoft-facial-recognition-ai-now-google>.

Nilsson, Nils J., The Quest for Artificial Intelligence (Cambridge, UK: Cambridge University Press, 2013).

Novikov, Ivan, "How AI Can Be Applied To Cyberattacks", Forbes (2018. március 22.), online: <https://www.forbes.com/sites/forbestechcouncil/2018/03/22/how-ai-can-be-applied-to-cyberattacks/>.

Oberoi, Gaurav, "Exploring DeepFakes", Hacker Noon (2018. március 5.), online: <https://hackernoon.com/exploring-deepfakes-20c9947c22d9>.

Ocbazghi, Emmanuel, "We put the iPhone X's Face ID to the ultimate test with identical twins - and the results surprised us" Business Insider (2017. október 31.), online: <https://www.businessinsider.com/can-iphone-x-tell-difference-between-twins-face-id-recognition-apple-2017-10>.

Olafenwa, Moses "Object Detection with lines 10of code", Towards Data Science (2018. június 16.), online: <https://towardsdatascience.com/object-detection-with-10-lines-of-code-d6cb4d86f606>.

Olsen, Dana, "2017-es év áttekintése: A legjobb kockázati tőkefinanszírozási fordulók &

- investors in AI", PitchBook News & Analysis (2017. december 20.), online:
<https://pitchbook.com/news/articles/2017-year-in-review-the-top-vc-rounds-investors-in-ai>.
- Oswald, Marion, et al, "Algoritmikus kockázatértékelési rendőrségi modellek: a durhami HART-modell tanulságai és a "kísérleti" arányosság" (2018) 27:2.
- Palin, Megan, "Big Brother: news.com.au (2018. szeptember 19.), online:
<https://www.news.com.au/technology/online/big-brother-chinas-chilling-dictatorship-moves-to-introduce-scorecards-to-control-everyone/news-story/6c821cbf15378ab0d3eeb3ec3dc98abf>.
- Papernot, Nicolas et al, "Practical Black-Box Attacks against Machine Learning" (2016) arXiv Working Paper, arXiv: [160202697cs], online: <http://arxiv.org/abs/1602.02697>.
- Paquet-Clouston, Masarah, Bernhard Haslhofer & Benoît Dupont, "Ransomware payments in the bitcoin ecosystem", (A 17th Annual Workshop on the Economics of Information Security (WEIS), 2018) online:
<https://arxiv.org/abs/1804.04080>.
- Pasquale, Frank, "Secret Algorithms Threaten the Rule of Law", MIT Technology Review (2017. június 1.), online:
<https://www.technologyreview.com/s/608011/secret-algorithms-threaten-the-rule-of-law-of-law/>.
- Pasternack, Alex, "Body camera maker will let cops live-stream their encounters", Fast Company (2018. augusztus 10.), online:

- <https://www.fastcompany.com/90247228/axon-new-body-cameras-will-live-stream-police-encounters>.
- Patton, Jessica, "Mi az a 'ShotSpotter'? Controversial gunshot detector technology approved by Toronto police", *Global News* (2018. július 20.), online:
<https://globalnews.ca/news/4344093/controversial-gunshot-detector-shotspotter-toronto-police/>; "Chicago aláírja a 23 millió dolláros többéves megállapodást a Shotspotterrel a lövésérzékelési lefedettség kiterjesztéséről a következő évtizedre", *ShotSpotter (honlap)* (2018. szeptember 5.), online:
- Pearson, Jordan, "Toronto Approves Gunshot-Detecting Surveillance Tech Days After Mass Shooting", *VICE Motherboard* (2018. július 25.), online:
https://motherboard.vice.com/en_us/article/7xqk44/toronto-approves-shotspotter-gunshot-detecting-surveillance-tech-danforth-shooting.
- Penney, Jon et al., "Advancing Human-Rights-By-Design In The Dual-Use Technology Industry", *Columbia Journal of International Affairs* (2018. augusztus), online:
<https://jia.sipa.columbia.edu/advancing-human-rights-design-dual-use-technology-industry>.
- Perry, Nancy, "How Axon is accelerating tech advances in policing", *Police One (Blog)* (2018. június 22.), online:
<https://www.policeone.com/police-products/body-cameras/articles/476840006-How-Axon-is-accelerating-tech-advances-in-policing/>
- Piekniowski, Filip, "AI winter is well on its way", *Piekniowski's Blog* (2018. május 28.), online:
<https://blog.piekniowski.info/2018/05/28/ai-winter-is-well->

on-its-way.

