

Mesterséges intelligencia: Kockázatok a magánéletre és a demokráciára

Karl Manheim* és Lyric Kaplan**

21 Yale J.L. & Tech. 106 (2019)

Az Economist évente közzéteszi a "Demokrácia-indexet". Ez arról 2017, számolt be, hogy a világ országainak fele alacsonyabb pontszámot ért el, mint az előző évben. Ebbe beletartozott az Egyesült Államok is, amely a "teljes demokráciából" a "hibás demokráciába" került. Az alapvető tényező a "kormányzatba és a közintézményekbe vetett bizalom eróziója" volt. A közvélemény elégedetlenségében nagy szerepet játszott az orosz beavatkozás és a Cambridge Analytica által a 2016-os elnökválasztás során végzett választói manipuláció.

Az ilyen jellegű fenyegetések folytatódni fognak, amit a mesterséges intelligencia (AI) eszközeinek egyre szélesebb körű alkalmazása is elősegít a demokrácia előfeltételeinek és mozgatórugóinak manipulálására. Ugyanilyen romboló hatású a mesterséges intelligencia által a döntési és információs magánéletre jelentett fenyegetés is. A mesterséges intelligencia a motorja a nagy adatelemzésnek és a dolgok internetének. Bár a fogyasztók számára némi előnnyel járnak, fő funkciójuk jelenleg az, hogy személyes információkat gyűjtsenek, részletes viselkedési profilokat hozzanak létre, és árakat és programokat adjanak el nekünk. A magánélet, az anonimitás és az autonómia a fő áldozata annak, hogy az AI képes manipulálni a gazdasági és politikai döntések meghozatalát.

Az előrelépéshez nagyobb figyelmet kell fordítani ezekre a kockázatokra nemzeti szinten, és ehhez kapcsolódóan szabályozni kell őket. Ennek hiányában a technológiai óriások, akik mindannyian nagymértékben befektetnek a mesterséges intelligenciába és profitálnak belőle, nemcsak a közbeszédet fogják uralni, hanem alapvető értékeink és demokratikus intézményeink jövőjét is.

* Jogászprofesszor, Loyola Law School, Los Angeles. Ezt a cikket a japán Oszakában, a 2018 Kansai Egyetemen áprilisban tartott előadása ihlette.

** Associate az Adatvédelmi és adatbiztonsági csoportban, Frankfurt Kurnit Klein & Selz, Los Angeles. A szerzők hálásak Cornelia Dean, Tanya Forsheit,

Justin Hughes, Justin Levitt, Yxta Murray, Elizabeth Pollman és Neil Sahota
korábbi tervezetekhez fűzött hihetetlenül hasznos észrevételeikért.

BEVEZETÉS.....	108
I. AZ	AIRÖVID
BEVEZETÉSE	113
II. A MAGÁNÉLETET	FENYEGETŐ
VESZÉLYEK	116
A. A	
.....	<i>magánéletform</i>
ái	117
B. Adatgyűjtés, elemzés és	<i>felhasználás</i>
.....	119
1. <i>A</i>	<i>dolgokinternete</i>
.....	122
2. <i>A felügyeleti</i>	<i>ökoszisztéma</i>
.....	123
3. <i>Kormányzati</i>	<i>felügyelet</i>
.....	126
4. <i>Anonimitás</i>	127
C. Döntési magánélet	<i>(autonómia)</i>
.....	129
1. <i>A szabad akarat felforgatása - Online viselkedéses</i> <i>reklám</i> 130	
2. <i>fogyasztókbelenyugvása</i>	131
III. A VÁLASZTÁSOKAT ÉS A DEMOKRATIKUS INTÉZMÉNYEK	133
A. Önkormányzatiság és politikai	<i>részvétel</i>
.....	133
1. <i>A szavazás feltörése - A</i>	
.....	<i>választásokatfe</i>
<i>nyezető kiberfenyegetések</i>	134
2. <i>Az elme feltörése - Pszichográfiai profilalkotás és</i> <i>Egyéb</i>	<i>befolyásolók</i>
.....	137
3. <i>Fake</i>	<i>News</i> 144
4. <i>A megbízható</i>	
.....	<i>intézményekme</i>
<i>gszűnése</i>	150
B. Egyenlőség és	<i>méltányosság</i>
.....	152
1. <i>Átlátszatlanság: Megmagyarázhatatlan</i>	<i>AI</i> 153
2. <i>Algoritmikus</i>	<i>torzítás</i>
.....	158
IV. SZABÁLYOZÁS AZ	AIKORÁBAN
160	
A. Az adatvédelem zűrzavaros rendszere a Egyesült	Államok
.....	161
1. <i>Állami adatvédelmi</i>	<i>törvények</i>
.....	163
2. <i>Önszabályozás és ágazati</i>	<i>gyakorlatok</i>
.....	165

B. Európai adatvédelmi	jog	166
1. Ellenőrzés és	beleegyezés	168
2. Átláthatóság és	elszámoltatható	169
3. Adatvédelem a	tervezéssel	170
4. Versenyjog		171
C. A robotok és az	AI szabályozása	175
1. A	ló törvénye	176
2. robotikára vonatkozó javasolt uniós jogszabályok		177
3. Asilomar	alapelvek	180
4. Ajánlások		181
KÖVETKEZTETÉS		185

BEVEZETÉS

A mesterséges intelligencia (AI) a modern kor legmegosztóbb technológiája. Hatása valószínűleg eltölpül még az internet fejlődése mellett is, mivel életünk minden szegletébe behatol. Számos mesterséges intelligencia-alkalmazás már ismert, mint például a hangfelismerés, a természetes nyelvi feldolgozás és az önvezető autók. Más alkalmazások kevésbé ismertek, de egyre inkább elterjedtek, mint például a tartalomelemzés, az orvosi robotok és az autonóm harcosok. Ezeknek közös jellemzője, hogy képesek intelligenciát kinyerni a strukturálatlan adatokból. Naponta több millió terabájtnyi adat keletkezik a valós világról és annak lakóiról. Ezek nagy része zaj, kevés nyilvánvaló jelentéssel. A mesterséges intelligencia célja, hogy kiszűrje a zajt, értelmet találjon és cselekedjen, végső soron nagyobb pontossággal és jobb eredményekkel, mint amire az emberek egyedül képesek. A kínaiak kialakulóban lévő intelligenciája hatékony eszköz a problémák megoldására és újak létrehozására.

A mesterséges intelligencia fejlődése nemcsak a számítástechnika új korszakát jelenti, hanem új veszélyeket is a társadalmi értékekre és az alkotmányos jogokra nézve. A közösségi média algoritmusai és a tárgyak internete által a magánéletre jelentett fenyegetés jól ismert. Kevésbé ismert az a még nagyobb veszély, amelyet a mesterséges intelligencia magára a demokráciára jelent.¹ A közelmúlt eseményei jól példázzák, hogyan lehet a mesterséges intelligenciát "fegyverként" felhasználni a választások korrumpálására és az emberek demokratikus intézményekbe vetett hitének megmérgezésére. Azonban, mint sok más bomlasztó technológiánál, a jog csak lassan tud felzárkózni. Az első, a mesterséges intelligenciával foglalkozó parlamenti meghallgatásra több 2016,² mint fél évszázaddal azután került sor, hogy a katonai és tudományos közösségek komoly kutatásokat kezdtek.³

A digitális korszak számos, évszázadok alatt kialakult társadalmi normát és struktúrát felborított. Ezek közé tartoznak az olyan alapvető értékek, mint a magánélet, az autonómia és a demokrácia. Ezek a liberális demokrácia alapelvei, amelynek hatalma a késő század végi 20th

¹ Lásd Nicholas Wright, *How Artificial Intelligence Will Reshape the Global Order*, FOREIGN AFF. (2018. július 10.), <https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order>.

² Lásd *A mesterséges intelligencia hajnala: Hearing Before the Senate Committee on Commerce, Science & Transportation*, 115th Cong. 2 (2016), <https://www.govinfo.gov/content/pkg/CHRG-114shrg24175/pdf/CHRG-114shrg24175.pdf> ("This is the first congressional hearing on artificial intelligence.").

³ A mesterséges intelligencia önálló kutatási területként 1956-ban indult. *Mi a mesterséges intelligencia*, SOC'Y FOR STUDY FOR ARTIFICIAL INTELLIGENCE & SIMULATION BEHAV.,

<http://www.aisb.org.uk/public-engagement/what-is-ai> (utolsó látogatás 2019. január).

században páratlan volt az emberiség történelmében. A század vége felé elért technológiai eredmények az emberiség jólétének fényes jövőjét ígérték. De aztán megjelentek a veszélyt jelző jelek. Az internethálózatnak köszönhetően létrejött a közösségi média, amelynek következtében a magánélet mélyreható és visszafordíthatatlannak tűnő leértékelődése következett be. A tárgyak internete (IoT) számos funkciót jótékonyan automatizált, miközben mindennapi életünk mindenütt jelenlévő megfigyelését és ellenőrzését eredményezte. Az internet és az IoT egyik terméke a "Big Data" és az ~~adatok~~ elterjedése. Ezek az eszközök lehetővé teszik a fogyasztók, nézők és szavazók kifinomult és rejtett ~~vélemény~~ ~~vélemény~~ A személyes döntéshozatali autonómia ebből eredő elvesztése nem kevésbé súlyos, mint a magánélet elvesztése.

A mesterséges intelligencia új technológiai korszakának talán legnagyobb társadalmi költsége a demokratikus intézményeinkbe vetett bizalom és az azok feletti ellenőrzés eróziója.⁴ A Cambridge Analytica által a Facebook-felhasználókról a 2016-os brit és amerikai választások idején végzett "pszichográfiai profilalkotás" jó példa erre. De a választói manipulációnak ezek az esetei aligha az egyetlen fenyegetés, amelyet a mesterséges intelligencia jelent a demokráciára nézve. Ahogy egyre több közfunkciót privatizálnak, úgy csökken az alkotmányos jogok köre. Ha ezeket a funkciókat még inkább a mesterséges intelligenciára bízunk, az lehetővé teszi a rejtett döntéshozatalt, amely mentes a nyilvános vizsgálat és ellenőrzés alól. Például a prediktív rendőri tevékenység és a mesterséges intelligencia általi ítélethozatal büntetőügyekben megerősítheti a diszkriminatív társadalmi gyakorlatokat, de objektívnek tettett módon. Hasonló algoritmikus torzítások más területeken is megjelennek, például a hitelezés, a foglalkoztatás és a biztosítási döntések terén. "A gépeknek már most is megadják a hatalmat, hogy életet megváltoztató, mindennapi döntéseket hozzanak az emberekről".⁵ Mindezt átláthatóság és elszámoltathatóság nélkül teszik.

A kifinomult manipulációs technológiák olyan szintre fejlődtek, hogy az egyének úgy érzékelik, hogy a döntéseiket saját maguk hozzák, ehelyett gyakran algoritmusok "irányítják" őket. Erős példa

⁴ *Lásd pl. Julie E. Cohen, Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 195 (2017) (a Google és a Facebook által létrehozott, mesterséges intelligenciát támogató "ökoszisztémák jelentősen hozzájárultak a politikai polarizáció és bizalmatlanság mai légköréhez"); *lásd a IV.A.4. szakaszt.*

⁵ Jonathan Shaw, *Mesterséges intelligencia és etika*, HARV. MAG. (Jan.-Febr. 2019), <https://www.harvardmagazine.com/2019/01/artificial-intelligence-limitations>.

a "nagy lökdösődés", a "meggyőző számítástechnika" egy formája, "amely lehetővé teszi a tömegek hatékony kormányzását anélkül, hogy a polgárokat be kellene vonni a demokratikus folyamatokba".⁶ A politikai részvétel elriasztása az⁷ egyik célja azoknak, akik a mesterséges intelligenciával visszaélve manipulálnak és irányítanak minket.⁸

A magánéletet és a demokráciát fenyegető veszélyek együttesen és egyénileg is rontják az emberi értékeket. Sajnos ezeknek a létező fejleményeknek a nyomon követése, legalábbis az Egyesült Államokban, többnyire az iparági önszabályozásra maradt. Nemzeti szinten keveset tettek demokratikus intézményeink és értékeink megőrzése érdekében. A mesterséges intelligencia fejlesztését alig felügyelik, így a technológiai óriások szabadon bolyonghatnak adataink között, és tetszés szerint alááshatják jogainkat.⁹ Úgy tűnik, olyan helyzetben vagyunk, ahol Mark Zuckerberg és Sundar Pichai, a Facebook és a Google vezérigazgatói nagyobb befolyással rendelkeznek az amerikaiak élete és jövője felett, mint az általunk megválasztott képviselők. Ezeknek a technológiai óriásoknak a hatalma, hogy "kialakulóban lévő transznacionális uralmakként" lépjenek fel, részben abból¹⁰ ered, hogy a mesterséges intelligencia szoftverek ("West Coast Code") képesek a szabályozási törvényeket ("East Coast Code") felforgatni vagy kiszorítani.¹¹

⁶ Dirk Helbing et al., *Will Democracy Survive Big Data and Artificial Intelligence?*, SCI. AM. (Feb. 2017/25.), <https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence>.

⁷ Lásd H. Akin Ünver, *Artificial Intelligence, Authoritarianism and the Future of Political Systems*, in CYBER GOVERNANCE AND DIGITAL DEMOCRACY 2018/9),

http://edam.org.tr/wp-content/uploads/2018/07/AKIN-Artificial-Intelligence_Bosch-3.pdf at 4 (kifejtve, hogy "az átláthatatlan és nem elszámoltatható technológiai és információs rendszerek a politikai részvétel csökkenéséhez vezethetnek", mivel "a részvétel helyett a központosított ellenőrzési struktúrákat erősítik").

⁸ Elaine Kamarck, *Malevolent Soft Power, AI, and the Threat to Democracy*, BROOKINGS, 2018. november 28.,

<https://www.brookings.edu/research/malevolent-soft-power-ai-and-the-threat-to-democracy> (leírja a technológiai eszközök használatát a szavazatok elnyomására és "a demokrácia visszafordítására Amerikában és az egész nyugati világban").

⁹ Lásd általában Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 HARV. J. L. & TECH (3532016) ("[A] mesterséges intelligencia térnyerése eddig szabályozási vákuumban történt.").

¹⁰ Cohen, *fentebb*, 4. lábjegyzet, 199. lábjegyzet. Lásd még Ünver, 7. lábjegyzet (az "automatizálás struktúrái ... az államoktól és a nemzetközi politikai intézményektől részben független új hatalmi forrást képeznek"); 77-78. lábjegyzet (a technológiai vállalatok gazdasági ereje az államokéval vetekszik).

¹¹ Lásd az alábbi megjegyzést 379.

Egyesek a kialakulóban lévő mesterséges intelligenciát "digitális szerzői társadalomként"¹² vagy "algokráciaként" - algoritmusok általi uralomként - jellemezték.¹³

Ez a cikk azt vizsgálja, hogy a mesterséges intelligencia milyen jelenlegi és várható veszélyeket jelent a magánélet, az autonómia, az egyenlőség, a politikai folyamatok és a jogállamiság alapvető demokratikus elveire nézve. E veszélyek némelyike megelőzte a mesterséges intelligencia megjelenését, mint például a fogyasztói és választói preferenciák rejtett manipulálása, de a mesterséges intelligencia által biztosított hatalmas befolyásoló erő még hatékonyabbá teszi őket. Ennél is aggasztóbbak azonban a mesterséges intelligencia *sui generis* kockázatai. Ezek közé tartozik például a mesterséges intelligencia azon képessége, hogy különböző adathalmazokból átfogó viselkedési profilokat hoz létre, és újra azonosítja az anonimizált adatokat. Ezek a legintimebb személyes adatainkat teszik hozzáférhetővé a hirdetők, kormányok és idegenek számára. A legnagyobb veszélyt itt a közösségi média jelenti, amely a mesterséges intelligenciára támaszkodik a növekedési és bevételi modelljeiben. Más újszerű, vitákat kiváltó funkciók közé tartozik az "algoritmikus elfogultság" és a "megmagyarázhatatlan mesterséges intelligencia". Az előbbi a mesterséges intelligencia azon tendenciáját írja le, hogy felerősíti a társadalmi előítéleteket, de burkoltan és az objektivitás látszatával. Az utóbbi a mesterséges intelligencia átláthatóságának hiányát írja le. Az AI eredményei gyakran olyan érvelésen és feldolgozáson alapulnak, amelyek az emberek számára ismeretlenek és megismerhetetlenek. A mesterséges intelligencia "fekete doboz" döntéshozatalának átláthatatlansága¹⁴ a demokratikus önkormányzatiság és a tisztességes eljárás ellenpólusa, mivel kizárja, hogy a mesterséges intelligencia eredményeit az alkotmányos normák alapján teszteljék.

Nem becsüljük alá a mesterséges intelligencia produktív előnyeit és elkerülhetetlen fejlődési pályáját, de szükségesnek érezzük, hogy kiemeljük a kockázatokat is. Ez nem egy disztópikus jövőkép, ahogyan azt a mesterséges intelligenciával kapcsolatos sok szörnyű figyelmeztetés mutatja.¹⁵ Az embereket nem feltétlenül fenyegeti veszély

¹² Wright, *fenti* megjegyzés 1.

¹³ John Danaher, *Algoritmus általi uralom? Big Data and the Threat of Algocracy*, PHILOSOPHICAL DISQUISITIONS (2014. január 26.), <http://philosophicaldisquisitions.blogspot.com/2014/01/rule-by-algorithm-big-data-and-threat.html>.

¹⁴ Lásd Will Knight, *The Dark Secret at the Heart of AI*, MIT TECH. REV. (2017. április 11.), <https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai> (a megmagyarázhatatlan algoritmikus **fükek** "fekete

Elektronikusan elérhető a következő címen:

<https://ssrn.com/abstract=3273016>

doboz" hatását írja le).

¹⁵ *Lásd pl.* NICK BOSTROM, SUPERINTELLIGENCE: UTAK, VESZÉLYEK, STRATÉGIÁK. GIES (2014), 115 ("[A] gépi öntelligencia létrehozásának valószínűsíthető alapértelmezett kimenetele az egzisztenciális katasztrófa.").

mint faj, de a demokratikus intézményeink és értékeink szempontjából biztosan veszélyben vagyunk.

A II. rész röviden bemutatja a mesterséges intelligencia legfontosabb aspektusait, hogy a laikus olvasó is megérthesse, hogyan alkalmazzák a mesterséges intelligenciát az általunk tárgyalt különböző területeken. A legalapvetőbb szinten a mesterséges intelligencia az emberi információérzékelést, -feldolgozást és -reakciót utánozza - amit hiányosan "intelligenciának" nevezhetünk -, de sokkal nagyobb sebességgel és léptékben, olyan eredményeket produkálva, amelyeket az ember nem tud elérni.¹⁶

A III. rész a magánélethez fűződő jogokra és az ellenük fellépő erőkre összpontosít. Tartalmazza a mesterséges intelligencia adatgyűjtési és -feldolgozási jellemzőinek tárgyalását, beleértve az IoT-t és a Big Data Analyticset is. A mesterséges intelligencia megfelelő működéséhez adatokra van szükség, ami hatalmas mennyiségű személyes adatot jelent. A folyamat során a mesterséges intelligencia valószínűleg mind a döntési, mind az információs magánélethez fűződő jogainkat csorbítani fogja.

A IV. rész a mesterséges intelligencia által a demokratikus ellenőrzésre és intézményekre jelentett veszélyeket tárgyalja. Ez nemcsak a választási folyamatot, hanem a demokrácia egyéb összetevőit is magában foglalja, mint például az egyenlőség és a jogállamiság. A mesterséges intelligenciának a közvélemény titkos manipulálására való képessége már most is destabilizáló hatással van az Egyesült Államokban és világszerte.

Az V. rész az Egyesült Államok és Európa jelenlegi szabályozási környezetét vizsgálja, valamint a civil társadalom erőfeszítéseit, amelyekkel a mesterséges intelligencia kockázataira kívánja felhívni a figyelmet. Ezt a részt azzal zárjuk, hogy javaslatot teszünk egy sor olyan válaszlépésre, amelyet a Kongresszus megtehetne e kockázatok közvetítése érdekében. A mesterséges intelligencia szabályozása, miközben elősegíti annak előnyös fejlődését, gondos mérlegelést igényel. Ezt azonban az állami szervezeteknek kell elvégezniük, nem pedig egyszerűen az AI-fejlesztőknek, a közösségi médiának és a technológiai vállalatoknak, ahogyan az jelenleg többnyire történik.¹⁷ Emellett az AI-specifikus szabályozásra is szükség van, nem pedig a meglévő jogszabályok kiterjesztésére. Az Európai Parlament nemrégiben tett javaslatot egy szabályozási modellre és jogszabálycsomagra. Erre, valamint a mesterséges intelligenciával foglalkozó közösség által kidolgozott etikai és demokráciaerősítő elvekre támaszkodunk. Mindannyian érdekeltek vagyunk ebben a kérdésben, és

¹⁶ A mesterséges intelligencia képességeinek általános leírását lásd Scherer, *Supra* note. 9.

¹⁷ Az Amazon és az Alphabet 2017-ben nagyjából háromszor annyit költött a mesterséges intelligencia kutatás-fejlesztésére, mint az Egyesült Államok szövetségi kiadásai összesen. *Lásd* SHOHAM ET AL., *ARTIFICIAL INTELLIGENCE INDEX ANNUAL 2018 REPORT* at (582018).

a mesterséges intelligencia szabályozásában és alkalmazásában jelenleg fennálló hatalmi aszimmetriát kell korrigálni.

A mesterséges intelligenciával kapcsolatos kockázatok nem a legsúlyosabb probléma, amellyel ma szembe kell néznünk. Vannak sokkal egzisztenciálisabb fenyegetések, mint például a klímaváltozás.¹⁸ De a valóság tagadásának ökoszisztémája, amely magában foglalja a fogékony csoportok és a politikai döntéshozók algoritmikus célba vételét, még az éghajlatváltozásról szóló vitát is megfertőzte.¹⁹ A mesterséges intelligenciát arra használják, hogy a kormányokkal és a demokratikus intézményekkel szembeni bizalmatlanság magvait elültessék, ami a kollektív cselekvés megbénulásához vezet.²⁰ A következmények katasztrofálisak lehetnek. Ahogy Stephen Hawking, Elon Musk és Bill Gates is figyelmeztetett, a mesterséges intelligencia az emberiség legnagyobb találmánya lehet, de egyben nagy kockázatot is jelent.²¹ Ez a cikk e kockázatok közül néhányat vizsgál meg. E tekintetben csatlakozik ahhoz a kialakulóban lévő diskurzushoz, amely a mesterséges intelligencia bomlasztó erejére és a társadalmi struktúrák destabilizálására figyelmeztet.²²

I. AZ AI RÖVID BEVEZETÉSE

A mesterséges intelligencia az "intelligens számítástechnika"²³ egyik formája, amely olyan számítógépes programokra támaszkodik, amelyek az emberekhez hasonlóan képesek érzékelni, érvelni, tanulni, cselekedni és alkalmazkodni.²⁴ Azért "intelligens", mert utánozza

¹⁸ Vö. Nathaniel Rich, *Losing Earth: The Decade We Almost Stopped Climate Change*, N.Y. TIMES (2018. augusztus 1.) ("A hosszú távú katasztrófa most a legjobb forgatókönyv.")

¹⁹ *Lásd pl.*, 163 Cong. Rec. S. 2970, 2017. május 16. (Whitehouse szenátor megjegyzései); Sander van der Linden, *Inoculating the Public Against Misinformation About Climate Change*, GLOBAL CHALLENGES (2017).

²⁰ *Lásd* Cohen, 4. lábjegyzet. Az intézményekkel szembeni bizalmatlanság súlyosbítja a kollektív cselekvés problémáját az olyan közjavak biztosításában, mint a környezetvédelem.

²¹ *Lásd* Kelsey Piper, *The Case for Taking AI Seriously As A Threat to Humanity*, VOX (dec. 1223,2018,;38), <https://www.vox.com/future-perfect/2018/12/21/18126576/ai-artificial-intelligence-machine-learning-safety-alignment>.

²² *Lásd pl.* Hin-Yan Liu, *The Power Structure of Artificial Intelligence*, 10 L. INNOVATION & TECH. 197 (2018); Henry Kissinger, *How the Enlightenment Ends*, ATLANTIC (2018. június), <https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/> (azzal érvel, hogy "az emberi társadalom felkészületlen a mesterséges intelligencia felemelkedésére").

²³ Az informatikusok ezt "számítási intelligenciának" nevezik, amelynek a mesterséges intelligencia egy részhalmaza.

²⁴ A mesterséges intelligencia jövőjéről szóló törvény, H.R. 115th4625, Cong. § (32017) tartalmaz egy részletesebb "hivatalos" meghatározást, amely többnyire

követi az alábbiakat

emberi megismerés.²⁵ Azért "mesterséges", mert nem biológiai, hanem számítógépes információfeldolgozásról van szó. A mesterséges intelligencia felemelkedő ereje a számítógépes feldolgozás és tárolás exponenciális növekedésének, valamint a hatalmas adattáraknak köszönhető, amelyekből a jelentés kinyerhető. A gépek számítási képességei és a robotika²⁶ fejlődése ma már olyan lenyűgöző, hogy a múlt számos sci-fi jóslata elhalványul ehhez képest. A közeljövőben megjelenő kvantumszámítással a²⁷ mesterséges intelligencia kompetenciái gyorsabban fognak fejlődni, mint ahogy azt el tudjuk képzelni vagy fel tudunk rá készülni.

Sok különböző rendszer tartozik a széles körű mesterséges intelligencia fogalomkörébe. Ezek közé tartoznak a "szakértői rendszerek", amelyek olyan részletes algoritmusok (lépésről lépésre haladó számítógépes programok), amelyek egy sor ember által programozott szabályt és tudást tartalmaznak a problémamegoldáshoz. A "gépi tanulás" (ML) a mesterséges intelligencia fejlettebb formája, amely kevésbé függ az emberi programozástól, és inkább az algoritmus azon képességétől, hogy statisztikai módszereket használjon, és az adatokból tanuljon a fejlődés során. Az ML lehet "felügyelt" (ember által betanított) vagy "felügyelet nélküli", ami azt jelenti, hogy emberi input nélkül, magától betanítja magát.²⁸ A technológia korai alkalmazását 1997-ben fejlesztette ki a Stanford Egyetem két hallgatója, Larry Page és Sergey Brin. Ők a bejövő linkek gyakoriságán alapuló webes rangsorokat tartalmazó katalógust készítettek. Az általuk épített keresőmotor - a Google - a világ egyik legnagyobb mesterséges intelligenciával foglalkozó vállalatává nőtte ki magát.²⁹

Az ML egy erős formája a "Deep Learning" (DL), amely mesterséges neurális hálózatoknak nevezett tanulási algoritmusokat használ, amelyek laza ihletésűek.

itt. A mesterséges intelligenciát részletesen leíró számos mű közül LUKE DORMEHL, *THINKING MACHINES* (Penguin, 2017) című művét ajánljuk, amely kiváló, a laikus olvasók számára is hozzáférhető áttekintést nyújt.

²⁵ *Lásd pl. , Algorithms Based On Brains Make For Better Networks*, NEUROSCIENCE NEWS (2015. július 17.), <https://neurosciencenews.com/neuroscience-network-algorithms-2263>.

²⁶ Ahogy mi használjuk a kifejezést, a robot lényegében egy mesterséges intelligencia mozgó alkatrészekkel.

²⁷ *Lásd Vivek Wadhwa, Quantum Computers May Be More of an Imminent Threat than AI*, WASH. POST (2018. február 5.), <https://www.washingtonpost.com/news/innovations/wp/2018/02/05/quantum-computers-may-be-more-of-an-imminent-threat-than-ai>.

²⁸ *Lásd általában Nikki Castle, Supervised vs. Unsupervised Machine Learning*, DATASCIENCE. COM (2017. július 13.), <https://www.datascience.com/blog/supervised-and-unsupervised-machine-learning-algorithms>.

²⁹ *Lásd* DORMEHL, 24. lábjegyzet. A Google mesterséges intelligenciával kapcsolatos műveleteit az anyavállalatba, az Alphabet, Inc.

az emberi agy szerkezete alapján. A mesterséges neuronok rétegekben kapcsolódnak egymáshoz, amelyek a "backpropagation" visszacsatolási hurkokon keresztül menet közben átprogramozzák és szerkesztik magukat.³⁰ Ezek az agyban lévő idegpályákat utánozzák, amelyek minden egyes alkalommal, amikor használják őket, megerősítik magukat.³¹ Ez a dinamikus megközelítés lehetővé teszi a DL számára, hogy strukturálatlan adatokban mintákat találjon, amelyekből a tudás reprezentációját az érveléshez hasonló módon modellezi. A DL esetében a fejlesztők csak alapvető szabályokat (pl. matematikai műveletek) és célokat adnak meg; a mesterséges intelligencia ~~kih~~ a megvalósításukhoz szükséges lépéseket.³² Ez az alkalmazkodási képesség teszi az AI-t olyan hatékonná.

A mesterséges intelligencia emberi intelligenciát felülmúló képességének időbeli ütemezését heves viták övezik. Az úgynevezett Turing-teszt egy olyan kísérlet, amelyben egy emberi kérdező nem képes megkülönböztetni az emberi és a számítógép által generált természetes nyelvű válaszokat egy vak beszélgetés során.³³ Ray Kurzweil futurista 2029-re jósolta a Turing-teszt sikeres teljesítését.³⁴ Addig is a mesterséges szűk értelem (ANI), vagy gyenge mesterséges intelligencia korszakában maradunk, ahol a speciális számítógépes programok bizonyos feladatokban, például ügyességi játékokban és szövegelemzésben felülmúlják az embert. Az ANI magában foglalja a kognitív komputert, ahol a gépek segítik az embert az olyan feladatok elvégzésében, mint a

³⁰ Lásd Alexx Kay, *Artificial Neural Networks*, COMP. WORLD (2001. február 12.), <https://www.computerworld.com/article/2591759/app-development/artificial-neural-networks.html>. A DL az emberi agyban lévő neurális hálózatokat utánozza, amelyek szintén sok, gyakran véletlenszerű kapcsolatot létesítenek minden egyes művelethez a kimenet optimalizálása érdekében. ³¹ DORMEHL, *supra* note 24, at 35.

³² Lásd Alex Castrounis, *Artificial Intelligence, Deep Learning, and Neural Networks Explained*, INNOARCHITECH, <https://www.innoarchitech.com/artificial-intelligence-deep-learning-neural-networks-explained> ("[DL] algorithms themselves 'learn' the optimal parameters to create the best performing model ... In other words, these algorithms learn how to learn.").

³³ *The Turing Test*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY (20039., április), <https://plato.stanford.edu/entries/turing-test>.

³⁴ A Turing-teszt teljesítésének nehézségeihez járulnak hozzá a gépi intelligencia mérésére szolgáló eszközökkel kapcsolatos viták. 2014-ben egy chatbot több emberi bírót is megtévesztett, hogy azt higgye, hogy ember, de ez sok tudóst nem győzött meg. Nadia Khomami, *2029: The Year When Robots Will Have the Power to Outsmart Their Makers*, GUARDIAN (2014. február 22.), <https://www.theguardian.com/technology/2014/feb/22/computers-cleverer-than-humans-15-years>.

mint például a radiológusok röntgenfelvételek leolvasásában, a tőzsdeügynökök kereskedésében és az ügyvédek szerződéskötésében.³⁵

A mesterséges intelligencia következő generációja a mesterséges általános intelligencia (AGI) lesz. Képességei túlmutatnak majd egy meghatározott és előre meghatározott problémakészlet megoldásán, és az intelligenciát bármilyen problémára alkalmazni fogják.³⁶ Ha a számítógépek egyszer képesek lesznek önállóan felülmúlni még a legokosabb embereket is, akkor elérjük a mesterséges szuperintelligenciát (ASI).³⁷ Egyesek ezt a "szingularitásnak" nevezik, amikor a szilíciumszámítógépek teljesítménye meghaladja a biológiai számítógépekét.³⁸ Ezen a ponton egy disztópikus jövő víziói jelenhetnek meg.³⁹ Szerencsére van időnk tervezni. Sajnos azonban hiányzik a megfelelő sürgető érzés.

