



Nagy Zoltán András¹

A mesterséges intelligencia és a jogi felelősség kérdése – 2010–2020-as évek fordulóján de lege ferenda

A cím némi magyarázatot igényel, jelen tanulmányunkban napjaink mesterséges intelligencia² technológiai fejlettségét vizsgálva tudunk a jogi szabályokról gondolkodni. Bár a technológiai fejlődés fő vonulata felsejlik, de végkimenetele még nem látható előre. Az egyik szcenárió a szingularitás (az emberek képességeinek, tudásának feljavítása az orvostudomány nanotechnológiai kísérletei alapján), ám más irányt is vehet a fejlődés (a robotok érzelemnyilvánításra, erkölcsi mérlegelésre képessé tétele, ami a felelősségük megítélését is meghatározza). Valószínűsíthető, hogy mindkét kutatási irány nagyot lép előre.

Az első – úgynevezett általános célú – számítógépek építésének hajnalán egy kiváló brit matematikus, Alan Turing (aki az Enigma megfejtésén is dolgozott) megfogalmazta azt, ha egy gép beszélgetést folytat egy emberrel, akit nem gépként észlel, akkor a gép elérte az emberi intelligenciát (TURING 1950). Ez a Turing-teszt, amely azóta is tudományos viták középpontjában áll, ám egyben – valljuk meg – izgató probléma. A mesterséges intelligencia fogalmát John McCarthy alkotta meg 1956-ban (RUSSELL–NORVIG 2005, 14.).

A mesterséges intelligenciával összefüggő kutatómunka sikeressége, – ezzel el nem titkolható összefüggésben – annak finanszírozása, meglehetősen hektikusként jellemezhető az elmúlt majd hét évtizedben.

Az 1950-es évek utolsó harmadában megindult kutatómunka az 1970-es évek közepén tört meg, amikor a látványos eredmények elmaradása miatt az érdeklődés, és ezzel a költségvetési támogatás, megcsappant az AI-kutatások irányába.

Az 1980-as évek az AI felé fordulás időszaka. A brit kormány támogatta az AI-kutatásokat, hogy legalább részben versenyezzen a sikeres japán (katonai) kutatásokkal.

¹ Nemzeti Közszerológati Egyetem Rendészettudományi Kar Bűnügyi, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék, egyetemi docens; Pécsi Tudományegyetem Állam- és Jogtudományi Kar Bűntetőjogi Tanszék, egyetemi docens.

² KAPLAN 2016; ZÓDI 2018; FUTÓ 1999; BARNATT 2017; SCHWAB 2017; GOODMAN 2015; AMB-RUS 2018; KESERŐ 2019.

Majd az 1980-as évek utolsó harmadától az 1990-es évek elejéig tartó időszakban ismét hullámvölgy következett, amelynek oka részben az, hogy a tudomány és a piac érdeklődése az internet felé fordult, annak kommercializálódása, magánfelhasználók által is engedélyezett birtokbevétele új lehetőségek sorát ígérte. Ez a változás együtt járt azzal, hogy ekkortájt az úgynevezett általános számítógépek piaca is beszűkült.

Az elektronikus adattároló és -feldolgozó kapacitás, illetve a gyorsaság növekedése új lökést adott az AI-kutatásoknak. Látványos sikert (és persze reklámot) hozott a kutatásnak és a gyártóknak az IBM-féle Deep Blue számítógép 1997-es sikere a sakkvilágbajnok Garri Kaszparov ellen (BARNATT 2017, 98.).

Napjainkban sokat áldoznak a kutatásokra, s az alkalmazás szinte már valamennyi szférában megjelent a hatékony adatfeldolgozásnak köszönhetően: az üzleti célú elemzésektől, a nagyipari alkalmazásokon, kereskedelmi-logisztikai tevékenységeken, a háztartási alkalmazásokon, a számítástechnikán, a beszéd- és arcfelismerésen, az orvosi diagnosztikán, műtéti tevékenységen át a kibervédelemig. Folyamatosan fejlődik a 3D-s nyomtatás, az önvezető autók pedig már a „sarkon állnak.”

Elöljáróban szögezzük le, hogy a mesterséges intelligencia és a robotika kifejezések két külön fogalom. Azonban a kettőt kombinálva létrehozható egy intelligens robot, amelyben az AI „agyként”, a robot pedig „testként” működik.