Ranum, Marcus, "Rosszabb, mint gondolnád: Robo-Profiling", Free Thought Blogs (2017. március 16.), online: <https://freethoughtblogs.com/stderr/2017/03/16/its-worse-than-you-think-robo-profiling/>.

Reedy, Christiana, "Kurzweil Claims That the Singularity Will Happen by 2045", Futurism (2017. október 5.), online: <https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045>.

Regalado, Antonio, "Investigators searched a million people's DNA to find Golden State serial killer", MIT Technology Review (2018. április 27.), online: <https://www.technologyreview.com/s/611038/investigators.-searched-a-million-peoples-dna-to-find-golden-state-serial-killer/>.

Revell, Timothy, "Computer vision algorithms pick out petty crime in CCTV footage", NewScientist (2017. január 4.), online: <https://www.newscientist.com/article/2116970-computer-vision-algorithms-pick-out-petty-crime-in-cctv-footage/>.

Rieland, Randy, "A mesterséges intelligenciát már a bűnözés előrejelzésére használják. But Is It Biased?", Smithsonian Magazine (2018. március 5.), online: <https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-way-predict-crime-is-it-biased-180968337/>.

Rinaldi, Eva, "Reese Witherspoon", Flickr (Weboldal), online: <https://goo.gl/a2sCdc>.

Rinaldi, Eva, "Russell Crowe", Flickr (honlap), online: <https://goo.gl/AO7QYu>.

- Roose, Kevin, "Here Come the Fake Videos, Too", The NY Times (2018. június 8.), online:
<https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html>.
- Rosenfeld, Amir, Richard Zemel & John K Tsotsos, "The Elephant in the Room" (2018) arXiv Working Paper, arXiv:1808.03305 [cs.CV] online:
<http://arxiv.org/abs/1808.03305>.
- Rubinstein, Benjamin IP et al, "ANTIDOTE: understanding and defending against poisoning of anomaly detectors" (előadás a 9th ACM SIGCOMM Conference on Internet Measurement, 2009), online:
<https://people.eecs.berkeley.edu/~tygar/papers/SML/IMC.2009.pdf>
- Rushe, Dominic, "End of the road: will automation put an end to the American trucker?", The Guardian (2017. október 10.), online:
<https://www.theguardian.com/technology/2017/oct/10/american-trucker-automation-jobs>.
- Russell, Jon, "China's CCTV surveillance network took just minutes to capture BBC reporter", Tech Crunch (2017. december 13.), online: <https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter/>.
- Ryan, Julie J.C.H., "How do computer hackers 'get inside' a computer?", Scientific American, online:
<https://www.scientificamerican.com/article/how-do-computer-hackers-g/>.
- Schroff, Florian, Dmitry Kalenichenko & James Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering",

- arXiv Working Paper, arXiv:1503.03832v3 [cs.CV], online:
<https://arxiv.org/pdf/1503.03832.pdf>.
- Schwartz, Oscar: "Azt hitted, hogy az álhírek rosszak? Deep fakes are where truth goes truth to die", *The Guardian* (2018. november 12.), online:
<https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth>.
- Sejnowski, Terrence, *The Deep Learning Revolution* (Cambridge, Massachusetts: The MIT Press, 2018).
- Seymour, John & Philip Tully, "Az adattudomány fegyverként való felhasználása a társadalmi mérnöki tevékenységhez: (A Black Hat USA DEF2016, CON 201624, konferencián elhangzott előadás), online:
<https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf>.
- Sharif, Mahmood, Sruti Bhagavatula, Lujo Bauer & Michael K. Reiter, "Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition", *Conference Paper* (2016. október), online:
<https://www.cs.cmu.edu/~sbhagava/papers/face-rec-ccs16.pdf>.
- Shed, Sam, "Google's Mysterious AI Ethics Board Should Be Transparent Like Axon's", *Forbes* (2018. április 27.), online:
<https://www.forbes.com/sites/samshead/2018/04/27/googles-mysterious-ai-ethics-board-should-be-as-transparent-as-axons/#12e80d0019d1>.
- Shenfield, Alex, David Day & Aladdin Ayesh, "Intelligens behatolás