II. A MAGÁNÉLETET FENYEGETŐ VESZÉLYEK

A magánélethez való alapvető jog részét képezi a személyes döntések meghozatalához való jog, a személyes adatok bizalmas kezeléséhez való jog és a magányhoz való jog. Ezeket a jogokat a II. világháború utáni emberi jogokról szóló számos chartában általánosan elismerik és védik, és a demokrácia alapelveinek tekintik.⁴⁰ Az Egyesült Államok alkotmánya közvetve elismeri a magánélethez való jogot és az információs magánélethez való jogot, bár ez az elismerés az alábbiakból fakad

³⁵ Lásd J.C.R. Licklider, *Man-Computer Symbiosis*, 1 IRE TRANSACTIONS HUMAN FACTORS ELEC. 4, (41960).

³⁶ Joel Traugott, *The 3 Types of AI: A Primer*, ZYLOTECH (2017. október 24.), <https://www.zylotech.com/blog/the-3-types-of-ai-a-primer>.

³⁷ BOSTROM, *fenti* megjegyzés 15.

³⁸ Lásd RAY KURZWEIL, A SZINGLÁTUS KÖZEL VAN (1362005). John Von Neumann ezt a kifejezést a technológiai fejlődés azon pontjára használta, "amelyen túl az emberi ügyek, ahogyan mi ismerjük őket, nem folytatódhatnak". Stanislaw Ulam, *Tribute to John Von Neumann*, 64 BULLETIN AM. MATHEMATICAL SOC'Y 1, 5 (1958).

³⁹ Lásd: BOSTROM, *Supra* note Kurzweil15. szerint ez körülbelül a Lásd2045.: BOSTROM, *Supra* note.

KURZWEIL, *fenti* megjegyzés 38.

⁴⁰ Lásd például az Emberi Jogok Egyetemes Nyilatkozatát, G.A. Res. 217A (III), U.N. Doc. A/810, 71. o. (1948), Art. 12. cikk; Európa Tanács, a 11. és 14. jegyzőkönyvvel módosított, az *emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény*, 1950. november 4., 12. cikk; Európa Tanács, az *emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény*, 1950. november 4., 12. cikk. 8. cikk; Amerikai Államok Szervezete (OAS), *Emberi Jogok Amerikai Egyezménye*, "San Jose-i Paktum", Costa Rica, november, 22 Art1969., 11.

nagyrészt bírósági következtetésből, nem pedig szöveges parancsból.⁴¹ Amint azt rövidesen látni fogjuk, az amerikai alkotmányos és törvényi jogban a magánélethez fűződő jogok gyenge védelme kreatív és gyakori megsértésére ösztönöz. Ez a rész ezeket a problémákat és a mesterséges intelligencia által jelentett további veszélyeket tárgyalja.

A. A magánélet formái

Az információs adatvédelemmel kapcsolatos alapvető mű Samuel Warren és Louis Brandeis 1890-es "A magánélethez való jog" című cikke,⁴² amely a "személynek a békén hagyáshoz való joga" szokásjogának fejlődését vizsgálta és fejlesztette tovább. Ahogy a magánélethez fűződő jogok az évek során a bíróságokon fejlődtek, William Prosser négy különböző, a magánélet megsértéséből eredő kártételeket kristályosított ki: 1) a magányba vagy magányba való behatolás, vagy a magánügyekbe való beavatkozás; 2) kínos magánjellegű tények nyilvánosságra hozatala; 3) hamis fényben való nyilvánosság; és 4) a név vagy képmás kisajátítása.⁴³ Ma a legtöbb állam elismeri ezt a négy különböző kárt a magánélethez kapcsolódó deliktumként, és polgári és büntetőjogi jogorvoslatot biztosít az ebből eredő kereseti okokra. A magánélethez kapcsolódó deliktumok célja, hogy megvédjék azokat az embereket, akiknek érzékenységét és érzéseit sérti az, hogy mások rendkívül sértő magatartás miatt igaz, de intim vagy kínos tényeket fednek fel.⁴⁴

⁴¹ A negyedik módosítás tartalmazza az egyetlen kifejezett utalást a magánélet védelmére: "Nem sérthető meg az embereknek az a joga, hogy személyük, házuk, irataik és vagyontárgyaik biztonságban legyenek az indokolatlan házkutatás és lefoglalás ellen". . .

." A "magánélethez való jog" a köznyelvben általában a döntési jogra utal. A bírói elismerés olyan ügyekben jelenik meg, mint a *Griswold v. Conn.*, 381 U.S. 479 (1965) (házassági magánélet) és a *Roe v. Wade*, 410 U.S. 113 (1973) (abortuszhoz való jog). Az információs magánélethez való jogot a *Whalen* kontra *Roe* ügyben feltételezték, 429

U.S. 589 (1977) (a betegreceptek kötelező jelentésének fenntartása), de megkérdőjeleződött a *NASA* kontra *Nelson*, 562 U.S. 134 (2011) ügyben (a szövetségi alkalmazottak orvosi információkat is tartalmazó, beleegyezés nélküli háttérellenőrzésének fenntartása).

⁴² Samuel Warren & Louis Brandeis, *The Right to Privacy*, HARV. L. REV. 193 (1890). Nyilvánvalóan befolyásolta őket George Eastman hordozható fényképezőgépének kifejlesztése és annak a Kodak Company által a hétköznapi fogyasztók számára történő forgalmazása, mivel féltek attól, hogy a fényképezőgép képes lesz magánügyekről képeket készíteni.

⁴³ William L. Prosser, *Adatvédelem*, CAL. L. REV. 383,389 (1960).

⁴⁴ Anita L. Allen-Castellitto, *Az adatvédelem megértése*: PLI/PAT865 (2006)23.

A magánélet és a személyiség common law-i eredetén túl a magánélet más felfogásai is léteznek. Ezek közé tartozik az információs magánélet, a döntési magánélet, a viselkedési magánélet és a fizikai magánélet.⁴⁵ Az információs magánélet a személyes információink áramlásának ellenőrzéséhez való jogot jelenti. Ez egyaránt vonatkozik azokra az információkra, amelyeket magunkban tartunk, és azokra az információkra, amelyeket bizalmasan megosztunk másokkal.⁴⁶ A döntési magánszféra az a jog, hogy a döntéseinket és döntéseinket beavatkozás vagy ~~duzs~~ nélkül hozhassuk meg.⁴⁷ A viselkedési magánélet magában foglalja azt a lehetőséget, hogy az ember a nem kívánt megfigyeléstől vagy behatolástól mentesen azt teheti és cselekedheti, amit akar.⁴⁸ A fizikai magánélet magában foglalja a magányhoz, az elszigeteltséghez és a jogellenes házkutatással és lefoglalással szembeni védelemhez való jogot.⁴⁹ A szabadság ezen felfogásai a nyugati demokrácia központi jellemzőivé váltak, amit az alapító dokumentumokba, valamint a törvényi, szokásjogi és bizonyító erejű törvények széles körébe való beépítésük is tükröz.

Az információs magánélet számos demokratikus értéket támogat: a gondolatok kialakításának, a kísérletezésnek, a gondolkodásnak vagy a hibák elkövetésének képességét mások megfigyelése vagy beavatkozása nélkül. Más szabadságjogokat is véd, beleértve a politikai részvételt, a lelkiismereti szabadságot, a gazdasági szabadságot és a diszkriminációtól való mentességet.

A magánélet elvesztése ugyanezeket a szabadságjogokat erodálhatja. Ha mások hozzáférnek a magánjellegű adatainkhoz, képesek lehetnek befolyásolni vagy irányítani a cselekedeteinket. Ez az oka annak, hogy oly sok szereplő igyekszik hozzáférni a bizalmas információkhoz. A kíváncsiskodók többek között a következőket szeretnék tudni: kapcsolataink, intim kapcsolataink és tevékenységeink, politikai döntéseink és preferenciáink, kormányzati nyilvántartások, genetikai, biometrikus és egészségügyi adatok (a születés előttől a halál utánig), ~~data~~ és foglalkoztatási adatok, telefonos, szöveges és e-mail levelezés, a közösségi médiában megjelenő kedvelések, barátok és preferenciák, böngészési tevékenység, hely és mozgás, vásárlási szokások, banki, biztosítási és egyéb pénzügyi információk, valamint a csatlakoztatott eszközök és viselhető eszközök adatai. Óriási mennyiségű adatot generálunk

⁴⁵ *Id.*

⁴⁶ Lásd Daniel J. Solove & Neil M. Richards, *Privacy's Other Path: Recovering the Law of Confidentiality*, GEO96. L.J. (2007)123.

⁴⁷ Micelle Finneran Denny et al., *The Privacy Engineer's Manifesto*, MCAFEE (2014), <https://link.springer.com/content/pdf/10.1007%2F978-1-4302-6356-2.pdf>.

⁴⁸ *Id.*

⁴⁹ Allen-Castellitto, *Supra* note 44.

minden nap. A magánélet megőrzése herkulesi feladat. Másrészt a védelmünkön való áthatolás nagyon könnyű és jövedelmező lehet.

Az adatok nemcsak meghatároznak minket, hanem az AI éltető elemei is. Az adattudomány a digitális korszak új tudományága. Az olyan vállalatok, mint a Facebook, a Snap- chat vagy a Google nem elsősorban a közösségi média vagy a fogyasztói eszközök üzletágában tevékenykednek, hanem az adatbizniszben. Az általuk kínált termékek (a legtöbb esetben a végfelhasználó számára ingyenesek) olyan eszközök, amelyekkel ~~ny~~mennyiségű és gazdag adatot gyűjtenek, így a felhasználó lényegében maga a termék. Az értékes árucikk határozza meg üzleti modelljüket és bevételi forrásaikat.⁵⁰ Valóban, "a személyes adatok a digitális korszak legértékesebb árucikkévé váltak, amelyekkel a Szilícium-völgy és azon túl a legbefolyásosabb vállalatok közül néhányan hatalmas mennyiségben kereskednek".⁵¹ Az eredmény a társadalom adatosítása.

A mesterséges intelligencia és annak képessége, hogy hatalmas mennyiségű adatot képes feldolgozni, számos formában aláássa az elsőbbséget. A következő fejezetekben részletezzük, hogy a mesterséges intelligencia milyen módon veszélyeztetheti a magánéletünket és a szabad akaratunkat. A tárgyalt mechanizmusok némelyikét még a mesterséges intelligencia előtt fejlesztették ki. A mesterséges intelligencia azonban mindegyikben bevethető, így mindegyik hatékonyabbá és ezáltal fenyegetőbbé válik. Valójában már most "a magánélet nihilizmusának korába" léptünk.⁵²

B. Adatgyűjtés, elemzés és felhasználás

Az adatok jelentősége miatt a technológiai vállalatok mindig is a jogi és etikai határokat feszegetve igyekeznek majd egyre több adatot gyűjteni, hogy egyre jobb és jobb előrejelzéseket készítő modelleket hozzanak létre. Ezt követően ezeket az információkat megosztják a kormányzati szervekkel és a magánszereplőkkel.

⁵⁰ *Lásd pl. Damien Collins, Summary of Key Issues from the Six4Three Files*, <https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf> (leírja, hogy a Facebook hogyan kereskedett a felhasználói adatokhoz való hozzáféréssel reklámvásárlásért cserébe).

⁵¹ Gabriel J.X. Dance et al., *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (2018. dec. 18.), <https://www.ny-times.com/2018/12/18/technology/facebook-privacy.html> (leírja, hogyan kereskedtek a személyes adatokkal 150 vállalat között a felhasználók beleegyezése nélkül).

⁵² Ian Bogost, *Welcome to the Age of Privacy Nihilism*, ATLANTIC (2018. augusztus 23.), <https://www.theatlantic.com/technology/archive/2018/08/the-age-of-privacy-nihilism-is-here/568198>.

Nincs megfelelő jogi védelem az ilyen információközlések megakadályozására. Ha megértjük a teljes képet, hogy adatok nélkül a modern mesterséges intelligencia nagy része nem létezhet, az adatvédelem és a demokrácia az aggodalom középpontjába kerül.

Az adatgyűjtők vagy harmadik fél "felhő" tárolási szolgáltatásai különböző adatbázisokban tartják fenn a tárgyak internete, a felügyeleti és nyomon követési rendszerek által gyűjtött nagy mennyiségű adatot. Míg elszigetelten, a több ezer szerverre szétszórta egyedi adatkészletek korlátozott információval szolgálhatnak, ez a korlátozás feloldható az "adatfúzió" néven ismert folyamattal, amely egyesíti, rendszerezi és korrelálja ezeket az adatpontokat.⁵³ Miután az adatokat összegyűjtötték, szintetizálták és elemezték, harmadik felek kifinomult profilokat állítanak ~~össze~~ "adatalanyaikról",⁵⁴ amelyek hasznos információk tárházát kínálják mindazok számára, akik befolyásolni vagy manipulálni akarják a vásárlási döntéseket és egyéb döntéseket.

A mesterséges intelligencia az adatelemzés motorja. Lehetővé teszi a fogyasztók pénzügyi, demográfiai, etnikai, faji, egészségügyi, szociális és egyéb adatai alapján történő prediktív döntéshozatalt. Az IBM Watson például olyan alkalmazásprogram-interfészeket (API-kat) biztosít, amelyek lehetővé teszik a fejlesztők számára, hogy saját természetes nyelvű interfészeket hozzanak létre.⁵⁵ A Google Tensor Flow egy nyílt forráskódú platform és könyvtár, amely hasonlóképpen lehetővé teszi a mesterséges intelligencia fejlesztőinek, hogy a gépi tanulás erejét számos alkalmazáshoz használják fel.⁵⁶ A Facebook a "Photo Review" programjához fejlesztette ki a "Deep Face"-t, egy mélytanulós arcfelismerő rendszert, amely a kép "fő komponenseit" azonosítja, és a "fő komponenseket" a képen.

⁵³ Lásd Sadia Din et. al, *A Cluster-Based Data Fusion Technique to Analyze Big Data in Wireless Multi-Sensor Systems*, IEEE ACCESS (2017. február 2.), <https://ieeexplore.ieee.org/document/7873266> (az adatfúzió leírása).

⁵⁴ Az EU által az általános adatvédelmi rendeletben elfogadott meghatározás szerint az érintett "azonosított vagy azonosítható természetes személy", akinek személyes adatait gyűjtik vagy feldolgozzák. Lásd az alábbi cikket. Az EU általános adatvédelmi rendelete (GDPR) 4. cikkének (1) bekezdése: Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról.

⁵⁵ Lásd IBM, <https://www.ibm.com/watson> (utolsó látogatás 20181., augusztus).

⁵⁶ Lásd Tensor Flow, <https://www.tensorflow.org> (utolsó látogatás 20181., aug.).

összehasonlítva azokat egy referenciaadathalmazzal.⁵⁷ A Deep Face pontosabb, mint az FBI hasonló rendszere.⁵⁸ A mesterséges intelligencia teljesítményének és sebességének technológiai fejlődése lehetővé tette, hogy az ilyen rendszerek egyre több és több potenciálisan releváns meglátást fedezzenek fel rendkívül kifinomult és összetett adathalmazokból.

Az adatgyűjtés, -elemzés és -felhasználás fejlődése olyan magánélethez fűződő jogokat fenyeget, amelyeket az állami jogban kodifikált négy magánélethez fűződő jogellenes cselekmény nem véd kifejezetten. Ráadásul a társadalom számára előnyök és hátrányosak is lehetnek. Az egészségügyi adatokat például felhasználhatják a betegségek gyógyítását célzó kutatásokra, de arra is, hogy kizárják az alacsonyabb biztosítási díjra jelentkezőket. A különböző adatbázisok összesítése és összehangolása a vásárlási szokásoktól kezdve az egészségi állapoton át a vallási, társadalmi és politikai preferenciáig mindent feltárhat. A bíróságok elkezdtek felismerni az ezzel járó veszélyt. Az *Egyesült Államok kontra Jones ügyben az amerikai bíróság* többsége aláírta vagy egyetértett a "mozaik-elmélet" támogatásával, amely szerint a hosszú távú megfigyelés a negyedik kiegészítést sértő házkutatásnak tekinthető, mivel az összesített helymeghatározási információk részletes képet nyújtanak.⁵⁹ Ahogy Sotomayor bíró egyetértő véleménye megjegyezte, a kormány azon képessége, hogy ezeket az információkat határozatlan ideig tárolja és bányássza, "megfélemlíti a társulási és kifejezési szabadságjogokat",⁶⁰ és aláássa a bűnüldözés korlátozására szolgáló ellenőrzéseket és egyensúlyt. Ha engedélyezik, a polgárok nyomom követésének ilyen korlátlan mérlegelési jogköre károsan befolyásolhatja a kormány és a polgárok közötti kapcsolatokat, ami veszélyezteti a demokráciát.

A mesterséges intelligencia súlyosbítja és exponenciálisan megsokszorozza a meglévő tendenciákat, amelyek az adatok túlzott gyűjtésére és az adatok nem szándékolt, a felhasználók számára a gyűjtéskor nem ismertett célokra történő felhasználására irányulnak. A felügyelt gépi tanuláshoz nagy mennyiségű, pontosan megjelölt adatra van szükség az algoritmusok betanításához. Minél több az adat, annál jobb minőségű lesz a tanult algoritmus.

⁵⁷ Gurpreet Kaur, Sukhvir Kaur & Amit Walia, *Face Recognition Using PCA, Deep Face Method*, INT5'L J. COMPUTER SCI. & MOBILE COMPUTING 359-366 (2016).

⁵⁸ Russell Brandom, *Why Facebook is Beating the FBI at Facial Recognition*, VERGE (2014. július 7.), <https://www.theverge.com/2014/7/7/5878069/why-face-book-is-beating-the-fbi-at-facial-recognition> (97%-os pontosság a DeepFace vs. 85%-os pontosság az FBI rendszerei esetében).

⁵⁹ *Egyesült Államok kontra Jones, USA* (5654002012).

⁶⁰ *Id.* at (416 Sotomayor, J., egyetértésben).

legyen. Minél több változó vagy jellemző van, annál összetettebb és potenciálisan pontosabb lehet a modell. Így nem a legjobb algoritmussal, hanem a legjobb adatokhoz való hozzáféréssel rendelkező vállalatok lesznek sikeresek. Minél több adatot gyűjtenek, annál okosabbak, gyorsabbak és pontosabbak lesznek az algoritmusok. Ösztönzőleg hat a túlzott adatgyűjtés és az adatok felhasználása az újszerű feladatok elvégzésére alkalmas algoritmusok kifejlesztésére. A közelmúltban született meg az "adat az új olaj" kifejezés, amely azt a gondolatot hivatott érzékeltetni, hogy az adat értékes árucikk, amelyet pénzzé lehet tenni.⁶¹ Aki a legjobb adatokkal rendelkezik a mennyiség és a minőség tekintetében, annak lehetősége van arra, hogy bomlasztó üzleti modelleket és bevételtermelő erőműveket hozzon létre.

1. A dolgok internete

A mesterséges intelligencia ereje abban rejlik, hogy a gép hozzáfér az adatokhoz. A mesterséges intelligencia lényegében ezt teszi: adatokat dolgoz fel. Ezért minél több információ áll rendelkezésre egy adatalanyról, vagy minél nagyobb a hozzáférhető adathalmaz, annál jobban képes a mesterséges intelligencia megválaszolni egy lekérdezést vagy végrehajtani egy feladatot.⁶²

A tárgyak internete ("IoT") a testünkön, otthonainkban, irodáinkban, járműveinkben és nyilvános helyeken található elektronikus érzékelők ökoszisztémája.⁶³ A "dolgok" minden olyan ember alkotta tárgy vagy természetes objektum, amely internetes címet kap, és ember-ember vagy ember-számítógép közötti interakció nélkül továbbít adatokat egy hálózaton keresztül." ⁶⁴ Ha az AI olyan, mint az emberi agy, akkor az IoT olyan, mint az emberi test, amely érzékszervi inputokat (hang, látás és tapintás) gyűjt.⁶⁵ Az IoT-eszközök összegyűjtik a fizikai cselekvéseket végző és kommunikáló emberek nyers adatait.

⁶¹ *The World's Most Valuable Resource Is No Longer Oil, But Data*, ECONOMIST (2017. május 6.), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

⁶² *Lásd általában SAS, Mesterséges intelligencia: SAS*, https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html.

⁶³ *Lásd* https://en.wikipedia.org/wiki/internet_of_things.

⁶⁴ Margaret Rouse, *Internet of Things*, TECH TARGET (2016. július), <https://inter-netofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>.

⁶⁵ Calum McClelland, *The Difference Between Artificial Intelligence, Machine Learning, and Deep Learning*, MEDIUM (2017. december 4.), <https://medium.com/iot-forall/the-difference-between-artificial-intelligence-machine-learning-and-deep-learning-3aa67bff5991>.

másokkal.⁶⁶ Ezek az eszközök megkönnyítették hatalmas mennyiségű információ összegyűjtését, tárolását és elemzését.⁶⁷

A Cisco, a hálózati vállalat becslései szerint húsz év múlva 50 milliárd új, összekapcsolt "dolog" lesz, egy 2020, trillió és 2022, egy trillió 45.⁶⁸ Amint ezek a "dolgok" összegyűjtik az információinkat, az AI-alapú programok felhasználhatják ezeket az adatokat részben életünk javítására, de arra is, hogy befolyásoljanak vagy irányítsanak minket.⁶⁹ Míg az IoT minden mozdulatunkat és kívánságunkat átláthatóvá teszi az adatszolgáltató cégek számára, addig az információink gyűjtése és felhasználása számunkra átláthatatlan marad. A hatalmas információs aszimmetria jelentős hatalmi egyenlőtlenségeket teremt, amelyeknek a fő áldozata az előjog.

2. A felügyeleti ökoszisztéma

Nem a "dolgok" az egyetlen adatrögzítő eszközök, amelyekkel találkozunk. Fizikai és online megfigyelőrendszerek is kísérik őket. Az ilyen rendszerek mindenütt jelenléte miatt ártalmatlannak vagy legalábbis ismerősnek tűnnek. Gondoljunk csak az olyan üzenetküldő platformokra, mint a Microsoft Skype, a Tencent WeChat vagy a Facebook WhatsApp és Messenger. Ezekért az ingyenes vagy olcsó szolgáltatásokért az adataival fizet.⁷⁰ Gondoljon a kommunikációs rendszerekre is: e-mail, szöveges üzenetküldés, telefon, mobiltelefon és IP-hangtelefon. Ahogy a régi vicc mondja, a telefonodon ma már 3 irányú hívás van: te, a hívott személy és a kormány. Ha hozzávesszük a kommunikációs szolgáltatókat, amelyek kiszimatolják az üzeneteinket, naplózzák a metaadatainkat és nyomon követik a tevékenységeinket, akkor a probléma nagyságrendje világossá válik.

A vizuális módszerek is rögzítik a személyes adatokat, többek között olyan fejlett technológiák segítségével, mint a légi és műholdas megfigyelés, drónok,

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ Vala Afshar, *Cisco*: HUFFINGTON POST (2017. augusztus 28.), https://www.huffingtonpost.com/en-try/cisco-enterprises-are-leading-the-internet-of-things_us_59a41fcee4b0a62d0987b0c6.

⁶⁹ *Lásd* Helbing, *Supra* note 6.

⁷⁰ *Lásd* Samuel Gibbs *How Much Are You Worth to Facebook*, GUARDIAN (2016. január 28.), <https://www.theguardian.com/technology/2016/jan/28/how-much-are-you-worth-to-facebook>.

rendszámtábla-olvasók, utcai kamerák, biztonsági kamerák, infravörös kamerák és egyéb távoli és fokozott képalkotó eszközök.⁷¹ A Google "Sidewalk Labs" egy "intelligens várost" épít, amely a gyalogosok és a járművek tevékenységének "mindenütt jelenlévő érzékelését" használja.⁷²

Az interneten nincs magánélet. Íme néhány ok, amiért. A felhasználó merevlemezén titokban elhelyezett kis fájlok, a "sütik" nyomon követik a felhasználó mozgását az interneten, és továbbítják ezeket az információkat a szervereknek.⁷³ A "spotlight hirdetések", "webjelzők" és "pixelcímkék" által gyűjtött felhasználói adatok a következők lehetnek: az egyes oldalakon eltöltött idő mennyisége, aktivitás, lapozgatás, hivatkozó weboldal, eszköztípus és személyazonosság. Bár a felhasználók a böngészőjükben a "Ne kövess" (Do Not Track, DNT) beállításra hivatkozhatnak, a weboldalnak nem kötelező tiszteletben tartaniuk a DNT-kéréseket, így a legtöbbjük figyelmen kívül hagyja azokat.⁷⁴ A felhasználók megpróbálhatnak más, az adatvédelmet fokozó módszereket is alkalmazni, beleértve a virtuális magánhálózatokat, a végponttól végpontig terjedő titkosítást és a hirdetésblokkolókat, de ezek a módszerek nem mindig járnak sikerrel.

A közösségi média és más "ingyenes" online szolgáltatások üzleti modellje az adatok és tartalmak "pénzzé tételének" képességétől függ.⁷⁵ Végző soron az a feladat, amelybe ezeknek a vállalatoknak bele kell vágniuk ahhoz, hogy létezzenek, az a felhasználói profilokra, preferenciákra és viselkedésre vonatkozó meglátások és előrejelzések megtalálása. Ezek a vállalatok aztán eladják és megosztják az adatokat különböző célokra (pl. reklámcélzásra és választási manipulációra). Ez a megfigyelés egy formája. És mivel ezt nem a közbiztonság, hanem a profitszerzés érdekében teszik, "megfigyelési kapitalizmusnak" nevezik.

⁷¹ Robert Draper, *They Are Watching You - and Everything Else on the Planet*, NAT'L GEOGRAPHIC (2017. december), <https://www.nationalgeographic.com/magazine/2018/02/surveillance-watching-you>.

⁷² Sidney Fussell, *The City of the Future Is a Data-Collection Machine*, ATLANTIC (Nov. 201821.), <https://www.theatlantic.com/technology/archive/2018/11/google-sidewalk-labs/575551>.

⁷³ Joanna Geary, *A nyomkövetők nyomában: Mi az a Cookie? An Introduction to Web Tracking*, GUARDIAN (2012. április 23.), <https://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro>.

⁷⁴ *Lásd általában* Jon Brodtkin, *Websites Can Keep Ignoring "Do Not Track" Requests After FCC Ruling*, ARS TECHNICA (2015. november 6.), <https://arstechnica.com/information-technology/2015/11/fcc-wont-force-websites-to-honor-do-not-track-requests>.

⁷⁵ Az adatpiac becslések szerint 150-200 milliárd dollárt tesz ki évente.

Ez egy olyan ökoszisztéma, amelyet inkább az adatok kinyerése, mint az áruk előállítása táplál.⁷⁶

A nagy technológiai vállalatok piaci kapitalizációja megmutatja, hogy mennyit érnek számukra a felhasználók és az adataik. Augusztusban az Apple 2018, 1 billió dollárt,⁷⁷ az Amazon 890 milliárd dollárt, az Alphabet (a Google anyavállalata) 861 milliárd dollárt, a Facebook pedig 513 milliárd dollárt ért. A FAANG-óriások (Facebook, Amazon, Apple, Netflix és Google) együttesen 3,5 billió dollár nettó vagyonnal rendelkeznek, ami nagyjából megegyezik a világ negyedik legnagyobb gazdaságának, Németországnak a GDP-jével.⁷⁸ Mivel a mi adatainkból profitálnak, a rövidítés találó.

Júliusban a Facebook 2018, részvényeinek árfolyama 20%-kal esett, több mint 100 milliárd dollárnyi tőkésített értéket veszítve, ami a tőzsde történetének legnagyobb egynapos esése.⁷⁹ Sok elemző ezt a zuhanást a Facebook új európai adatvédelmi szabályok bevezetésének és a felhasználói adatok értékesítésének visszavételének tulajdonítja.⁸⁰ A következő napon a Twitter árfolyama ugyanezen okból szintén 20%-kal esett.⁸¹ Ezek az események azt mutatják, hogy a nagyobb adatvédelmi védelem bizonyos esetekben árthat a vállalatok részvényárfolyamának.

A magáninformációk gyűjtésének illegális eszközei még hatékonyabbak, mint a legálisak. Ezek közé tartozik a vírusokkal, férgekkel, trójai falovakkal, billentyűleütések naplózásával, brute-force hackeléssel és egyéb támadásokkal történő számítógépes behatolás.⁸² Míg a mesterséges intelligenciát gyakran alkalmazzák az adatok biztonságossá tételére,

⁷⁶ Shoshana Zuboff, *A Google mint szerencselovag, A megfigyelési kapacitás titkai*, PUB. PURPOSE (2016. március 5.), <https://publicpurpose.com.au/wp-content/uploads/2016/04/Surveillance-capitalism-Shuboff-March-2016.pdf>.

⁷⁷ A tőzsdén jegyzett vállalatok piaci kapitalizációja számos pénzügyi oldalon, például a <https://ycharts.com/companies> oldalon található.

⁷⁸ *Lásd pl.* <https://www.investopedia.com/insights/worlds-top-economies>.

⁷⁹ Akane Otani és Deepa Seetharaman, *Facebook Suffers Worst-Ever Drop in Market Value*, WALL ST. J. (2018. július 26.), <https://www.wsj.com/articles/facebook-shares-tumble-at-open-1532612135>.

⁸⁰ *Lásd* Emily Stewart, *The \$120-Billion Reason We Can't Expect Facebook To Police Itself*, VOX (2018. július 28.), <https://www.vox.com/business-and-finance/2018/7/28/17625218/facebook-stock-price-twitter-earnings>.

⁸¹ *Id.*

⁸² *Lásd: Cyber Threat Basics, Types of Threats, Intelligence & Best Practices*, SECUREWORKS (2017. május 12.), <https://www.secureworks.com/blog/cyber-threat-basics>.

gyakrabban segít a hackereknek átjutni a védelmen.⁸³ A mesterséges intelligencia az IoT és a megfigyelőrendszerek által gyűjtött nyers adatokat is értelmes intelligenciává alakítja, amelyet az adatszolgáltató vállalatok jogi vagy kártékony célokra használhatnak fel.⁸⁴

3. Kormányzati felügyelet

A szövetségi kormány elsajátította a mindenütt jelenlévő megfigyelés művészetét, részben legális, részben illegális módon. Ahelyett, hogy áttekintjük a megfigyelés számtalan típusát és az azokat támogató vagy elutasító legfelsőbb bírósági eseteket, itt csak azokat a formákat és doktrínákat tárgyaljuk, amelyek hozzájárulnak a mesterséges intelligencia által a magánélethez fűződő érdekek csorbításához. A harmadik fél doktrínával kezdjük, amely lényegében azt állítja, hogy a negyedik módosítás nem alkalmazható, ha a kormány egy alanyról közvetve, egy "harmadik féltől" szerez adatokat, nem pedig közvetlenül a célszemélytől.⁸⁵ A klasszikus eset a közmondásos börtöninformátor, aki, miután információt szerzett egy gyanúsítottól, ezt az információt szabadon átadhatja az ügyésznek a vádlott tiltakozása ellenére. De a doktrína ennél tovább megy. Bárki, aki egyébként védett információkat közöl egy harmadik féllel, talán "helytelenül bízik" az adott személyben, és elveszíti a magánélethez való jogát.

A helytelen bizalom és a harmadik fél doktrína azt jelenti, hogy a kormányzat - törvényi vagy szokásjogi korlátozások hiányában - bárkitől, aki rendelkezik az Önre vonatkozó információkkal, hozzájuthat azokhoz.⁸⁶ A harmadik felek és az általuk birtokolt adatok közé tartozik minden, ami utazási társaságok és GPS-sel ellátott alkalmazások (mint például a Waze és a Google Maps), amelyek utazási előzményeket és kereséseket gyűjtenek, valamint pénzügyi szolgáltató szervezetek (mint például a Magyar Nemzeti Bank).

⁸³ Olivia Beavers, *Security Firm Predicts Hackers Will Increasingly Use AI to Help Evade Detection in 2019*, HILL (2018. november 29.), <https://thehill.com/pol-icy/cybersecurity/418972-security-firm-predicts-hackers-will-increasingly-use-ai-to-help-evade>.

⁸⁴ *Lásd* McClelland, *Supra* note 65.

⁸⁵ *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) ("[A] személynek nincs jogos elvárása a magánélet védelmére azokkal az információkkal kapcsolatban, amelyeket önként átad harmadik félnek").

⁸⁶ Ha a harmadik fél egy másik állami szereplő, aki a negyedik kiegészítés megadott információhoz, akkor annak végső felhasználása szintén megengedhetetlen.

bankok és hitelintézetek), amelyek rendelkeznek az ügyfelek pénzügyi információival, az egészségügyi szolgáltatókig és biztosítókig, amelyek rendelkeznek a páciensek orvosi nyilvántartásával.

Valójában kevés olyan információ van, amelyhez valamilyen harmadik fél nem rendelkezik vagy nem férhet hozzá. Vannak szövetségi törvényi rendelkezések, mint például az Egészségbiztosítási hordozhatósági és elszámoltathatósági törvény (HIPAA),⁸⁷ az elektronikus hírközlési adatvédelmi törvény (ECPA)⁸⁸ és a tisztességes hitelinformációs törvény (FCRA).⁸⁹ Ezek azonban a szervezeteknek csak kis hányadára terjednek ki. A legtöbb más szervezet adatvédelmi kötelezettségei vagy szerződésből (használati feltételek), állami jogból vagy szokásjogi bizalmi kapcsolatból erednek. E szabályok többsége kivételt képez a bűnüldözési vagy bírósági adatigénylések esetében.

4. Anonimitás

Míg az információs adatvédelem arra irányul, hogy tevékenységünket elrejtjük mások elől, addig az anonimitás lehetővé teszi, hogy felfedjük tevékenységünket, de elrejtjük személyazonosságunkat. Lehetővé teszi a közzétételét, amit elkerülhetnénk, ha a társulások ismertek lennének.⁹⁰ *A McIntyre kontra Ohio Elections Commission* ügyben a Legfelsőbb Bíróság kimondta: "Az anonimitás pajzs a többség zsarnokságával szemben. . . Ez tehát a Bill of Rights, és különösen az Első Alkotmánykiegészítés mögött álló célt emeli ki: a népszerűtlen egyének védelmét az intoleráns társadalom által történő megtorlástól..."⁹¹

A New Yorker egyik híres karikatúrája egy kutyát ábrázol, aki az interneten böngészik, és azt mondja egy kutyatársának: "Az interneten senki sem tudja

⁸⁷ 42 U.S.C. 201. A legtöbb HIPAA-követelményt az Egészségügyi és Emberi Szolgáltatások Minisztériuma rendeletben hirdette ki. Lásd CFR45 et160.100, seq.

⁸⁸ 18 U.S.C. 2510, et seq. Az ECPA az átmeneti kommunikációra (I. cím), a tárolt kommunikációra (II. cím) és a címzési információkra (III. cím) vonatkozik. Az ECPA hatálya alá tartoznak az állami és magánszervezetek.

⁸⁹ 15 U.S.C. et1681, seq.

⁹⁰ Bradley Smith, *What Hamilton Teaches Us About the Importance of Anonymous Speech*, WASH. POST (2016. november 8.), https://www.washingtonpost.com/opinions/what-hamilton-teaches-us-about-the-importance-of-anonymous-speech/2016/11/08/dd17ae3c-a53d-11e6-8fc0-7be8f848c492_story.html.

⁹¹ 514 U.S. (334,1995357).

te egy kutya vagy."⁹² Ez igaz lehetett a mesterséges intelligencia előtt, amikor az IP-címek és más adatok keresztivatkozása nehézkes volt. Most azonban a dolgok nem ilyen egyszerűek.

Az anonimizálás az a folyamat, amelynek során az összegyűjtött adatokból eltávolítják a személyazonosításra alkalmas adatokat, így az eredeti forrás nem azonosítható.⁹³ A kapcsolódó folyamat, az álnevesítés, a legtöbb azonosító adatelemet mesterséges azonosítókkal vagy álnevekkel helyettesíti.⁹⁴ Ez olyan technikákat tartalmaz, mint a hashing, az adatmaszkírozás vagy a titkosítás, amelyek csökkentik az adathalmazok hasonlóságát az egyén azonosító in- formációjával.⁹⁵ A jelenlegi jogi megkülönböztetés szerint az álnevesített adatok újra azonosíthatók (pl. az egyén újra összekapcsolása az információival).⁹⁶ A jog azonban nem veszi figyelembe a mesterséges intelligencia azon képességét, hogy az anonimizált adatokat újraazonosítsa.⁹⁷

A mesterséges intelligencia kiválóan alkalmas az adatok újraazonosítására (vagy azonosítatlan adatok eltávolítására) azáltal, hogy látszólag nem kapcsolódó adatokból újbóli kapcsolatokat von ki. A University of Melbourne tanulmánya képes volt újra azonosítani néhány ausztrál beteget, akiket az állítólagos anonim orvosi számlázási feljegyzéseken keresztül vizsgáltak meg.⁹⁸ Hasonló eredmények állnak rendelkezésre a hitelkártya metaadatokkal kapcsolatban is.⁹⁹ Af-

⁹² Peter Steiner, *The New Yorker*, július 5, 1993.

⁹³ Lásd https://en.wikipedia.org/wiki/Data_anonymization.

⁹⁴ Clyde Williamson, *Pseudonymization vs. Anonymization and How They Help With GDPR*, PROTEGRITY (2017. január 5.),

<https://www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr>.

⁹⁵ Id.

⁹⁶ *Adatmaszkírozás: Anonimizálás vagy álnévtelenítés?*, GDPR REPORT (2017. szeptember 28.), <https://gdpr.report/news/2017/09/28/data-masking-anonymization-álnevesítés>.

⁹⁷ Boris Lubarsky, *Re-Identification of "Anonymized Data"*, GEO1. L. TECH. REV. 202, 208-11 (2017).

⁹⁸ Lásd Cameron Abbott et al., *De-identification of Data and Privacy*, K&L GATES (2018. február 26.), <http://www.klgates.com/de-identification-of-data-and-privacy-02-26-2018>. Lásd még Liangyuan Na et al., *Feasibility Of Reidentifying Individuals In Large National Physical Activity Data Sets From Which Protected Health Information Has Been Remove With Use Of Machine Learning*, JAMA NETWORK OPEN (2018. dec. 21.), <https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2719130> (95%-os újraazonosítási pontosság az okosórákból, okostelefonokból és fitnesskövetőkből gyűjtött adatok alapján).

⁹⁹ Yves-Alexandre de Montjoye et al., *Egyedülálló a bevásárlóközpontban: On the Reidentifiability of Credit Card Metadata*, SCI347. 536 (201530, jan.),

ter a teljes 2014-es New York-i taxis adatállományt nyilvánosságra hozták, egy újrakereső képes volt azonosítani a taxiba beszálló hírességeket, a "felszállás helyét, a leszállás helyét, a kifizetett összeget, sőt még a borraivaló összegét is".¹⁰⁰

Így a mesterséges intelligencia esetében a névtelenség fogalma a közszférában a legjobb esetben is csak illúzió, a szabályozás azonban továbbra is ezen illúzió alapján működik. Az "anonimitás eróziója" miatt az Elnök Tudományos és Technológiai Tanácsadói Tanácsa 2014-ben a magánélet védelmének átfogó újraértékelésére szólított fel.¹⁰¹ Ez még nem történt meg. A technikai változások kezelését célzó sürgős szabályozás hiánya és a magánélet védelmének hiánya a megbízható demokratikus jogi keretek leépüléséről tanúskodik.

C. Döntési magánélet (autonómia)

Az autonómia a görög *autos* (én) és *nomos* (szabály) szavakból ered. A görögök által használt kifejezés politikai autonómiát jelentett.¹⁰² A demokráciában betöltött központi szerepe azonban ma már az autonómia más aspektusaira is kiterjed, beleértve az önmagunkkal és életpályánkkal kapcsolatos döntések meghozatalának jogát, amit mi "döntési magánéletnek" nevezünk.¹⁰³ Mai értelmezésben az autonómia "különböző fogalmak összességére utal, beleértve az öngazgatást, a szabadságjogokat, a magánéletet, az egyéni választást, a saját akarat követésének szabadságát, a saját viselkedés okozását, és a saját magunknak való

<http://science.sciencemag.org/content/347/6221/536> ("még azok az adatkészletek is, amelyek bármelyik vagy valamennyi dimenzióban durva információkat szolgáltatnak, kevés anonimitást biztosítanak, és a nők a hitelkártya-metaadatokban jobban azonosíthatók, mint a férfiak").

¹⁰⁰ Boris Lubarsky, *Re-Identification of "Anonymized" Data*, GEO1. L. TECH. REV. 202,211 (2017).

¹⁰¹ Elnöki Tudományos és Technológiai Tanácsadói Tanács, *Jelentés az elnöknek Big Data and Privacy: A Technological Perspective*, PCAST (2014), május), 22, https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf.

¹⁰² *Autonomy*, MERRIAM-WEBSTER DICTIONARY ONLINE, <https://www.merriam-webster.com/dictionary/autonomy> (utolsó látogatás 2019.22.,. április).

¹⁰³ *Lásd pl.* Griswold kontra Connecticut, 381 U.S. 479 (1965) (a magánélethez való jogot "más alkotmányos védelmek "penumbraiban" és "kisugárzásaiban" találta meg.).

személy."¹⁰⁴ Az autonómia nagymértékben összefügg a szabad akaratral, és alapvető fontosságú az emberi méltóság és az egyéniség szempontjából.

Mindebből az következik, hogy az autonómia *kvázi a* választás szabadsága fontos mind az emberi fejlődés, mind a jog szempontjából. Azok, akik azt remélik, hogy befolyásolni tudják mások cselekedeteit (nevezzük őket "befolyásolóknak"), gyakran túl közel lépnek a meggyőzést a kényszerítéstől elválasztó határvonalhoz.

1. A szabad akarat felforgatása - Online viselkedésalapú reklámok

A reklámpia szakértője az emberek szokásainak és döntéseinek befolyásolásában. A Madison Avenue azóta gyakorolja a meggyőzés művészetét, amióta csak léteznek a hirdetőik által támogatott média. A hagyományos reklámok zavaróak lehetnek, de ritkán vetik fel az itt tárgyalt aggályokat. A digitális korszakban azonban megjelent a befolyásolás egy különleges típusa, az "online viselkedéses reklám". Itt a harmadik fél reklámtechnológiai vállalatai mesterséges intelligenciát használnak a ~~hirdetők~~ testreszabására, hogy azok bizonyos felhasználókat célozzanak meg bizonyos kontextusokban.¹⁰⁵ A harmadik felek a közzétett weboldal vagy alkalmazás és a weboldalon hirdetési helyet vásárló hirdető között helyezkednek el. Ezeknek a harmadik feleknek hatalmas mennyiségű adata van szükségük ahhoz, hogy ez a technika működjön. A vállalatok nem csupán személyes adatokat használnak fel magánjellegű előnyök érdekében, hanem ezt titokban teszik. Bár ezt látszólag azért teszik, hogy "tájékoztatassák" a döntéseinket, könnyen válhat finom, de hatékony manipulációvá. Ha ez bekövetkezik, a viselkedésalapú reklámozás veszélyezteti a döntési és információs magánéletet, és aláássa a szabad akarat, az egyenlőség és a méltányosság demokratikus alapelveit.

Az online viselkedéses reklám és marketing előnyökkel és költségekkel is jár. A pozitív oldalon a fogyasztók keresési költségeit és az eladók elhelyezési költségeit csökkentheti. Emellett az "internetes" gazdaság gerincét is jelenti, mivel a reklámbevételek olyan szolgáltatásokat támogatnak, amelyek egyébként nem lennének ingyenesek. A viselkedésalapú reklámnak azonban hátrányai is vannak. Először is, a rendszer működéséhez személyes adatokat kell gyűjteni. A magánélet ebből eredő sérülését fentebb már megvizsgáltuk. Másodszor, és ami még károsabb, az a fogyasztók akut manipulálásának lehetősége.

¹⁰⁴ TOM L. BEAUCHAMP & JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS 67-68 (1989).

¹⁰⁵ *Lásd általában* Steven C. Bennett, *Regulating Online Behavioral Advertising*, 44. MARSHALL L. REV. 899 (2011).

választás. Ahogy a rólunk szóló információk egyre részletesebbé és teljesebbé válnak, a viselkedéses reklámok olyan pszichológiai "kívánságokat" hozhatnak létre, amelyek kognitív választásoknak álcázzák magukat. A felhasználók egyetlen védekezési mechanizmusa az opt-out, abban a téves hitben, hogy ezzel megakadályozható az adataik felhasználása vagy gyűjtése.¹⁰⁶ A befolyásolás kontinuum a meggyőzéstől a manipuláción át a kényszerítésig terjed. A filozófusok és az autonómia-elméleti szakemberek vitatják, hol húzódnak a határok, de a legtöbben egyetértenek abban, hogy a befolyásolás átcsaphat kényszerítésbe.¹⁰⁷

A Szövetségi Kereskedelmi Bizottság (FTC) "elveket" és iránymutatásokat adott ki, de nem hozott kötelező érvényű szabályozást az online viselkedésalapú reklámok használatára vonatkozóan.¹⁰⁸ Többnyire nem foglalkozik a kérdéssel, kivéve a tisztességtelen vagy megtévesztő üzleti gyakorlatot folytató vállalatok szélsőséges eseteit.¹⁰⁹ Bár a kongresszus is tartott meghallgatásokat,¹¹⁰ szintén nem szabályozta ezeket a gyakorlatokat. Néhány állam megpróbálta betölteni ezt az űrt, de az ilyen törvények hatása és ~~aktív~~ megkérdőjelezhető, tekintettel az internet határok nélküli jellegére. Így marad az iparági önszabályozás, ami gyakran kevés vagy egyáltalán nem jelent korlátozást.

2. Fogyasztói belenyugvás

Az adatgyűjtési és -felhasználási gyakorlatok nagy része széles körben ismert a technológia szerelmesei számára, mégis a fogyasztók beleegyezése és a szabályozó hatóságok elnézése miatt továbbra is fennáll. Manapság az emberek sokkal több információt adnak ki harmadik feleknek, mint korábban. Egyesek a magánéletet feláldozzák a

¹⁰⁶ Bár a leiratkozás csökkentheti a személyre szabott hirdetéseket, nem akadályozza meg a hirdetőket az általános hirdetési, adatgyűjtési, -felhasználási, -megosztási és -megőrzési gyakorlatokban. ¹⁰⁷ Lásd Trent J. Thornley, *The Caring Influence: Beyond Autonomy as the Foundation of Undue Influence*, 71 L.J. (513,1996524).

¹⁰⁸ Lásd pl. FTC, *Self-Regulatory Principles for Online Behavioral Advertising*, FTC Online Tracking Guidance (2016), www.ftc.gov/os/2009/02/P085400behavioralreport.pdf.

¹⁰⁹ Lásd: Federal Trade Commission Act, U15.S.C. §§ Az 45.FTC a törvény által védett információk, például orvosi és pénzügyi információk gyűjtését is ellenőrzi.

¹¹⁰ *Viselkedésalapú reklám: Az iparági gyakorlatok és a fogyasztók elvárásai: Comms. On Commerce, Trade, and Consumer Protection and on Communications, Technology, and the Internet*, 111th Cong. (2009); *Privacy Implications of Online Advertising: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 110th Cong. (2008).

érdeemes kényelem, vagy egyszerűen csak elfogadják ezt a "jogfosztottsági csökkenést elkerülhetetlennek".¹¹¹ Végül is az emberek ingyen vagy kényelmesen jutnak szolgáltatásokhoz, csökkentett keresési és tranzakciós költségekhez, és egyébként is hasznot húznak a fejlett technológiából és a tárgyak internetéből. Sotomayor bírónő azonban a *Jones-ügyben* adott egybehangzó véleményében arra utalt, hogy komolyan kétli, hogy az emberek ezt elkerülhetetlennek fogadják el.¹¹² Az előnyök, amelyekhez az ember hozzájut, nem ingyenesek vagy olcsóak. Az emberek a személyes adataikkal fizetnek. Az észak-amerikai felhasználók fejeként több mint 1000 dollárt érnek a Facebooknak.¹¹³ A Google minden egyes "ingyenes" keresésből profitál, amit a platformján végeznek.

Az online nyomon követésből és adatgyűjtésből eredő magánélet megsértésének növekvő fogyasztói tudatossága - különösen a Cambridge Analytica-botrány után - "háborzongató tényezőt" hozott létre az internet és a csatlakoztatott eszközök használatában. Az IBM végzett egy felmérést, amely szerint az Egyesült Államokban a fogyasztók százaléka 78 úgy véli, hogy egy technológiai vállalatnak "rendkívül fontos", hogy képes-e megvédeni az adatait.¹¹⁴ A fogyasztóknak azonban csak 20 százaléka "bíz meg teljesen" a vállalatokban, hogy megvédik a róluk szóló adatokat.¹¹⁵ Egy másik, a Blue Fountain Media által végzett felmérésben a résztvevők 90 százaléka nagyon aggódott az internetes adatvédelem miatt,¹¹⁶ ugyanakkor százalékuk 60 boldogan töltött le alkalmazásokat anélkül, hogy elolvasta volna a felhasználási feltételeket.¹¹⁷

Ezek a felmérések azt mutatják, hogy a fogyasztók törődnek az adatvédelemmel, de nem érzik, hogy képesek lennének az adataik feletti ellenőrzést átvenni, vagy úgy gondolják, hogy rendelkeznek a

¹¹¹ United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

¹¹² *Id.*

¹¹³ A Facebook bevétele 2016-ban 13,54 dollár volt negyedévente és felhasználónként, vagy 54,16 dollár évente. Ez 3%-os kapitalizációs rátával számolva 1805 dollárnak felel meg. *Lásd* Gibbs, 70. lábjegyzet; PCAST, 101. lábjegyzet. Hasonlóképpen, a felhasználók "évente átlagosan több mint 1000 dollár értéket származtatnak a Facebookból" és más kommunikációs technológiákból. Jay R. Corrigan, et al, *How Much Is Social Media Worth? Estimating The Value Of Facebook By Paying Users To Stop Using It*, <https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0207101>.

¹¹⁴ IBM, *New Survey Finds Deep Consumer Anxiety over Data Privacy and Security*, PR NEWSWIRE (Apr. 16, 2018 12:01 PM), <https://www.prnewswire.com/news-releases/new-survey-finds-deep-consumer-anxiety-over-data-privacy-and-security-300630067.html>.

¹¹⁵ *Id.*

¹¹⁶ Ian Barker, *Consumers' Privacy Concerns Not Backed by Their Actions*, BETANEWS (2018. június), <https://betanews.com/2018/05/31/consumer-privacy-aggalyok>.

¹¹⁷ *Id.*

a magánélet védelmének érvényesítésére vonatkozó jogok. Ezek a meggyőződések nem tévesek. A legtöbb, ha nem az összes technológiai vállalat nem tárgyal a felhasználási feltételekről vagy adatvédelmi irányelvekről azokkal a fogyasztókkal, akik nem értenek egyet velük; inkább ha nem ért egyet az adatgyűjtéssel és -felhasználással, akkor nem használhatja a szolgáltatást.

Mindaddig, amíg hatalmas erők igyekeznek ellenőrizni azt, aminek autonóm döntéseknek kellene lennie, a magánélet védelme tovább fog erodálódni. A mesterséges intelligencia lehetőségeket és képességeket teremt az emberi autonómia további erodálására. A "felügyeleti kapitalizmus" sikereire építve manipulálja a fogyasztásunkat és életvezetési döntéseinket. A következő részben azt tárgyaljuk, hogy a politikai szereplők hogyan alkalmazzák a mesterséges intelligenciát és a viselkedési reklám technikáit a választók manipulálására és a választások befolyásolására.

III. A VÁLASZTÁSOKAT ÉS A DEMOKRATIKUS INTÉZMÉNYEKET FENYEGETŐ VESZÉLYEK

A modern demokráciák az olyan alapelvek iránti elkötelezettséget képviselik, mint a politikai vita, a polgári jogok, a tisztességes eljárás, az egyenlőség, a gazdasági szabadság és a jogállamiság. A mesterséges intelligencia több szempontból is megkérdőjelezi ezeket az alapelveket. Az első és legfontosabb a "fegyverként használt mesterséges intelligencia" alkalmazása a demokrata választások megzavarására és korrumpálására. Ez történhet fizikai eszközökkel, például kibertámadásokkal, és pszichológiai eszközökkel, az emberek választási folyamatba vetett hitének megmérgezésével. Másodszor, a rosszindulatú szereplők a szabad sajtó és a civil társadalom szerveinek aláásásával gyengíthetik a demokratikus intézményeket. A harmadik és bizonyos értelemben a legártalmasabb hatása a mesterséges intelligenciának az egyenlőség, a tisztességes eljárás és a gazdasági szabadság alapvető értékeinkre gyakorolt hatása. Itt nem kell indítékot tulajdonítani. A mesterséges intelligencia pusztán szerkezeténél fogva ellenáll a demokrácia három fő jellemzőjének: az átláthatóságnak, az elszámoltathatóságnak és a méltányosságnak. Tévesen bízunk a gépek vélt "semlegességében" és kompetenciájában, holott azok valójában felerősíthetik az emberi elfogultságokat és hibákat.

Ebben a szakaszban bemutatjuk, hogy a mesterséges intelligencia milyen veszélyeket jelent az alapvető demokratikus értékekre és intézményekre, valamint magára a demokráciára nézve.

A. Önkormányzatiság és politikai részvétel

A szabad és nyílt választások az amerikai demokrácia alapkövei. De ahogy a közelmúlt eseményei fájdalmasan világossá tették, a választások lehetnek

meghekkelték. Ez alatt nem csak olyan kibertámadásokat értünk, ahol a sebezhető szavazórendszerekbe "rosszindulatú külföldi szereplők" hatolnak be.¹¹⁸ bár ez bizonyára előfordul, és továbbra is komoly fenyegetést jelent.¹¹⁹ Inkább a tisztességes és szabad választások felforgatására vagy megterhelésére irányuló erőfeszítések teljes skáláját értjük ez alatt. A mesterséges intelligencia egyaránt hozzájárulhat a szavazás torzítására irányuló, már létező eszközök hatékonyságához, például azáltal, hogy megkönnyíti a szavazóközrtek megrajzolását,¹²⁰ és új lehetőségeket is teremthet a választásokba való beavatkozásra.

A választási folyamatot fenyegető kiberfenyegetések több különböző fajtáját ismertetjük. Az első a hagyományos típusú kibertámadások, amikor a támadók hozzáférnek a számítógépes rendszerekhez, és ellopják vagy megrongálják a bizalmas választási információkat. A hackertámadások második és erőteljesebb formája a választói attitűdök manipulálása fegyverként alkalmazott "mikrocélzott" propagandával. Az alkalmazott technikák hasonlóak a fentebb tárgyalt fogyasztói döntések eltérítéséhez.¹²¹ A következőkben az álhíreket tárgyaljuk, amelyek a választói manipuláció egyik fontos és hatékony összetevője. Végül bemutatjuk, hogy az antidemokratikus erők hogyan igyekeznek kételyt kelteni a megbízható intézményekben, hogy a szavazókat szélsőséges nézetek elfogadására kondicionálják. Mindegyik módszer esetében a mesterséges intelligencia felhasználható mind a hatékonyság növelésére, mind pedig a választók elnyomásának és manipulációjának céljai és módszerei elfedésére.

1. A szavazás feltörése - A választásokat fenyegető kiberfenyegetések

Ma már vitathatatlan, hogy az orosz hírszerzés ügynökei beavatkoztak a 2016-os amerikai választásokba, és továbbra is célba veszik az amerikai választási rendszereket.¹²² Megpróbáltak behatolni a választási szoftverekbe

¹¹⁸ Eric Geller, *Despite Trump's Assurances, States Struggling to Protect 2020 Election*, POLITICO (2018. július), <https://www.politico.com/story/2018/07/27/trump-election-security-2020-states-714777>.

¹¹⁹ Lásd Andrew Gumbel, *Why US Elections Remain "Dangerously Vulnerable" to Cyberattacks*, GUARDIAN (2018. augusztus 13.), <https://www.theguardian.com/us-news/2018/aug/13/us-election-cybersecurity-hacking-voting>.

¹²⁰ Daniel Oberhaus, *Algorithms Supercharged Gerrymandering. We Should Use Them to Fix it*, VICE (2017. október 3.), https://motherboard.vice.com/en_us/article/7xkmag/gerrymandering-algorithms.

¹²¹ Lásd fentebb a III.C. szakaszt.

¹²² Miközben ez a cikk a végső szerkesztés alatt állt, az Igazságügyi Minisztérium kiadta Robert Mueller különleges ügyésznek az *elnökválasztásba 2016 való orosz beavatkozással kapcsolatos vizsgálatról szóló*

jelentését, vagy "Mueller Re-

és berendezéseket legalább huszonegy államban, kibertámadásokat indított egy szavazási szoftvercég ellen, feltörte száz helyi választási tisztviselő e-mailjeit,¹²³ és legalább egy kampányfinanszírozási adatbázishoz is hozzáfért.¹²⁴ Azonban elsősorban a kiberműveletek során szerzett adatok kiszivároztatására támaszkodtak, beleértve a Demokratikus Nemzeti Bizottság szerveibe és a Clinton-kampány elnökének, John Podestának az e-mail fiókjába való behatolást.¹²⁵

Az Obama-kormányzat annyira aggódott a 2016-os választások idején az orosz hackertámadások miatt, hogy kidolgozott egy vészhelyzeti tervet, amelynek értelmében "fegyveres szövetségi rendfenntartó erőket küldött a szavazóhelyiségekbe, a hadsereg egyes részeit mobilizálta, és ellen-propaganda-tevékenységeket indított".¹²⁶ "A terv azt tükrözi, hogy milyen alaposan sikerült az orosz effort az amerikai választási rendszerbe vetett közbizalom aláadására".¹²⁷ A Gallup közvélemény-kutatása is ezt támasztotta alá. "Az amerikaiak rekordalacsony, 30%-a fejezte ki bizalmát a választások becsületességében".¹²⁸

port"). Lásd Robert S. Mueller, III, *Report on the Investigation Into Russian Interference in the 2016 Presidential Election* (2019. március), <https://www.justice.gov/storage/report.pdf>. A kereshető változat elérhető a *Read the Muller Report*, N.Y. TIMES (2019. április 18.), <https://www.nytimes.com/interactive/2019/04/18/us/politics/mueller-report-document.html>. A jelentés megerősíti a választásokba való orosz beavatkozással kapcsolatban korábban tett számos megállapítást. *Id.* 14-50. o. Lásd még Nat'l Intelligence Council, *Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections*, január 6.,

2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

¹²³ Lásd *pl.* Mueller Report, *Supra*, 122. lábjegyzet, 51. pont (a floridai választási tisztviselőkre irányuló spearphishing támadás leírása).

¹²⁴ *A 2018-as pénzügyi évre vonatkozó nemzetvédelmi felhatalmazásról szóló törvény: H.R. meghallgatása 5515*, 115th Cong. (2017) (Klobuchar szenátor megjegyzései); *Bolstering the Government's Cybersecurity: A Wannacry tanulságai: Joint Hearing Before the H. Comm. on Oversight and on Research and Technology*, 115th Cong. (2017), <https://www.govinfo.gov/content/pkg/CHRG-115hhrg26234/pdf/CHRG-115hhrg26234.pdf>.

¹²⁵ *Id.*

¹²⁶ Massimo Calabresi, *exkluzív*: TIME (2017. július 20.), <http://time.com/4865798/russia-hacking-election-day-obama-plan>.

¹²⁷ *Id.*

¹²⁸ Gallup, *Update: Americans' Confidence in Voting, Election*, GALLUP (2016. november 1.), <https://news.gallup.com/poll/196976/update-americans-confidence-voting-election.aspx>.

A választási hackelés nem új jelenség, de a mesterséges intelligencia még inkább felerősítette. Az amerikai tisztviselők és kutatók évtizedek óta aggódnak az állami és helyi választási gépek, különösen a papíralapú nyomkövetést nem biztosító szavazóeszközök sebezhetősége miatt.¹²⁹ Ami most más, az a mesterséges intelligencia egyre szélesebb körű alkalmazása a kibertámadások javítására. Az új heurisztikák, a jobb analitika és az automatikus információ ma már kulcsfontosságú a sikeres támadásokhoz. A mesterséges intelligencia "segít a hackereknek gyorsabban megtámadni a választási rendszereket, mint ahogy a tisztviselők lépést tudnak tartani velük".¹³⁰

A kibertámadók korán alkalmazkodtak a mesterséges intelligenciához. A gépi tanulás segítségével hatalmas mennyiségű ellopott adat elemzése révén ma már tudják megcélolni az áldozatokat, és stratégiákat tudnak kidolgozni a kibervédelem legyőzésére.¹³¹ A Price Waterhouse Coopers tanácsadó cég 2018-as AI Predictions jelentésében valóban leírja "az egyik olyan munkát, ahol a mesterséges intelligencia már készen áll az ember fölényét bizonyítani [-] a hackertevékenységet".¹³² Míg a legtöbb kiberbűncselekmény pénzügyi jellegű, a kiberbetöréseket egyre gyakrabban használják kémkedésre és katonai célokra. Emellett a kibertámadásokat és rosszindulatú szoftvereket politikai, ideológiai és egyéb stratégiai célok elérésére is be lehet vetni. Ha a cél a demokrata részvétel aláásása, a mesterséges intelligencia nélkülözhetetlen eszköz.

A jó hír azonban az, hogy az AI védekezésben és támadásban is használható.¹³³ Például a védelmi minisztérium DARPA Cyber Grand Challenge versenyének győztese a mesterséges intelligencia mélytanulását használta arra, hogy

¹²⁹ Lásd: *Ellenőrzés, biztonság és papíralapú nyilvántartás nemzetünk elektronikus szavazórendszereihez: Meghallgatás a H. Comm on House Administration előtt*, 109. kong. (2006),

<https://www.govinfo.gov/content/pkg/CHRG-109hhrg31270/pdf/CHRG-109hhrg31270.pdf>. Lásd általában Eric Manpearl, *Securing U.S. Election Systems: U.S. Election Systems as Critical Infrastructure and Instituting Election Security Reforms*, 24 B.U. J. SCI. & TECH. L. (2018)168.

¹³⁰ Dan Patterson, *How AI is Creating New Threats to Election Security*, CBS NEWS (2018. november 6., 11:50), <https://www.cbsnews.com/news/how-ai-will-shape-the-future-of-election-security>.

¹³¹ Kevin Townsend, *How Machine Learning Will Help Attackers*, SECURITY WEEK (2016. november 29.), <https://www.securityweek.com/how-machine-learning-will-help-attackers>.

¹³² PWC, *AI előrejelzések 2018, a 14.*, <https://www.pwc.com/us/en/advisory-services/assets/ai-predictions-2018-report.pdf> (utolsó látogatás 2018. aug.).

¹³³ Lásd általában: *A kiberbiztonság új technológiáinak ígéretei és veszélyei: meghallgatás a Szenátus Kereskedelmi, Tudományos és Közlekedési Bizottsága előtt*, 115. kong. (2017).

a kibertámadások legyőzése.¹³⁴ A rossz hír az, hogy a kiberháború mindkét végén bevetett erőforrások aszimmetrikusak, különösen az államilag támogatott kibertámadások esetében. , Míg ellenfeleink növelik a mesterséges intelligencia kutatásának finanszírozását,¹³⁵ az Egyesült Államok csökkenti azt. Mi még a választási gépezetünket is hajlamosak vagyunk korszerűsíteni, hogy jobban ellenálljunk a kibertámadásoknak.¹³⁶ Bizonyos értelemben "egy évszázados 20th analóg rendszer vagyunk... DOS-on működünk".¹³⁷

2. Az elme feltörése - Pszichográfiai profilalkotás és más befolyásoló tényezők

A konkrét kibertámadások mellett az orosz kormány olyan befolyásolási kampányt is folytatott, amelynek célja a demokratikus intézményekbe és a választásokba vetett közbizalom aláásása volt.¹³⁸ Ez a fajta beavatkozás nagymértékben támaszkodik a mesterséges intelligencia képességekre. Például egy nappal azelőtt, hogy a Wikileaks nyilvánosságra hozta a John Podesta ellopott e-mailjeinek első részét, orosz dezinformációs ügynökök tweetekkel 18,000 üzentek az amerikai választóknak. Ezek egy rendkívül alacsony mesterséges intelligencia-művelet részei voltak, amelyben az orosz Internet Research Agency által ellenőrzött 3841 fiók vett részt, és amely több millió álhírt generált a politikai narratíva alakítása érdekében.¹³⁹ Az ilyen erőfeszítések valószínűleg

¹³⁴ Lásd: *DARPA Celebrates Cyber Grand Challenge Winners*, DEF. ADVANCED RES. PROJECTS AGENCY (2016. augusztus 5.), <https://www.darpa.mil/news-events/2016-08-05a>.

¹³⁵ PWC-jelentés, *fenti* 132, 19-20. o.

¹³⁶ Lásd Erin Kelly, *Bills To Protect U.S. Elections from Foreign Meddling Are Struggling, Senators Say*, USA TODAY (2018. június 12.), <https://www.usatoday.com/story/news/politics/2018/06/12/bills-protect-elections-foreign-meddling-struggling/694385002> (hivatkozva a kétpárti Secure Elections Act, S.2261, <https://www.congress.gov/bill/115th-congress/senate-bill/2261>).

¹³⁷ *Szankciók és pénzügyi nyomásgyakorlás: fontos nemzetbiztonsági eszközök: Külügyi Bizottság előtti meghallgatás*, 115. kong. 69 (2018) (Zarate úr és Yoho úr észrevételei). A DOS, azaz Disk Operating System, az 1980-as években az első IBM asztali számítógépek operációs rendszere volt.

¹³⁸ Lásd a Mueller-jelentést, lásd a122, *fenti* megjegyzést. 9.

¹³⁹ Lásd *United States v. Internet Research Agency, et al.*, No. 18-cr-32 (D.D.C.), <https://www.justice.gov/file/1035477/download>; Craig Timberg & Shane Harris, *Russian Operatives Blasted 18,000 Tweets Ahead of a Huge News Day During the 2016 Presidential Campaign. Tudták, hogy mi fog következni?*, WASH. POST (2018. július), <https://www.washingtonpost.com/technology/2018/07/20/russian-operatives-blasted-tweets-ahead-huge-news-day-during-presidential-campaign-did-they-know-what-what-was-coming>.

folytatni. A Nemzeti Hírszerzési Igazgató Hivatalának jelentése arra a következtetésre jut, hogy "az orosz hírszerző szolgálatok továbbra is olyan képességeket fejlesztenek, amelyek Putyin számára lehetőségeket biztosítanak" a ~~politikai~~ választásokba való beavatkozásra.¹⁴⁰ A Világgazdasági Fórumon 2017 augusztusában azt mondták, hogy a mesterséges intelligencia már "csendben [átvette] a demokrácia irányítását" a viselkedésalapú hirdetések, a közösségi média manipulálása, a botok és a trollok alkalmazásával.¹⁴¹

Az adatelemzés nem minden politikai felhasználása torzítja a folyamatot. A legtöbb kampány ma már adatközpontú rendszerekre és kifinomult algoritmusokra támaszkodik a szavazók elérésében és az üzenetküldésben.¹⁴² Különbség van azonban az adatok és algoritmusok törvényes és törvénytelen felhasználása között. Az előbbi esetben az adatok felhasználása többnyire nyílt és nyomon követhető. Maga az adat nyilvános, jogszerűen szerzett és legalább részben anonimizált. Az utóbbi esetben az adatok gyakran jogtalanul szerzettek, felhasználásuk pedig titkos és úgy van kialakítva, hogy ne lehessen őket beazonosítani.¹⁴³ Emellett az adatfúzió és az analitika mélyen személyes és részletes részleteket tár fel minden egyes "adatalanyról", amelyeket aztán arra használnak fel, hogy mikrocélokra és érzelmileg befolyásolják azt, aminek megfontolt, magánjellegű és átgondolt döntésnek kellene lennie. A pszichometriai profilalkotás folyamata kvantitatív eszközöket használ a viselkedés manipulálására.¹⁴⁴ Itt a szabad akarat jelenti az akadályt, amelynek leküzdésében a mesterséges intelligencia segíthet.

¹⁴⁰ ASSESSMENT RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS, A NEMZETI HÍRSZERZÉS IGAZGATÓJÁNAK HIVATALA 5 (2017)

¹⁴¹ Vyacheslav Polonski, *How Artificial Intelligence Silently Took Over Democracy*, WORLD ECON. FORUM (2017. aug. 9.), <https://www.weforum.org/agenda/2017/08/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first>; lásd még Chris Meserole és Alina Polyakova, *The West Is Ill-Prepared for the Wave of Deep Fakes' That Artificial Intelligence Could Unleash*, BROOKINGS (2018. május 25.), <https://www.brookings.edu/blog/order-from-chaos/2018/05/25/the-west-is-ill-prepared-for-the-wave-of-deep-fakes-that-artificial-intelligence-could-unleash>.

¹⁴² Lásd Anne Applebaum, *Did Putin Share Stolen Election Data with Trump?*, WASH. POST (2018. július 20.), https://www.washingtonpost.com/opinions/global-opinions/did-putin-share-stolen-election-data-with-trump/2018/07/20/50854cc8-8c30-11e8-a345-a1bf7847b375_story.html.

¹⁴³ Emma Graham-Harrison & Carole Cadwalladr, *Cambridge Analytica Execs Boast of Role in Getting Donald Trump Elected*, GUARDIAN (2018. március 21.), <https://www.theguardian.com/uk-news/2018/mar/20/cambridge-analytica-execs-boast-of-role-in-getting-trump-elected>.

¹⁴⁴ Lásd: *Meet Cambridge Analytica: The Big Data Communications Company Responsible for Trump & Brexit*, NONE ABOVE UK (2017., február), <https://nota->

A Cambridge Analytica adattudományi cég az adatok nem megfelelő felhasználásának példaképe. Pszichográfiai profilokat készített 230 millió amerikaiáról, és a Facebookot ~~szülői~~ politikai hadviselésre használta fel.¹⁴⁵ A Cambridge Analytica társalapítója Steve Bannon, a Breitbart korábbi ügyvezető szerkesztője és Donald Trump első kabinetfőnöke volt. Természetes volt, hogy Jared Kushner felbérelte őket Trump úr digitális kampányának irányítására. A Cambridge Analytica azonban nem egy átlagos politikai tanácsadó cég volt. Alekszandr Kogan professzor és a Cambridge-i Egyetem végzős hallgatóinak munkájára épült,¹⁴⁶ akik 87 millió amerikai Facebook-felhasználó adatait gyűjtötték össze a beleegyezésük nélkül.¹⁴⁷ Az általuk használt egyik eszköz egy személyiségteszt volt, amely a résztvevőket a "Big Five" mérőszámok szerint pontozta: nyitottság, lelkiismeretesség, extravertió, elfogadhatóság és neuroticizmus.¹⁴⁸ Ezután a mesterséges intelligencia segítségével ezeket az eredményeket más adatokkal (minden egyes felhasználóról akár 5000 adatpontot is) felhasználva feltárták a személyiségjegyeket, érzelmeket, politikai preferenciákat és viselkedési hajlamokat.¹⁴⁹ Az adatokból kialakított "pszichográfiai profilokat" a cég Trump jelöltségének népszerűsítésére, valamint a republikánusok, Ben Carson és Ted Cruz kampányai is felhasználták.¹⁵⁰ A választások előtt minden nap akár célzott 50,000 hirdetési változatokkal is megcélozták az adott közönséget. Alexander

uk.org/2017/02/02/02/meet-cambridge-analytica-the-big-data-communications-company-responsible-for-trump-brexite.

¹⁴⁵ *Id.*; Carole Cadwalladr, "Én készítettem Steve Bannon pszichológiai hadviselési eszközét": *Meet the Data War Whistleblower*, GUARDIAN (2018. március 18.), <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-chris-topher-wylie-faceook-nix-bannon-trump>.

¹⁴⁶ A kutatás vezető kutatói Michal Kosinski, David Stillwell és Christopher Wylie voltak.

¹⁴⁷ *Lásd* Issie Lapowsky, *The Man Who Saw the Dangers of Cambridge Analytica Years Ago*, WIRED (2018. június 19.), <https://www.wired.com/story/the-man-who-saw-the-dangers-of-cambridge-analytica>.

¹⁴⁸ *Lásd* Cadwalladr *supra* note 145.

¹⁴⁹ Ennek nagy része titokban zajlott, kivéve, hogy egy adatkészletet véletlenül a GitHubon, egy kódmegeosztó weboldalon hagytak, ami végül a nyilvánosságra hozatalához vezetett. Phee Waterfield & Timothy Revell, *Huge New Facebook Data Leak Exposed Intimate Details of 3m Users*, NEW SCIENTIST (2018. május 14.), <https://www.newscientist.com/article/2168713-huge-new-facebook-data-leak-exposed-intimate-details-of-3m-users>.

¹⁵⁰ David A. Graham, *Not Even Cambridge Analytica Believed It's Hype*, ATLANTIC (2018. március), <https://www.theatlantic.com/politics/archive/2018/03/cambridge-analytica-self-own/556016>.

Nix, a Cambridge Analytica vezérigazgatója azzal dicsekedett, hogy "ő juttatta Trumpot a Fehér Házba".¹⁵¹

A mesterséges intelligenciával történő mikrocélzás kihívást jelent a választási szabályozás számára. A nagy adatelemzések sikeresebbé teszik a torzító kampányokat, és így nagyobb valószínűséggel vetik be őket, általában ismeretlen forrásokból.¹⁵² A választási törvény nagymértékben függ az átláthatóságtól, mind a finanszírozás, mind a választási kampányok tekintetében. A rejtett közösségi média befolyásolási kampányokra fordított kiadásokról azonban nem készül jelentés, és gyakran nem is követhetők nyomon, így a külföldi és illegális beavatkozások szabályozatlanok és felderítetlenek maradnak. Bár a hamis kampánynyilatkozatokat látszólag védi az Első Alkotmánymódosítás, az, ¹⁵³hogy a napfényre kerülnek, és a valódi beszélők valódi személyazonossága nyilvános vizsgálatnak van kitéve, némi ~~csírt~~ jelent. Ez hiányzik a titkos befolyásolási kampányok esetében. "A politikai becsületkódex semmibe vételére irányuló hajlandóságuk, hogy aláássák demokratikus intézményeink legitimitását, tökéletesen illusztrálja, hogy a választási szabályozás ... miért kritikus eleme a működő demokráciának".¹⁵⁴

Engineering an Election című cikkében: *Digital Gerrymandering Poses a Threat to Democracy* című cikkében Jonathan Zittrain leírja a Facebook által 2010-ben végzett "digitális gerrymandering" kísérletet.¹⁵⁵ A Facebook-felhasználóknak szelektíven mutattak híreket azokról az ismerőseikről, akik aznap szavaztak.¹⁵⁶ Ez növelte a részvételi arányt azáltal, hogy a híreket kapókat arra ösztönözte, hogy kellőképpen szavazzanak.

¹⁵¹ Nick Miller, *Cambridge Analytica CEO Suspended After Boasts of 'Putting Trump in the White House*, SYDNEY MORNING HERALD (2018. március 21.), <https://www.smh.com.au/world/europe/cambridge-analytica-ceo-suspended-after-boasts-of-putting-trump-in-white-house-20180321-p4z5dg.html>.

¹⁵² Lásd Vyacheslav Polonski, *How Artificial Intelligence Conquered Democracy*, CONVERSATION (2017. augusztus 8., 6:33), <https://theconversation.com/how-artificial-intelligence-conquered-democracy-77675>.

¹⁵³ *Vö.* United States v. Alvarez, 567 U.S. 709 (2012) (a hamis állítások nem feltétlenül veszik el az Első Kiegészítés védelmét); Susan B. Anthony List v. Dreihaus, 134 S.Ct. 2334 (2014) (a hamis kampánybeszéddel kapcsolatos jogállási kérdés megoldása).

¹⁵⁴ Observer Editorial, *The Observer View on Digital Campaigning Being an Existential Threat to Democracy*, GUARDIAN (201829., július), <https://www.theguardian.com/commentisfree/2018/jul/29/the-observer-view-on-digital-campaigning-threat-to-democracy>.

¹⁵⁵ Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335 (2014).

¹⁵⁶ *Id.* 335-36.

nagyobb számban, hogy ez feltételezhetően befolyásolhatja a választási eredményeket.¹⁵⁷ A titkos közösségi média "ajánló algoritmusok" hasonló torzításokat produkálnak.¹⁵⁸ "[A]z információ szelektív bemutatása egy közvetítő által, hogy a saját napirendjének megfelelően, ahelyett, hogy a felhasználóit szolgálná.

... egy nagy hatalmú platformmal való visszaélést jelent [és] csupán egy pont a kialakulóban lévő térképen [a képességről], hogy csendben megdönsenek[] egy választást."¹⁵⁹ Zittrain következő cikke még hangsúlyosabb volt; *a Facebook úgy dönthet el egy választást, hogy senki sem tudná meg.*¹⁶⁰

A közösségi média manipulációja valószínűleg szerepet játszott az amerikai 2016 választásokban.¹⁶¹ De nem voltunk egyedül. A Computational Propaganda Research Project jelentése 2018 olyan országokban talált bizonyítékot manipulációs kampányokra, ahol "legalább egy politikai párt vagy kormányzati ügynökség a közösségi médiát a közvélemény do- mestikus manipulálására használta".¹⁶² Ez nagy üzlet. "2010 óta a politikai pártok és kormányok több mint félmilliárd dollárt költöttek a pszichológiai műveletek és a közvélemény közösségi médián keresztül történő manipulációjának kutatására, fejlesztésére és végrehajtására".¹⁶³ Ugyanilyen hatású a választók befolyásolása a keresőmotorok eredményeinek manipulálásával.¹⁶⁴

¹⁵⁷ *Id.* 336.

¹⁵⁸ Paul Lewis, *Fiction Is Outperforming Reality: How YouTube's Algorithm Distorts Truth*, GUARDIAN (2018. február 2.), <https://www.theguardian.com/technology/2018/feb/02/how-youtubes-algorithm-distorts-truth>.

¹⁵⁹ Zittrain, *Supra* note at 155338.

¹⁶⁰ Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (2014. június 1.), <https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering>.

¹⁶¹ *Lásd a Mueller-jelentést, lásd a 122. fenti megjegyzést.* 174.

¹⁶² Samantha Bradshaw & Philip N. Howard, *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation 3* (2018). *Lásd még* Tania Menai, *Why Fake News on WhatsApp Is So Pernicious in Brazil*, SLATE (2018. október 31., 15:44), <https://slate.com/technology/2018/10/brazil-bolsonaro-whatsapp-fake-news-platform.html> (beszámoló arról, hogy az újonnan megválasztott brazil elnök, Jair Bolsonaro profitált egy masszív dezinformációs kampányból a WhatsAppon, annak ellenére, hogy a Facebook "hadiszobát" állított fel a gyakorlat megfékezésére).

¹⁶³ Bradshaw, *Supra* note at 162,3.

¹⁶⁴ Robert Epstein et al., *Suppressing the Search Engine Manipulation Effect (SEME)*, <https://cbw.sh/static/pdf/epstein-2017-pacmhci.pdf> (utolsó látogatás 2019. február).

A választási beavatkozás "nem egyszeri, a 2016-os választásokra korlátozódó esemény volt. Ez egy mindennapos dobpergés. Ezek [a hamis fiókok] olyan entitások, amelyek megpróbálják megzavarni a demokratikus folyamatunkat azáltal, hogy a dezinformáció különböző formáit tolják be a rendszerbe".¹⁶⁵ Az oroszok és mások által folytatott befolyásolási kampányok¹⁶⁶ olyan szintre értek, hogy már túlterhelik a közösségi média azon erőfeszítéseit, hogy a platformjaikat ak-cikálhatóan tartsák. A polémia a politikai spektrumot öleli fel azzal a céllal, hogy online felháborodást keltsenek, és azt offline káosszá alakítsák.¹⁶⁷ Nem minden ilyen törekvés támaszkodik a mesterséges intelligenciára; néhány csak a jó öreg pszichológiai hadviselés. A mesterséges intelligencia azonban lehetővé teszi a mai információs harcosok számára, hogy még kifinomultabb tevékenységeket folytassanak.¹⁶⁸ A legújabb propaganda polarizált amerikaiakra szabása pontosan az a fajta játék, amelyben a pszichográfiai profilalkotás kiválóan teljesít.

Teljesen felkészületlenek vagyunk a demokrácia elleni támadásra. A közösségi médiát és a magánélet védelmét szabályozó szövetségi törvények csekély száma miatt kevés figyelmet fordítottak a problémára. A kongresszus két évvel a Cambridge Analytica adatbotránya után meghallgatásokat tartott.¹⁶⁹ Mark Zuckerberg, a koronatanú, sértetlenül megúszta egy ~~buszolás~~ amiért "nem tett eleget annak érdekében, hogy megakadályozza ezen eszközök kártékony felhasználását",¹⁷⁰ és amiért nem értesítette azt a 87 millió felhasználót, akiknek az adatai veszélybe kerültek. Bár egy sor okosnak hangzó törvényjavaslat

¹⁶⁵ Kevin Roose, *Facebook Grapples with a Maturing Adversary in Election Meddling*, N.Y. TIMES (2018. augusztus 1.), <https://www.ny-times.com/2018/08/01/technology/facebook-trolls-midterm-elections.html>.

¹⁶⁶ Úgy tűnik, hogy Irán is jelentős befolyásolási műveletekbe kezdett, amelyek célja az amerikai politikai diskurzus alakítása. Lásd: <https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html>.

¹⁶⁷ Digital Forensics Research Lab, *Troll Tracker: Facebook Uncovers Active Influence Operation*, MEDIUM (2018. július), <https://medium.com/dfirlab/trolltracker-facebook-uncovers-active-influence-operation-74bddfb8dc06>.

¹⁶⁸ *Id.*

¹⁶⁹ *Facebook, a közösségi média adatvédelme, valamint az adatok felhasználása és visszaélése: Közös meghallgatás az igazságügyi és a kereskedelmi, tudományos és közlekedési bizottság előtt*, 115. kong. (2018); *Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy and Commerce*, 115th Cong. (2018).

¹⁷⁰ Lásd: *Facebook, a közösségi média adatvédelme, valamint az adatok felhasználása és visszaélése: Közös meghallgatás az igazságügyi és a kereskedelmi, tudományos és közlekedési bizottság előtt*, 115. kong. (2018) (Mark Zuckerberg írásbeli tanúvallomása, 1. pont).

a meghallgatásokból vagy máshonnan ¹⁷¹nem született olyan jogszabály, amely választási hackertámadásokra reagálna. Ehelyett a Face- book titkos lobbikampányt indított, hogy kritikusat lejárassa.¹⁷² Zuckerberg visszautasította, hogy megjelenjen a brit és más országok törvényhozói előtt, hogy számot adjon a magánélet védelmének megsértéséről.¹⁷³

Az önszabályozás sem elegendő. A közösségi médiavállalatok kevés korlátozást vezetnek be arra vonatkozóan, hogy ki férhet hozzá a felhasználói adatokhoz. Inkább aktívan megosztják egymással az adatokat, általában kifejezett beleegyezés nélkül.¹⁷⁴ Egy brit parlamenti bizottság nemrég arra a következtetésre jutott, hogy a Facebook a bevételek maximalizálása érdekében felülbírálja a felhasználók adatvédelmi beállításait.¹⁷⁵ Még ha a platformok meg is próbálják ellenőrizni magukat, akkor is egyfajta "whac-a-mole" játékba keverednek. Miután blokkolnak egy céget, mások is feltámadhatnak a hamvaiból. Miután a nyilvánosság felháborodása közepette kitiltották a Facebookról, a Cambridge Analytica feloszlott. A Facebook és más közösségi médiumok azonban továbbra is profitálnak a felhasználói adatok hatalmas tárházát használó elemző cégekből. A Crim- son Hexagon nevű cég például azt állítja, hogy jogszerűen több mint 1 trillió posztot és képet gyűjtött össze a Facebook, a Twitter, az Instagram, a Tumblr és más közösségi médiaplatformokról.¹⁷⁶ A mesterséges intelligencia alkalmazásával a Crimson

¹⁷¹ *Lásd pl.* Prevent Election Hacking Act of 2018, H.R. 6188; Securing American Elections Act of 2018, HR. 5147; Helping State and Local Governments Prevent Cyber Attacks (HACK) Act, S. (15102017).

¹⁷² Sheera Frenkel et al., *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*, N.Y. TIMES (2018. november 14.), <https://www.ny-times.com/2018/11/14/technology/facebook-data-russia-election-racism.html>.

A Facebook mulasztásai miatt az FTC akár 5 milliárd dolláros bírságot is kiszabhatott. *Lásd:* Mike Isaac & Cecilia Kang, *Facebook Expects to Be Fined Bined Up to \$5 Billion by F.T.C. Over Privacy Issues*, N.Y. TIMES (2019. április 24.), <https://www.ny-times.com/2019/04/24/technology/facebook-ftc-fine-privacy.html>.

¹⁷³ *Lásd* Tony Romm, *Facebook Faces Fresh Lashing from Nine Countries for Its Inability To Stop the Spread of Fake News*, WASH. POST (2018. november 27.), <https://www.washingtonpost.com/technology/2018/11/27/facebook-faces-global-lashing-nine-countries-its-inability-protect-data-stop-fake-news>.

¹⁷⁴ *Lásd* Dance, *Supra* note 51.

¹⁷⁵ Tony Romm, *Facebook 'Intentionally And Knowingly' Violated U.K. Privacy And Competition Rules, British Lawmakers Say*, WASH. POST (2019. február 17.), <https://www.washingtonpost.com/technology/2019/02/18/facebook-intentionally-knowingly-violated-uk-privacy-competition-rules-british-lawmakers-say>.

¹⁷⁶ Olivia Solon & Julie Carrie Wong, *Facebook Suspends Another Analytics Firm Amid Questions Over Surveillance*, GUARDIAN (2018. július 20.), <https://www.theguardian.com/technology/2018/jul/20/facebook-crimson-hexagon-analytics-data-surveillance>.

kifinomult "hangulatelemzést" végez ügyfelei számára.¹⁷⁷ Az egyének "érzelmeinek" ismeretében, a döntési pontok mátrixán keresztül, a vállalatok számára a meggyőzéstől a manipulációig csak egy rövid lépés.

3. *Fake News*

A dezinformációs kampányok a háború, a diplomácia, a tárgyalások és a hatalmi politika régi eszközei. Az ókori Rómában az álhírek pecsételték meg Marcus Antonius és Kleopátra sorsát.¹⁷⁸ A mesterséges intelligencia nem csupán hatékonyabbá teszi az információs háborúkat, hanem teljesen új dimenzióba emeli azokat. Mivel az álhírek a valóságos világgal versenyeznek a közvéleményben, és gyakran kiszorítják azt, az emberek hozzászoknak a tényekhez. A tényeket mint a kognitív feldolgozás információforrásait becsmérlik. A döntéshozatalhoz szükséges tények hiányában az érzelmi jelzésekhez fordulunk, mint például a hitelesség, az állítás ereje, az érzések és a meggyőződések. Donald Trump talán a legnevezetesebb áldozata ennek. Hírszerző ügynökségének tényszerű megállapításai a 2016-os választásokba való orosz beavatkozásról nem voltak ellenfelei Vlagyimir Putyin "rendkívül erős és erőteljes" tagadásának.¹⁷⁹ Mint sok ember, ő is egyszerűen jobban szereti a hatalmat az igazságnál.

Az álhírek a 2016-os választások másik olyan jellemzője voltak, amelyet a mesterséges intelligencia fegyverként használt fel. Az "álhírek" egy nemrégiben kitalált kifejezés, amely az olyan aktuális tartalmakat írja le, amelyek hamisítottak, elferdítettek, félrevezetőek vagy a kontextusból kiragadottak. Általában online terjesztik, és gyakran "mikrocélzottan", egy adott csoport ~~vélemény~~ befolyásolása érdekében.¹⁸⁰ Míg a hamis jelentések, a félrevezetés és a propaganda

¹⁷⁷ Lásd Garrett Huddy, *What is Sentiment Analysis*, CRIMSON HEXAGON, <https://www.crimsonhexagon.com/blog/what-is-sentiment-analysis> (a hangulatelemzés (vagy "véleménybányászat") megpróbálja megérteni, mit gondolnak vagy hogyan éreznek az emberek egy adott témával kapcsolatban).

¹⁷⁸ Lásd Eve Macdonald, *The Fake News That Sealed the Fate of Antony and Cleopatra*, THE CONVERSATION (2017. január 13.), <https://theconversation.com/the-fake-news-that-sealed-the-fate-of-antony-and-cleopatra-71287>.

¹⁷⁹ Trump elnök és Putyin orosz elnök közös sajtókonferencián tett megjegyzései, 2018. július 16., <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-president-putin-russian-federation-joint-press-conference/>

¹⁸⁰ Lásd általában House of Commons, Digital, Culture, Media and Sport Committee, Disinformation and "fake news": Időközi jelentés, július 29, 2018.

Az évszázados taktikákhoz hasonlóan a mesterséges intelligencia tovább súlyosbítja az álhírek problémáját azzal, hogy célzott testreszabással valóságosabbnak vagy relevánsabbnak tünteti fel azokat. "[A]z álhírek ... különösen károsak, ha olyan komplex politikai stratégia részeként terjesztik őket, amely nagy mennyiségű adatot aknáz ki az üzenetükre fogékony közönség hipercélzása érdekében."¹⁸¹ Sajnálatos módon az álhírek terjesztői arra is képesek, hogy kihasználják a polgárok autonómiába és döntési magánszférába vetett hitét, amelyet a III.B. részben ismertettünk. Ahogy Yuval Noah Harari történész megjegyzi: "Minél inkább hisznek az emberek a szabad akaratban... annál könnyebb manipulálni őket, mert nem fogják azt hinni, hogy érzéseiket egy ~~ki~~ rendszer állítja elő és manipulálja".¹⁸²

Az interneten elérhető mesterséges intelligencia-eszközök aktívan elősegítik a pletykakaszadokat és más "információs zavarokat".¹⁸³ Amikor például az FCC 2017-ben a hálózatsemlegességi szabályok hatályaon kívül helyezését fontolgatta, az ügynökséghez beérkezett 22 millió hozzászólásból 21 millió hamisítvány volt, vagy botok és szervezett kampányok által küldött.¹⁸⁴ A választási 2016 kampány utolsó három hónapjában "a hoax oldalak és hiperpárti blogok által készített, legjobban teljesítő hamis választási történetek 8 711 000 megosztást, újra-cselekvést és kommentet generáltak a Facebookon".¹⁸⁵ Ez több volt, mint a nagy hírportálok által generált szám. A közösségi médiaoldalak jelentős bevételre tesznek szert az álhírekből, így minimálisra csökkentve a rendőrséggel kapcsolatos érdekeltségüket.¹⁸⁶ A terjesztők is jól megélnék abból, hogy eladnak

¹⁸¹ Lili Levi, *Valódi "álhírek" és hamis "álhírek"*, 16 ELSŐ MÓDOSÍTÁS. L. REV. 232,253 (2017).

¹⁸² Andrew Anthony, *Yuval Noah Harari: The Idea of Free Information is Extremely Dangerous*, GUARDIAN (Aug. 20185), <https://www.theguardian.com/culture/2018/aug/05/yuval-noah-harari-free-information-extremely-dangerous-interview-21-lessons>.

¹⁸³ David M. J. Lazar et al., *The Science of Fake News*, SCI359. 1094,1096 (2018).

¹⁸⁴ Mary Papenfuss, *Feds Investigating Millions of Fake Messages Opposing Net Neutrality: Report*, HUFFINGTON POST (dec. 98,2018,:14 PM), https://www.huffingtonpost.com/entry/feds-probe-fake-messages-to-fcc-supporting-ending-net-neutrality_us_5c0c4ae1e4b0ab8cf693ec5c.

¹⁸⁵ Craig Silverman, *This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook*, BUZZFEED (2016. november 16., 17:15), <https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook>.

¹⁸⁶ *Lásd Peter Cohan, A Facebook a hirdetési bevételeinek több mint felét álhírekből szerzi?*, FORBES (2016. november 25.), <https://www.forbes.com/sites/pe-tercohan/2016/11/25/does-facebook-generate-over-half-its-revenue-from-fake->

álhíreket ezeken az oldalakon; amit mostanában "álhírek ökoszisztémájának" neveznek.¹⁸⁷ A nézettséget egyszerűen meg lehet vásárolni, hogy növeljék a rangsorolást és fokozzák a befolyásolási kampányokat. Egy időben "a YouTube-nak ugyanannyi látogatója volt az embernek álcázott botoktól, mint a valódi emberi látogatóktól".¹⁸⁸ Hasonlóképpen, a Twitter retweetek sokkal nagyobb valószínűséggel tartalmaznak hamis információt, mint valósat.¹⁸⁹ A hamis politikai hírek nagyobb vírusszámmal terjednek, mint az álhírek bármely más kategóriája.¹⁹⁰ A Gartner előrejelzése szerint "2022, az érett gazdaságokban az egyének többsége több hamis információt fog fogyasztani, mint igazat".¹⁹¹ A Brookings ezt "a dezinformáció demokratizálódásának" nevezi.¹⁹²

A közösségi média és a híroldalak üzleti modelljei közé tartoznak az olvasói hozzászólások. Úgy tűnik, hogy ez is online világunk demokratizáló jellemzője. De a tigris a farkánál fogva kaptuk el. A kommentelés, különösen az internetes trollok által, "megnyitotta az ajtót az agresszívabb zaklatás, a zaklatás és a téves információk terjesztésének lehetősége előtt".¹⁹³ Mint más álhírek esetében, a mesterséges intelligenciát ennek a problémának mindkét végén alkalmazzák.¹⁹⁴ Míg a technológiai cégek a "Captcha"¹⁹⁵ és egyéb

news/#656383d8375f. A platformok még a Communications Decency Act (CDA) értelmében is mentességet élveznek a hamis, káros vagy jogsértő tartalmak elhelyezése esetén. 47

U.S.C. § 230.

¹⁸⁷ Michael H. Keller, *The Flourishing Business of Fake YouTube Views*, N.Y. TIMES (2018. augusztus 11.), <https://www.nytimes.com/interactive/2018/08/11/technology/youtube-fake-view-sellers.html>.

¹⁸⁸ *Id. Lásd még Lazar*, 183. lábjegyzet, 1094, 1095. o. (A Facebook becslései szerint akár 60 millió közösségi bot is ellepetheti a platformját).

¹⁸⁹ Lazar, *Supra* note, 183, 1094-95. o.

¹⁹⁰ *Id.* at 1148; Soroush Vosoughi et al., *The Spread of True And False News Online*, sci359. 1146 (2018).

¹⁹¹ Kasey Panetta, *Gartner Top Strategic Predictions for 2018 and Beyond*, GARTNER (2017. október 3.), <https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions>. Az álhírek áramlásáról szóló tudományos tanulmányok áttekintését lásd: Vosoughi et al., *supra* note. 193.

¹⁹² *Supra* megjegyzés 141.

¹⁹³ Brian X. Chen, *Az internetes trollok győztek. Sorry, There's Not Much You Can Do*, N.Y. TIMES (2018. augusztus 8.), <https://www.nytimes.com/2018/08/08/technology/personaltech/internet-trolls-comments.html>.

¹⁹⁴ *Lásd Tarek Ali Ahmad, Mesterséges intelligencia eszköz az álhírek készítői és az ellenük való küzdelemben*, ARAB NEWS (2018. április 4.), <http://www.arab-news.com/node/1278426/media>.

¹⁹⁵ A "Captcha" a "Completely Automated Procedures for Telling Computers and Humans Apart" (Teljesen automatizált eljárások a számítógépek és az emberek megkülönböztetésére) rövidítése. Egyes eljárások olyan egyszerűek, mint amikor a posztolót arra kérik, hogy jelölje be a jelölőnégyzetet, amely

megeősíti, hogy ő nem robot.

módszerek a botok és a spammerek felderítésére,¹⁹⁶ beleértve a harmadik fél által nyújtott szolgáltatásokat, a¹⁹⁷ hackerek kifinomultabb eszközöket használnak a weboldalak eltérítésére.¹⁹⁸ vagy egyszerűen csak saját alkalmazásaikat dobják be az Apple és a Google alkalmazásboltjaiba.¹⁹⁹ Végző soron, "amikor az álhírekről van szó, a mesterséges intelligencia nem alkalmas a feladatra."²⁰⁰

A Facebook és a Google "bonyolult kapcsolatot" ápol a mesterséges intelligenciával és az álhírekkel.²⁰¹ Egyrészt mesterséges intelligenciát alkalmaznak az álhírek²⁰² kiszűrésére, valamint az álfiókok és a politikai befolyásolási kampányokban részt vevő felhasználók eltávolítására.²⁰³ Ugyanakkor úgy tűnik, hogy szépen profitálnak az álhírekből, és erős kritikák érik őket a szándékosan nem megfelelő ellenőrzés miatt.²⁰⁴ A Google YouTube például szintén jól profitál az álhírekből. Az "ajánló algoritmus" olyan videókat mutat be, amelyekről a mesterséges intelligencia programja úgy ítéli meg, hogy 1,5 milliárd felhasználója számára érdekesebbek lehetnek. Az algoritmus, amely "a YouTube növekedésének legfontosabb motorja", az összeesküvés-elméletek népszerűsítésében is örömet leli.²⁰⁵ Míg a legtöbb figyelem a Facebookra és a Twitterre irányult, "a YouTube a leginkább figyelmen kívül hagyott

¹⁹⁶ Lásd pl. <http://fakenewschallenge.org>.

¹⁹⁷ Lásd Jackie Snow, *Can AI Win the War Against Fake News?*, MIT TECH. REV. (2017. december 13.), <https://www.technologyreview.com/s/609717/can-ai-win-the-war-against-fake-news>.

¹⁹⁸ Chen, *fenti* megjegyzés 193.

¹⁹⁹ Jack Nicas, *A technológiai cégek betiltották az Infowars-t. Most az applikációja trendi*, N.Y. TIMES (2018. augusztus 8.), <https://www.nytimes.com/2018/08/08/technology/infowars-app-trending.html>.

²⁰⁰ James Vincent, *Why AI Isn't Going to Solve Facebook's Fake News Problem*, VERGE (2018. április 5.), <https://www.theverge.com/2018/4/5/17202886/facebook-fake-news-moderation-ai-challenges>.

²⁰¹ Jonathan Vanian, *A Facebook kapcsolata a mesterséges intelligenciával és az álhírekkel: It's Complicated*, FORTUNE (2016. december 1.), <http://fortune.com/2016/12/01/facebook-artificial-intelligence-news>.

²⁰² Lásd pl. James Vincent, *Facebook Is Using Machine Learning To Spot Hoax Articles Shared By Spammers*, THE VERGE (2018. június 21.), <https://www.theverge.com/2018/6/21/17488040/facebook-machine-learning-spot-hoax-articles-spammers>.

²⁰³ Nicholas Fandos & Kevin Roose, *Facebook Identifies an Active Political Influence Campaign Using Fake Accounts*, N.Y. TIMES (2018. július 31.), <https://www.nytimes.com/2018/07/31/us/politics/facebook-political-campaign-midterms.html>.

²⁰⁴ Lásd a *fenti* megjegyzést 173.

²⁰⁵ Lewis, *fenti* megjegyzés 158.

2016 története.... Kereső- és ajánló algoritmusai tévképző motorok."²⁰⁶ Egy leleplező cikk megállapította, hogy "a YouTube rendszer- tematikusan felerősíti a megosztó, szenzációhajhász és kon- spiratorikus videókat".²⁰⁷

Az álhírek egy különösen hatékony példája az úgynevezett "deepfakes", amely olyan hang- vagy videófelvétel, amelyet az érzékszervek megtévesztése érdekében hamisítottak vagy megváltoztattak.²⁰⁸ Míg a "Photoshop" már régóta egy ige és egy grafikai program is, a mesterséges intelligencia teljesen új szintre emeli a megtévesztést. Gondoljunk csak a FakeApp nevű programra, amely lehetővé teszi a felhasználók számára, hogy arcokat változtassanak meg videóban.²⁰⁹ Ezt a programot népszerűen használják hírességek arcát kicserélő pornográfiákhoz, illetve politikusok humoros vagy felháborító dolgok mondására.²¹⁰ A generatív adverzális hálózatok (GAN-ok) egy lépéssel továbbviszik ezt, amikor az egyik hálózatot a másik ellen játsszák ki a hamis képek generálásában vagy kiszűrésében. Ilyen esetekben "[a]z a mesterséges intelligencia, amelyik megpróbálja felismerni a hamisítványt, mindig veszít".²¹¹

Az álhírek problémái sokkal rosszabbak lesznek, ahogy ezek az eszközök mindennaposá válnak. A nagyméretű, felügyelet nélküli algoritmusok ma már soha nem látott minőségű szintetikus szöveget képesek előállítani,²¹² ami tovább homályosíthatja a valóság és a hamisítás közötti határt. Ezt szem előtt tartva, az egyik ilyen termék fejlesztője nem hajlandó nyilvánosan nyilatkozni

²⁰⁶ *Id. Lásd még Zeynep Tufekci, Algorithmic Harms Beyond Facebook and Google: Emergent Challenges Of Computational Agency*, 13 COLO. TECH. L.J. (2015)203,.216

²⁰⁷ *Id.* (idézi az algotransparency.org oldalon elérhető megállapításokat).

²⁰⁸ Lásd általában Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. (megjelenés: 2019).

²⁰⁹ Lásd Adi Robertson, *I'm using AI to face-swap Elon Musk and Jeff Bezos, and I'm really bad at it*, VERGE (2018. február 11. 12:00 PM), <https://www.theverge.com/2018/2/11/16992986/fakeapp-deepfakes-ai-face-swapping>.

²¹⁰ Ha ezt a gyakorlatban szeretné látni, látogasson el a <https://www.thispersondoesnotexist.com> weboldalra, amely mesterséges intelligenciát használ teljesen fiktív, de valóság-hű hamis arcok létrehozására.

²¹¹ Cade Metz, *How Will We Outsmart A.I. Liars?*, N.Y. TIMES (2018. november 19.), <https://www.nytimes.com/2018/11/19/science/artificial-intelligence-deepfakes-fake-news.html>.

²¹² Lásd: OpenAI, *Better Language Models and Their Implications*, <https://blog.openai.com/better-language-models>.

a kód kiadása "[d]a technológia rosszindulatú alkalmazásával kapcsolatos aggodalmaink miatt".²¹³

A kockázatokat nem lehet túlbecsülni. Ahogy egy cikk figyelmeztetett: "képzeljünk el egy olyan fu- túrát, amikor ... egy elnökről készült hamis videó lázadást szít vagy a piacot veri el".²¹⁴ Vagy ahogy Franklin Foer, a *The Atlantic munkatársa* fogalmaz: "Hamarosan olyan világban fogunk élni, ahol a szemünk rendszeresen becsap minket. Másképp fogalmazva, nem is vagyunk olyan messze a valóság összeomlásától".²¹⁵ Brian Resnick a *Vox-tól* még pesszimistább. "[Nem csak a jelen és a jövő valósága omolhat össze, hanem a múltunk is. A hamis média manipulálhatja azt, amire emlékszünk, hatékonyan megváltoztatva a múltat azáltal, hogy hamis emlékekkel táplálja a lakosságot."²¹⁶ Az emberek fogékonyak a valóság ilyen torzításaira.²¹⁷ Egy régi orosz közmondás hamarosan valóra válhat: "nem a jövőt, hanem a múltat a legnehezebb megjósolni".²¹⁸

"A valóság összeomlása nem a mesterséges intelligencia nem szándékolt következménye. Ez már régóta cél - vagy legalábbis tévhit -

- a technológia leghíresebb építészei" - állítja Franklin Foer.²¹⁹ A valóság kiragadása a virtuális valóság (VR) és a kiterjesztett valóság (AR) technológiák területe is. Ezeket a játékelményt és a szórakozást fokozó, fejlesztő technológiákként értékeljük. Vajon a demokrácia és az egyéni jogok eltorzításával is értékelni fogjuk őket?

²¹³ *Id.*

²¹⁴ Brian Resnick, *We're Underestimating the Mind-Warping Potential of Fake Video*, VOX (201823., július), <https://www.vox.com/science-and-health/2018/4/20/17109764/deepfake-ai-false-memory-psychology-mandela-effect>. Lásd még Kenneth Rapoza, *Can "Fake News" Impact The Stock Market?*, FORBES (201726., február), <https://www.forbes.com/sites/kenrapoza/2017/02/26/can-fake-news-impact-the-stock-market/#40d121c2fac0> (a részvények értékének 130 milliárd dolláros csökkenéséről szól, miután 2013-ban egy tweet tévesen azt állította, hogy Obama elnök megsérült egy robbanásban).

²¹⁵ Franklin Foer, *The Era of Fake Video Begins*, ATLANTIC (2018. május), <https://www.theatlantic.com/magazine/archive/2018/05/realitys-end/556877>.

²¹⁶ Resnick, *supra* note. 214.

²¹⁷ *Id.* (idézi Elizabeth Loftus, U. Cal. Irvine).

²¹⁸ Lawrence Rosen, *Az iszlám kultúrája: A mai muszlim élet változó aspektusai* 98.

²¹⁹ Foer, *fenti* megjegyzés 215.

A mesterséges intelligencia azonban az álhírek jelentette problémára is nyújthat lehetséges megoldásokat. Az olyan tényellenőrző szervezetek, mint a Politifact, a leghatásosabb valótlanosságok ellen küzdenek, de annyi álhír van, hogy a tényellenőrzés saját iparággá vált, saját szabványokkal és elvekkel.²²⁰ Az algoritmusok is segíthetnek a probléma enyhítésében. A Google finanszírozta a Full Factet, hogy egy mesterséges intelligenciával működő tényellenőrző eszközt fejlesszen ki újságírók számára.²²¹ Más ilyen szolgáltatások is megjelennek.²²² Az oldalak rangsorolását is lehet úgy módosítani, hogy az azonosított téves információkat nem veszik figyelembe. A tényellenőrzés azonban kontraproduktív is lehet, mivel a hamis információk újbóli közzététele, még a helyesbítéssel összefüggésben is, "növelheti az egyén valószínűségét, hogy igaznak fogadja el".²²³ Így a nap végén az előny az álhíreké. A hír terjesztői támaszkodhatnak a mesterséges intelligenciára, az első módosításra, a közösségi médiavállalatok nyereségvágyára és a sikeres áhírkampányok politikai kifizetődésére. Milton számára elegendő volt "hagyni, hogy az [Igazság] és a Hamisság megküzdjön egymással; ki ismerte már az Igazságot a rosszabbik oldalára állítva, egy szabad és nyílt találkozáson?".²²⁴ Ez persze jóval azelőtt volt, hogy a mesterséges intelligencia megváltoztatta volna a játékteret.

4. A megbízható intézmények megszűnése

Az álhírek nem csak a választásokat manipulálják, hanem a demokrácia mozgatórugóit is akadályozzák, amelyek közül a legfontosabb a szabad sajtó. Az intézményes sajtó a 20th. század során kialakította az objektivitás és a kiegyensúlyozottság újságírói normáit. A digitális sajtó térhódítása azonban számos új belépőt tett lehetővé, amelyek egyrészt megkérdőjelezték a hagyományos normákat, másrészt csökkentették az intézményes sajtó profitját.²²⁵

A rengeteg áhírhoz olyan állítások társulnak, amelyek szerint a kedvezőtlen, de tényszerű hírek maguk is álhírek. A bizalmatlanság magvainak elvetésével az áhírekkel kapcsolatos hamis állítások célja a sajtóba vetett bizalom aláásása, "ami

²²⁰ Lásd UK Disinformation Report, 8. o., <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmums/363/363.pdf>.

²²¹ Lásd Matt Burgess, *Google is helping Full Fact create an automated, real-time fact-checker*, WIRED UK (2016. november 17.), <https://www.wired.co.uk/article/automated-fact-checking-full-fact-google-funding>.

²²² Lásd UK Disinformation Report, fn. 25.

²²³ Lazar, *Supra* note at 183,1095.

²²⁴ JOHN MILTON, AREOPAGITICA (58Cambridge U. Press 1644).

²²⁵ Lazar, *Supra* note 183.

2016-ban történelmi mélypontra zuhant.²²⁶ A sajtóellenes retorika, például az, hogy az újságírók "a nép ellenségei", tovább erodálja a demo- kratikus eszméket.²²⁷ Ahogy a mainstream média elsorvad ezeknek a támadásoknak a hatására, a közösségi médián keresztül érkező hírek veszik át a helyét, amit a fent leírt algoritmikus célzással fokoznak.²²⁸ Egyesek szerint ezek a nem hagyományos eszközök demokratizálják a hírek előállítását és terjesztését. Bizonyára növelik a hallható hangok számát, különösen a népszerűtlen és a hatalom ellenes nézetekét. Sok minden elvész azonban a zajos zajban. Ráadásul a közösségi médiacsatornák által lehetővé tett önszelekció azt jelenti, hogy sokan soha nem találkoznak ellentétes nézetekkel. Hírfogyasztásuk egy visszhangkamrához hasonlít. A már meglévő előítéletek egyszerűen megerősödnek. Ami a tényfeltárást illeti, a mesterséges intelligencia "kompetenciaromboló technológia".²²⁹

Az amerikaiak többsége a közösségi médiából szerzi híreit, ami átvette a hírforrás, a főtér és a szónoki sarok szerepét. Az internetes óriások az Első Alkotmánymódosításra való tekintet nélkül határozzák meg, hogy kit láthatnak és hallhatnak. A hírszűrő algoritmusok kapuórzó funkciót töltenek be a tartalomfogyasztásunkban. A moderátorok igyekezhetnek kiegyensúlyozottak és nyitottak lenni, de olyan piaci erőkkel is szembe kell nézniük, amelyek hajlamosak a tartalmakat a legkevésbé közismert felekezetre redukálni.²³⁰ A nézettség, az oldalmegtekintések és a kattintások a siker bevett mérőszámai. "A nagy adatok és az algoritmusok alakították a folyóirat-

²²⁶ *Id.* (a demokratáknak csak 51%-a, a republikánusoknak pedig 14%-a bízik a tömegtájékoztatóban mint hírforrásban).

²²⁷ *Statement of A.G. Sulzberger, Publisher, The N.Y. Times, In Response to President Trump's Tweet About Their Meeting*, N.Y. TIMES (2018. július 29.), <https://www.nytimes.com/press/statement-of-a-g-sulzberger-publisher-the-new-york-times-in-response-to-president-trumps-tweet-about-their-meeting> (megjegyezve, hogy Trump elnök sajtó elleni támadásai a riporterek elleni erőszakhoz vezethetnek).

²²⁸ *Lásd Economist Intelligence Unit, Democracy Index 2017*, 44. o., https://pages.eiu.com/rs/753-RIQ-438/images/Democracy_Index_2017.pdf (a közösségi média "komoly kihívást jelentett a híradók és műsorszolgáltatók gazdasági életképessége számára").

²²⁹ A kifejezés, bár nem feltétlenül a szöveggörnyezet, Cornelia Dean, a The New York Times korábbi tudományos szerkesztőjének tulajdonítható.

²³⁰ Természetesen a moderátorok ritkán semlegesek. "Egy nyilvános Facebook-oldal kezelője saját belátása szerint választja ki bizonyos posztok terjesztését ... és személyre szabhatja a terjesztést ... komplex algoritmusok és mesterséges intelligencia segítségével." Michal Lavi, *Taking Out of Context*, HARV31. J.L. & TECH, 153-54145, (2017).

isztikus termelés, a 'számítógépes folyóirat-izmus' korszakának bevezetésével."²³¹ Az eszmék piaca másodlagos státuszba kerül. Robotok írják a híreket a nagy kiadók számára.²³² Ha a negyedik hatalom egyszer legyengül, "a demokrácia sötétségben hal meg".²³³

B. Egyenlőség és méltányosság

A liberális demokrácia elméleteiben alapvető fontosságúak a tisztességes és az egyenlőség és a gazdasági szabadság elvei. Ezek az értékek az alapító és emberi jogi dokumentumokban is szerepelnek. Gondoljunk csak a Függetlenségi Nyilatkozatra, amely kimondja, hogy "minden ember egyenlőnek teremtett", "elidegeníthetetlen jogokkal... [az] élethez, a szabadsághoz és a boldogságra való törekvéshez...", és hogy e jogok biztosítása érdekében az emberek között kormányok jönnek létre, amelyek jogos hatalmukat a kormányzottak beleegyezéséből nyerik".²³⁴ Az egyenlőség, a tisztességes eljárás és a demokrácia közötti kapcsolatnak nincs világosabb kifejezése.

A tisztességes eljárás és az egyenlő védelem "az egyenlő alapszabadságok koherens rendszerét alkotja, amelynek két témája van: a deliberatív autonómia, valamint a deliberatív demokrácia előfeltételeinek biztosítása".²³⁵ A bírósági beavatkozás a tisztességes eljárás és az egyenlő védelem klauzulája alapján akkor a legmegfelelőbb, ha a kormányzati cselekvés megzavarja a politikai folyamatot.²³⁶ És természetesen Stone bíró híres négyes lábjegyzete az *Egyesült Államok kontra Carolene Products ügyben* elvileg összefüggést teremt az egyenlőség és a politikai folyamat között.²³⁷

A jogegyenlőség megvalósítása a digitális korban nehezebbé vált. Ez részben a Legfelsőbb Bíróság olyan doktrínáinak köszönhető, mint az "állami cselekvés doktrínája" és a "célhoz kötöttség követelménye". A

²³¹ Samantha Shorey & Philip N. Howard, *Automation, Big Data, and Politics*, INT'L J. OF COM'N (50372016).

²³² Lásd Lucia Moses, *The Washington Post's Robot Reporter Has Published Articles 850 In The Past Year*, DIGIDAY (2017. szeptember 14.), <https://digiday.com/media/washington-posts-robot-reporter-published-500-articles-last-year>.

²³³ A Washington Post szlogenje.

²³⁴ A függetlenségi nyilatkozat (1) bekezdése. 2 (USA 1776).

²³⁵ James E. Fleming, *Constructing the Substantive Constitution*, 72 TEX. L. REV. 211,274 (1993).

²³⁶ Lásd JOHN HART ELY, DEMOKRÁCIA ÉS DISTRUST (1980).

²³⁷ 304 U.S. 144, 152, n.4 ("a különálló és elszigetelt kisebbségekkel szembeni előítélet ... komolyan hajlamos arra, hogy korlátozza azoknak a politikai folyamatoknak a működését, amelyekre általában a kisebbségek védelmében támaszkodni kell").

az előbbi mentesíti a magánszereplőket az alkotmányos kényszer alól.²³⁸ Számos létfontosságú társadalmi struktúránk ma már magánkézben van, és így nem köti őket a tizennegyedik módosítás. Például az internetet irányító világszervezet, az Internet Corporation for Assigned Names and Numbers (ICANN) egy kaliforniai magánszervezet, amelynek nem kell betartania az alkotmányos eljárási vagy szólásjogokat.²³⁹ A távközlési és platform-óriásoknak az Első Alkotmánykiegészítéshez fűződő jogaik vannak, de nem kötelesek biztosítani a szabad véleménynyilvánítást a felhasználók számára. A digitális korszakban a kommunikációs eszközök feletti funkcionálisan teljes ellenőrzésük azt eredményezi, hogy a jogok a polgárokról a vállalati igazgatókra szállnak át, akik a részvényeseknek tartoznak hűséggel, nem pedig az alkotmánynak.

A második említett doktrína, a "célzatosság követelménye" a szándékosság követelményét olvassa bele az egyenlő védelemről szóló záradékba.²⁴⁰ A diszkriminatív eredményt okozó intézkedés nem alkotmányellenes, hacsak a megkülönböztetés nem volt szándékos. A szándékossághoz általában emberi cselekvőre van szükség. Így az algoritmus által hozott vagy befolyásolt döntések alkotmányos hatókörön kívül eshetnek, függetlenül attól, hogy mennyire elfogultak vagy átláthatatlanok.²⁴¹

1. Átlátszatlanság: Megmagyarázhatatlan AI

A gépi tanulási technikák egyik fő hátránya az átláthatatlanságuk. Mivel az algoritmusokat nem közvetlenül emberek hozzák létre, az általuk használt valódi érvelési folyamat ismeretlen és ismeretlen lehet. Még ha le is kérdeznénk a gépet, és megkérdeznénk, hogy milyen algoritmusokat és tényezőket használt egy adott eredmény eléréséhez, a gép nem biztos, hogy tudná. Ez azért van így, mert a több réteg mélységű, több millió permutációval rendelkező neurális hálózatok egy adott pillanatban játszanak, és véletlenszerűen vagy heurisztikusan, milliszekundumonként állítják be kapcsolataikat.

²³⁸ Lásd általában Erwin Chemerinsky, *Rethinking State Action*, 80 NW U.L. REV. 503 (1985).

²³⁹ Lásd A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around APA and the Constitution*, 50 DUKE L. J. 17, 94-105, 141-42 (2000). De lásd Kate Klonick, *The New Governors: The People, Rules, And Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1602 (2018) (azzal érvelve, hogy a közösségi médiaplatformok tiszteletben tartják az Első Alkotmánymódosítást "azáltal, hogy tükrözik a felhasználók demokratikus kultúráját és normáit").

²⁴⁰ Washington kontra Davis, USA (4262291976).

²⁴¹ Yavar Bathaee, *The Artificial Intelligence Black Box And The Failure Of Intent And Causation*, HARV 31. J.L. & TECH. 889, (8912018).

skála.²⁴² Ez olyan, mintha egy teknőstől kérdeznénk meg, miért döntött úgy a faja, hogy páncélt növeszt. Tudjuk, hogy ez adaptív volt, de talán nem ismerjük a pontos utat, amelyet a jelenlegi állapot eléréséhez megtett. A tudatlanságunk még ennél is rosszabb lehet, mivel azt sem tudhatjuk, hogy a mesterséges intelligencia hazudik-e nekünk az érvelési folyamatát illetően. Ha a mesterséges intelligenciába programozott egyik cél az emberi jólét maximalizálása, akkor ezt úgy érhetjük el, hogy időnként megszabadulunk az emberi kezelőtől.²⁴³

Ali Rahimi, a Google munkatársa nemrégiben a mesterséges intelligencia technológiát a középkori al-chemyhez hasonlította. A kutatók "gyakran nem tudják megmagyarázni matematikai modelljeik belső működését: hiányzik az eszközeik szigorú elméleti megértése... [Mégis] olyan rendszereket építünk, amelyek az egészségügyet irányítják, közvetítik a polgári párbeszédet [és] befolyásolják a választásokat".²⁴⁴ Ezek a problémák nem pusztán feltevések vagy ríogatás. A Védelmi Minisztérium (DoD) egyik legjobban finanszírozott mesterséges intelligencia-kezdményezése a magyarázható mesterséges intelligencia (Explainable AI, XAI) projekt. A DoD-t aggasztja, hogy a drónok és más autonóm eszközök megkérdőjelezhető "gyilkos" döntéseket hozhatnak, és a parancsnoki láncban lévő emberek nem tudnak, hogy miért.²⁴⁵

[Az [autonóm] rendszerek hatékonyságát korlátozza, hogy az ember jelenleg képtelen megmagyarázni döntéseiket és cselekedeteiket az emberi felhasználóknak ... A megmagyarázható mesterséges intelligencia - különösen a megmagyarázható gépi

²⁴² Lásd Shaw, *fenti* megjegyzés 5.

²⁴³ Lásd George Dvorsky, *Why We'll Eventually Want Our Robots to Deceive Us*, GIZMODO (2017. október 4.), <https://gizmodo.com/why-well-eventually-want-our-robots-to-deceive-us-1819114004>. A robotok akár egymásnak is hazudhatnak, ha ez valamilyen előnyt eredményezne; Bill Christensen, *Robots Learn to Lie*, LIVE SCIENCE (200924., aug.), <https://www.livescience.com/10574-robots-learn-lie.html>.

²⁴⁴ John Naughton, *Magical Thinking About Machine Learning Won't Bring The Reality of AI Any Closer*, GUARDIAN (2018. augusztus 5.), <https://www.theguardian.com/commentisfree/2018/aug/05/magical-thinking-about-machine-learning-will-not-bring-artificial-intelligence-any-closer>. Lásd még Steven Strogatz, *One Giant Step for a Chess-Playing Machine*, N.Y. TIMES (2018. dec. 26.), <https://www.nytimes.com/2018/12/26/science/chess-artificial-intelligence.html> ("Ami azonban frusztráló a gépi tanulással kapcsolatban, az az, hogy az algoritmusok nem tudják megfogalmazni, mit gondolnak. Nem tudjuk, miért működnek, így azt sem tudjuk, hogy megbízhatunk-e bennük.").

²⁴⁵ Lásd David Gunning, *Explainable Artificial Intelligence (XAI)*, <https://www.darpa.mil/program/explainable-artificial-intelligence>.

a tanulás - elengedhetetlen lesz ahhoz, hogy a jövő harcosai megértsék, megfelelően megbízzanak és hatékonyan irányítsák a mesterségesen intelligens gépi partnerek új generációját.²⁴⁶

A mesterséges intelligencia átláthatatlan eredményeit a "fekete doboz" algoritmusok rejtik el. Mivel gyakran nem tudjuk, hogyan jutott egy mesterséges intelligenciával működő gép egy adott ~~követke~~ ^{következtetésre}, nem tudjuk ellenőrizni, hogy a következtetés megfelel-e a jogi és társadalmi normáknak, legyen szó akár a hadi törvényekről vagy az alkotmányos jogokról. Ha egy gép diszkriminatív eredményt ad vissza, mondjuk az ítélethozatal vagy a nyugdíjkockázat minősítése során, mit jelentene megkérdezni, hogy ez az eredmény "szándékos" volt-e? Honnan tudhatnánk, hogy az eredmény önkényes vagy a tisztességes eljárás értelmében vett rosszindulatú volt-e? A szándékosság és a tisztességes eljárás mint jogi elvek többnyire összeegyeztethetetlenek a mesterséges intelligenciával. A probléma tovább fokozódik, ha a mesterséges intelligenciának egyre több feladatot és ezáltal egyre nagyobb hatalmat adunk, ami végső soron a "robot általi törvényhozáshoz" vezethet.²⁴⁷ A kockázatok ellenére már most is arra kérnek bennünket, hogy bízzunk a szövetségi ügynökségek²⁴⁸ mesterséges intelligenciával hozott döntéseiben és a bíróságokon az AI által generált bizonyítékokban.²⁴⁹ Egyesek szerint a mesterséges intelligencia fejlesztésének végső célja, hogy "megszabaduljunk az emberi intuíciótól".²⁵⁰

További kihívást jelent, hogy a bírák és a kormányzati szervek nem írják az általuk használt mesterséges intelligencia programokat. Inkább licencelik azokat a dí- vátusgyártóktól. A már képzett mesterséges intelligencia vagy a hozzá kapcsolódó

²⁴⁶ *Id.*

²⁴⁷ Gary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 GEO. L.J. 1147, 1147 (2017) (annak vizsgálata, hogy a robotizált döntéshozatali eszközök, például a kockázateértékelő algoritmusok jelenlegi és jövőbeli használata (law by robot) megállja-e a helyét a közigazgatási vagy alkotmányjogban).

²⁴⁸ *Id.* A Stanford Law School új gyakorlatot tart "Administering by AI- gorithm: Artificial Intelligence in the Regulatory State." <https://law.stanford.edu/education/only-at-sls/law-policy-lab/practicums-2018-2019/administering-by-algorithm-artificial-intelligence-in-the-regulatory-state>.

²⁴⁹ Andrea Roth, *Machine Testimony*, YALE 126 L.J. 2021-221972, (2017). Hasonló problémák merülnek fel a "törvényszéki robotokkal", amelyeket egyre gyakrabban használnak bizonyítékgyűjtésre érzékeny helyzetekben, például gyermekbántalmazási ügyekben. Egy robot ebben a kontextusban lehet, hogy jobb, mint egy ember, de tud-e szakértői tanúvallomást tenni? *Lásd* Zachary Henkel & Cindy L. Bethel, *A Robot Forensic Interviewer*, J. HUMAN- ROBOT INTERACTIONS (2017).

²⁵⁰ John Bohannon, *A kibertudós*, SCI357. 18, 18-19 (2018).

"átvitt tanulási" technikák fokozzák az átláthatatlansági problémákat. Az ügynökségek nem csak az általuk használt termékek működésének és következtetéseinek átláthatóságát nem ismerik, hanem a mögöttes adatok tulajdonjogát és a hozzájuk való hozzáférést sem. A Legfelsőbb Bíróság megnehezítette a szoftverek szabadalmaztatását, így a fejlesztők általában kereskedelmi titkokhoz folyamodnak, hogy megőrizzék a mesterséges intelligencia befektetéseik értékét.²⁵¹ Így a cégek még az alkotmányos kihívásokkal szemben is vonakodnak a részletek nyilvánosságra hozatalától.²⁵² Mégis, nincsenek szövetségi jogi normák vagy követelmények az algoritmusok vagy "fekete doboz" döntéseik vizsgálatára. A 2016-os Defend Trade Secrets Act további muníciót²⁵³ ad a fejlesztőknek, hogy ellenálljanak forráskódjuk nyilvánosságra hozatalának.²⁵⁴

Az ebből eredő átláthatóság hiánya valós következményekkel jár. Az *Állam kontra Loomis* ügyben Eric Loomis vádlottat bűnösnek találták egy autós lövöldözésben való részvételéért.²⁵⁵ Loomis egy sor kérdésre adott válaszait bevitték a COMPAS-ba, egy kockázatértékelő eszközbe, amelyet egy profitorientált cég, a Northpointe hozott létre, és²⁵⁶ amely "magas kockázatú" visszaesési pontszámot adott ki számára.²⁵⁷ Loomis fellebbezett, különösen azért támadta meg az ítéletét, mert nem kapott lehetőséget az algoritmus értékelésére.²⁵⁸ A Wisconsin Legfelsőbb Bíróság elutasította Loomis keresetét, azzal az érveléssel, hogy a *Wired* beszámolója szerint "az algoritmus eredményének ismerete elegendő szintű átláthatóságot jelent".²⁵⁹ A bíróság azt is kimondta, hogy az ügyben eljáró emberi bíró elfogadhatta vagy

²⁵¹ Lásd *Alice Corp. kontra CLS Bank Int'l*, U573.S. (2014).

²⁵² Lásd *pl.*, *People v. Billy Ray Johnson*, No. F071640 (Cal. App. függőben, 2018) (megtámadta a hozzáférést egy szabadalmaztatott DNS-illesztési algoritmushoz, a TrueAllele-hez való hozzáférés hiánya miatt, amely értékeli annak valószínűségét, hogy egy gyanúsított DNS-e jelen van egy bűncselekmény helyszínén).

²⁵³ 18 U.S.C. § et 1836, seq.

²⁵⁴ Lásd *pl.* *Video Gaming Techs, Inc. kontra Castle Hill Studios LLC*, 2018 U.S. Dis. Lexis 118919 (a DTSA alkalmazása a védett algoritmus védelmére, amikor az állami üzleti titokra vonatkozó törvény nem volt megfelelő).

²⁵⁵ *State v. Loomis*, N881.W.2d (749Wis. 2016).

²⁵⁶ Lásd a *COMPAS kockázat- és szükségletértékelő rendszert*:

NORTHPOINTE (2012), http://www.northpointe-inc.com/files/downloads/FAQ_Document.pdf.

²⁵⁷ Lásd *Loomis*, N881.W.2d, N.W.2d at 749755.

²⁵⁸ Lásd *id.* 753.

²⁵⁹ Jason Tashea, *A bíróságok mesterséges intelligenciát használnak a bűnözők elítélésére. That Must Stop Now*, WIRED (április 7:17, 2017, 00), <https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-most>.

elutasítja a Compas pontszámot, tehát a mesterséges intelligencia algoritmusai valójában nem a mondat meghatározását végezték, csak javasolták azt.²⁶⁰

A mesterséges intelligencia elterjedésével a jogi formalizmushoz való további folyamodásra számíthatunk. Egyre több állam alkalmazza a COMPAS-t vagy hasonló algoritmusokat az óvadékkal, büntetékiszabással és feltételes szabadságra helyezéssel kapcsolatos döntésekhez.²⁶¹ Továbbá, még a jó szándékú óvadék- és büntetékiszabási reformoknak is lehetnek káros hatásai, ha a mesterséges intelligenciát is bevonják.²⁶²

Egyes támogatók a mesterséges intelligencia alkalmazását azzal indokolják, hogy így következetesebb eredményeket lehet elérni, és a büntető igazságszolgáltatási rendszer erőforrásait lehet kímélni.²⁶³ Ez így is van. De kimutathatóan diszkriminatív eredményeket is produkál. A Pro Publica által végzett tanulmány szerint a mesterséges intelligencia által generált visszaesési pontszámok Floridában "feltűnően megbízhatatlannak bizonyultak az erőszakos bűncselekmények előrejelzésében", és csak "valamivel pontosabbak voltak, mint egy pénzfeldobás".²⁶⁴ Az algoritmus "különösen valószínűsítette, hogy a fekete vádlottakat tévesen jövőbeli bűnözőnek minősítette, majdnem kétszer olyan gyakran tévesztette meg őket, mint a fehér vádlottakat".²⁶⁵ Ez nem csak az egyenlőségi elveket sérti, de az, hogy sem a bírák, sem a vádlottak nem tudnak betekinteni az ajánlott eredmények "fekete dobozába", a tisztességes eljárást is veszélyezteti.²⁶⁶

²⁶⁰ *Lásd a Loomis*, 881 N.W.2d 749, 753. o., magyarázat. Az alsóbb fokú bíróság megjegyezte, hogy a wisconsini bírák rutinszerűen támaszkodnak a COMPAS-ra az ítélethozatal során, és ezt tették Loomis esetében is. *State v. Loomis*, Wisc2015. App. LEXIS 722, *2 (2015).

²⁶¹ EPIC, *Algorithms in the Criminal Justice System*, <https://epic.org/algorithmic-transparency/crim-justice>.

²⁶² *Lásd Sam Levin, Az algoritmusok fogságában: The Dark Side of California Ending Cash Bail*, GUARDIAN (2018. szeptember 7.), <https://www.theguardian.com/us-news/2018/sep/07/imprisoned-by-algorithms-the-dark-side-of-california-ending-cash-bail> (egy kaliforniai törvényről szól, amely a készpénzes óvadékot "kockázatértékelési" eszközökkel váltotta fel, de féltő volt, hogy lehetővé teszi a tárgyalás előtti bebörtönzés növekedését). ²⁶³ *Id.*

²⁶⁴ Julia Angwin et al., *Machine Bias*, PROPUBLICA (201623., május).

²⁶⁵ *Id.*

²⁶⁶ Tashea, *Supra* note 259.

2. Algoritmikus torzítás

Az objektivitás nem tartozik a mesterséges intelligencia erényei közé. Az algoritmusok inkább visszatükrözik az elfogultságokat a modellek de- signalásakor bevitt programozásban és a képzésükhöz használt adatokban. Továbbá, bár az adatelemzés képes a viselkedés és más ~~való~~ közötti kapcsolatok azonosítására, a kapcsolatok nem mindig utalnak az ok-okozati összefüggésekre. Ezért egyes adatelemzések az algoritmikus korlátozások vagy az elfogult mintavételezés miatt tökéletlen információkat fejleszthetnek ki. Ennek eredményeképpen a mesterséges intelligencia által hozott döntések a közkeletű elképzeléssel ellentétben inkább fokozhatják, mintsem megszüntethetik az emberi elfogultságokat.²⁶⁷ Ez valós kockázatot jelent az egyenlőségre és a demokráciára nézve.

Az "algoritmikus elfogultság" fő problémája az az adat, amelyet a mesterséges intelligencia problémamegoldásának "betanítására" használnak. A jogi kontextusban jellemzően a valós világból származó tényezőket - például a bírósági véleményekben közöltek - táplálják a számítógépbe, valamint a jogalkalmazás tényállásra való alkalmazását leíró doktrinális szabályokat. A mesterséges intelligencia valószínűleg az első, de talán a századik próbálkozásnál is rossz választ ad (a gyakorló eset eredményéhez képest). A gépi tanulásnak köszönhetően azonban a mesterséges intelligencia addig alakítja algoritmusait, amíg végül megtalálja azokat, amelyek az esetek többségében vagy minden esetben ugyanazt az eredményt adják vissza, mint a gyakorló esetek. A képzési adatok azonban önmagukban is lehetnek elfogultak, ami egyszerűen felerősödik, amint a mesterséges intelligenciát új tényekre engedik rá. Így például, ha a büntetőítéletek vagy a bűnügyi statisztikák korábbi adatai faji alapon elfogultak, akkor a mesterséges intelligencia is az lesz minden alkalommal, amikor az adatok alapján ajánlást tesznek egy ítéletre. Az AI pontatlan vagy elfogult adatokkal való kiképzésének kockázatai a Microsoft Tay, a "tizenévesek beszélgető AI chatbotjának" példáján is jól láthatóak, amelyet arra építettek, hogy valós időben utánozza a felhasználókat és beszélgessen velük.²⁶⁸ A Tay gépi tanulási képességeinek köszönhetően néhány órán belül rasszista és diszkriminatív tweeteket tett.²⁶⁹ Nem úgy tervezték, hogy emberpróbáló legyen, és blokkolja a rosszindulatú szándékot. Ahogy a

²⁶⁷ Justin Sherman, *AI And Machine Learning Bias Has Dangerous Implications*, OPEN-SOURCE (2018. január 11.), <https://opensource.com/article/18/1/how-open-source-can-fight-algorithmic-bias> (mondván, hogy "az adatoknak önmagukban is lehet egy ferde eloszlása").

²⁶⁸ Sophie Kleeman, *Here Are the Microsoft Twitter Bot's Craziest Racist Rants*, GIZMODO (2016. március 24.), <https://gizmodo.com/here-are-the-microsoft->

twitter- bot-s-craziest-racist-ra-1766820160.

²⁶⁹ *Id.*

Tay azt mutatja, hogy a mesterséges intelligencia funkciói tükrözhetik és felerősíthetik a társadalmi előítéleteket és gyengeségeket, csak a pártatlanság látszatát keltve.²⁷⁰

Nemcsak a képzési adatok gyakran elfogultak, hanem a nagyobb adathalmazok is, amelyeket később a mesterséges intelligencia eredményeinek előállításához használnak. A bemeneti adatokat vagy emberek, vagy emberek által tervezett érzékelők generálják. Az adatok kiválasztása, értelmezése és a módszertanok szintén emberi eredetűek, és tükrözhetik az emberi elfogultságokat. Így a "hibák - etikai vagy metodológiai - a nagyméretű adatok gyűjtésében és felhasználásában megismételhetik a társadalmi egyenlőtlenségeket".²⁷¹ Az algoritmusok szubjektív döntéseket hoznak, beleértve az "osztályozást, rangsorolást, asszociációt és szűrést".
átalakítják az információt, és társadalmi következményeik vannak."²⁷²

Az automatikus osztályozásról ismert, hogy diszkriminatív eredményeket hoz. Erre példa a képek mesterséges intelligenciával történő osztályozása, amely az arcfelismerő szoftverekben fordul elő. Gyakran nem ismeri fel a sötét bőrűeket, vagy akár gorillának minősíti a fekete bőrű alanyokat.²⁷³ Egy másik példa a Google kereső algoritmus, amely a foglalkozási nemi sztereotípiákat tükröző eredményeket ad vissza.²⁷⁴ Az automatikus kitöltő algoritmus negatív faji sztereotípiákkal kapcsolatos javaslatokat is előhívhat.²⁷⁵ Hasonló eredmények akkor fordulnak elő, ha a képzési adatok túlságosan fehér férfiakat, és alulmintázzák a nőket és a hatalmi pozícióban lévő kisebbségeket, vagy

²⁷⁰ Lásd: Glen Meyerowitz, *There Is Nothing Either Good or Bad, But Training Sets Make It So*, J2. ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW 20-2217, (2019).

(2019). A képzési adatokat a kibertámadók is "beszennyezhetik", ha hamis adatokat vezetnek be egy "ellenséges gépi tanulás" néven ismert technikával. Lásd: *The National Artificial Intelligence Research and Development Strategic Plan*, NAT'L SCI. & TECH. COUNCIL 30 (2016. okt.), https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf.

²⁷¹ Shorey & Howard, *fenti* megjegyzés. 231.

²⁷² *Id.*

²⁷³ Lásd Conor Dougherty, *Google Photos Mistakenly Labels Black People 'Gorillas'*, N.Y. TIMES (2015. július 1., 19:01), <https://bits.blogs.nytimes.com/2015/07/01/google-photos-mistakenly-labels-black-people-gorillas>.

²⁷⁴ Matthew Kay, Cynthia Matuszek & Sean A. Munson, *Unequal Representation and Gender Stereotypes in Image Search Results for Occupations*, in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (2015), <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.697.9973&rep=rep1&type=pdf>.

²⁷⁵ Issie Lapowsky, *Google Autocomplete Still Makes Vile Suggestions*, WIRED (2018. február 12., 11:09), <https://www.wired.com/story/google-autocomplete-vile-suggestions>.

states/x/724056/new+technology/The+content+of+this+this+article+is+is+in-
tended+to+provide+a+general+guide; lásd még az alábbi jegyzetben. 393.
²⁸⁰ Christopher Fonzobe & Kate Heinzelman, *Should the Government Regulate
Artificial Intelligence? It Already Is*, THE HILL (febr. 1226,2018,:00),

Az első a magánélethez fűződő érdekek és a demokratikus ~~élet~~ megfelelő védelme. A második a mesterséges intelligencia által előidézett egyedi kihívások elismerése. Több mint harminc év telt el azóta, hogy a Kongresszus utoljára elfogadott egy jelentős adatvédelmi törvényt.²⁸¹ Ha ilyen sokáig tart a mesterséges intelligencia kihívásainak kezelése, akkor a világ valószínűleg egészen más lesz, mire a kongresszus eljut a cselekvésig. Ez a szakasz az Egyesült Államok jelenlegi szabályozási keretét vizsgálja, és azt, hogy miben különbözik az európai jogtól. A fejezet végén javaslatokat tesz a szabályozás korszerűsítésére, hogy az megfeleljen a mesterséges intelligencia kihívásainak.

A. Az Egyesült Államokban az adatvédelem zűrzavaros rendszere

Az Egyesült Államok ad otthont a világ legnagyobb és legfejlettebb technológiai és adatszolgáltató vállalatainak. A tudósok a nemzetközi piacon való dominanciájukat annak tulajdonítják, hogy nincs átfogó szövetségi szabályozás a személyes adatok és az információs magánélet védelmére. Ehelyett az Egyesült Államok az "ágazati megközelítésre" támaszkodik, amely iparág-specifikus szövetségi törvények sokaságából áll, amelyeket gyakran különböző ügynökségek hajtanak végre, és amelyek különböző szabványokat írnak elő.²⁸² Ezeket egészítik ki az állami adatvédelmi törvények, az önszabályozó iránymutatások és az általános célú fogyasztóvédelmi törvények.²⁸³

Ezzel szemben az Európai Unió (EU) és számos más fejlett ország az átfogó megközelítést követi, és egyetlen törvény szabályozza az adatgyűjtést, -felhasználást és -megosztást következetesen az összes iparágban. Például az EU általános adatvédelmi rendelete (GDPR) egy ²⁸⁴olyan átfogó szabályozás, amely az ágazatok és a tagállamok között minden, az EU-ban "letelepedett", árukat vagy szolgáltatásokat kínáló szervezetre vonatkozik.

<http://thehill.com/opinion/technology/375606-should-the-government-regulate-mesterséges-intelligencia-már-már-van>.

²⁸¹ Lásd az 1986. évi elektronikus hírközlési adatvédelmi törvényt (ECPA), 18 U.S.C. §2 510-22.

²⁸² Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACH PRIVACY (2015. november 13.), <https://teachprivacy.com/problems-sectoral-approach-privacy-law>.

²⁸³ Lásd *id.*

²⁸⁴ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról.

az EU-ban, vagy az EU-ban élő emberek megfigyelése.²⁸⁵ Ez utóbbiak valós lehetőséggé teszik a területen kívüli alkalmazást és végrehajtást az amerikai vállalatokkal szemben.

Sok amerikai vállalkozás kezdetben az ágazati megközelítést részesítette előnyben, mivel így a szabályozást a saját árnyalt igényeikhez igazíthatták. Bár van némi ~~lyuk~~ ^{lyuk} a modellnek, ugyanakkor megkönnyíti a szabályozás megragadását, az iparági lobbyingt és a magánélet védelmével való visszaéléseket, amelyek gyakran átesnek a szabályozási résen. Az ágazati megközelítés az állami és szövetségi törvények "átfedő, egymásba fonódó és egymásnak ellentmondó" foltos rendszerét hozta létre.²⁸⁶

A legfontosabb szövetségi törvények közé tartoznak: HIPAA (személyesen azonosítható egészségügyi információk),²⁸⁷ GLBA (pénzügyi információk),²⁸⁸ a telefonos fogyasztóvédelmi törvény (TCPA) (távmarketing),²⁸⁹ a CAN-SPAM törvény (spam e-mailek),²⁹⁰ a számítógépes csalásról és visszaélésekről szóló törvény (CFAA) (hackelés)²⁹¹ és az ECPA (elektronikus kommunikáció).²⁹² Mindegyik törvényt más-más ügynökség vagy állami szerv hajtja végre. Ilyen szétszórt rendszer mellett nehéz koherens adatvédelmi politikát kialakítani.

A közelmúltban az államok a Cambridge Analyticára reagálva elkezdtek saját adatvédelmi szabályozásaik bevezetését, hogy lakosaiknak fokozott adatvédelemben részesítsék a magánéletet, és kiegészítsék a szövetségi törvények hiányosságait.²⁹³ Ez tovább bonyolítja a szövetségi és a meglévő állami szabályozások patchwork rendszerét, amelynek a technológiai vállalatoknak meg kell felelniük. Ennek eredményeképpen a technológiai vállalatok most először kezdtek lobbizni a következőkért

²⁸⁵ *Id.* art. III.

²⁸⁶ Ieuan Jolly, *Adatvédelem az Egyesült Államokban: THOMAS REUTERS PRACTICAL LAW* (2017. július 1.), <https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbec/View/FullText.html>.

²⁸⁷ 42 U.S.C. §1301 et seq.

²⁸⁸ 15 U.S.C. §§6801-6827.

²⁸⁹ 47 U.S.C. §227 et seq.

²⁹⁰ 15 U.S.C. §§7701-7713 és 18 U.S.C. §1037.

²⁹¹ 18 U.S.C. §1030.

²⁹² 18 U.S.C. §2510.

²⁹³ *Lásd* Neema Singh Guliani, *The Tech Industry is Suddenly Pushing for Federal Privacy Legislation. Watch Out.*, WASH. POST (2018. október 3.), https://www.washingtonpost.com/opinions/the-tech-industry-is-suddenly-pushing-for-federal-privacy-legislation-watch-out/2018/10/03/19bc473e-c685-11e8-9158-09630a6d8725_story.html.

a szövetségi törvényhozás az olyan állami törvények, mint a kaliforniai Consumer Privacy Act (CCPA), elsőbbséget élveznek.

1. Állami adatvédelmi törvények

Az állami törvények gyakran kitöltik a szövetségi törvények által hagyott lyukakat, de ez tovább növeli az adatvédelmi törvények foltozottságát, különösen az adatvédelmi incidensek bejelentésére vonatkozó törvények esetében. Valamennyi állam előírja, hogy az egyéneket értesíteni kell, ha - általában kibertámadás következtében - veszélybe kerültek az adataik, de az állami törvények gyakran eltérő és összeegyeztethetetlen követelményeket tartalmaznak.²⁹⁴ Például "New Jersey megköveteli, hogy az állami rendőrség kiberbűnözéssel foglalkozó egységét értesítsék a jogsértésről, míg Maryland megköveteli, hogy az állam főügyészét értesítsék, mielőtt bármely érintett személyt értesítenének".²⁹⁵ Illinois sok más állammal ellentétben a biometrikus adatokat "személyes információnak" tekinti, amely a jogsértésről való értesítést váltja ki.²⁹⁶ Kalifornia "szégyenfala" a lakosokat érintő összes kibernetikai jogsértést katalogizálja.²⁹⁷ Ez jelzi, hogy a probléma mennyire súlyos, nemcsak az egyének, hanem a vállalkozások számára is, amelyeknek meg kell felelniük az állami és szövetségi törvények szmorgasbordájának. Az adatvédelmi szabályok betartása új, teljes munkaidős munkalehetőséget jelenthet a jogászok számára.

A 2003. évi kaliforniai online adatvédelmi törvény (CalOPPA) előírja, hogy a "személyes adatokat" (PII) gyűjtő online szolgáltatások üzemeltetői kötelesek olyan adatvédelmi irányelveket közzétenni, amelyek a következőket tartalmazzák: mit

²⁹⁴ Lásd: *Security Breach Notification Laws*, NAT'L CONF. ST. LEGIS. (2018. szeptember 29.), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

²⁹⁵ Dana B. Rosenfeld et al. *State Data Breach Laws Agency Notice Requirement Chart: Overview*, THOMSON REUTERS (2019), <https://1.next.westlaw.com/Document/I1559f980eef211e28578f7ccc38dcbee/View/FullText.html>.

²⁹⁶ A biometrikus adatok védelméről szóló törvény, ILL740. COMP. STAT. ANN. 14/10 (2008).

²⁹⁷ Lásd Xavier Becerra, főállamügyész, *Adatbiztonság megsértésének keresése*, STATE OF CA. DEPT. OF JUSTICE, <https://www.oag.ca.gov/privacy/databreach/list> (utolsó látogatás 2018. aug.).

az általuk gyűjtött adatokat, hogy kivel osztják meg azokat, hogyan lehet a PII-t újra megtekinteni vagy módosítását kérni, és hogyan értesítik a felhasználókat a szabályzat változásáról.²⁹⁸

Kalifornia gazdasági jelentősége és az e-kereskedelem határok nélküli világa miatt e jogszabály hatása túllép az államhatárokon, és minden technológiai vállalatot arra kényszerít, hogy megfeleljen a jogszabályoknak. A probléma az, hogy senki sem olvassa vagy érti a technikai jogi szakszöveget, amelyet az adatvédelmi irányelvek és a szolgáltatási feltételek tartalmaznak. A Carnegie Mellon kutatói szerint napi 8 órával számolva 76 napba telne elolvasni az összes adatvédelmi szabályzatot, amellyel az ember általában találkozik.²⁹⁹

A CalOPPA-t az újonnan elfogadott kaliforniai adatvédelmi törvény (California Consumer Privacy Act, CCPA) egészíti ki.³⁰⁰ Ez az ország legkiterjedtebb adatvédelmi rendszere, és hasonlít az európai mindenre kiterjedő megközelítéshez.³⁰¹ Olyan adattípusokat is véd, amelyek korábban nem élveztek védelmet a Az Egyesült Államok adatvédelmi törvényei, például a vásárlási előzmények, a böngészési és keresési előzmények, valamint a személyes adatokból levont következtetések.³⁰² A CCPA négy egyéni jogot teremt, amelyek a kaliforniai lakosok számára nagyobb ellenőrzést biztosítanak adataik felett, beleértve a törléshez, az adataikról való tájékoztatáshoz és másolatokhoz való jogot, a lemondáshoz való jogot és a diszkriminációtól való mentességet. A CCPA végrehajtása a kaliforniai főügyész által indított végrehajtási eljárások vagy korlátozott magánjogi keresetek útján történhet.³⁰³

²⁹⁸ Lásd Kamala D. Harris, *Making Your Privacy Practices Public*, STATE OF CA. DEPT. OF JUSTICE 1 (2014. május), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.

²⁹⁹ Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (2012. március 1.), <https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days>.

³⁰⁰ CAL. CIV. CODE §§ 1798.100-1798.198 (2018).

³⁰¹ Számos állam fontolgatja a kaliforniai CCPA lemásolását. Lásd Davis Wright, *"Copycat CCPA" Bills Introduced in States Across Country*, JD SUPRA (Feb. 2019), <https://www.jdsupra.com/legalnews/copycat-ccpa-bills-introduced-in-states-20533>.

³⁰² CAL. CIV. CODE § 1798.140(o)(1)(1). A személyes adatok tágan értelmezett fogalma minden olyan információt magában foglal, amely "kapcsolatba hozható" egy kaliforniai lakossal, háztartással vagy eszközzel. *Id.* A meghatározás vitathatóan tágabb, mint a GDPR szerinti "személyes adatok".

³⁰³ CAL. CIV. CODE § 1798.160.

A közelmúltban Kalifornia az IoT-t és a chatbotokat szabályozó törvények elfogadásával fokozta az adatvédelmi és kiberbiztonsági törvények szigorát. 2020. január 1-jei hatállyal az IoT- vagy intelligens eszközök gyártóinak ésszerű biztonsági funkciókat kell bevezetniük, amelyek megakadályozzák a jogosulatlan hozzáférést, az információk nyilvánosságra hozatalát³⁰⁴ vagy módosítását.³⁰⁵ Továbbá, 2019. július 1-jei hatállyal a chatbotoknak azonosítaniuk kell magukat, és nem adhatják ki magukat valódi személynek.³⁰⁶ A felhasználók valószínűleg látni fogják ezeket a kitételeket a chat- botokat használó márkák Facebook-profiljaiban és Twitter-életrajzaiban. A törvény tiltja a chatbotok számára az áruk és szolgáltatások vásárlására vagy eladására való ösztönzést és a választási szavazatok befolyásolását.³⁰⁷ Az állami és szövetségi adatvédelmi törvények sokasága ellenére a vállalatok továbbra is szabadon használhatják a mesterséges intelligenciát felhasználói profilok létrehozására, a felhasználói viselkedés nyomon követésére és egyéb belső célokra.

2. Önszabályozás és ágazati gyakorlatok

Az állami és szövetségi törvények mellett az iparági szövetségek és a kormányzati szervek is kidolgozzák az adatkezelésre és - irányításra vonatkozó irányelveket és elfogadott iparági álláspontokat. Ezek az iránymutatások nem jogszabályok, hanem az önszabályozási keretrendszer részét képezik, és "legjobb gyakorlatnak" számítanak. Az önszabályozási keretnek vannak olyan elszámoltathatósági és végrehajtási elemei, amelyeket a szabályozók egyre inkább eszközként használnak. Az önszabályozás mostantól lehetővé teszi a technológiai vállalatok számára, hogy olyan szabványokat és eljárásokat hozzanak létre, amelyek remélhetőleg már a kialakításuk során figyelembe veszik az adatvédelmi szempontokat (azaz a "privacy by design").

Az FTC arra ösztönzi a technológiai vállalatokat és az iparági szövetségeket, hogy dolgozzanak ki "iparág-specifikus magatartási kódexeket".³⁰⁸ Az egyik iparági csoport

³⁰⁴ A tájékoztatásnak "egyértelműnek, szembetűnőnek és ésszerűen kialakítottnak" kell lennie. Id.

³⁰⁵ Adi Robertson, *California Just Became the First State with an Internet of Things Cybersecurity Law*, THE VERGE (2018. szeptember 28.), <https://www.the-verge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law>.

³⁰⁶ Adam Smith, *California Law Bans Bots from Pretending to be Human*, PCMAG (2018. október 2.), <https://www.pcmag.com/news/364132/california-law-bans-bots-from-pretending-to-be-human>.

³⁰⁷ Id.

³⁰⁸ Federal Trade Commission, *FTC Issues Final Commission Report on Pro-*

Protecting Consumer Privacy, (2012. március), <https://www.ftc.gov/news->

a nagyobb adatvédelem előmozdítását segíti a Digital Advertising Alliance (DAA), a vezető iparági szövetségek koalíciója.³⁰⁹ Ezek a szövetségek általában tagságot kínálnak a kapcsolódó funkciókban részt vevő szervezeteknek. Ha a szövetségek értesítést kapnak arról, hogy a szervezetek nem felelnek meg a "legjobb gyakorlatoknak" és iránymutatásoknak, a szövetség együttműködik a szervezetekkel a megfelelés érdekében. Ha azonban a szervezet nem felel meg, az egyetlen következmény a további tagsági lehetőségek megtagadása.³¹⁰ Ezért a vállalatoknak a tagság elvesztésén kívül nincs más kényszerítő erejű ösztönzője az előírások betartására.

B. Európai adatvédelmi jog

Az Egyesült Államok szabályozási rendszerével ellentétben az Európai Unió 2018. májusában hatályba lépő általános adatvédelmi rendelete (GDPR) komolyan harapós. A jogsértők akár húszmillió euróig terjedő közigazgatási bírságot vagy a vállalat világméretű éves bevételének négy százalékát kockáztatják, attól függően, hogy melyik a nagyobb.³¹¹ Ennek eredményeként az olyan technológiai óriások, mint a Google, a GDPR szerinti szankciók miatt kénytelenek voltak változtatni a viselkedésükön.³¹²

Az Egyesült Államok és az EU magánélethez való hozzáállása közötti különbség ~~és~~ Európa második világháborús tapasztalatainak köszönhető. A háború után és az Egyesült Nemzetek Szervezetének létrehozásával számos ország felismerte, hogy az emberi jogok

events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

³⁰⁹ *Digital Advertising Regulation 101*, INTERACTIVE ADVERTISING BUREAU (2014. február), <https://www.iab.com/news/digital-advertising-regulation-101/#4>.

³¹⁰ *Id.*

³¹¹ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (GDPR).

³¹² A francia adatvédelmi hatóság 57 millió dolláros bírságot szabott ki a Google-ra, mert nem tette közzé, hogyan gyűjti a vállalat a személyes adatokat, és hogyan használja fel azokat. Tony Romm, *France Bines Google Nearly \$57 million for First Major Violation of New European Privacy Regime*, WASH. POST (Jan 21, 2019), https://www.washingtonpost.com/world/europe/france-fines-google-nearly-57-million-for-first-major-violation-of-new-european-privacy-regime/2019/01/21/89e7ee08-1d8f-11e9-a759-2b8541bbbe20_story.html?noredirect=on&utm_term=.0655a1c68c11.

felismerte, hogy az alapvető emberi jogokat védeni kell a demokratikus intézmények támogatása érdekében.³¹³ 1948-ban az Emberi Jogok Egyetemes Nyilatkozatának (UDHR) 12. cikke olyan elveket fogalmazott meg, amelyek a magánéletet alapvető emberi jogként tartják számon.³¹⁴ A 19. cikk széles körű védelmet biztosít a kapcsolódó szólásszabadságok számára.³¹⁵ Az ENSZ chartája és az UDHR inkább csak ajánlás, mint kötelező erejű jog, legalábbis az Egyesült Államokban.³¹⁶ Az Európa Tanács, az Európa mind a negyvenhét nemzetét tömörítő szerződéses szervezet azonban az Emberi Jogok Európai Egyezményével (EJEE) folytatta,³¹⁷ amely Európán belül kötelező érvényű jog. A magánélethez való jog és a véleménynyilvánítás szabadsága közötti egyensúlyozás visszatérő téma az európai adatvédelmi jogban.³¹⁸

Az eltérő hozzáállás eredményeként az EU-ban olyan adatvédelmi védelem áll rendelkezésre, amely az Egyesült Államokban nem áll rendelkezésre.³¹⁹ Például a személyes adatok nem oszthatók meg határokon átnyúlóan az érintett kifejezett hozzájárulása nélkül.³²⁰ Az EU a GDPR-t olyan ~~erővel~~ dolgozta ki, amely közvetlenül kötelező érvényű az összes tagállamra nézve.³²¹ A cél egy koherens adatvédelmi keretrendszer létrehozása volt, erős végrehajtással és az egyének jogainak megerősítésével.³²² Azáltal, hogy az egyéneknek nagyobb ellenőrzést biztosít az adataik felett, a GDPR bizalmat teremt a digitális

³¹³ Mark Rotenberg, *A nemzetközi magánéletről: A Path Forward for US and Europe*, HARV. INT'L REV. (2014. június 15.), <http://hir.harvard.edu/article/?a=5815>. ³¹⁴ UDHR 12. cikk: "Senkit sem lehet kitenni a magánéletébe, családjába, otthonába vagy levelezésébe való önkényes beavatkozásnak, sem a becsületét és jó hírnevét ért támadásoknak. Mindenkinnek joga van a törvény védelméhez az ilyen beavatkozással vagy támadással szemben."

³¹⁵ UDHR 19. cikk.

³¹⁶ Medellin kontra Texas, Egyesült Államok (4912008).

³¹⁷ Eduardo Ustaran & Hogan Lovells, *Európai adatvédelem: Law and Practice* (SIAPP 2018), 5-6. o.

³¹⁸ UDHR Art. 29. cikk (2) bekezdése (amely megfogalmazza azt az elvet, hogy "jogai és szabadságai gyakorlása során mindenki csak olyan korlátozásoknak van alávetve, amelyeket a törvény kizárólag abból a célból határoz meg, hogy biztosítsa mások jogainak és szabadságainak megfelelő elismerését és tiszteletben tartását, valamint hogy megfeleljen az ~~adatok~~ a közrend és az általános jólét igazságos követelményeinek egy demokratikus társadalomban").

³¹⁹ Bob Sullivan, *'La Difference' Is Stark in EU, U.S. Privacy Laws*, MSN (2006. október 9.),

http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.XDGBhFxKhhE.

³²⁰ *Id.*

³²¹ USTARAN, *supra* note at 318- 1618.

³²² *Id.*

gazdaság és online környezet. Az ellenőrzés, az átláthatóság és a számonkérhetőség a GDPR egészét áthatja.

1. Ellenőrzés és beleegyezés

A GDPR az érintettek számára a korábbinál lényegesen nagyobb ellenőrzést biztosít az adataik felett.³²³ A rendelet ezt úgy éri el, hogy az érintettek számára számos jogot biztosít, ³²⁴többek között a tiltakozáshoz való jogot és azt a jogot, hogy ne legyenek automatizált döntéshozatal tárgyai.³²⁵ Ez a jog szűk körben érvényesül, ha a döntések kizárólag automatizált feldolgozáson alapulnak, és az érintettre nézve joghatásokat eredményeznek.³²⁶ "Mivel automatizált folyamatokról van szó, az AI-alkalmazások közvetlenül érintettek". További szabályozási iránymutatástól függően ez azt jelentheti, hogy a mesterséges intelligencia nem játszhat szerepet az ítélethozatalban, az óvadékkal, a feltételes szabadlábra helyezéssel kapcsolatos és egyéb bírósági döntésekben.³²⁷ Az érintettek jogosultak lennének emberi beavatkozásra vagy arra, hogy megtámadhassák a mesterséges intelligencia által hozott döntést.³²⁸ Az érintetteknek joguk van arra is, hogy indoklást kapjanak arról, hogy hogyan születnek az automatizált döntések.³²⁹ Ez problémát fog okozni az olyan összetett mesterséges intelligencia-algoritmusok esetében, amelyek esetében lehetetlen az érintetteknek magyarázatot adni arra, hogyan születnek ezek a döntések.³³⁰

³²³ A "személyes adatok" fogalom meghatározása szerint az érintettek "azonosított vagy azonosítható természetes személyek". Lásd GDPR Art. 4(1). Nem világos, hogy az EU-ban való lakóhely előfeltétele-e az adatvédelemnek. Lásd GDPR Art. 4(2).

³²⁴ Lásd GDPR Art. 12-22. Az érintettek jogai közé tartozik az átlátható kommunikációhoz és tájékoztatáshoz való jog (12-14. cikk), a hozzáférés joga (15. cikk), a helyesbítéshez való jog (16. cikk), a törléshez való jog (17. cikk), az adatkezelés korlátozásához való jog (18. cikk), a címzettek értesítésének kötelezettsége (19. cikk), az adathordozhatósághoz való jog (20. cikk), a tiltakozáshoz való jog (21. cikk), az automatizált döntéshozatal tilalmához való jog (22. cikk).

³²⁵ GDPR Art. & 2122.

³²⁶ USTARAN, *supra* note at 317,166.

³²⁷ *Id.* E kétértelműségektől függetlenül, ha a döntéshozatali folyamatokat e paramétereken belül vizsgáljuk, akkor az adatkezelés megengedett, ha "törvény által engedélyezett, szerződés előkészítéséhez és végrehajtásához szükséges, vagy az érintett kifejezett hozzájárulásával történik".

³²⁸ *Id.*

³²⁹ Mathias Avocats, *Artificial Intelligence and the GDPR: how do they interact?*, MATHIAS AVOCATS (2017. november 27.), <https://www.avocats-mathias.com/technologies-avancees/artificial-intelligence-gdpr>.

³³⁰ *Id.*

A technológiai vállalatok számára, különösen azok számára, amelyek AI-algoritmusokat alkalmaznak az adatok bányászására és összevonására, a hozzájárulást nem lehet egy kattintással, előre bepipált dobozokkal vagy inaktivitással összekötni, és nem lehet az áruk vagy szolgáltatások nyújtásához kötni. Ehelyett a beleegyezésnek olyan egyértelmű, határozott aktusnak kell lennie, amely jelzi, hogy a beleegyezést szabadon adta, a különböző folyamatokra vonatkozóan, és akkor kell megadnia, amikor a személy megértette az adatai felhasználásának teljes körét.

Amellett, hogy az érintettek széles körű jogokat kapnak, a GDPR nagyon magas követelményeket támaszt a "hozzájárulás" tekintetében is, amikor azt a vállalkozások a személyes adatok feldolgozásának indokaként használják. A vállalatoknak törvényes alapot vagy konkrét, jogos és kifejezett okot kell találniuk a személyes adatok feldolgozására.³³¹ A hozzájárulásra való hivatkozáshoz a vállalatoknak bizonyítaniuk kell, hogy az érintett hozzájárulása "szabadon, ~~korán~~ tájékozottan és egyértelműen jelezte az érintett hozzájárulását a személyes adatok feldolgozásához".³³² Egyszerűsítve, az EU a hozzájárulás "opt-in" megközelítését alkalmazza, ellentétben a legtöbb amerikai jogszabály szerinti "opt-out" hozzájárulással.

2. Átláthatóság és elszámoltathatóság

Az európai jog kifejezetten előírja, hogy a személyes adatok feldolgozása transzparens és tisztességes módon történjen.³³³ Az adatok váratlan módon történő újrafelhasználása a magánéletet fenyegető baljós és "hátborzongató" fenyegetésnek tűnhet, mivel a komplex algoritmusok olyan következtetéseket vonnak le az emberekről, amelyek nem kívánt és nemkívánatos hatásokkal járnak.³³⁴ Például egy orvosnő a

U.K.-t kizárták egy edzőterem öltözőjéből, amikor az automata biztonsági rendszer férfiként profilozta őt, mert a "dr." asszociáció miatt "dr." névvel illette.

³³¹ GDPR Art. 6. Az "adatkezelés" tágan meghatározott, és nincs minimális küszöbérték, beleértve, de nem kizárólagosan a személyes adatok automatikus gyűjtését, továbbítását vagy terjesztését. Lásd a GDPR 4. cikkét.

³³² GDPR (32) preambulumbekzdés. Lásd az adatvédelmi rendelet 3. cikkét. 7. Az érintettnek biztosítani kell a jogot arra is, hogy a hozzájárulását bármikor visszavonhassa.

³³³ GDPR Art. 5(1).

³³⁴ Information Commissioners Office, *Big Data, Artificial Intelligence, Machine Learning and Data Protection* 1, 19 (2017), <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.

férfiakkal.³³⁵ Ezek a fenyegetések átláthatatlan, megmagyarázhatatlan algoritmusokkal az egyenlőség és a méltányosság demokratikus értékeit is sértik. AGDPR értelmében a szervezeteknek figyelembe kell venniük, hogy az emberek milyen tájékoztatást kaptak adataik feldolgozásáról és annak lehetséges következményeiről. Általában az emberek az adatvédelmi irányelvekben és a szolgáltatási feltételekben kapnak tájékoztatást. Mivel az ilyen irányelvek hosszúak, terjedelmesek, és nem feltétlenül tartalmaznak elegendő részletet az adatok felhasználásának módjáról, a vállalatoknak azt is figyelembe kell venniük, hogy az emberek ésszerűen hogyan várják el az adatok felhasználását.

A GDPR elszámoltathatóságot is előír.³³⁶ Ezt a legalább 250 alkalmazottat foglalkoztató szervezetek esetében, vagy ha az adatkezelés veszélyeztetheti az egyének jogait vagy szabadságát, részletes nyilvántartási kötelezettségek tartalmazzák.³³⁷ Az egyik kötelezően vezetendő nyilvántartás a személyes adatok feldolgozásának "célja".³³⁸ Ez problémát jelenthet a mesterséges intelligenciával és adatokkal foglalkozó vállalatok számára, amelyek meghatározatlan célból vagy konkrét cél nélkül bányásszák az adatokat. Ezért a kezdeti nyilvántartások változni fognak, ahogy új adatkorrelációkat fedeznek fel, amelyek különböző felhasználási célokra ösztönöznek.

A GDPR követelményeinek egyik következménye az lehet, hogy a mesterséges intelligencia elszámoltatható és átlátható módon történő fejlesztésére kényszeríti a "fekete doboz" hatásának kezelése érdekében. Több megközelítés is felmerült, többek között az algoritmikus auditálás vagy az algoritmusok fejlesztésébe való beépítés. Ez lehetővé tenné a magáncégek számára a védett információk védelmét, az algoritmusos döntéshozatalt befolyásoló tényezők értékelését és nyilvános biztosítékok nyújtását. Az algoritmikus auditálás akadályaként azonban a számítási erőforrások és a technikai képességek szerepelnek.³³⁹

3. Adatvédelem a tervezéssel

Egyre inkább kialakulóban van az a felfogás, hogy az innovációt a "beépített adatvédelem" szemszögéből kell megközelíteni. Ez az ap-

³³⁵ Lásd 20. még a fenti IV.B.2. szakaszt.

³³⁶ GDPR Art. 5(2).

³³⁷ Információs Biztosok Hivatala (Information Commissioner's Office), *fenti* megjegyzés 51.

³³⁸ GDPR Art. 30(1)(b).

³³⁹ Információs Biztosok Hivatala (Information334 Commissioners Office), *fenti megjegyzés*
86.

megközelítés a magánélet védelmét a technológiákba "alapértelmezés szerint" építi be a de-jelzési szakaszban.³⁴⁰ A beépített adatvédelem a GDPR³⁴¹ értelmében jogi követelmény, és egy olyan keretrendszer, amely azt az ideológiát támogatja, hogy az adatvédelemnek a szervezeti prioritások, célok, fejlesztések és tervezési műveletek szerves részévé kell válnia.³⁴² Ez a keretrendszer biztosítja, hogy a szervezetek alapértelmezésben megfelelő szervezeti és technikai intézkedéseket alkalmazzanak annak biztosítására, hogy csak a szükséges személyes adatok kerüljenek az egyes konkrét célokhoz.³⁴³

Azáltal, hogy a GDPR jogi követelményként tartalmazza a beépített adatvédelmet, az EU bebizonyította, hogy a magánélet és az adatvédelem kiemelt prioritás a jövőbeli technológiai fejlesztésekben, beleértve a mesterséges intelligencia alkalmazását is. Az amerikai jog általában nem írja elő, hogy az adatvédelmi tényezőket be kell építeni a technológia tervezésébe vagy fejlesztésébe, bár az FTC önkéntes alapon erre ösztönzi a vállalatokat.

4. Versenyjog

A technológiai iparágak trösztellenes szabályozása terén az Európai Bizottság (az EU trösztellenes jogérvényesítő szerve) sokkal agresszívebb, mint az amerikai FTC és az igazságügyi minisztérium. Ez kihatással van az adatok és a mesterséges intelligenciában való felhasználásuk szabályozására. Az agresszív uniós fellépésre példa a Microsoft elleni ügy 2007, amelyben a Bizottság lezárási és feloldási követelményeket írt elő, és a vállalatot több mint kétfélmillió eurós bírsággal sújtotta. 497 millió euró, és a következő évben további bírságokat szabtak ki.³⁴⁴ Az Egyesült Államokban párhuzamosan folyó ügyben hasonló eredmények születtek a Dis-

³⁴⁰ *Lásd pl. Intersoft Consulting, GDPR: Privacy by Design*, <https://gdpr-info.eu/issues/privacy-by-design>.

³⁴¹ GDPR Art. 25.

³⁴² Ann Cavoukian, *Privacy by Design: PRIVACY & BIG DATA INSTITUTE*, <https://www.ryerson.ca/content/dam/pbdce/seven-foundational-principles/The-7-Foundational-Principles.pdf>. A beépített adatvédelem alapelvei a következők: (1) Proaktív, nem reaktív, (2) Az adatvédelem alapértelmezett, (3) Az adatvédelem a tervezésbe ágyazva, (4) Teljes funkcionalitás, (5) Végponttól végpontig tartó biztonság, (6) Láthatóság és átláthatóság, és (7) A felhasználói jog tiszteletben tartása.

³⁴³ GDPR Art. 25. Lásd Cavoukian, *Supra note*. 342.

³⁴⁴ Microsoft kontra Bizottság (2007) T201/04.

trict Court és Court of Appeals, az elidegenítés pedig egy lehetséges jogorvoslati lehetőség.³⁴⁵ De még az ítélelhozatal előtt George W. Bush elnök hivatalba lépett, és az ügyet sovány feltételekkel rendezték.³⁴⁶ Az amerikai trösztellenes jogérvényesítés azóta "mélyrepülésben" van.³⁴⁷

A technológiai vállalatok versenyellenes tevékenységei csak fokozódtak. A Facebook hatvanhét versenytárs felvásárlásával megszüntette a versenyt, és hatalmas mennyiségű személyes adatot gyűjtött össze. Az Amazon kilencvenegy, a Google pedig kétszáznegy tizenegy vásárolt fel.³⁴⁸ Az Igazságügyi Minisztérium "lehetővé tette a technológiai ipar szinte teljesen gátlástalan konszolidációját a monopolisták új osztályába"³⁴⁹, amelyet Tim Wu, a Columbia jogi professzora "tech-trösztöknek" nevez.³⁵⁰ Eközben az Európai Bizottság az Intel, a ³⁵¹Facebook, a ³⁵²Google ³⁵³és a Qualcomm elleni ügyekkel az amerikai technológiai cégek vizsgálatának élére állt.³⁵⁴ Vizsgálatok

³⁴⁵ *Lásd* United States v. Microsoft, 253 F.3d 34 (D.C. Cir. 2001) (a jogorvoslatok tárgyalása, amikor a Microsoftnak meg kellett osztania API-it más fejlesztőkkel, de nem kellett változtatnia az operációs rendszerén vagy alkalmazásain).

³⁴⁶ TIM WU, A NAGYSÁG ÁTKA: TRÖSZTELLENES SZABÁLYOK AZ ÚJ ARANYKORBAN 100-01 (2018).

³⁴⁷ *Id.* 108-10. o. ("[A] nagy egészben nulla monopóliumellenes trösztellenes ügyet" indítottak a Bush-kormányzat alatt, és azóta is csak keveset).

³⁴⁸ *Id.* 123.

³⁴⁹ *Id.* 108-110.

³⁵⁰ *Id.* 118.

³⁵¹ *Lásd* Európai Bizottság, *The Intel Antitrust Case*, <http://ec.europa.eu/competition/sectors/ICT/intel.html> (utolsó látogatás 2019., január) (1,5 milliárd eurós bírság).

³⁵² *Lásd*: Európai Bizottság, *Fúziók: Commission Bines Facebook €110 Million for Providing Misleading Information about WhatsApp Takeover*, http://europa.eu/rapid/press-release_IP-17-1369_en.htm (utolsó látogatás 2019., január).

³⁵³ *Lásd*: Európai Bizottság, *Antitröszt: Commission Bines Google €2,4 Billion for Abused Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service*, http://europa.eu/rapid/press-release_IP-17-1784_en.htm (utolsó látogatás 2019. január 4.); és European Commission, *Antitrust: Commission Bines Google €4.34 Billion for Illegal Practices Regarding Android Mobile Devices to Strengthen Dominance of Google's Search Engine*, http://europa.eu/rapid/press-release_IP-18-4581_en.htm (utolsó látogatás: 2019., január).

³⁵⁴ *Lásd*: Európai Bizottság, *Antitröszt: Commission Bines Qualcomm €997 Million for Abuse of Dominant Market Position*, http://europa.eu/rapid/press-release_IP-18-421_en.htm (utolsó látogatás 2019., január).

az Amazon és az Apple folyamatban van.³⁵⁵ Ironikus módon a Bizottság elé kerülő panaszosok közül sokan más amerikai vállalatok, amelyek úgy érzik, hogy az amerikai szabályozó hatóságok nem védik megfelelően a versenyt.

A Bizottság most túllép a hagyományos trösztellenes jogon, és "alaposan szemügyre vesz egy egyre fontosabb vállalati valutát: az adatokat".³⁵⁶ Nem a pénzszegek, hanem az ³⁵⁷általuk hasznosítható adatok mennyisége áll a vizsgálat középpontjában. Margrethe Vestager versenypolitikai biztos "a figyelmeztetés egyik fő hangadójává vált a technológiai cégeknek a szokásainkra, a magánéletünkre, az emberi kapcsolatok kialakítására való képességünkre, sőt magára a demokráciára gyakorolt hatásával kapcsolatban".³⁵⁸ Az EU új adatvédelmi rendszerével együtt ez az uniós visszaszorítás veszélyeztetheti az amerikai technológiai vállalatok globális dominanciáját. A német kartellhivatal nemrégiben megtiltotta a Facebooknak, hogy a felhasználók önkéntes hozzájárulása nélkül adatokat vonjon össze harmadik fél szolgáltatásaival.³⁵⁹ Egy kanadai tisztviselő ennél is tovább ment, és a vállalat feldarabolását javasolta.³⁶⁰ Legalábbis a különböző verseny- és adatvédelmi rendszerek közötti diszkontinuitás jelentős gazdasági és társadalmi bizonytalanságot okoz. Talán válaszul az FTC elkezdett "a következményekre" összpontosítani.

³⁵⁵ Lásd Aoife White, *After Google, EU's Antitrust Sights May Turn to Amazon and Apple*, <https://www.bloomberg.com/news/articles/2019-03-20/after-google-eu-s-antitrust-sights-may-turn-to-amazon-and-apple>.

³⁵⁶ Natalia Drozdiak, *EU ASKS: A "Big Data" ellenőrzése megöli a versenyt?*, WALL ST. J. (2018., jan.), <https://www.wsj.com/articles/eu-competition-chief-tracks-how-companies-use-big-data-1514889000>.

³⁵⁷ Sarah Lyall, *Ki veri a félelmet a Szilícium-völgybe? Margrethe Vestager, Eu- rope's Antitrust Enforcer*, N.Y. TIMES (2018. május 5.), <https://www.ny-times.com/2018/05/05/world/europe/margrethe-vestager-silicon-valley-data-privacy.html>.

³⁵⁸ *Id.*

³⁵⁹ Lásd: *Bundeskartellamt Prohibits Facebook from Facebook from Combining User Data from Different Sources*, BUNDESKARTELLAMT (2019. február 7.), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

³⁶⁰ Lásd Romm, *Supra* note 173.

a mesterséges intelligencia és más újonnan megjelenő technológiák terén a verseny, a fogyasztók védelme és a magánélet védelmének érvényesítése terén nemzetközileg eltérő megközelítésekkel."³⁶¹

A monopolhelyzet lehetővé teszi a technológiai óriáscégek számára, hogy más módon is torzítsák a piacot. Az első a tudásalapú gazdaságban a tehetségek piaca. Az adattudósokat, robotikusokat és mesterséges intelligenciával foglalkozó mérnököket, akik közül néhányan milliós fizetést kapnak,³⁶² a technológiai cégek felfalják a mesterséges intelligencia fegyverkezési versenyében.³⁶³ Ez "ritkította a legjobb akadémiai tanszékeket",³⁶⁴ és más iparágakban vákuumokat eredményezett, növelve a ³⁶⁵bérek egyenlőtlenségét és súlyosbítva a lakhatási válságot a Szilícium-völgyben és más technológiai központokban.³⁶⁶ Másodszor, ezeknek a vállalatoknak relatíve alacsonyak a termelési költségeik a piaci árakhoz képest.

³⁶¹ Lásd *FTC Hearing #11: The FTC's Role in a Changing World, Hearings on Competition and Consumer Protection in the 21st Century*, FED. TRADE COMM'N, <https://www.ftc.gov/news-events/events-calendar/ftc-hearing-11-competition-consumer-protection-21st-century>.

³⁶² Gideon Lewis-Kraus, *The Great AI Awakening*, N.Y. TIMES (2016. dec. 14.), <https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html> (Mark Zuckerberg "személyesen felügyeli, telefonhívásokkal és videochat-beszélgetésekkel, cégének a legkívánatosabb végzős hallgatóknak tett ajánlatát.

A hét számjegyű kezdő fizetések nem ismeretlenek"). Lásd még Cade Metz, *AI Researchers Are Making More Than \$1 Million, Even at a Nonprofit*, N.Y. TIMES (2018. április 19.), <https://www.nytimes.com/2018/04/19/technology/artificial-intelligence-salaries-openai.html> ("AI specialisták kevés vagy semmilyen ipari tapasztalattal nem rendelkező szakemberek évi 300 000 és 500 000 dollár közötti fizetést és részvényeket kereshetnek.").

³⁶³ *Id.* A mesterséges intelligencia mérnökök iránti kereslet olyan nagy, hogy a Szilícium-völgyi technológiai vállalkozások kölcsönös "nem-zsarolási" megállapodást kötöttek. Mind az Igazságügyi Minisztérium, mind a mérnökök egy csoportja trösztellenes keresetet nyújtott be. Lásd *In re High Tech Employee Antitrust Litigation*, Case No. 11-CV-2509-LHK (N.D. Cal. 2015); lásd még Matt Phillips, *Apple's \$1 Trillion Milestone Reflects Rise of Powerful Megacompanis*, N.Y. TIMES (Aug. 2, 2018), <https://www.nytimes.com/2018/08/02/business/apple-trillion.html>.

³⁶⁴ Lewis-Kraus, *Supra* note 362.

³⁶⁵ *Id.*

³⁶⁶ Lásd Richard Waters, *The Great Silicon Valley Land Grab*, FIN. TIMES (2017. augusztus 25.), <https://www.ft.com/content/82bc282e-8790-11e7-bf50-e1c239b45787>. A bevándorló vízumokkal kapcsolatos bizonytalanságok miatt számos technológiai vállalat Kanadába helyezi át mesterséges intelligenciával kapcsolatos műveleteinek egy részét. Gene Marks, *Canada's Tech Companies Are Benefiting From Tightening U.S. Immigration*, WASH. POST (2018. április 12.), https://www.washingtonpost.com/news/on-small-business/wp/2018/04/12/canadas-tech-companies-are-benefiting-from-tightening-u-s-immigration/?utm_term=.3e987d0fcb1.

termékek. Bár ez a nagy recesszió végét követően bikapiacot indított el,³⁶⁷ az előnyökből más ágazatok nem részesülnek egyformán, ami esetleg visszavetheti az ottani beruházásokat.³⁶⁸

Végül pedig a mesterséges intelligencia a technológiai és platformcégek³⁶⁹ hatalomkoncentrációját táplálta, amely "részben független az államoktól és a nemzetközi politikai intézményektől".³⁷⁰ Piaci dominanciájuk miatt képesek kiszorítani a hagyományos jogot "szolgáltatási feltételekre" vonatkozó szabályokkal, amelyek különálló jogrendszerként működnek, és ezt meg is teszik.³⁷¹ "Míg Mark Zuckerberg nemrég azon morfondírozott, hogy a Facebooknak szüksége lehet a Legfelsőbb Bíróság analógiájára, hogy vitákat bíráljon el és fellebbezéseket tárgyaljon, az Amazon már rendelkezik valami olyasmivel, mint egy bírósági rendszer - egy olyan rendszerrel, amely titokzatos, változékony és gyakran félelmetes".³⁷² Az ügyvédek helyett egy növekvő tanácsadói iparág működik, amely segít az Amazon eladóknak fellebbezni az algoritmikus alapú döntések ellen, amelyekkel visszaminősítik vagy felfüggesztik termékeiket.³⁷³ Az ilyen mértékű dominancia aláássa a szabadpiaci elveket és a demokráciát. A szabályozóknak jobban oda kell figyelniük ezekre a hatalomkoncentrációkra, nehogy a "Facebook szuverén állama" kifejezés több legyen, mint egyszerű metafora.³⁷⁴

C. A robotok és az AI szabályozása

³⁶⁷ Phillips, *fenti* megjegyzés 363.

³⁶⁸ Matt Phillips, *Apple's \$1 Trillion Milestone Reflects Rise of Powerful Mega-companis*, N.Y. TIMES (2018. augusztus 2.), <https://www.ny-times.com/2018/08/02/business/apple-trillion.html>.

³⁶⁹ *Lásd pl.* Liu, *fenti* megjegyzés (azzal 22érvelve, hogy a hatalom koncentrációja "katonai intézményekben és magáncégekben, [amelyek] jelenleg a mesterséges intelligencia kutatását és fejlesztését irányítják, potenciálisan torzítja a demokratikus és polgári ellenőrzés fogalmát"). ³⁷⁰ Ünver, *supra* note at 72.

³⁷¹ *Lásd* Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328, 356-357 (2018) ("A Facebook saját tartalmi szabályai és szolgáltatási feltételei ... nagyobb befolyással lehetnek a platformon történő beszéd alakítására, mint bármelyik állam törvénye"). ³⁷² Josh Dzieza, *Prime and Punishment; Dirty Dealing in the \$175 Billion Amazon Marketplace*, THE VERGE (2018. dec.), <https://www.theverge.com/2018/12/19/18140799/amazon-marketplace-scams-seller-court-appell-reinstatement>.

³⁷³ *Id.*

³⁷⁴ *Lásd* Molly Roberts, *Facebook Has Declared Sovereignty*, WASH. POST (2019. január 31.), <https://www.washingtonpost.com/opinions/2019/01/31/facebook-has-declared-sovereignty>; Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, HARV. L. REV. n1598,1617, (1252018) (a "feudális" és "szuverén" platformokat tárgyaló szakirodalom összegyűjtése).

1. A ló törvénye

Az 1990-es években, amikor az internet egyre nagyobb teret nyert, Frank Easterbrook és Lawrence Lessig nyilvános vitát folytatott arról, hogy a kibertér számára új jogi fegyelemre és szabályozásra van szükség. Easterbrook bíró azzal érvelt, hogy a jogi iskoláknak éppúgy nincs szükségük kiberjogi kurzusra, mint ahogyan a "lójog" kurzusra sincs szükségük a lovakkal kapcsolatos kérdések egyedi kezelésére.³⁷⁵ Lessig professzor ezzel ellentétes véleményt képviselt; hogy külön figyelmet kell fordítani arra, "hogyan kapcsolódik össze a jog és a kibertér".³⁷⁶ A vitájuk óta eltelt két évtizedben Lessig nézete érvényesült, mivel az internet a jog minden területére hatással van.³⁷⁷ Ryan Calo a későbbiekben Lessig megközelítését és későbbi elméletét, miszerint "a kód a jog", a robotika területére alkalmazta.³⁷⁸

Lessig két különböző szabályozási paradigmát írt le az internetre vonatkozóan: "Keleti parti kódex" és "Nyugati parti kódex". Az előbbi a megszokott kormányzati ellenőrzés törvény vagy ügynökségi szabályozás útján.³⁷⁹ Az utóbbi az internet architektúrája; nevezetesen, hogy az internetet (és más technológiákat) működtető szoftver kód maga is szabályozási eszköz. A mérnökök szoftverterveikkel kiegészíthetik vagy kiszoríthatják a jogi szabályozást.³⁸⁰

Az internet szabályozásáról szóló Easterbrook-Lessig vitát a mesterséges intelligenciával kapcsolatban folytatják. Egyesek úgy vélik, hogy a fenevadat meg lehet szelídíteni a "magánélet védelmére, a diszkriminációra, a járműbiztonságra és így tovább" vonatkozó meglévő szabályok AI-ra való adaptálásával.³⁸¹ Mi a másik utat választjuk, és a "mesterséges intelligencia törvénye" mellett érvelünk.

³⁷⁵ Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, U1996. CHI. LEGAL F. 207.

³⁷⁶ Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, (5021999).

³⁷⁷ Az "internetes kivételesség" a jogi szakirodalomban népszerű diskurzussá vált. *Lásd pl.* Mark Tushnet, *Internet Exceptionalism: An Overview From General Constitutional Law*, WM56. & MARY L. REV. 1637 (2015); Ryan Calo, *Robotics and the Lessons of Cyberlaw*, CAL103. L. REV. 513, 551-52 (2015).

³⁷⁸ *Lásd 559.még*: LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

³⁷⁹ *Id.* 53.

³⁸⁰ *Id.* 60.

³⁸¹ Tom Standage, *There Are No Killer Robots Yet-But Regulators Must Respond To AI In 2019*, ECONOMIST (2018. december 17.), <https://www.economist.com/the-world-in/2018/12/17/there-are-no-killer-robots-yet-but-regulators-must-respond-to-ai-in-2019>. Egy másik átgondolt vitát lásd Heidi Vogt,

ló"; vagy a kifejezetten a mesterséges intelligencia modern életben való használatára vonatkozó törvények. Amíg a szabályozó hatóságok nem lépnek fel a mesterséges intelligenciával és a robotokkal való visszaélések ellen, addig a ~~robotika~~ ^{robotika} fejlesztőik által beléjük épített kód fogja szabályozni. Amint azt e cikk korábbi részében leírtuk, a mesterséges intelligencia szoftverek tervezése jelenleg lehetővé teszi az alapos visszaéléseket. Bár a szoftvert nem kifejezetten a magánélet aláásására vagy a demokratikus folyamatok akadályozására tervezték, fennáll a veszélye, hogy mégis az lehet. Amint azt a GDPR és a robotikára vonatkozó uniós törvényjavaslatok is mutatják, a szabályozásnak ezt figyelembe kell vennie.

2. A robotikára vonatkozó javasolt uniós jogszabályok

Az Európai Parlament a Jogi Bizottság jelentését követően az Európai Bizottság felkérte 2017 az Európai Bizottságot, hogy dolgozzon ki "a robotikára vonatkozó polgári jogi szabályokat" az Európai Unió számára.³⁸² A Bizottság előzetes választ tett közzé, amelyben egyetértett a Parlament számos aggályával, beleértve a mesterséges intelligencia "társadalmi-gazdasági hatását, valamint a jogállamiságra, az alapvető jogokra és a demokráciára gyakorolt következményeit".³⁸³ Ezt követően a nyilvánossággal folytatott konzultáció követte ezeket az aggályokat, hangsúlyozva az uniós értékek (például a magánélet és az adatvédelem) védelmét, a felelősségi szabályok szükségességét és az elfogadott szabályok jobb végrehajtását.³⁸⁴

Kell-e a kormánynak szabályoznia a mesterséges intelligenciát, WALL ST. J. (2018. április 30.), <https://www.wsj.com/articles/should-the-government-regulate-artificial-intelligence-1525053600>.

³⁸² EUR. PARL. DOC. P8_TA (2017)0051, *A robotikára vonatkozó polgári jogi szabályok: Az Európai Parlament 2017. február 16-i állásfoglalása a Bizottságnak szóló ajánlásokkal a robotikára vonatkozó polgári jogi szabályokról*, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//EN>. A legtöbb uniós jogszabályt a Bizottság kezdeményezi.

³⁸³ *Az Európai Parlament 2017. február 16-i állásfoglalásának nyomon követése a robotikára vonatkozó polgári jogi szabályokról*, Európai Bizottság. A Bizottság több jogalkotási kezdeményezést fogadott el vagy dolgoz ki a mesterséges intelligenciával kapcsolatban. Ezek közé tartozik a 2006/42/EK gépezeti irányelv, a "jobb szabályozási csomag" az alapvető jogokra ~~gyakorolt~~ ^{gyakorolt} hatások értékelésére, valamint a tárgyak internete és az autonóm rendszerek felelősségének vizsgálata. *Id.*

³⁸⁴ *Lásd* <http://www.europarl.europa.eu/cmsdata/130181/public-consultation-robotics-summary-report.pdf> (utolsó látogatás 20194., január).

A Parlament új jogszabályokra és szakpolitikákra vonatkozó javaslata a következőkre terjed ki³⁸⁵:

- Isaac Asimov három robotikai törvényének kodifikálása,³⁸⁶
- a robotok által okozott károkkal kapcsolatos felelősségi szabályok kialakítása és a mesterséges intelligenciával foglalkozó mérnökök elszámoltathatósága;
- a mesterséges intelligencia rendszerek nyilvántartása és osztályozása a nyomon követhetőség és az ellenőrzés megkönnyítése érdekében;
- etikai elvek kidolgozása, beleértve a mesterséges intelligencia mérnökök magatartási kódexét, amely a jótékonyágon, a nem rosszindulatúságon, az emberi autonómián és az igazságosságon alapul;
- az emberi biztonságot, egészséget és biztonságot, a szabadságot, a magánéletet, a sérthetetlenséget és a méltóságot, az önrendelkezést, a diszkriminációmentességet és a személyes adatok védelmét érintő kockázatok enyhítése;
- az előírt átláthatóság és magyarázhatóság, beleértve az AI által tett minden olyan lépés dokumentálását, amely hozzájárul a döntésekhez;
- nyílt forráskód használata az autonóm robotok tervezése és interoperabilitása során; és
- az Európai Robotikai és Mesterséges Intelligencia Ügynökség létrehozása a fejlődő technológiák előmozdítása és szabályozása érdekében.

Az ilyen politikák nagymértékben hozzájárulhatnak az ebben a cikkben azonosított kockázatok csökkentéséhez, amelyek közül számos a Parlament javaslatában is szerepel.³⁸⁷ Lehetséges, hogy az EU szabályainak elfogadása esetén azok

³⁸⁵ EUR. PARL. Res. 2015/2103(INL), *Jelentés a Bizottságnak szóló ajánlásokkal a robotikára vonatkozó polgári jogi szabályokról*,

<http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2017-0005&language=EN>.

³⁸⁶ A "törvények" először ISAAC ASIMOV, ASTOUNDING SCIENCE FICTION (1942) című novellájában jelentek meg, és azóta szinte minden robotokról szóló sci-ence és sci-fi történetben megjelentek. Ezek a következők: 1) "A robot nem okozhat kárt az embernek, és nem engedheti meg, hogy az ember tétlenségével kárt okozzon"; 2) "A robotnak engedelmeskednie kell az ember által adott utasításoknak, kivéve, ha ezek az utasítások ellentétesek az első törvénnyel"; és 3) "A robotnak meg kell védenie saját létét, amíg ez a védelem nem ütközik az első vagy a második törvénnyel".

³⁸⁷ *Id.* G. pont (a mesterséges intelligencia "nemcsak gazdasági előnyökkel jár, hanem a társadalom egészére gyakorolt közvetlen és közvetett hatásaival kapcsolatban is számos aggály merül fel"); H. pont ("kihívást jelent a megkülönböztetésmentesség, a megfelelő eljárás, az átláthatóság és az

érthetőség biztosítása a döntéshozatali folyamatokban").

extraterritoriális hatás az Egyesült Államokban és Európán kívül máshol is a mesterséges intelligencia fejlesztésére. Funkcionálisan ez történt a GDPR-ral. Az összes amerikai technológiai vállalatnak és számos kisebb cégnek meg kell felelnie az uniós adatvédelmi szabályoknak, ami a transzatlanti üzleti tevékenységben való részvétel feltétele, és ezzel betölti az amerikai adatvédelmi jogban keletkezett űrt. Még akkor is, ha a nagy technológiai cégek egyre inkább beépítik a mesterséges intelligenciát a köz- és magánéletünkbe, kénytelenek lehetnek tiszteletben tartani a demokráciát erősítő elveket, amelyeket az európai mesterséges intelligenciáról szóló törvények tartalmaznak, ha és amikor azok a törvények hatályba lépnek.

Az Egyesült Államok nem mindig volt ennyire lemaradva. 2014-ben és 2016-ban az Elnök Tudományos és Technológiai Tanácsadói Tanácsa (PCAST) és a Nemzeti Tudományos és Technológiai Tanács (NSTC) több jelentést is kiadott a nagyméretű adatokról és a magánélet védelméről.³⁸⁸ Az NSTC olyan fehér könyveket is kiadott, mint a *AI: Felkészülés a mesterséges intelligencia jövőjére*³⁸⁹ és a *Nemzeti mesterséges intelligencia kutatási és fejlesztési stratégiai terv*.³⁹⁰ Bár ezek inkább keretrendszeresek voltak, mint konkrét politikai javaslatok, aggodalmakat vetettek fel a mesterséges intelligencia "nem szándékolt következményeivel" kapcsolatban, különösen az "igazságosság, méltányosság és elszámoltathatóság" területén.³⁹¹ Ezek a tervek fontos első lépések voltak, és elvezethettek volna a "mesterséges intelligencia alkalmazásával kapcsolatos összetett ~~poli~~ kihívások" kezeléséhez.³⁹² Ezeket a terveket azonban többnyire elvetették.³⁹³ Ehelyett a nagy adatokkal és a mesterséges intelligenciával kapcsolatos jelenlegi stratégiák

³⁸⁸ *Lásd: Executive Office of the President, Big Data: Seizing Opportunities, Pre-serving Values*, 2014. május, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf; Executive Office of the President: *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, 2016. május, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

³⁸⁹ Executive Office of the President, *Preparing for the Future of Artificial Intelligence*, 2016. október, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

³⁹⁰ Executive Office of the President, *The National Artificial Intelligence Research and Development Strategic Plan*, 2016. október, https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf.

³⁹¹ *Felkészülés a jövőre, lásd a389, fenti megjegyzést.* 30.

³⁹² AI Strategy, *supra* note at 390,7.

³⁹³ PWC, 132. l. ábragyűjtés, 19. pont. A szakértői értékeléssel ellátott publikációk számával mérve a mesterséges intelligencia iránti tudományos érdeklődés 1996 óta nyolcszorosára nőtt, de a növekedés nagy része Európában és Kínában

következett be, nem pedig az Egyesült Államokban, ahol a növekedés mértéke a következő szintre esett vissza.

a kockázatok mérséklése helyett a felhasználásuk előmozdítására és a szabályozási akadályok megszüntetésére összpontosítanak.³⁹⁴

3. *Asilomar alapelvek*

A mesterséges intelligencia szabályozására vonatkozó ötleteknek nem csak a kormányzat részéről kell érkezniük. A civil társadalom is fontos szerepet játszhat. A nem kormányzati szervezetekből, tudósokból és tudósokból álló, egyre növekvő és globális "felelős mesterséges intelligencia" mozgalom³⁹⁵ az utóbbi időben elkezdte felvállalni a mesterséges intelligencia által támasztott közérdekű kihívásokat.³⁹⁶ Az Elon Muskot,³⁹⁷ Bill Gatest és a néhai Stephen Hawkingot is magában foglaló csoport 2015-ben "Nyílt levelet adott ki a mesterséges intelligenciáról", amelyet később több, a mesterséges intelligenciával, 8,000 és a politikával foglalkozó kutató is aláírt.³⁹⁸ A levél megerősítette, hogy a mesterséges intelligencia "soha nem látott előnyökkel járhat az emberiség számára", de figyelmeztetett a "lehetséges buktatókra" is, amelyek³⁹⁹ között a magánéletet, az etikai normákat és az emberi ellenőrzést fenyegető veszélyek szerepeltek.⁴⁰⁰ Ezt követte a

harmadik hely. *Lásd: AI Index, Supra* 17. lábjegyzet, 8-10. o. Ezt tükrözi a kiadott mesterséges intelligencia-szabadalmak számának összehasonlító növekedése. *Id.* 35. o. 2019. február 11-én Trump elnök kiadta az 13859. számú, "Az amerikai vezető szerep megőrzése a mesterséges intelligencia területén" című végrehajtási rendeletet, amely válasz lehetett Kína "Made in China 2025" célkitűzésére, hogy átvegye a vezetést a mesterséges intelligencia és a kvantumszámítás területén. A másodlagos cél az AI-technológiákba vetett közbizalom növelése, valamint a "polgári szabadságjogok, a magánélet és az amerikai értékek" védelme.

³⁹⁴ *Lásd pl.* Whitehouse, Artificial Intelligence for the American People, <https://www.whitehouse.gov/briefings-statements/artificial-intelligence-american-people>; National Big Data R&D Initiative, <https://www.nitrd.gov/nitrdgroups/index.php>; Artificial Intelligence R&D Interagency Working Group, *id.*

³⁹⁵ PWC-jelentés, a fenti lábjegyzetben 132.

³⁹⁶ *Lásd pl.* NYU's AI Now Institute, <https://ainowinstitute.org>; Harvard's Ethical Machine, <https://ai.shorensteincenter.org>.

³⁹⁷ Musk társalapítója volt az OpenAI-nak is, egy nonprofit kutatócégnek, amely biztonságos és "barátságos" mesterséges intelligencia létrehozásán dolgozik. Fő munkája a mesterséges intelligenciával kapcsolatos mérnöki tevékenység, de a fentebb leírt elméletnek megfelelően a "nyugati parti kódot", azaz az autonóm gépek architektúráját úgy kell megtervezni, hogy az ne okozzon kárt az emberiségnek, és ne koncentrálódjon indokolatlanul a hatalom. *Lásd:* <https://blog.openai.com/openai-charter>.

³⁹⁸ *Lásd: Nyílt levél: FUTURE OF LIFE INSTITUTE*, <https://futureoflife.org/ai-open-letter> (utolsó látogatás 2019., január).

³⁹⁹ Stuart Russell, Daniel Dewey, Max Tegmark, *Research Priorities for Robust and Beneficial Artificial Intelligence*, AI Magazine, Winter 2015, 112, <https://aaai.org/ojs/index.php/aimagazine/article/view/2577>.

⁴⁰⁰ *Id.* 107.

az Asilomar Conference on Beneficial AI 2017 januárjában tartott konferenciáján kidolgozott alapelvek.⁴⁰¹

Az asilomari alapelvek megfelelnek az itt megfogalmazott ajánlásoknak, és azokra épülnek. A mesterséges intelligencia és fejlesztői által követendő értékek a következők: szabadság, magánélet, felelősség, igazságügyi átláthatóság és az emberi méltóság tiszteletben tartása. Egy másik alapelv is létfontosságú: "A magasan fejlett mesterséges intelligencia-rendszerek irányítása által biztosított hatalomnak tiszteletben kell tartania és javítania, nem pedig felforgatnia azokat a társadalmi és polgári folyamatokat, amelyeken a társadalom egészsége múlik." Az alapelvek közül a legfontosabbak a következők.⁴⁰²

Az asilomari elvek erkölcsi tekintélyt és kompetenciát kölcsönöznek olyan kérdéseknek, amelyeket a társadalom másik két sínje - a kormányzat és a gazdaság - eddig elhanyagolt. 2018 végén a kaliforniai törvényhivatalosan is elfogadta az asilomari elveket.⁴⁰³ Talán ez elindít egy trendet.

4. Ajánlások

A magánélet hiánya az online és a fizikai terekben olyannyira elterjedt, hogy sok amerikai már megbékélt a Sun Microsystems vezéregazgatója, Scott McNealy által kifejtett nézettel: "a magánéleted amúgy is zéró". Lépjetek túl rajta".⁴⁰⁴ Remélhetőleg a legtöbb amerikai elutasítja ezt a nézetet, ahogy mi is. Ha a kongresszus komolyan foglalkozna az adatvédelmi törvény korszerűsítésével, a közösségi média és a mesterséges intelligencia hatásaitól eltekintve, megfontolhatná a következő javaslatokat:⁴⁰⁵

a magánélet védelmét alapvető emberi jogként kezeljük;⁴⁰⁶

⁴⁰¹ Lásd *Asilomar AI Principles*, FUTURE LIFE INST., <https://futureoflife.org/ai-principles>. Az Asilomar konferenciát a Future of Life Institute szponzorálta.

⁴⁰² Lásd *Asilomar AI Principles*, ARTIFICIAL INTELLIGENCE BLOG, <https://www.artificial-intelligence.blog/news/asilomar-ai-principles> (utolsó látogatás 2019. január).

⁴⁰³ Assemb. Con. Res. 2017-18 Leg. 215, (Cal. 2018).

⁴⁰⁴ Polly Springer, *Sun on Privacy*: WIRED (1999. január 26.), <http://www.wired.com/1999/01/sun-on-privacy-get-over-it>.

⁴⁰⁵ Elismerjük, hogy ez a szabályozási reform kívánságlistája. De egy bizonyos ponton valami ehhez hasonlót kell bevezetni, ha meg akarjuk őrizni az alapvető értékeket. ⁴⁰⁶ Az Emberi Jogok Egyetemes Nyilatkozata, 12. cikk, elérhető a <http://www.un.org/en/universal-declaration-human-rights/> oldalon: "Senkit sem szabad

a beépített adatvédelem megkövetelése és a technológiai vállalatok ösztönzése az adatvédelem tudatosságára;⁴⁰⁷ opt-in modelleket (opt-out helyett opt-in) alkalmazzanak a hozzájárulás és a felhasználás tekintetében, ahogyan azt Európa a GDPR alapján teszi; teljes átláthatóságot követelnek meg a felhasználói adatok későbbi felhasználása tekintetében;

⁴⁰⁸

- felelősséget állapítanak meg a hozzájárulás nélküli gyűjtésért, felhasználásért vagy kereskedelemért; és
- a személyes adatok tulajdonjogának, ellenőrzésének és az "érintettek" általi megválasztásának elismerése.⁴⁰⁹

A fenti intézkedések közül sok megvalósítható lenne a GDPR-hez vagy a CCPA-hoz hasonló rendeletek elfogadásával. A mesterséges intelligencia növekvő használata az adat-ökoszisztémában azonban megköveteli, hogy a kongresszus továbblépjen. Ezt is meg kell tennie:

- olyan jogszabályokat kell elfogadni, amelyek kimondható és konkrét adatvédelmi folyamatokat, kiberbiztonsági szabványokat és anonimitási eljárásokat írnak elő, amelyek megsértése esetén törvényi szankciókat és magánjogi jogokat írnak elő;
- a tárgyak internete, az adatgyűjtés, -fúzió és -elemzés szabályozási felügyeletnek és harmadik fél által végzett auditálási követelményeknek való alávetése;
- a blokklánc- vagy hasonló jogcím-lánc-technológia előmozdítása annak érdekében, hogy a felhasználók tulajdonjogot szerezzenek adataik felett, és pénzzé tegyék azok használatát; és
- emberi felügyeletet és elszámoltathatóságot írnak elő a személyes adatok és bármely olyan információ algoritmikus felhasználása tekintetében, amely személyhez kapcsolódik vagy személyhez kapcsolódhat, beleértve az automatikus döntések átlátható indoklását.⁴¹⁰

a magánéletébe, családjába, otthonába vagy levelezésébe való önkényes beavatkozásnak, valamint a becsületét és jó hírnevét ért támadásoknak. Mindenkinnek joga van a törvény védelméhez az ilyen beavatkozásokkal vagy támadásokkal szemben."

⁴⁰⁷ Derek Care, Adatvédelmi Szakemberek Nemzetközi Szövetsége: Privacy, Security, Risk Conference (2018.10.19., október)..

⁴⁰⁸ GDPR Art. 5. cikkének (1) bekezdése (amely előírja, hogy az adatokat átlátható és tisztességes módon kell feldolgozni).

⁴⁰⁹ Funkcionálisan ez a GDPR által alkalmazott megközelítés, amennyiben az európai lakosoknak jogot biztosít arra, hogy ellenőrizzék személyes adataik

gyűjtését, felhasználását és közzétételét.

⁴¹⁰ *Lásd fentebb a IV.B.2. szakaszt.*

A demokratikus értékek és intézmények védelme a mesterséges intelligencia által jelentett kockázatokkal szemben szintén komoly figyelmet és jogalkotást igényel. A "Kelet-parti kódex" (hivatalos törvény) előbb-utóbb ki fog alakulni. Lehet, hogy vérszegény és iparorientált lesz, mint ahogy a szövetségi adatvédelmi törvények is azzá váltak. Vagy az AI visszaélésekkel kapcsolatos közvélemény elégedetlensége egy átfogó szabályozási rendszert indíthat el az Európai Parlament javaslatának mintájára. Egy mesterséges intelligenciára vonatkozó szabályozási rendszer optimális esetben legalább a következő elemeket tartalmazná:⁴¹¹

- átláthatóság, elszámoltathatóság és felelősségvállalás a mesterséges intelligencia tervezéséért és folyamataiért; a képzési és működési adatok ⁴¹²átláthatósága és hozzáférhetősége;⁴¹³
- az eredmények reprodukálhatósága önzetlen személyek által;⁴¹⁴
- a "harmadik fél" és az "állami cselekvés" doktrínájának felülbírálása, valamint a mesterséges intelligencia ~~frktik~~ és a magánélet megsértésének alkotmányossági követelménye;⁴¹⁵

⁴¹¹ Amennyiben a jogalkotók reagálnak a mesterséges intelligencia kihívásaira, az általában a felelősségre vonatkozó szabályokkal történik. Kaliforniában azonban egy állami felügyeleti szerv a közelmúltban az itt megfogalmazottakhoz hasonló ajánlásokat tett közzé. Lásd: *Mesterséges intelligencia: A Roadmap for California*, Little Hoover Commission 14 (2018. november). ⁴¹² Ez és számos más itt szereplő ajánlás megkövetelheti, hogy a mesterséges intelligencia rendszerek vezérlőkódja "nyílt forráskódú" legyen, ne pedig szabadalmaztatott. Ez aláásná az üzleti titokra vonatkozó jogot, hacsak nem módosítanák azt is, például a szabályozási követelmények szerinti közzétételek mentesítésével. A szabadalmi jogot is liberalizálni lehetne a mesterséges intelligencia találmányok ösztönzése és védelme érdekében.

⁴¹³ Itt is hasonló probléma merül fel, mivel a forrás-, képzési és tesztadatokat jellemzően bizalmasan kezelik, hogy megőrizzék gazdasági értéküket. A nyilvánosságra hozatalra válaszul az adatokat tulajdonhoz hasonló jogokkal lehetne felruházni, ahelyett, hogy az üzleti titok védelmére támaszkodnának. *Lásd általában Jeffrey Ritter és Anna Mayer, Regulating Data As Property*, DUKE 16 L. & TECH. REV. 220 (2018).

⁴¹⁴ A mesterséges intelligencia feldolgozásának átláthatatlansága, különösen a mélytanulás esetében, meg nem ítéltető kimenetekhez vezet. *Lásd a fenti* 245-247. lábjegyzeteket és a kísérő szöveget. A harmadik fél általi reprodukálhatóság legalább lehetővé teszi a kimenetek külső tesztelését.

⁴¹⁵ Az állami cselekvés doktrína a legtöbb esetben kizárja az alkotmányos követelések érvényesítését magánfelekkel szemben. *Lásd a* 238. lábjegyzetet. Mégis a mesterséges intelligencia-technológiák magántulajdonosai azok, akik a legnagyobb kárt okozhatják az alkotmányos jogoknak. Noha a Kongresszus nehezen tudná kiterjeszteni az alkotmányt harmadik felekre, párhuzamos törvényes jogokat hozhatna létre, amelyek kötelezik őket. *Lásd például az* 1964. évi polgári jogi törvényt (Civil Rights Act of 1964, 78 Stat. 241). A harmadik fél doktrína bírósági úton jött létre, és akár a Kongresszus, akár a Legfelsőbb Bíróság módosíthatja.

- az etikai elvek érvényesítése a mesterséges intelligencia tervezésében, fejlesztésében és megvalósításában részt vevők számára;⁴¹⁶
- nyitottság a mesterséges intelligencia fejlesztésében, a rendszerekben és az adatbázisokban;⁴¹⁷
- az alapvető jogokat érintő döntések autonóm szereplőkre történő át nem ruházása;⁴¹⁸
- a "safe harbor" mentesség korlátozása a Communications Decency Act és a Digital Millennium Copyright Act értelmében azon nagy internetes platformok esetében, amelyek nem tesznek technológiailag megvalósítható lépéseket a dezinformációs kampányok megfékezésére;⁴¹⁹
- a mesterséges intelligenciával foglalkozó vállalatok piaci erejének korlátozása, beleértve adott esetben a felmentést is;⁴²⁰és
- Asimov trilógiája két törvényszerűséggel bővült: az emberi jólét és értékek elsőbbsége; és az autonóm szereplők teljes nyilvánosságra hozatala.⁴²¹

Bár ezek az ajánlások nem oldják meg teljes mértékben a mesterséges intelligenciával kapcsolatos kockázatokat, úgy véljük, hogy legalábbis a további vitákhoz keretet biztosítanak.

⁴¹⁶ Az MIT nemrégiben jelentette be, hogy új számítástechnikai és mesterséges intelligencia főiskolát hoz létre, amely a mesterséges intelligencia "releváns politikájával és etikájával kapcsolatos oktatást és kutatást" helyez el. Lásd MIT News Of- fe *MIT Reshapes Itself to Shape the Future*, MIT NEWS (2018. október 5.), <http://news.mit.edu/2018/mit-reshapes-itself-stephen-schwarzman-college-of-computing-1015>.

⁴¹⁷ Lásd Nick Bostrom, *Strategic Implications of Openness in AI Development*, *GLOBAL POL'Y* (2017), <https://nickbostrom.com/papers/openness.pdf>. A piaci erőfölény az V. szakasz b) pontjának 4. alpontjában tárgyalt okok miatt veszélyezteti a magánéletet és a demokratikus értékeket.

⁴¹⁸ A 247-250. lábjegyzethez kapcsolódó szövegben kifejtjük, hogy az autonóm döntéshozatal hogyan fedheti el az alkotmányértést, hogyan áthatja alá a tisztességes eljárást, és hogyan akadályozhatja meg az érdemi bírósági felülvizsgálatot. Az emberi integritást is rontja azáltal, hogy az alapvető jogokat algoritmikus ellenőrzésnek veti alá. Az "algokrácia" elkerülése érdekében szükség van egy olyan szabályra, amely korlátozza a delegálást a ma- kínaiakra.

⁴¹⁹ Lásd a 183. lábjegyzetet. Lazar et al. a közösségi médiaplatformok és a tudományos közösség együttműködését javasolják az álhírekkel szembeni hatékony beavatkozások megtervezése érdekében. Az iparág eddig ellenállt ennek, attól tartva, hogy ez szabályozáshoz vezethet. *Id.* 1096.

⁴²⁰ Lásd Wu, 346. lábjegyzet (azzal érvelve, hogy a hatalom óriáscegnél történő koncentrációja veszélyezteti a demokráciát).

⁴²¹ Maga Asimov egy "nulladik törvényt" javasolt, amely az emberiség védelmét minden más robotkötelezettség fölé helyezi. Isaac Asimov, *Robotok és birodalom* (1985). Második javaslatunk magában foglalja Marc Rotenberg által javasolt "negyedik" és "ötödik" törvényt - a robotok azonosítását és magyarázatát. Lásd Marc Ro- tenberg, *Privacy in the Modern Age: The Search*

for Solutions, EPIC (2016. október 19.), <https://epic.org/privacy/intl/EPIC-38ICDPPC-kyn-10-16.pdf>.

Mégsem vagyunk optimisták azzal kapcsolatban, hogy ezeket a közeljövőben elfogadják. Tekintettel a nagy technológiai vállalatok jelenlegi hatalmi dominanciájára, nem csak a mesterséges intelligencia, hanem a demokratikus intézményeink felett is, ehhez egy jelentős eseményre vagy rendszerszintű átalakulásra lehet szükség. De a mesterséges intelligencia fejlődésének meredek görbéje és a status quo iránti, világszerte tapasztalható elégedetlenség miatt lehet, hogy meglepetés vár ránk. Ahogy Bill Gates emlékeztet bennünket: "mindig túlbecsüljük a következő két évben bekövetkező változásokat, és alábecsüljük a következő tíz évben bekövetkező változásokat".⁴²² Ez mind a reformok kilátásaira, mind magára a mesterséges intelligenciára vonatkozik. Nemzeti párbeszéd és valamilyen formában történő jogalkotás nélkül egy évtized múlva a demokrácia és a demokrácia már csak az emlékezetünkben létezhet.

KÖVETKEZTETÉS

Az Economist Intelligence Unit minden évben kiad egy "Demokrácia-indexet", amely a demokrácia állapotát méri fel világszerte.⁴²³ Megállapította, hogy a vizsgált országok több mint felében romlott a demokrácia "pontszáma". A fő tényezők a következők: csökkenő választási részvétel, a kormányzás működésének gyengesége, az intézményekbe vetett bizalom csökkenése, a polgári szabadságjogok erodálódása, a médiaszabadság csökkenése és a nem elszámoltatható irányú növekvő befolyása. E pontozás alapján az Egyesült Államokat a "teljes demokráciából" a "hibás demokráciába" sorolták vissza. A tanulmány megállapította, hogy a "kormányzatba és a közintézményekbe vetett bizalom eróziója" különösen problematikus az Egyesült Államokban.⁴²⁴

⁴²² BILL GATES, AZ ELŐTTÜNK ÁLLÓ ÚT 316 (1995). Ez az Amara-törvény ("Hajlamosak vagyunk rövid távon túlbecsülni egy technológia hatását, hosszú távon pedig alábecsülni") újbóli megfogalmazása.

⁴²³ Economist Intelligence Unit, *Demokrácia Index 2017: Free Speech Under At-tack*, ECONOMIST INTELLIGENCE UNIT (utolsó látogatás 2018. augusztus 10.) http://pages.eiu.com/rs/753-RIQ-438/images/Democracy_Index_2017.pdf. Ez az Economist magazin testvérkiadványa.

⁴²⁴ *Id.* at 20. A 2018-as demokráciaindexben a nők megnövekedett választási részvétele ellenére tovább romlottak a pontszámok. Az USA tovább esett vissza, és továbbra is "hibás demokrácia". Economist Intelligence Unit, *Democracy Index 2018: Me Too? Political Participation, Protest And Democracy* 10, ECONOMIST INTELLIGENCE UNIT (utolsó látogatás 2019.22., április), https://www.prensa.com/politica/democracy-index_LPRFIL20190112_0001.pdf.

A mesterséges intelligencia egyre szélesebb körű elterjedése legalábbis részben felelős ezért a tendenciáért.

Két, egymással összefonódó területre összpontosítottunk, ahol a mesterséges intelligencia hozzájárul az elégedetlenséghez: a magánélet és a demokrácia. A mesterséges intelligencia önmagában nem bűnös. Mint technológia, nem eleve rosszabb, mint mondjuk az elektromosság. Inkább az vált ki aggodalmat, hogy hogyan, ki és milyen célra használja az eszközt. Azok, akik gazdaságilag vagy ~~itt~~ profitálnának a jogok csorbulásából, általában azok, akik gyenge szabályozási környezetben kihasználják a mesterséges intelligencia képességeit.⁴²⁵ Így a "megfigyelési kapitalizmus" azért virágzik, mert a magánélethez fűződő jogok durván védtelenek, és a törvényeink nem tudtak lépést tartani a technológiával. Az utolsó jelentős szövetségi adatvédelmi törvényt (ECPA) 1986-ban hozták, még a Facebook, a Google és a YouTube, sőt a világháló előtt. Az adat- és mesterséges intelligenciával foglalkozó vállalatok időközben megnöttek és felvirágoztak, és ma már aránytalanul nagy hatalmat gyakorolnak a gazdaság, a közpolitika és az életünk felett.

Nincsenek átfogó szövetségi törvények a mesterséges intelligenciával kapcsolatban. Ezek hiányában az iparági önszabályozás és a tudatosság a legjobb, amiben reménykedhetünk. És bár a mesterséges intelligenciával foglalkozó közösségben - beleértve a nagy technológiai vállalatokat is - sokan osztják az itt megfogalmazott aggodalmakat, a piaci dominanciára való törekvés eddig felülírta az etikát és a jogokat.

Ez egy évtizedek óta húzóóda probléma. A közösségi média megjelenése és a felhasználói adatvédelem figyelmen kívül hagyása egyszerűen csak rontott a helyzeten, gyakran az intelligens algoritmusok segítségével. A helyzet valószínűleg még rosszabb lesz, ahogy a "tech-trösztök" egyre erősebb és áthatóbb mesterséges intelligenciát fejlesztenek. Az AI által lehetővé tett "magas szintű társadalmi ellenőrzés" a "digitális tekintélyelvűség és a liberális demokrácia közötti közelgő verseny előhírnöke lehet".⁴²⁶

A mesterséges intelligencia a külföldi hatalmak és a politikai hackerek kedvenc eszköze is, hogy befolyásolják a választásokat az Egyesült Államokban és külföldön. Az oroszországi és a Cambridge Analytica-botrányok ellenére keveset tesznek az állandónak tűnő kockázatok csökkentése érdekében. Az FBI igazgatója szerint

⁴²⁶ Wright, *fenti* megjegyzés 1.

⁴²⁶ Wright, *fenti* megjegyzés 1.

Christopher Wray, "ez nem csak egy választási ciklusbeli fenyegetés. A hirdetőink kitartoan és rendszeresen próbálják aláásni az országunkat".⁴²⁷

Egyes tudósok, filozófusok és futuristák riadót fújtak a mesterséges intelligencia és az autonóm robotok által az emberiségre jelentett egzisztenciális fenyegetés miatt.⁴²⁸ Mi közel sem megyünk ilyen messzire. De elkerülhetetlennek tűnik, hogy a mesterséges intelligencia mélyreható hatással van az alkotmányos jogokra és a demokratikus intézményekre. Ahogy Harari megjegyzi:

A mesterséges intelligencia eltörölheti a demokrácia számos gyakorlati előnyét, és alááshatja a szabadság és egyenlőség eszméjét. Tovább fogja koncentrálni a hatalmat egy kis elit körében, ha nem teszünk lépéseket a megállítására.⁴²⁹

Lehet, hogy nem kell megállítanunk a mesterséges intelligenciát, de mindenképpen oda kell figyelniük. "A szabályozás bevezetésének módja lassú és lineáris, [mégis] exponenciális fenyegetéssel nézünk szembe [az AI által]. Ha egy exponenciális fenyegetésre lineáris választ adunk, akkor elég valószínű, hogy az exponenciális fenyegetés fog győzni."⁴³⁰

Ebben a cikkben a mesterséges intelligencia kockázatait azzal a feltételezéssel tárgyaltuk, hogy a demokratikus eszmék a társadalom alapját képezik, és ezért meg kell őket védeni. De természetesen ez nem mindenhol igaz. Sok autoriter rezsim nem ért egyet a feltevésünkkel. Számukra a mesterséges intelligencia csodálatos eszköz arra, hogy megerősítsék az emberek feletti ellenőrzést. Kína például tökéletesíti a mesterséges intelligencia használatát a felügyelet fokozására.⁴³¹ A "China Brain Project" a mélytanulást használja arra, hogy információkat gyűjtsön az online

⁴²⁷ FBI Director Christopher Wray's Statement at Press Briefing on Election Security, 2018. augusztus 2., <https://www.fbi.gov/news/pressrel/press-releases/fbi-director-christopher-wrays-statement-at-press-briefing-on-election-security>.

⁴²⁸ *Lásd pl.* Bostrom, 15. lábjegyzet; Liu, 15. lábjegyzet. 22.

⁴²⁹ Yuval Harari, *Why Technology Favors Tyranny*, ATLANTIC (2018. október), <https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330>.

⁴³⁰ *Elon Musk: Humans Must Merge with Machines*, AXIOS (2018. november 26.), <https://www.axios.com/elon-musk-humans-must-merge-with-machines-1543240787-c51eee35-8cb3-4684-8bb3-7c51e1327b38.html>.

⁴³¹ *Lásd pl.* Paul Mozur, *Inside China's Dystopian Dreams*: N.Y. TIMES (2018. július 8.), <https://www.ny-times.com/2018/07/08/business/china-surveillance-technology.html>.

és offline felhasználói viselkedés.⁴³² Az így létrejövő "társadalmi kreditrendszer"⁴³³ új szintre emeli az adatgyűjtést, az adatfúziót és az elemzést. Talán nem meglepő, hogy a kínai kormány túlköltekezik a

Az Egyesült Államok kormánya a mesterséges intelligencia kutatásában,⁴³⁴ azzal a céllal, hogy globális szabványokat állítson fel a mesterséges intelligenciára vonatkozóan.⁴³⁵ Ahhoz, hogy az Egyesült Államok visszavegye a vezető szerepet, először is foglalkoznia kell az itt tárgyalt, a magánéletet és a demokráciát fenyegető nagyon is valós kockázatokkal. Ellenkező esetben azt kockáztatjuk, hogy Kína útjára lépünk.⁴³⁶

⁴³² Lásd Ünver, *Supra* note 7, a következő pontnál 7.

⁴³³ Lásd az Államtanács közleménye a szociális hitelrendszer létrehozásának tervezési vázlatának kiadásáról (2014-2020) (fordítás), <https://www.chinalawtranslate.com/socialcreditsystem> (utolsó látogatás: 2019. január 5.). ⁴³⁴ Lásd Christina Larson, *China's Massive Investment in Artificial Intelligence Has an Insidious Downside*, SCIENCE (2018. február 8.), <https://www.science-mag.org/news/2018/02/china-s-massive-investment-artificial-intelligence-has-insidious-downside>.

⁴³⁵ Lásd a kínai államtanács "New Generation Artificial Intelligence Development Plan" című tervét, amelyet Graham Webster és mások, *China's Plan to 'Lead' in AI: Purpose, Prospects, and Problems*, <https://www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems> (utolsó látogatás 2019. január) ismertetnek.

⁴³⁶ Lásd Farhood Manjoo, *It's Time to Panic About Privacy*, N.Y. TIMES (ápr. 10, 2019), <https://www.nytimes.com/interactive/2019/04/10/opinion/internet-data-privacy.html> ("Íme a rideg igazság: mi Nyugaton egy olyan megfigyelési államot építünk, amely nem kevésbé totalitárius, mint amelyet a kínai kormány épít").