

A MESTERSÉGES INTELLIGENCIA ADATVÉDELMI VONATKOZÁSAI¹

Ibolya Stefán

BEVEZETÉS

Az utóbbi években jelentősen megugrott a mesterséges intelligenciával (a továbbiakban: MI)² kapcsolatos kutatások, tanulmányok száma. Az emberiség elért a technológiai fejlődés azon fokára, melyen szinte minden feltétel adott az MI „életre kelteséhez”³. Ez az új, izgalmas technológia ugyanakkor feltáratlan is egyben, hiszen számos információnak vagyunk a hiányában. A mindennapi életünket lassan teljesen átszövő létező sokak számára ismeretlen, ahogyan annak adatvédelmi vonatkozásai. Ugyanakkor az utóbbi témakör nem elhanyagolható, hiszen napjainkban számos okos eszköz vagy applikáció alkalmazza a technológia által vezérelt arcfelismerő szoftvereket, melyekről később szólunk.

Jelen tanulmányban röviden meghatározzuk a mesterséges intelligencia fogalmát, valamint leggyakrabban felhasználási területeit. Ezt követően kitérünk a mesterséges intelligencia adatvédelmi vonatkozásaira az érintettek helyzetét tekintve. Továbbá megvizsgáljuk azt is, hogy a technológia megjelenése a személyes adatok védelme kapcsán milyen változásokat hozhat az általános adatvédelmi rendelet,⁴ illetve az információs önrendelkezési jogról és az információszabadságról szóló törvény⁵ szabályainak figyelembevételével. Végezetül pedig a feltárt adatvédelmi aggályok kapcsán ismertetünk néhány megoldási javaslatot.

¹ A kutatást az EFOP-3.6.2-16-2017-00007 azonosító számú, *Az intelligens, fenntartható és inkluzív társadalom fejlesztésének aspektusai: társadalmi, technológiai, innovációs hálózatok a foglalkoztatásban és a digitális gazdaságban* című projekt támogatta. A projekt az Európai Unió támogatásával, az Európai Szociális Alap és Magyarország költségvetése társfinanszírozásában valósul meg.

² A kifejezés angol megfelelője „artificial intelligence” (a továbbiakban: AI), a két kifejezés jelentéstartalma azonos, ezen oknál fogva a tanulmányban az „AI” rövidítést is alkalmazzuk, mint az „MI” idegen nyelvű megfelelőjét.

³ Jesus Rodriguez: About Google’s Self-Proclaimed Quantum Supremacy and its Impact on Artificial Intelligence. <https://towardsdatascience.com/about-googles-self-proclaimed-quantum-supremacy-and-its-impact-on-artificial-intelligence-63cb12d96527> (Letöltés ideje: 2020.02.09.)

⁴ 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 rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). A kifejezés angol megfelelője: General Data Protection Regulation (a továbbiakban: GDPR).

⁵ 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: Infotv).

1. A mesterséges intelligencia fogalmának meghatározása és megjelenése a mindennapokban

1.1. A mesterséges intelligencia definiálására tett kísérlet

Az MI általános, egységes definíciójának meghatározása embert próbáló feladat, hiszen számos szerző eltérő nézőpont szerint szemléli a technológiát, így más-más szempontot tart fontosnak a definiálás során. Ennél fogva úgy véljük az a legcélravezetőbb, ha az Európai Unió által megalkotott fogalmat vesszük alapul. 2018-ban az Európai Bizottság kiadta a „*Mesterséges intelligencia Európa számára*” elnevezésű dokumentumot, melyben röviden az alábbiak szerint határozták meg az MI fogalmát: „*A mesterséges intelligencia intelligens viselkedésre utaló rendszereket takar, amelyek konkrét célok eléréséhez elemzik a környezetüket és – bizonyos mértékű autonómiával – intézkedéseket hajtanak végre*”⁶. Ezt követően az Európai Bizottság által kifejezetten a mesterséges intelligencia tanulmányozására létrehozott magasszintű, független szakértői testület cizellálta az entitásra vonatkozó meghatározást. „*Az új fogalom szerint a mesterséges intelligencia alapú rendszerek olyan ember által tervezett szoftverek (és lehetőség szerint hardveres alapú rendszerek), melyek adott; meghatározott komplex célok elérése érdekében cselekszenek a fizikai vagy digitális dimenzióban, és elemzik környezetüket adatgyűjtés; az összegyűjtött rendszerezett vagy rendszertelen adatok értelmezése; tudásalapú érvelés vagy az információfeldolgozás által, a származtatott adatokból a legjobb, legmegfelelőbb cselekvést valósítják meg a meghatározott cél elérése érdekében.*”⁷ Ugyanakkor a fogalommal kapcsolandó kiemelő, hogy

⁶ „*Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals*”.

Mesterséges intelligencia Európa számára – A Bizottság közleménye az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. COM(2018) 237 final/2 (a továbbiakban: COM(2018) 237 final/2). Brüsszel, 2018. 06. 26, 1: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/HU/COM-2018-237-F2-HU-MAIN-PART-1.PDF> (Letöltés ideje: 2020.02.09).

⁷ „*Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions*”.

Independent High-Level Expert Group on Artificial Intelligence: A Definition of AI: Main Capabilities and Disciplines. Brussels, 2019.04.08.

Stéfán Ibolya: A mesterséges intelligencia fogalmának polgári jogi értelmezése. Pro Futuro, 2020/1. szám (megjelenés alatt) (A magyar nyelvű meghatározás a szerző saját fordítása).

az „nem kőbe vésett”, hiszen a technológia változásával a definíció maga is módosuláson eshet át a későbbiekben.

Az AI kapcsán fontos szólnunk arról, hogy a mesterséges intelligenciára elsősorban, mint szoftverre gondolunk. A technológia nem összekeverendő a fejlett robotokkal vagy önvezető autókkal, melyek akár MI-vel is működtethetők.

1.2. Az MI megjelenése napjainkban és a technológiával kapcsolatos adatvédelmi aggályok

Ahogy arra már a *Bevezetésben* utaltunk az AI észrevétlenül ugyan, de mindennapjaink szerves részét képezi. Sokan bizonyára elgondolkodnak azon, ez mégis hogyan valósulhat meg, hiszen nem látjuk folyamatosan a mesterséges intelligenciát. Sőt, a nevezett technológia leggyakrabban a szórakoztató irodalomban vagy filmekben jelenik meg. Közismert, hogy az MI legszorosabban a számítástechnikához kapcsolódik. Az AI-val közelebbi kapcsolatba a technológiai eszközök – úgy, mint az *okostelefonok*⁸, *számítógépek* – útján kerülhetünk.

A továbbiakban a nevezett technológia néhány gyakori megjelenési formáját, kívánjuk ismertetni, melyek a téma szempontjából relevanciával bírnak:

1. *Elektronikus levelezés:* A mai felgyorsult világban szinte mindenkinek van elektronikus levelezési címe. Eme alternatíva segítségével a különböző levelek, üzenetek gyorsabban érkeznek meg a címzetthez, mint a klasszikus postai kézbesítés esetében. Ezen oknál fogva a magánszemélyeken túl az üzleti szférában és az állami közegben is igen kedvelt levelezési forma, melyhez kapcsolódóan az MI számos hasznos feladatot lát el úgy, mint a kénytelen elektronikus levelek kiszűrése,⁹ a nyelvhelyesség ellenőrzése vagy a levélírás automatizálása¹⁰.

⁸ Az okostelefon fogalma nem egyértelműen meghatározott. Az Encyclopedia Britannica meghatározása szerint az eszközök olyan „számítógépes kijelzővel ellátott, beépített személyes információkezeléssel kapcsolatos programokkal rendelkező mobiltelefonok, melyekben jellemzően megtalálható egy személyes digitális asszisztens és egy operációs rendszer, ami lehetővé teszi más számítógépes szoftverek telepítését – internetes böngészéshez, e-mailekkel; zenével; videókkal kapcsolatos vagy egyéb alkalmazásokhoz. Az okostelefon úgy tekinthető, mint egy mobiltelefonba integrált kézi számítógépet”.

Hosch, William L.: Smartphone. Britannica Encyclopedia: <https://www.britannica.com/technology/smartphone> (Letöltés ideje: 2020.02.12).

⁹ Vincent, James: Gmail is now blocking 100 million extra spam messages every day with AI.: <https://www.theverge.com/2019/2/6/18213453/gmail-tensorflow-machine-learning-spam-100-million> (Letöltés ideje: 2020.02.22).

¹⁰ Thubron, Rob: New AI-powered Gmail feature can write emails for you.: <https://www.techspot.com/news/74533-new-ai-powered-gmail-feature-can-write-emails.html#commentsOffset> (Letöltés ideje: 2020.02.22).

2. *Digitális személyi asszisztensek*: A legismertebb személyi asszisztensek az Amazon által fogalmazott Alexa, az Apple által létrehozott Siri, illetve a Google Asszisztens. A hangvezérléssel irányítható eszközök közös pontja a mesterséges intelligencia általi működés¹¹. A készülékek felhasználási lehetőségei meglehetősen széles skálán mozognak, hiszen összekapcsolhatóak különböző okos eszközökkel úgy, mint okosóra, aktivitásmérő, okos televízió, okos hangfal, s a sor továbbfolytatható különböző háztartási eszközökkel. Lényegük abba áll, hogy a felhasználó által szóban elmondott feladatokat végrehajtják, így például válaszolnak a feltett kérdésre, lejátszanak egy meghatározott dalt vagy lekapcsolják a villanyt¹². Sőt egyes eszközök esetében még az érzelmek feltárására, az érzelmi állapot elemzésére is lehetőség van, melyhez a felhasználó mondatainak vizsgálatával jutnak hozzá¹³.

3. *Azonosítás*: Az MI felhasználása ezen a területen a legjelentősebb. Mi sem mutatja ezt jobban, mint az az előrejelzés, ami szerint a technológia piaca 2016-ban 16 milliárd dollár volt, ám ez az összeg 2020-re várhatóan 38,9 milliárd dollár lesz, ezzel 19,5%-os növekedést produkálva¹⁴. A kategórián belül megkülönböztethetjük az arcfelismerő rendszereket, a tárgyak felismerését – az említett két esetet nevezhetjük képfelismerésnek is –, illetve a hangalapú azonosítást. Mindhárom azonosítási forma ugyanazon a technológián alapszik, ám mi mégis az arcfelismerést kívánjuk ismertetni, mivel a téma kapcsán ennek van igazán jelentősége. A folyamat lényegében úgy történik, hogy egy adott képet – egy személy arcképét – összevetik mások, egy meghatározott adatbázisban szereplő arcképével. A technológia megjelenik például a Windows Azure¹⁵ vagy a Windows Hello programban, utóbbi arcfelismerés – biometrikus azonosítás – alkalmazásával teszi lehetővé a bejelentkezést¹⁶.

¹¹ TOP Intelligens asszisztensek: <https://www.aican.hu/blog/2018/06/29/top-intelligens-asszisztensek/> (Letöltés ideje: 2020.02.22).

¹² <https://www.apple.com/siri/> (Letöltés ideje: 2020.02.20).

¹³ Furey, Eoghan – Blue, Juanita: Alexa, Emotions, Privacy and GDPR. Proceedings of the 32nd International BCS Human Computer Interaction Conference, 2018 July, 2: https://www.scienceopen.com/document_file/0ecd5de8-97ee-43ef-a292-c957af52076a/ScienceOpen/BHCI-2018_Furey.pdf (Letöltés ideje: 2020.02.20).

¹⁴ Image Recognition Market by Technology (Digital Image Processing), Component (Hardware, Software, Service), Application (Augmented Reality), Deployment Type (On-Premises, Cloud), Industry Vertical, and Region – Global Forecast to 2021: <https://www.marketsandmarkets.com/Market-Reports/image-recognition-market-222404611.html> (Letöltés ideje: 2020.02.23).

¹⁵ <https://azure.microsoft.com/hu-hu/services/cognitive-services/face/#demo> (Letöltés ideje: 2020.02.23).

¹⁶ <https://www.microsoft.com/en-ie/windows/windows-hello> (Letöltés ideje: 2020.02.23).

A mesterséges intelligenciával kapcsolatos adatvédelmi probléma meglehetősen összetett. A probléma egyrészt a *technológia természetéből fakad*, hiszen működéséhez igen nagy mennyiségű adat szükséges, melyek később feldolgozásra, elemzésre és tárolásra kerülnek, melyek utóbb bármikor hozzáférhetőek. Ezekhez a tevékenységekhez minél több és jobb minőségű adatra van szüksége a technológiának, melyeken keresztül tanítja, fejleszti magát. Másrészt, az érintett adatok kapcsán aggályokat vet fel, hogy *nem egyértelműen meghatározott adatok köréről* vagy „*általános*” *adatokról van szó*, hanem legtöbb esetben olyan személyes adatokról, melyek érzékeny adatnak minősülnek, mint például a felhasználók egészségügyi vagy biometrikus adatai. A nevezett adatokhoz való hozzáférést lényegében maguk a felhasználók adják meg azzal, hogy használják az eszközöket, ám ennek nincsenek tudatában.

2. Az általános adatvédelemi szabályozás alapja

2.1. Az adatvédelmi szabályozás története

Majtényi László az adatvédelmi szabályozás *három generációját* különbözteti meg¹⁷. A továbbiakban az ő felfogása szerint vizsgáljuk az adatvédelmi szabályozás egyes generációit.

Az *első generációs adatvédelmi szabályozás* az 1960-as, 1970-es évekre tehető. A korszakban megjelentek az elektronikus alapú állami nyilvántartások, melyek lehetővé tették a nagyobb mennyiségű adat kezelését, s a nyilvántartásokban történő gyorsabb keresést. Továbbá ebben az időszakban került sor Európában az első adatvédelmi törvény elfogadására is. Az adatvédelmi tárgyú jogszabályok címzettje az állam volt, mivel lényegében – a nyilvántartások miatt – ő volt az egyetlen adatkezelő. A korabeli joganyagok célja egyrészt a megjelent új technológia szabályozása, másrészt az adatkezelés átláthatóságának megteremtése volt. Az adatalanyok jogai tekintetében kiemelendő, hogy pusztán részjogosítványokkal rendelkeztek, mint például a helyesbítéshez való jog.

A *második generációs szabályozás* vonatkozásában lényeges változást hoztak az 1980-as években megjelenő számítógépek, majd az 1990-es években megjelenő internet. Az egyre növekvő adatmennyiség miatt az üzleti szférában is megjelentek adatkezelők, így az adatvédelmi szabályozás hatályát ezen szereplőkre is kiterjesztették. A megjelölt időszakban a nemzetközi adattovábbítás kapcsán számos probléma merült fel, melyekre

¹⁷ Majtényi László: Az információs szabadságok – Adatvédelem és közérdekű adatok nyilvánossága. Complex Kiadó, Budapest, 2006, 94.

a jogalkotók igyekeztek megoldást találni. Ennek eredményeként 1981-ben megszületett a 108. Egyezmény, majd pedig 1995-ben az Európai Unió adatvédelmi irányelve.

Jelenleg a *harmadik generációs szabályozás* korát éljük. Az elmúlt 15–20 évben olyan jelentős technológiai változások mentek végbe, melyek miatt az 1990-es évek közepén, végén kialakított szabályozás folyamatos revíziója szükséges¹⁸. Jelen időszakra jellemző, hogy az egyének sokkal tudatosabbak az adatkezelést illetően, s megjelent részükről az igény a személyes adatok magas szintű védelmére, mivel adataik révén nem akarnak kiszolgáltatottá válni.

2.2. Az adatvédelem alkotmányos alapja és megjelenése egyes nemzetközi dokumentumokban

Az adatvédelem definiálása meglehetősen nehézkes, hiszen számos szerző eltérő álláspontot képvisel, más-más elemet hangsúlyoz a fogalomban. Ennélfogva annak általános definícióját legegyszerűbben a hazai szerző, *Majtényi László* fogalmazza meg az alábbiak szerint: „Az adatvédelem a személy, az ember, más szóval: az adatalany védelmét, nem pedig magának az adatnak a védelmét jelenti”¹⁹.

Az állam bizonyos feladatainak ellátása érdekében – pl. adózás – évszázadok óta nyilvántartást vezet. A modern állam egyre növekvő teendőinek eredményeként egyre több adat nyilvántartása; kezelése vált szükségessé, melyben az idővel megjelenő számítástechnika nagy segítséget nyújtott. Mindezek eredményeként megjelent az adatvédelem; a személyes adatok védelméhez való jog, mint alkotmányos alapjog. A nevezett alapjog a harmadik generációs jogok csoportjába tartozik, mely létrejöttét lényegében az utóbbi évtizedek technológiai fejlődésnek köszönheti²⁰. Mivel azonban a személyes adatok védelméhez való jog szoros kapcsolatban áll a magán- és család élet tiszteletben tartásához való joggal, s a magánszféra védelmének egyaránt eszköze, ezért a személyi szabadságjogok körébe is tartozik²¹.

¹⁸ Szöke Gergely László: Az adatvédelem szabályozásának történeti áttekintése. Infokommunikáció és jog, 2013/ 3. szám, 108–111: https://infojog.hu/wp-content/uploads/pdf/201356_SzokeGergelyLaszlo.pdf (Letöltés ideje: 2020.01.13).

¹⁹ Majtényi László: Adatvédelem, információszabadság, sajtó. Alkotmány- és Jogpolitikai Intézet, Budapest, 1997, 6.

²⁰ Sári János – Somody Bernadett: Alapjogok – Alkotmánytan II. (Negyedik, átdolgozott kiadás) Osiris Kiadó, Budapest, 2008, 133.

²¹ Balogh Zsolt – Gárdos-Orosz Fruzsina: A személyes adatok védelme és az információs önrendelkezési jog. In.: Halász Iván (szerk.): *Studia Universitatis Communia: Alkotmányjog. Dialóg Kampusz Kiadó, Budapest, 2018, 270.*

Az Alaptörvény szerint: „Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez”²². Az alapjog érvényesülése és garanciális védelme érdekében az Alaptörvény kimondja, hogy azt „sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi”²³, ez hazánkban a Nemzeti Adatvédelmi és Információszabadság Hatóság. Az Alaptörvény 2012. január 1-jén történő hatályba lépését megelőzően, Magyarország Alkotmánya is biztosította a személyes adatok védelméhez való jogot²⁴. Továbbá kimondta, hogy „A személyes adatok védelméről szóló törvény elfogadásához a jelenlévő országgyűlési képviselők kétharmadának szavazata szükséges”²⁵, így az alapjog a lehető legteljesebb védelemben részesült.

Az Alaptörvényben, illetve azt megelőzően az Alkotmányban a személyes adatok védelméhez való jog *expressis verbis* jelenet meg, ám az Alkotmánybíróság által hozott határozatok alapján az információs önrendelkezési jognak is kiemelkedő szerepe van. A 15/1991 (IV.13) AB határozatában „Az Alkotmánybíróság – a 20/1990. AB határozat szerinti eddigi gyakorlatát folytatva a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezi, hanem annak aktív oldalát is figyelembe véve, információs önrendelkezési jogként”²⁶. Ennek eredményeként a személyes adatok védelme nem pusztán az egyén, s adatainak védelmét jelenti, hanem azt is, hogy adatainak sorsáról ő maga dönthet. Továbbá a személyi szám alkotmányellenességéről szóló 15/1991 (IV.13) AB határozatában a „testület egyrészt állást foglalt a személyi szám mint korlátozás nélkül használható, általános és egységes személyazonosító jel alkotmányellenességéről, másrészt – a határozat indokolásában megalapozta a későbbi adatvédelmi törvény koncepcióját”²⁷.

A személyes adatok védelméhez való jog kapcsán szólni kell néhány szót az alapjog megjelenéséről is az egyes nemzetközi dokumentumokban. A korábbi emberi jogi dokumentumokban adatvédelemről nem esett szó, ami érthető is, hiszen az alapjog csak az utóbbi évtizedekben jelent meg. Ugyanakkor kiemelendő az Emberi Jogok Európai Egyezménye, mely

²² Magyarország Alaptörvénye (2011. április 25.), VI. cikk (3) bekezdés,

²³ Magyarország Alaptörvénye (2011. április 25.), VI. cikk (4) bekezdés,

²⁴ 1949. évi XX. törvény A Magyar Köztársaság Alkotmánya, 59. § (1) „A Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog”.

²⁵ 1949. évi XX. törvény A Magyar Köztársaság Alkotmánya, 59. § (2).

²⁶ 15/1991. (IV. 13.) AB határozat: <http://public.mkab.hu/dev/dontesek.nsf/0/1CE263A376458F27C1258382003C412C?OpenDocument> (Letöltés ideje: 2020.01.12).

²⁷ Sári – Somody: i. m., 134.

ugyan nem tartalmazza a személyes adatok védelméhez való jogot, ám annak 8. cikke – a magán- és családi élet tiszteletben tartásához való jogról – adatvédelmi szempontból meghatározó, hiszen az Európa Tanács Miniszteri Bizottsága számos adatvédelmi határozatában hivatkozott az említett cikkekre. Végül az Európa Tanács 1981-ben kidolgozta az *egyének védelméről a személyes adatok gépi feldolgozása során elnevezésű 108. Egyezményt*, mely mind a magánszektor, mind az állami szektor által végzett adatkezelésre vonatkozik. Ennek kapcsán fontos megjegyeznünk, hogy az Egyezmény rendelkezései csak az azt megerősítő államok vonatkozásában bírnak kötelező erővel, s azon országok számára is biztosított az Egyezményhez való csatlakozás lehetősége, amelyek nem tagjai az Európa Tanácsnak²⁸.

A személyes adatok védelméhez való jog kifejezetten pusztán az Európai Unió Alapjogi Chartájában²⁹ jelenik meg, az alábbiak szerint: „*Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni*”³⁰.

3. A mesterséges intelligencia adatvédelmi vonatkozásai

3.1. A mesterséges intelligencia hatása a személyes adat fogalmára

Az adatvédelmi alapok részletes ismertetését követően áttérünk a technológia adatvédelmi vonatkozásaira. Fontos megjegyeznünk, hogy az adatvédelmi kérdések kapcsán az általános adatvédelmi rendelet és az információs önrendelkezési jogról és az információszabadságról szóló törvény szabályanyagát együttesen vesszük figyelembe. A technológia alkalmazása során – természetéből fakadóan – igen nagy mennyiségű adatot gyűjt, dolgoz fel és kezel. Sőt még olyan adatokat is gyűjt, melyekre nem is gondolnánk. Ennek eredményeként arra a következtetésre jutottunk, hogy a személyes adatok köre az MI elterjedésével bővülni fog és olyan információk is relevánssá válnak, melyeknek korábban nem

²⁸ Európai adatvédelmi jogi kézikönyv (2018. évi kiadás). Kiadja az Európai Unió Alapjogi Ügynöksége és az Európa Tanács, 2019.

²⁹ 1981 után jóval később, 2000-ben került aláírásra az Európai Unió Alapjogi Chartája, mely az uniós tagállamok vonatkozásában kötelező erővel bír.

Lásd: Varga Zsófia: Az Alapjogi Charta alkalmazási köre I. Európai Jog 2013/5., 17-29.: <https://europaialkotmanyjog.eu/?p=820> (2020.03.02).

³⁰ Európai Unió Alapjogi Chartája 8. cikk (1) – (2) bekezdés: <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:12016P/TXT&from=HU> (Letöltés ideje: 2020.01.12).

tulajdonítottunk jelentőséget. Ennélfogva, akár az érzelemre vonatkozó információ is lehet személyes adat³¹, mivel ezek az információk az adott személytől elválaszthatatlanok, akárcsak a politikai nézetre vagy vallási hovatartozásra vonatkozó információk. Állításunkat alátámasztja az Andrew McStay egyik tanulmányában ismertetett eset, mely szerint egy cég fel akarta mérni, vásárlói, hogyan reagálnak érzelmileg egy reklámra. Ennek érdekében a vállalat létrehozott egy fiktív márkát, ami kávé értékesítéssel foglalkozott. A reklám lejátszását követően rejtett kamerákkal figyelték meg a vásárlói reakciókat, s az arckifejezések elemzéséből következtettek az érzelmekre³². Az így megszerzett adatok elemzését követően, akár az egyének manipulációjára is sor kerülhet a feltárt preferenciák tükrében.

A személyes adat fogalmát tekintve megállapíthatjuk, hogy a hazai szabályozás meglehetősen röviden határozza meg a fogalmat, az alábbiak szerint: „*az érintettre vonatkozó bármely információ*”³³. Ezzel szemben az általános adatvédelmi rendelet jobban cizellálja a fogalmat³⁴, ám a tartalmát tekintve elmondható, hogy a két fogalom azonos. A két szabályanyag ezt követően áttér az ún. szenzitív – érzékeny – adatok fogalmának meghatározására, teszi ezt azonos tartalommal és kifejezések használatával. Ennek keretében meghatározza a genetikai, biometrikus és egészségügyi fogalmát³⁵. Az említett fogalmakat vizsgálva láthatjuk, hogy az érzelem

³¹ A szakirodalomban megjelenő álláspont kapcsán, lásd:

Sedenberg, Elaine – Chuang, John: Smile for the Camera: Privacy and Policy Implications of Emotion AI

McStay, Andrew: Emphatic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy). Big Data and Society, 2016 July – December.

³² McStay, Andrew: Emphatic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy). Big Data and Society, 2016 July – December., 3.

³³ Infotv. 3. § 2. pont.

³⁴ GDPR. 4. cikk 1. pont: „személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

³⁵ Infotv. 3. § 3a. – 3c., GDPR. 4. cikk 13. – 15. pont

genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;

biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;

egészségügyi adat: egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

kifejezés egyik meghatározásban sem jelenik meg. Abban az esetben, ha mégis szeretnénk az érzelmekre vonatkozó információkat valamelyik adat kategóriájába sorolni, a biometrikus adatok köre lenne a legmegfelelőbb, mivel a technológia az érzelmekre vonatkozó információkhoz leginkább az arc egészének, egyes részeinek, a hanglejtés vagy a szívverés elemezésével juthat hozzá³⁶. Az érzelmekre vonatkozó információk kategorizálásával kapcsolatban, a szakirodalomban fellelhető olyan álláspont is, ami szerint a nevezett adatoknak, a személyes adatok új kategóriáját kellene képeznie³⁷. Ezzel szemben úgy véljük, hogy az említett kérdéskörrel kapcsolatban esetlegesen felmerülő problémák a hatályos szabályok szerint is megoldhatóak.

A szabályozás kapcsán meg kell jegyeznünk, hogy a GDPR főszabály szerint tiltja a különleges kategóriába – biometrikus, egészségügyi és genetikai adatok – tartozó személyes adatok kezelését, ám ez alól kivételek is ismertek, mint például az adat, érintett általi nyilvánosságra hozatala vagy a hozzájárulás megadása³⁸. A mesterséges intelligencia alkalmazása kapcsán a hozzájárulás megadása kérdéseket vethet fel hiszen, a hozzájárulás előtt szükséges az érintett megfelelő tájékoztatása, ám ez a technológia komplexitása miatt problémákat vethet fel, erre a következő alfejezetekben részletesen kitérünk.

3.2. Az adatkezelés alapelvei

Az adatvédelem érvényesülése szempontjából kiemelten fontosak az *adatkezelés alapelvei*. Az adatkezelés alapelvei lényegében garanciát nyújtanak, biztonságot jelentenek az érintetteknek, adatalanyoknak. Ezen oknál fogva fontos annak vizsgálata, hogy a mesterséges intelligencia kapcsán ezek az alapelvek hogyan érvényesülhetnek.

1. A célhoz kötöttség elve: értelmében az adatkezelés meghatározott, s jogszerű célból történhet, melynek az adatkezelés minden egyes szakaszában érvényesülnie kell³⁹. Utóbbi kapcsán fontos megjegyeznünk, hogy az adatkezelő saját belső szervezetén belüli adatkezelése

³⁶ Kiemelendő, hogy az adatvédelmi biztos gyakorlata szerint, már 2000-es évek elejétől személyes adatnak minősülnek „*a biometrikus azonosítók, vagyis mérhető testi jellemzők, így az ujjlenyomat, a retina és az írisz képe, a kéz geometriája, a hang és az arc jellemzői*”.

Jóri András – Soós Andrea Klára – Bártfai Zsolt – Hári Anita: A GDPR magyarázata. HVG-ORAC Lap-és Könyvkiadó Kft., Budapest, 2018, 76.

³⁷ McStay, Andrew: i. m., 6.

³⁸ GDPR. 9. cikk (1) – (2).

³⁹ A célhoz kötöttség elve megjelenik a 15/1991. (IV. 13.) AB határozatban, illetve a 65/2002. (XII. 3.) AB határozatban is.

vonatkozásában is érvényesülnie kell. Továbbá az alapelvnek az önként nyilvánosságra hozott adatok és a hozzájáruláson alapuló adatkezelés esetén is érvényre kell jutnia. A célhoz kötöttség elve olyan fontos adatvédelmi, adatkezelési alapelv, hogy a cél megváltozása esetén új adatkezelésre kerül sor. Ugyanakkor az adatvédelmi biztos gyakorlatában fellelhetőek olyan esetek – például az üdülő és adóhatóság közötti adatszolgáltatás – mikor jogszerűnek minősült az adatkezelés akkor is, ha az, az eredeti céltól eltért ugyan, de azzal összeegyeztethető volt⁴⁰.

2. *A tisztességes és törvényes adatkezelés*: alapján az adatkezelésnek jogszerűnek és lényegében az érintettek számára is átláthatónak kell lenni. Ez utóbbi kapcsán felmerül a kérdés, hogy az adatkezelés során történő MI alkalmazása esetén, eme követelménynek hogyan fognak eleget tenni, hiszen maga a technológia is meglehetősen bonyolult⁴¹ és a szakértők számára is számos ismeretlen komponenst tartalmaz, így produkálhat olyan eseteket, amelyekre korábban nem volt példa. Ez történt a Facebook chatbotok alkalmazása esetén is, mikor azok feladatvégzés közben az előre meghatározott angol nyelvről saját maguk által létrehozott nyelvre tértek át egymás közötti kommunikációjuk megkönnyítése érdekében, azonban ezt a nyelvet kutatók nem ismerték⁴². Ennélfogva, még inkább fontossá válik az etikusság, átláthatóság.

Továbbá a Nemzeti Adatvédelmi és Információszabadság Hatóság gyakorlatából kitűnik, hogy igyekeznek az alapelven keresztül a magánszféra védelmére is értelmezni a hatáskörüket, ez történt a termékbemutatók kapcsán⁴³. *„Tisztességtelen, az érintett személyes adatai védelméhez, illetve magánszférájához való jogát sértő módszer, ha termékbemutatót szervező, terméket ily módon értékesítő cégek az adatkezelés Infotv.-ben megjelölt körülményeiről valótlan, félrevezető tájékoztatást adnak annak érdekében, hogy a „tisztes hasznon” túl minél nagyobb profitra tegyenek szert, és így üzleti céljuk elérése érdekében az érintettek információs önrendelkezési*

⁴⁰ Jóri András – Soós Andrea Klára: Adatvédelmi jog – Magyar és európai szabályozás. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest 2016, 142–149.

⁴¹ Többek között idetartozik az ún. mélytanulási – deep learning – folyamata és az ún. fekete doboz – black box –, többek között az említett kérdéskörökkel foglalkozik Stuart Russel és Peter Norvig, a „Mesterséges intelligencia – Modern megközelítésben” című műben.

Lásd: Russell, Stuart J. – Norvig, Peter: Mesterséges intelligencia – Modern megközelítésben. (második, átdolgozott, bővített kiadás). Panem Könyvkiadó, Budapest, 2005.

⁴² Clark, Bryan: Facebook’s AI accidentally created its own language.: <https://www.businessinsider.com/facebook-chat-bots-created-their-own-language-2017-6> (Letöltés ideje: 2020. 02. 26.)

⁴³ Jóri – Soós: i. m., 154–155.

jogának gyakorlását korlátozzák”⁴⁴. A magánszféra védelme az AI kapcsán is fontos feladata, hiszen ahogyan arra már korábban utaltunk meglehetősen nagy mennyiségű adatot gyűjt és dolgoz fel. A magánszféra védelmének szükségességét jól szemlélteti az Amazon Alexa példája. Az incidens Németországban és az Egyesült Államokban is nagy visszhangot váltott ki, hiszen az eszköz világszerte számos háztartásban fellelhető. A nevezett esetben Amazon intelligens asszisztense Alexa felvette egy amerikai felhasználó beszélgetését, és azokat – szám szerint 1700 hangfelvételt – egy német felhasználónak továbbította. A problémára akkor derült fény, mikor a német felhasználó saját hangfelvételeit hallgatta vissza, idővel rájött, hogy a felvételek más felhasználóhoz tartoznak⁴⁵.

3. *Az adattakarékosság, adatminimalizálás elve*: az alapelv lényege, hogy az adatok kezelése a cél eléréséhez szükséges adatok körét érintően, csak a szükséges időtartamra és cselekményre korlátozódjon. Ennek kapcsán említésre méltó, hogy abban az esetben, ha az adatkezelő több azonos költségű eljárás közül választhat, amellyel a kívánt cél elérhető, akkor azt kell választania, ami az adatminimalizálás elvét a leginkább szolgálja, tehát kevesebb személyes adatot érint. Továbbá fontos, hogy az említett adattakarékosságnak a hozzájáruláson alapuló adatkezelés esetén is érvényesülnie kell⁴⁶.

4. *A pontosság és korlátozott tárolhatóság elve*: értelmében az adatoknak adatkezelés során pontosnak, teljesnek, s naprésznek kell lennie. A korlátozott tárolhatóság célja, hogy csak szükséges ideig tárolják az adatokat, s az adatalany is meghatározott ideig legyen beazonosítható⁴⁷. Ahogyan arról már korábban szóltunk az MI ember számára szinte felfoghatatlan mennyiségű adattal és rengeteg adatbázissal dolgozik. Ezen túlmenően az adatokat tárolja, elemzi saját tanulása, fejlesztése érdekében. Ennélfogva felmerül a kérdés mégis, hogyan feleltethető meg ez a technológia az adattakarékosság és a korlátozott tárolhatóság elvének.

Érdeemes néhány szót szólni az *integritás és bizalmi jelleg elvéről*, ami nem található meg az információs önrendelkezési jogról és az információszabadságról szóló törvényben, ám azt a GDPR tartalmazza.

⁴⁴ A Nemzeti Adatvédelmi és Információszabadság Hatóság jelentése a termékbemutatók adatvédelmi követelményeiről, 2015. március 4: <https://www.naih.hu/files/adatved-jelentes-termekbem.pdf> (Letöltés ideje: 2020.01.16).

⁴⁵ Statt, Nick: Amazon sent 1,700 Alexa voice recordings to the wrong user following data request.: <https://www.theverge.com/2018/12/20/18150531/amazon-alexa-voice-recordings-wrong-user-gdpr-privacy-ai> (Letöltés ideje: 2020.02.26).

⁴⁶ Jóri – Soós: i. m., 157–163.

⁴⁷ Infotv. 4. § (4) bekezdés.

Az alapelve lényege, hogy a személyes adatok kezelése során az adatok biztonsága biztosítva legyen különböző technikai, szervezési intézkedések által. Az adatbiztonsági intézkedések pedig lényegében az adatvédelem követelményét – az adatok védelmét – biztosítják. Ezzel kapcsolatot kívánnak teremteni az adatvédelem és az adatbiztonság között⁴⁸. Az alapelv kiemelkedő jelentőséggel bír az MI kapcsán, hiszen a megszerzett adatok igen sokfélék lehet, nem ritkán genetikai vagy biometrikus adatok kezelésére is sor kerülhet, éppen ezért fontos a technológia specifikus biztonsági intézkedések megtétele.

3.3. Az érintettek jogai

Az érintettek jogaival kapcsolatos számos rendelkezés közül csak a legáltalánosabbakat kívánjuk kiemelni, az egyéb szabályokkal nem kívánunk részletesen foglalkozni. Az érintettek jogainak érvényesülése igen fontos a mesterséges intelligencia alkalmazása során, a visszaélések elkerülése érdekében.

1. *Előzetes tájékoztatáshoz való jog: melynek értelmében az érintett jogosult arra, hogy tájékoztatást kapjon az adatkezelés megkezdése előtt*⁴⁹. Az adatkezelő, illetve adatfeldolgozó a nevezett jog érvényesülése érdekében az adatkezelés megkezdése előtt vagy azt követően haladéktalanul tájékoztatni köteles az érintettet többek között az adatkezelés céljáról, jogalapjáról és a személyes adatok forrásáról⁵⁰. A Nemzeti Adatvédelmi és Információszabadság Hatósága 2015. október 9-én ajánlást bocsátott ki az előzetes tájékoztatás követelményeiről, ami az érintettek jogaival kapcsolatos hatósági elvárásokat tartalmazza. Továbbá az Alkotmánybíróság gyakorlatára tekintettel a tájékoztatás kapcsán a közérthetőséget is megköveteli. „Az Alkotmánybíróság állandó gyakorlata alapján Magyarország Alaptörvénye VI. cikk (2) bekezdésében rögzített személyes adatok védelméhez való jog egyik legfontosabb alkotmányos követelménye az, hogy »mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatkezelés egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatait.« Ezen alkotmányos követelmény az adatkezelés megkezdése előtt az előzetes tájékoztatáson keresztül érvényesülhet”⁵¹. Az ajánlás által felhívott

⁴⁸ Jóri – Soós – Bártfai – Hári: i. m., 216.

⁴⁹ Infotv. 14. § a) pontja.

⁵⁰ Infotv. 16. § (1) – (2) bekezdés.

⁵¹ A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása az előzetes tájékoztatás adatvédelmi követelményeiről: <https://www.naih.hu/files/tajekoztato-ajanlas-v-2015-10-09.pdf> (Letöltés ideje: 2020.01.21).

törvényhely szövegezése módosításra került, így az idézett rész kikerült az Alaptörvényből, ám a továbbiakban is az ajánlásban megfogalmazottakra tekintettel kell eljárni. A tájékoztatáshoz való jog és a már korábban említett átláthatóság alapelve ugyanazt a problémát veti fel, nevezetesen azt, hogyan lehet az alapelv és az alapjog érvényesülését biztosítani a laikus felhasználók számára – akik nem rendelkeznek komoly számítástechnikai, programozási ismeretekkel – úgy, hogy a meglehetősen bonyolult folyamatokat megértsék, s a jövőre nézve megfontolt döntéseket tudjanak hozni a technológia igénybevétele kapcsán.

2. *Hozzáféréshez való jog: alapján az érintett kérelmére bármely az adatkezeléssel összefüggő információt tudomására kell hozni.* A 2018-as módosítást megelőzően lényegében az „*utólagos felvilágosításkérés jogaként*” jelent meg az információs önrendelkezési jogról és az információszabadságról szóló törvényben. A hozzáféréshez való jog az adatkezelés jogszerűségének ellenőrzését és az átláthatóságot hivatott szolgálni⁵². A nevezett jog érvényesülése az AI kapcsán sem elhanyagolható a korábban már említett széleskörű adatkezelés miatt.

3. *Helyesbítéshez való jog: szerint az érintett, kezelt adatai vonatkozásában kérheti, azok kiegészítését, helyesbítését*⁵³. A 2018. évi törvénymódosítást követően a helyesbítés joga már az adatok kiegészítését is magában foglalja.

4. *Adatkezelés korlátozásához való jog: értelmében az érintett, az adatkezelőhöz intézett kérelmében kérheti az adatkezelés korlátozását*⁵⁴. Az adatkezelés korlátozásához való jog célja, hogy a bizonytalan adatkezelési helyzeteket rendezze. Ez lényegében az adatok zárolását jelenti. Az eltérő terminológia használatának oka, hogy a jogalkotó ezzel kívánt reagálni az általános adatvédelmi rendeletben foglaltakra az érintettek jogai kapcsán⁵⁵.

5. *Törléshez való jog: alapján az adatkezelő törli az érintett személyes adatait, annak kérelmére*⁵⁶. A törlés kapcsán kiemелendő az ún. logikai törlés esete, mely szerint az adatok csak logikailag kerülnek törlésre,

⁵² Jóri – Soós – Bártfai – Hári: i. m., 280–281.

⁵³ Infotv. 14. § c) pontja.

⁵⁴ Infotv. 14. § d) pontja.

⁵⁵ 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 rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).

18. cikk Az adatkezelés korlátozásához való jog (1) „Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést...” <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679#d1e2128-1-1> (Letöltés ideje: 2020.01.21).

⁵⁶ Infotv. 14. § e) pontja.

fizikailag nem, a NAIH álláspontja szerint ez az eljárás nem megfelelő a törlés helyett⁵⁷.

Kétség sem fér hozzá, hogy az adatalanyok jogai fontosak, ám úgy véljük, hogy az MI használatával kapcsolatban talán az adatkezelés korlátozhatóságának és a törléshez való jognak van a legnagyobb relevanciája, hiszen a technológia által működtetett, összekapcsolt eszközök számos információt gyűjtenek és osztanak meg egymással. Ezen két jog a személyes adatok védelmén túl, lényegében lehetővé teszi a mesterséges intelligencia kordában tartását, ezáltal pedig az egyének magánéletének védelmét.

4. Megoldási javaslatok

A fentiek alapján látható, hogy a nevezett technológiával kapcsolatos adatvédelmi kérdések meglehetősen összetettek és bonyolultak. Éppen ezért a felmerülő problémák megoldása során a jogi keretek kijelölése mellett, figyelembe kell venni a mesterséges intelligencia sajátosságait is. Egyrészt fontos a megfelelő szabályozási környezet kialakítása, melynek a jogi rendelkezéseken túl erkölcsi-etikai szabályokat is tartalmaznia kell az entitásra vonatkozóan. Másrészt, a szoftverfejlesztőknek kell beépíteniük bizonyos garanciális elemeket a technológiába, melyek lehetővé teszik a megfelelő működést, ezzel elkerülve vagy legalábbis minimálisra csökkentve az adatvédelmi incidensek bekövetkezését, végső soron pedig az AI-val szemben megfelelő védelmet nyújtanak arra az esetre, ha valamilyen oknál fogva súlyosabb hiba következne be.

Ezen túlmenően fontos lenne, hogy a mesterséges intelligencia csak a legszükségesebb adatokhoz férjen hozzá és azokat ténylegesen csak meghatározott – lehetőség szerint minél rövidebb – ideig tárolja. Az érintettek kapcsán megfontolandó lehet a technológia működésére vonatkozó egyszerű, általános leírás, tájékoztató készítése. Ezzel biztosítva az átláthatóságot és hozzásegítve az érintetteket saját adataik védelméhez, valamint az érintetti jogok legteljesebb érvényesüléséhez. Ezen túlmenően szintén célravezető lenne, hogy minél több laikus ismerkedjen meg a mesterséges intelligenciával, a technológiára vonatkozó közérthető oktatás keretében.

Továbbá lényeges, hogy visszaszorításra kerüljenek az olyan technológiák, mint az arc-, vagy hangfelismerő szoftverek. Ezek kiemelt jelentőségét, s hasznosságát elismerjük a bűnüldözés terén, ugyanakkor az egyéb, MI által működtetett, azonosítás céljára szolgáló eszközök

⁵⁷ Jóri – Soós: i. m., 209.

adatvédelmi aggályokat vetnek fel. Ennek oka, hogy ezekkel a készülékekkel meglehetősen széles körben szerezhetőek be információk, érintve ezzel a legintimebb, legérzékenyebb adatokat, mint például egészségügyi, világnézetre vonatkozó vagy érzelmi állapottal kapcsolatos adatok.

Az arcfelismerő rendszerekkel kapcsolatos aggályok már megjelentek Franciaországban és Svédországban. Ezzel szemben a Fehér Ház 2020 januárjában arra kérte az uniós jogalkotókat, hogy tartózkodjanak a mesterséges intelligencia túlzott szabályozásától, hiszen az gátja lehet az innovációnak⁵⁸. Az AI szabályozásával kapcsolatos uniós „*Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése*” című dokumentumot az Európai Bizottság 2020. február 19-én adta ki, melyben nem tiltják ugyan az MI alkalmazásával kapcsolatos azonosító rendszereket, ám az alkalmazásukban rejlő veszélyeket figyelembe veszik⁵⁹. A Fehér Könyvből kitűnik, hogy az Európai Unió nem akar gátat szabni a fejlődésnek, támogatja az innovációt, mégis fontosnak tartja az esetleges adatvédelmi aggályok realizálását és igyekszik felkészülni a folyamatosan fejlődő technológiában rejlő veszélyekre.

KONKLÚZIÓ

A mesterséges intelligencia még csak gyermekcipőben jár, megjelenése mégis számos pozitív változást hozott, elegendő, ha csak a technológia által elvégzett hasznos feladatokra gondolunk. Vélhetően a technológia fejlődésével, az általa biztosított lehetőségek száma is bővülni fog. Ezen új entitás várható hatása leginkább úgy írható le, mint a gőzgépek vagy az elektromosság megjelenését követő változások. Ugyanakkor az MI-ben rejlő veszélyek sem elhanyagolhatók, jelenleg az AI a legnagyobb kockázatot a személyes adatok védelmére, s a magánélethez való jogra jelenti.

A technológiához kapcsolódó adatvédelmi kérdések meglehetősen bonyolultak és szerteágazóak. A komplexitás maga a mesterséges intelligencia természetéből fakad, ami lényegében egy sajátos módon működő szoftver. Működéséhez nagy mennyiségű adat szükséges, melynek érdekében rendkívül széleskörű adatgyűjtés történik. Ezen adatokat adatbázisokba rendszerezi, s eltárolja saját fejlesztése érdekében.

⁵⁸ Shepardson, David: White House proposes regulatory principles to govern AI use.: <https://www.reuters.com/article/us-tech-ces-ai-white-house-idUSKBN1Z60GL> (Letöltés ideje: 2020.02.23).

⁵⁹ Az Európai Bizottság által kiadott Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése. COM(2020) 65 final, Brussels, 2020.02.19.: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (Letöltés ideje: 2020.02.23).

Az adatvédelem kérdésköre kapcsán igyekeztünk rámutatni arra, hogy a személyes adatok köre az AI elterjedésével várhatóan növekedni fog. Ezen túlmenően igyekeztünk a mesterséges intelligencia által az adatkezelési alapelvekre, valamint az érintettek jogaira gyakorolt hatásokat vizsgálni, s rávilágítani az egyes problémás helyzetekre. Továbbá igyekeztünk a technológia szabályozásával kapcsolatban olyan javaslatokat megfogalmazni, amelyek megoldásként szolgálhatnak a felmerülő adatvédelmi aggályokra.

ÖSSZEGZÉS

Kutatásunk célja, hogy röviden ismertessük a sokak számára még ismeretlen, ám mindennapjainkban megjelenő mesterséges intelligenciát. Továbbá, hogy rávilágítsunk a technológia alkalmazásával kapcsolatos legfontosabb adatvédelmi aggályokra. Nevezetesen a személyes adatok körének várható bővülésére, illetve arra, hogy az adatvédelmi alapelvekre és az érintettek jogaira milyen hatást gyakorolhat a nevezett technológia. Ezen túlmenően a technológia szabályozása kapcsán megoldási javaslatokat fogalmaztunk meg az alapelvek és az adatalányok jogainak legteljesebb érvényesülése érdekében.

FELHASZNÁLT IRODALOM

1. Halász Iván (szerk.): *Studia Universitatis Communia: Alkotmányjog*. Dialóg Kampusz Kiadó, Budapest, 2018.
2. Furey, Eoghan – Blue, Juanita: *Alexa, Emotions, Privacy and GDPR*. Proceedings of the 32nd International BCS Human Computer Interaction Conference.
3. Jóri András – Soós Andrea Klára: *Adatvédelmi jog – Magyar és európai szabályozás*. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest 2016.
4. Jóri András – Soós Andrea Klára – Bártfai Zsolt – Hári Anita: *A GDPR magyarázata*. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2018.
5. Majtényi László: *Adatvédelem, információszabadság, sajtó*. Alkotmány- és Jogpolitikai Intézet, Budapest, 1997.
6. Majtényi László: *Az információs szabadságok – Adatvédelem és közérdekű adatok nyilvánossága*. Complex Kiadó, Budapest, 2006.
7. McStay, Andrew: *Emphatic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy)*. *Big Data and Society*, 2016 July – December, 1–11.
8. Sári János – Somody Bernadett: *Alapjogok – Alkotmánytan II.* (Negyedik, átdolgozott kiadás) Osiris Kiadó, Budapest, 2008.

9. Stefán Ibolya: A mesterséges intelligencia fogalmának polgári jogi értelmezése. *Pro Futuro*, 2020/1. szám (megjelenés alatt).

10. Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése. *Infokommunikáció és jog*, 2013/3. szám, 107–112.

11. Varga Zsófia: Az Alapjogi Charta alkalmazási köre I. *Európai Jog* 2013/5., 17–29.

Information about author:

Ibolya Stefán,
PhD hallgató
Miskolci Egyetem
Polgári Jogi Intézeti Tanszék

DOI <https://doi.org/10.30525/978-9934-588-43-3/1.4>