- detection systems using artificial neural networks" (2018) 4:2 ICT Express 95.
- Shoham, Yoav, Raymond Perrault, Erik Brynjolfsso & Jack Clark, "Mesterséges intelligencia index: 2017 AI Index (2017. november) online: <http://cdn.aiindex.org/2017-report.pdf>.
- Silver, David & Demis Hassabis, Cade Metz, "In Two Moves, AlphaGo and Lee Sedol Redefined the Future", Wired (2016. március 16.), online: <https://www.wired.com/2016/03/two-moves-alphago-lee-sedol-redefined-future/>.
- Simonite, Tom, "AI and 'Enormous Data' Could Make Tech Giants Like Google Harder to Topple", Wired (2017. július 13.), online: <https://www.wired.com/story/ai-and-enormous-data-could-make-tech-giants-harder-to-toppe/>.
- Solon, O. "The rise of 'pseudo-AI': how tech firms quietly use humans to do bots' work", The Guardian (2018. július 6.), online: <https://www.theguardian.com/technology/2018/jul/06/artificial-intelligencia-ai-emberek-robotok-tech-vallalatok>.
- Stanford, Stacy, "The Best 50 Public Datasets for Machine Learning", Data Driven Investor (2018. október 2.), online: <https://medium.com/datadriveninvestor/the-50-best-public-datasets-for-machine-learning-d80e9f030279>.
- Stanley, Jay, "Secret Service Announces Test of Face Recognition System Around White House", ACLU Free Future (2018. december 4.), online:

- <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/secret-service-announces-test-face-recognition>.
- Stats NZ, "Algorithm assessment report" (Wellington: New Zealand Government, 2018) online: <https://www.data.govt.nz/assets/Uploads/Algorithm-Assessment-Report-Oct-2018.pdf>.
- Streitfeld, David, "Book Reviewers for Hire Meet a Demand for Online Raves", The New York Times (2012. augusztus 25.), online: <https://www.nytimes.com/2012/08/26/business/book-reviewers-for-hire-meet-a-demand-for-online-raves.html>.
- Su, J. D. Vasconcellos Vargas, & K. Sakurai, "One pixel attack for fooling deep neural networks", (2017) arXiv Working Paper, arXiv:1710.08864 [cs.LG], online: <https://arxiv.org/abs/1710.08864v4>.
- Subramanian, Sankar, "The effects of sample size on population genomic analyses - implications for the tests of neutrality" (2016) 17:123 BMC Genomics.
- Swaine, Jon, "Russian propagandists targeted African Americans to influence US2016 election", The Guardian (2018. december 17.), online: <https://www.theguardian.com/us-news/2018/dec/17/russian-propagandisták-célzott-afrikai-amerikaiak-2016-választás>.
- Szegedy, Christian, et al., "Intriguing properties of neural networks" (2013) arXiv Working Paper, arXiv:1312.6199 [cs.CV], online: <http://arxiv.org/abs/1312.6199>.
- Az adatvédelmi szakértő útmutatója a mesterséges intelligenciához és a gépi tanuláshoz (Future of Privacy forum, 2018).

- Usersub, "Nick Cage DeepFakes Movie Compilation", online:
https://www.youtube.com/watch?time_continue=25&v=B U9YAHigNx8.
- Uz, Fidan Boylu, "GPUs vs CPUs for deployment of deep learning models", Microsoft Azure (2018. szeptember 11.), online:
<https://azure.microsoft.com/en-us/blog/gpus-vs-cpus-for-deployment-of-deep-learning-models/>.
- VanNostrand, Marie & Kenneth Rose, "Pretrial Risk Assessment In Virginia", Virginia Department of Criminal Justice (honlap), online:
<https://www.dcjs.virginia.gov/sites/dcjs.virginia.gov/files/publications/corrections/virginia-pretrial-risk-assessment-report.pdf>.
- Vincent, James & Russell Brandom, "Axon launches AI ethics board to study the dangers of facial recognition", The Verge (2018. április 26.), online:
<https://www.theverge.com/2018/4/26/17285034/axon-ai-ethics-board-facial-recognition-racial-bias>.
- Vincent, James, "This is when AI's top researchers think artificial general intelligence will be achieved", The Verge (2018. november 27.), online:
<https://www.theverge.com/2018/11/27/18114362/ai-artificial-general-intelligence-when-achieved-martin-ford-book>.
- Vincent, James, "Twitter taught Microsoft's friendly AI chatbot to be a racist asshole in less than a day", The Verge (2016. március 24.), online:
<https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist>.