Az AI, az öntanulás (*deep learning*), a robotok fizikai mozgási lehetőségeinek bővülése, az IoT-ba kapcsolt rendszerek és a robotok általi 3D-nyomtatása a jövő.

A modern technológiák alkalmazásának oktatása sürgető feladat. Számtalan égető kérdés kopog (dübörög) az ajtónkon: miből lesz bevétele az embereknek? lesz alapjövedelem? a robot fog adót fizetni? – *iam proximus ardet*.

A jogászok számára is kihívást jelent a modern technológiák működése során felmerülő veszélyek, károk beillesztése a hagyományos jogi keretek közé.

Az AI alkalmazása során a különböző jogágakban ismert károk keletkezhetnek:

- személyt, vagyontárgyat veszélyeztető vagy sértő;
- pénzügyi forrásokat, eszközöket érintő;
- immateriális javakat veszélyeztető vagy sértő;
- a *privacyt* érintő károk.

A továbbiakban a *Felelősség a Mesterséges Intelligencia és más feltörekvő digitális technológiáikért* (Liability for Artificial Intelligence and Other Emerging Digital Technologies) című jelentést vesszük górcső alá.

A jelentésben három szereplő felelősségét vizsgálják: a gyártó, az üzemben tartó és a működtető – ez utóbbi néha egy személy (szervezet) is lehet.

Az adatalapú döntést végrehajtó technológia jogi felelősségi szabályainak kimunkálásakor az alábbi körülmények figyelembevételét javasolja a bizottság:³

- a) a technológia összetettsége,
- b) átláthatatlansága,
- c) nyitottsága,
- d) autonóm működése,
- e) kiszámíthatatlansága,
- f) sebezhetősége.

Más szempontok is relevánsak lehetnek, amelyek a jogalkotás irányát, tartalmát is befolyásolhatják.

Ad a) A digitális technológiát az AI még bonyolultabbá teszi. Képzeljünk el egy hálózatot, amelyben rendszerbe kapcsolt eszközök (*Internet of Things* – dolgok, eszközök internete) működnek, továbbá a szenzorok, radarok, webkamerák által érzékelt impulzusokat – 5G adatátviteli technológiával – valamely felhőszolgáltatónál rögzítik, és az AI az innen kapott adatokat dolgozza fel, értelmezi, és hozza meg a döntését.

Látható tehát, hogy egy ilyen rendszer rendkívül bonyolult és összetett. Ebben az adatvezérelt hálózatban több eszköz és technológia működik, és ez elsősorban gyártó és az üzembentartó felelősségének megállapítására hat ki.

Ad b) A rendszer technológiailag bonyolult, és jelen pillanatban némileg szürke zóna az AI öntanulási folyamatának megértése. A hibaforrás azonosítása (mi okozta a rendellenes működést valójában, egyedi hiba vagy típushiba), ezzel a felelősség megítélése szintén rendkívül nehéz – elemeiben, részeiben nem csak a laikusok számára átláthatatlan.

Ad c) A technológia telepítését követően a digitális világban szükségszerű az operációs rendszer, a felhasználói programok, adatforrások frissítése (*firmware update*). A frissítések viszonylagos gyakorisággal vagy egy felmerült új problémára, veszély elhárítására, kivédésére reagálnak. A technológiának tehát nyitottnak kell lennie. Ugyanakkor a frissítés is lehet hibás, okozhat kárt, ezáltal a frissítés egy újabb (gyors) frissítésre is szorulhat.

Mivel a frissítés kötelezettsége a gyártót terheli, ez a termékfelelősség körébe tartozik, és az erre vonatkozó felelősségi szabályok szerint kell eljárni. Természetesen figyelemmel arra, ha a felhasználó szakszerű tanácsadás, kiképzés vagy leírás (protokoll) ellenére szakszerűtlenül telepíti a gyártó felajánlott frissítéseit.

³ Lásd: <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting-Doc&docid=36608> (A letöltés dátuma: 2020. 03. 10.)

Ad d) A technológia bizonyos feladatokat akár teljes mértékben önállóan, emberi beavatkozás vagy felügyelet nélkül hajt végre. Az AI döntését az öntanuláshoz kapott – *input* – adatok határozzák meg. A felelősség ismét csak az emberé, *in concreto*, milyen adatok elérését teszi lehetővé az AI számára. Az AI nem tud különbséget tenni „jó” és „rossz”, „helyes” és „helytelen” között, hanem a betáplált adatokból hozza meg a „saját” döntését.

Ad e) Némileg árnyaltabbá teszi a fenti megállapítást az, hogy a technológia nemcsak előre meghatározott impulzusokra reagál, hanem képes új impulzusokat is azonosítani, osztályozni, öntanulásának részévé tenni. Minél kifinomultabb a technológia, annál nehezebb megjósolni azt, hogy az öntanulás folyamata során mi lesz az AI döntésének eredménye, következménye. Az előre modellezett döntést fogja meghozni vagy egy ettől eltérőt?

Ad f) Az adatvezérelt hálózatok minél több elemből, egységből állnak, és minél több külső forrásból nyernek információkat, annál több potenciális sebezhetőségi pontjuk van. Így különösen ki vannak téve a kibertérből érkező támadásoknak, amelyek célja sokféle lehet: hacking, adathalászat, malware- vagy terheléses támadás, a rendszer működésének megzavarása, megbénítása. Kritikus infrastruktúrák ellen rendkívül szofisztikált, nehezen észlelhető, szakaszokra osztott, különböző támadási típusokat felhasználó, a védekező figyelmét elterelő „kamuveszélyeztetéssel” zajló APT- (*advanced persistent threat* – folyamatos fenyegetést jelentő) támadások a jellemzők.

A jó hír az, hogy jelen technológiai fejlettségi szinten nóvummal nemigen kell számolnunk. De ne bízzuk el magunkat, mert a jövőben ez változhat.

(1) *A technológia működtetőjének felelőségéről.* A jelentésben megfogalmazott ajánlás szerint, akik olyan megengedett technológiát működtetnek nyilvános térben, például az intelligens robotokat, amely működésével megnöveli más személyek károsodásának kockázatát, a veszélyes üzemi felelősség szabályai szerint tartoznak felelősséggel a károkért. Ha nem nyílt területen működik vagy mások károsodásának lehetősége kizárható (például háztartási robot, autonóm porszívó, autonóm fűnyíró), akkor az általános kárfelelősségi szabályok is elegendők.

A magyar polgári jogban a veszélyes üzem minden olyan tevékenységet felölel, amely működési rendellenessége esetén az átlagoshoz képest fokozottabb veszélyt hordoz magában.

A veszélyes üzem fogalma törvényben nem szerepel, életszerűtlen és felesleges a felsorolás a folyamatos technikai és műszaki fejlődés folyamatában. A bírói gyakorlat e körbe vonta általában a gépjármű és az egyéb, gépi működtetésű berendezések, eszközök, szerszámok használatát, kivéve a relatíve veszélytelen

eszközök, például a háztartási gépek működtetését. A magyar bíróság jelen fel-fogása találkozhat az EU-s szakbizottság javaslatával.

A veszélyes üzemi felelősség szigorúbb volta azt jelenti, hogy a veszélyes üzem működtetése esetén a károkozó csak akkor mentesül, ha bizonyítja, hogy a kárt olyan elháríthatatlan ok idézte elő, amely a fokozott veszéllyel járó tevékenység körén kívül esik, tehát a károkozó felelőssége nem függ attól, hogy vétkes-e a kár előidézésben (Ptk. 6:535. §).⁴

A mentesüléshez egyfelől azt kell bizonyítani, hogy a kár elháríthatatlan ok következménye. E szempont értékelésénél azt kell vizsgálni, hogy létezik-e olyan megoldás, amellyel a káreset elkerülhető lett volna. Tehát a műszaki és technikai előírások betartása önmagában nem mentesít a felelősség alól, ha a kár elkerülhető lett volna, ám nem tett meg mindent annak elhárítása érdekében.

A mentesülés másik feltétele, hogy a kárt a tevékenység körén kívül eső körülmény hozta létre, például vis maior (természeti katasztrófák, háborúk), továbbá a károsult vagy más külső személy elháríthatatlan ténykedése.

Veszélyes üzemi felelősség esetében nem kizárt a kármegosztás, különös tekintettel a károsult esetleges közrehatására (*victim blaming*).

Sőt, a Kúria további szempont figyelembevételét tartja szükségesnek a veszélyes üzem üzemeltetőjének kártérítése megállapításánál, így a károkozó vagy az üzemeltető netán felróható közrehatása mellett az üzem veszélyességét is figyelembe kell venni az üzemeltető terhére, amennyiben ez a veszélyes üzem károsodásában közrehatott (PK 38.).⁵

A veszélyes üzemi felelősség három év alatt évül el, de az AI-vel vezérelt és a folyamatosan frissített gépek, eszközök esetében indokoltnak tűnik – *de lege lata* – az öt évre emelés.

Olyan helyzetekben, amikor a szolgáltató magasabb szintű ellenőrzést gyakorol, mint a mesterséges intelligencia által vezérelt tényleges termék vagy szolgáltatás tulajdonosa vagy felhasználója, ezt figyelembe kell venni annak meghatározásakor, hogy elsősorban ki a technológia üzemeltetője.

(2) *Az üzemeltető felelősségéről.* Az üzemeltető felelőssége a működési körében szükséges és alkalmazható megfelelő AI-rendszer kiválasztása, e rendszer felügyelete, karbantartása, szakszerű működtetése, beleértve a frissítések telepítésének biztosítását. E kötelezettségek megszegéséért felelősséggel tartozik.

Ha például a mesterséges intelligencia által vezérelt drónt viharos időben használták, és emiatt a drón személyben, épületben, parkoló autóban stb. kárt okozott, a károkért a drón üzemeltetője a felelős.

⁴ Lásd: <https://net.jogtar.hu/jogszabaly?docid=a1300005.tv> (A letöltés dátuma: 2020. 03. 10.)

⁵ Lásd: <https://kuria-birosag.hu/hu/koll-allasfoglalasok/pk-38> (A letöltés dátuma: 2020. 03. 10.)

A technológia működtetője, gyártója és az üzembentartó közötti kármegosztás akkor jön szóba, ha a rendszer, az eszköz rendellenes működésében is vétkes.

Ugyanakkor a technológia gyártóját vagy működtetőjét terheli a felelősség a rendszer telepítésével, működésével, üzemeltetésével kapcsolatos információk megosztásáért az üzemeltetővel, az üzemeltetéshez szükséges technológiai ismeretek hozzáférhetővé tételéért, a protokollok megismertetéséért szöveges vagy képi formában, akár folyamatosan, a rendszer, az eszköz frissülését követve.

(3) *Az AI által vezérelt eszközért, rendszerért való termékfelelősségről.* A gyártók felelnek a termékek, illetve a digitális tartalmak beépítésével okozott hibákért.

Digitális tartalmak – 2019/771. EU-direktíva⁶ 28–31. bekezdései szerint – önállóan adásvétel tárgyai lehetnek (az áruk adásvételére irányuló szerződések egyes vonatkozásairól).

A felelősség a digitális tartalmak frissítésére is kiterjed.

(4) *A technológia bonyolultsága miatt a károsult személyeknek a bizonyítási teher megkönnyítendő.* Az EU-szakbizottság példaként említi azt az egyszerű esetet, amikor egy AI által vezérelt füstérzékelő nem jelezte a tüzet, és a lakás ezért leégett. Ugyanakkor a felhasználó azt nem fogja tudni megmondani, miért nem működött a füstjelző készülék.

(5) *A tevékenység naplózása.* A digitális világban a különféle operációs rendszerek és programok szöveges naplót (naplófájlokat) tartalmaznak, amelyek a rendszer, az eszköz működésbe helyezésétől annak befejezéséig – időbélyegzőt használva – rögzítik a végrehajtott tevékenységeket. Ezen információkat az úgynevezett *.log* fájlok tartalmazzák. Ha a *.log* fájlok hozzáférhetőek és teljesek, épek (nem manipuláltak), akkor mint bizonyítékok döntő fontosságúak a felek közötti – akár peres – vitában. Ugyanakkor a naplózott adatok mind a gyártó, mind a működtető számára rendkívül fontos információkat jelentenek a technológia működéséről, hibái jellegéről. A *.log* fájlokat tekinthetjük az AI-használat „feketedobozának”.

(6) *Immateriális javak megtérítésének kötelezettsége.* A sértett adatainak megsemmisítését károknak kell tekinteni a törvényhozás során, ezek, ha lehetséges, megtérítendőek vagy beszámítandók.

Ha az eltűnt, elveszett, „ellopott”, felülírt elektronikus adat meghatározott pénzüsszeget jelöl, akkor a kár egyértelműen megállapítható. Ha az AI szemé-

⁶ Lásd: https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2019.136.01.0028.01.ENG&toc=OJ.L:2019:136:TOC (A letöltés dátuma: 2020. 03. 10.)

lyiségi jogot sért működésével, akkor a magyar jogban a sérelemdíj intézménye alkalmazhatónak tűnik.

A sérelemdíj egyfelől egyértelműen a sérelmet szenvedett fél anyagi kárpót-lása, kompenzálása, másfelől az értékelési szempontjai a büntetőjogi szankcióban rejlő generális és speciális prevenció céljához viszi közel. A szankció kifejezi a kárt okozónak, hogy viselje magatartása következményét, és egyben alkalmas tevén-kenysége társadalmi rosszallásának megjelenítésére is (Ptk. 2:52. 3. §.).⁷ Emellett a jogsértőtől a kár megtérítése a követelhető (Ptk. 2:53.).⁸

(7) *Nem szükséges jogi személyiséggel felruházni az AI-t.* Az EP előterjesztése során felmerült az a kérdés, hogy az AI felelősségét a jogi személy felelősségéhez hason-lóan kellene-e megítélni. A szakbizottság megállapítása az, hogy nem szükséges a rendszereket, eszközöket (például robotokat) jogi személyiséggel felruházni, mivel az általuk okozott károk konkrét személyekhez köthetők, akik viselik a felelősséget.

A mesterséges intelligencia ma még nem rendelkezik azon érzelmi képes-séggel, etikai mérlegelési lehetőséggel, amellyel az ember. Az intelligens robot felróhatóságon alapuló felelősségéhez az emberi agy érzelmi életét⁹ kell(ene) meg-ismernünk, és átültetnünk gépekbe. Tudjuk, hogy az agy milliárd és milliárd neuront tartalmaz. Gondolkodunk, tanulunk, érzelmeink vannak, elvontan gondolkodunk azáltal, hogy elektromos kapcsolat jön létre a különféle neuro-nok között. Megválaszolatlan kérdés, hogy eme kapcsolatok miként hozzák létre e folyamatokat. A „komplex áramkör” ma még érthetetlennek tűnik... Minden, amit évezredek során megismertünk, tudunk, tehetünk, érzünk, egy szoftverrel egy gépbe telepíthető? Ez a jövő?

Irodalomjegyzék

- AMBRUS Éva (2018): Mesterséges intelligencia a közösségi médiában. *Hadmérnök*, 13. évf. 3. sz. 353–361.
- BARNATT, Christopher (2017): *Digital Genesis: The future of Computing, Robots, and AI*. H. n., ExplainingComputers.com.
- FUTÓ Iván szerk. (1999): *Mesterséges intelligencia*. Budapest, Aula.
- GOODMAN, Marc (2015): *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*. London, Penguin.

⁷ Lásd: <https://net.jogtar.hu/jogszabaly?docid=a1300005.tv> (A letöltés dátuma: 2020. 03. 10.)

⁸ Lásd: <https://net.jogtar.hu/jogszabaly?docid=a1300005.tv> (A letöltés dátuma: 2020. 03. 10.)

⁹ Richard J. Davidson és Sharon Begley által jegyzett könyv címe. Magyarul az Akadémiai Kiadó gondozásában jelent meg 2013-ban.

- KAPLAN, Jerry (2016): *Artificial Intelligence: What Everyone Needs to Know*. Oxford, Oxford University Press.
- KESERŰ Barna Arnold (2019): A mesterséges intelligencia néhány magánjogi aspektusáról. In GLAVANITS Judit szerk.: *A gazdasági jogalkotás aktuális kérdései*. Budapest, Dialóg Campus. 109–123.
- KOÓS Gábor – SZTERNÁK György (2019): A mesterséges intelligencia katonai felhasználásának lehetőségei. *Felderítő Szemle*, 18. évf. 4. sz. 117–134.
- MISKOLCZI Barna – SZATHMÁRY Zoltán (2018): *Büntetőjogi kérdések az információk korában. Mesterséges intelligencia, Big Data, profilozás*. Budapest, HVG-Orac.
- NAGY Zoltán András (2018): A jövő tegnap óta tart. A modern technikai-technológiai folyamatok kihívásai a jog területén. *Belügyi Szemle*, 66. évf. 10. sz. 36–55. DOI: <https://doi.org/10.38146/BSZ.2018.10.3>
- RUSSELL, Stuart – NORVIG, Peter (2005): *Mesterséges Intelligencia – Modern megközelítésben*. Budapest, Panem.
- SCHWAB, Klaus (2017): *The Fourth Industrial Revolution*. London, Penguin.
- TURING, Alan M. (1950): Computing Machinery and Intelligence. *Mind*, Vol. 59, No. 236. 433–460. DOI: <https://doi.org/10.1093/mind/lix.236.433>