- Vincent, James, "Watch Jordan Peele use AI to make Barack Obama deliver a PSA about fake news", The Verge, (2018. április 17.), online:
<https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peeel-buzzfeed>.
- Voss, Peter, "From Narrow to General AI", Intuition Machine (2017. október 3.), online:
<https://medium.com/intuitionmachine/from-narrow-to-general-ai-e21b568155b9>
- Votipka, Daniel et al, "Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes" (Az IEEE 2018 Symposium on Security and Privacy, San Francisco, CA, 2018), online:
<https://ieeexplore.ieee.org/document/8418614>.
- Wagner, David & Paolo Soto, "Mimicry Attacks on Host-Based Intrusion Detection Systems" (előadás a 9. ACM konferencián a számítógépes és kommunikációs biztonságról, Washington DC, 2002), online:
<https://dl.acm.org/citation.cfm?id=586145> a következő címen. 10.
- Washan, Nitin & Sandeep Sharma, "Beszédfelismerő rendszer: International Journal of Computer Applications online 7, :
<https://pdfs.semanticscholar.org/8f2c/b3f70bb75b6235514b192b83e413a0e23dd8.pdf>.
- Weller, Chris, "Van egy titkos technológia 90 amerikai városban, amely a lövéseket hallgatja a nap 24 órájában", Business Insider (2017. június 27.), online:
<https://www.businessinsider.com/how-shotspotter-works-microphones-detecting-gunshots-2017-6>.

- Whittaker , Meredith et al., "AI Now Report", AI Now Institute (2018. december), online:
https://ainowinstitute.org/AI_Now_2018_Report.pdf; AI Now Institute,"After a Year of Tech Scandals, Our 10 Recommendations for AI", AI Now Institute (2018. december 6.), online:
<https://medium.com/@AINowInstitute/after-a-year-of-tech-skandálok-az-10-ajánlásaink-ai-95b3b2c5e5>.
- Winick, Erin, "Lawyer-bots are shaking up jobs", MIT Technology Review (2017. december 12.), online:
<https://www.technologyreview.com/s/09556/lawyer-bots-6-are-shaking-up-jobs/>.
- Winston, Ali & Ingrid Burrington, "A predictive policing pioneer in predictive policing is starting a troubling new project", The Verge (2018. április 26.), online:
<https://www.theverge.com/2018/4/26/17285058/predictive-policing-predpol-pentagon-ai-racial-bias>.
- Wolff, Honorable Michael A, "Bizonyítékalapú bírói mérlegelés: Promoting Public Safety Through State Sentencing Reform" (2008) 83:5 New York University Law Review 1389, online:
<https://www.nyulawreview.org/wp-content/uploads/2018/08./NYULawReview-83-5-Wolff.pdf>.
- Yuan, Xiaoyong et al, "Adversarial Examples: (2017) arXiv Working Paper, arXiv:1712.07107 [cs, stat], online:
<http://arxiv.org/abs/1712.07107>.
- Zenaida Kotala, "Orlando Crime Scene Video Analysis Goes High-Tech With \$1.3 Million Grant to UCF" Space Coast Daily,(2016. április 19.), online)

<http://spacecoastdaily.com/2016/04/orlando-crime-scene-video-analysis-goes-high-tech-goes-high-tech-with-1-3-million-grant-to-ucf/>.

Zubairi, Amira, "Magnet Forensics launches Magnet.AI to fight child exploitation", Betakit (Website) (2017. május 16.), online:

<https://betakit.com/magnet-forensics-launches-magnet-ai-to-fight-child-exploitation/>.

Zucconi, Alan, "Understanding the Technology Behind DeepFakes", Alan Zuconi (2018. március 14.), online:

<https://www.alanzuconi.com/2018/03/14/understanding-the-technology-behind-deepfakes/>.

Mesterséges intelligencia a bűnözés és a büntető igazságszolgáltatás kontextusában

Először július 19-én jelent meg 2019

© In Sup Han

Nyomtatás: Szöul, Korea

Koreai Kriminológiai Intézet által

Regisztrálva márciusban 21-

14320, 1990

+82-2-575-5282

<https://eng.kic.re.kr/>

KRW 10,000

Ez a kiadvány szerzői jogvédelem alatt áll. A jogszabályi kivételek és a vonatkozó kollektív licencszerződések rendelkezései alapján a Koreai Kriminológiai Intézet írásos engedélye nélkül semmilyen rész nem sokszorosítható.

ISBN 979-11-89908-25-6



Mesterséges intelligencia akövetkező
kontextusban
Bűnözés és büntető
igazságszolgáltatás

ELŐZMÉNYSZÁMÚ KÖZLEMÉNYEK SZÁMÁRA

Elektronikusan elérhető a következő címen: