ACTA HUMANA • 2022/3. 95–123. • DOI: 10.32566/ah.2022.3.4

A mesterséges intelligencia felhasználásával történő adatkezelések egyes sajátos szempontjai[1]

NECZ DÁNIEL[2]

Jelen tanulmány a mesterséges intelligencia felhasználásával való adatkezelések egyes sajátos szempontjait ismerteti, ideértve különösen az adatkezelés jogszerűségével és megszervezésével, valamint az érintettek jogainak gyakorlásával kapcsolatos szempontokat, illetve a technológiából következő kihívásokat, továbbá kiemelt jelentőséget tulajdonít az egyes, technológiával kapcsolatos etikai szempontok és problémák feltárásának, illetve ennek az adatkezelésre gyakorolt lehetséges hatásait is ismerteti. A tanulmány mindemellett kitér a mesterséges intelligencia szabályozásával kapcsolatos európai jogfejlődésre, valamint az Amerikai Egyesült Államok szabályozási vívmányaira, továbbá ismerteti az európai és az amerikai megközelítés közötti különbségeket. Mindemellett a tanulmány látleletet ad a mesterséges intelligencia felhasználásával történő adatkezelések egyes szektorális kérdéseiről és problémáiról, különösen a munkahelyi, az egészségügyi és a reklámcélú adatkezelések területén.

Kulcsszavak: mesterséges intelligencia, adatvédelem, fekete doboz, átláthatóság, etika

Certain Aspects of Data Processing Using Artificial Intelligence

The paper describes certain aspects of data processing using artificial intelligence, including in particular aspects related to the lawfulness and organisation of processing, the exercise of data subjects' rights and the challenges posed by the technology. The paper also focuses on the identification of ethical aspects and problems related to the technology and their possible implications for data processing. The paper further discusses the

1 A tanulmány az ELTE-ÁJK adatbiztonsági és adatvédelmi szakjogász képzésén írt *A mesterséges intelligencia felhasználásával történő adatkezelések* című szakdolgozata alapján, annak felülvizsgálatával, illetve a felülvizsgálat tekintetében az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

2 Ügyvéd, doktori hallgató, Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Kar, e-mail: dnecz@llm22.law.harvard.edu

development of European law concerning the regulation of artificial intelligence and the regulatory solutions of the United States, and highlights the differences between the European and the American approaches. It also provides an overview of some of the sectoral issues and problems of data processing relying on artificial intelligence, in particular regarding in the areas of workplace, healthcare and advertising.

Keywords: artificial intelligence, data protection, black box, transparency, ethics

Bevezetés

A mesterséges intelligencia (MI) fokozatosan változtatja meg mindennapjainkat. Gyorsabbá és hatékonyabbá teszi a közlekedést, gördülékenyebbé a kommunikációt és az ügyintézést, tehermentesíti a napi munkát. Találkozhatunk vele éppúgy kórházakban, mint repülőtereken vagy a munkahelyünkön; az MI-ben, valamint az általa végzett adatfeldolgozási megoldásokban fekvő potenciál pedig a nagyvállalatokat és a kutatóintézeteket is további fejlesztésekre és befektetésekre sarkallja. Nem vitás, hogy az MI jól megfér napjaink globalizálódó termelési-értékesítési folyamatait teljes mértékben elektronizáló digitális gazdaságában,[3] az MI hatásai pedig szinte valamennyi területen egyre inkább tetten érhetők, a pénzügyi piacok brókereket helyettesítő algoritmusain át az okos egészségügyi megoldásokig, valamint a különböző festészeti vagy épp irodalmi alkotásokat létrehozó szoftverekig. Természetesen az előnyök mellett a technológiával járó kockázatok köre is beláthatatlannak mondható. 2017-ben például a Facebook nevű amerikai közösségimédia-szolgáltató kényszerült arra, hogy az egyik MI-alapú megoldását lekapcsolja, miután az kifejlesztett egy olyan gépi nyelvet, amelyet sem a felhasználók, sem maguk a programozók nem voltak képesek megérteni.[4] Az ilyen esetek pedig intő jelül szolgálnak arra, hogy milyen következményekkel is járhat, ha a mesterséges intelligenciát megfelelő fékek, illetve kontroll nélkül alkalmazzuk.

Akár a technológia előnyeit, akár annak hátrányait nézzük, mindenképpen leszögezhető, hogy az MI lételeme az adat. A beláthatatlan mennyiségű személyes adatot és egyéb információt összesítő adathalmazok (big data) különösen fontosak a tanulási fázisban, ahol a mesterségesintelligencia-megoldást megtanítják valamilyen műveletre, e fázisok pedig jellemzően az adott megoldás teljes életciklusát végigkísérik, így maguk az alapul fekvő adatok is folyamatos átvizsgálásra, továbbképzésre vagy „tisztításra" szorulnak. Képfelismerési szoftverek esetén például jellemző, hogy több ezernyi vagy akár milliónyi fényképet is beolvas, majd összevet egymással a szoftver, mire eljut arra a szintre, hogy egy bizonyos személyt felismerjen, kellő pontossággal azonosítson. Figyelembe véve pedig az MI e tulajdonságát, leszögezhető, hogy

3 Perecz 2012, 18.
4 Bradley 2017

az érintettek adatvédelmi jogait különös súllyal érintik a különböző MI-alapú megoldások általi adatelemzések, mivel ezek jellemzően lehetővé teszik az egyes személyek jellemzőinek, szokásainak, véleményének, fizikai és egyéb ismertetőjegyeinek részletes kiértékelését, marketing- vagy egyéb célú felhasználását, és más személyekkel való tömeges összehasonlítását. Minderre tekintettel pedig leszögezhető, hogy az európai MI-szabályozás, valamint a tagállamok nemzeti MI-stratégiájának alapvető kapcsolódási pontjaként különösen a személyes adatok védelme említhető, amely a mesterséges intelligenciával kapcsolatos tudományos és szabályozási törekvések számára is fogódzkodót jelent. A személyes adatok védelme továbbá az Amerikai Egyesült Államok MI-szabályozásában is jelentős szerepet tölt be, nagyobb fokú felelősséget várva el a jelentős számú személyes adatot kezelő, valamint az MI általi döntéshozatalra támaszkodó vállalkozásoktól.

A fentiekre tekintettel tanulmányomban a mesterséges intelligencia általi adatkezelés helyes megszervezésének főbb kritériumaira kívánok koncentrálni, a legújabb szabályozási törekvésekre, adatvédelmi hatósági gyakorlatra és egyes szektorális adatkezelési problémákra is tekintettel. Fel kívánom tárni továbbá az etikus mesterséges intelligenciával kapcsolatos elvárások adatvédelmi kapcsolódási pontjait, bizonyítva, hogy a mesterségesintelligencia-megoldásokat alkalmazó adatkezelők nem nélkülözhetik az etikai szempontok figyelembevételét sem az adatkezelés megszervezésénél, akár az európai, akár az amerikai szabályozást nézzük.

A mesterséges intelligencia meghatározása és etikai szempontjai

A mesterséges intelligencia története egy idős a gondolkodó gépekről és egyéb alkotásokról szóló mesékkel és mondákkal. Már Ovidius, a római költő is lejegyezte Pygmalion, a szobrász történetét, aki szerelmes lett a saját művébe, amelynek ihlető ereje hatására a szobor életre kelt, és a későbbi korok alkotói is gyakran törekedtek önműködő vagy annak hitt gépek létrehozására (ideértve például Kempelen Farkas sokáig önműködőnek gondolt sakkozógépét).

Bár e korai automatizált gépezetek működési elve és hatékonysága mai szemmel erősen megkérdőjelezhető, és nehézkesen nevezhetnénk őket mesterséges intelligenciának, létezésük önmagában bizonyítja azt a határtalan érdeklődést, amelyet a gondolkodó gépek és ezek potenciális képességei keltettek az emberekben. Ezt a lelkesedést ragadták meg az irodalom nagyjai is, akik a 19., valamint a 20. század során fokozatosan foglalkoztak az MI-ben rejlő lehetőségekkel, valamint a robotok tömeges megjelenésével járó társadalmi hatásokkal és veszélyekkel, ideértve különösen Isaac Asimov munkásságát és az általa lefektetett robotika alaptörvényeit.[5]

Mindezen művek fogódzkodót jelentettek a későbbi tudományos kutatások számára is, akárcsak maga az emberi elme és annak felépítése. Ezen időszak egyik

5 A robotika alaptörvényei elsőként Isaac Asimov *Runaround* (magyarul *Körbe-körbe*) című novellájában jelentek meg, az *Astounding* című amerikai fantasztikus folyóirat 1942. márciusi számában.

meghatározó fejleményének tekinthető az angol matematikus, Alan Turing által alkotott és később róla elnevezett, az 1950-ben megjelent *Számítógép és értelem* című tanulmányában publikált Turing-teszt. A teszt egyfajta imitációs játéknak is tekinthető. A játék lényege, hogy a kérdező meg tudja-e állapítani beszélgetőpartneréről, hogy az illető ember-e vagy gép (program).[6] A teszten ez idáig a legfényesebb eredményeket egy számítógépes program produkálta, amely 2014-ben meg tudta győzni a brit Royal Society tagjainak jelentős részét arról, hogy egy ukrán kisfiú, nem pedig egy MI-alapú megoldás, amelyet Vladimir Veselov és Eugene Demchenko programozók fejlesztettek ki.[7] Mindezek alapján az MI elmúlt évtizedekben bekövetkezett rohamos fejlődését tekintve számos kutató és véleményformáló veti fel napjainkban a kérdést, hogy meddig is tudjuk kordában tartani majd az MI-t, és mikor jut el a technológia arra a pontra, hogy emberi kontroll nélkül hozzon saját döntéseket. Ahhoz azonban, hogy a vonatkozó kockázatokat felbecsülhessük, nem árt tisztázni bizonyos alapfogalmakat.

A mesterséges intelligencia napjainkban nem rendelkezik egységes és általánosan alkalmazható definícióval. Az egyes szakirodalmakban elterjedt meghatározások – a korábbi irodalmi és technológiai előzményeket figyelembe véve – főként a technológia problémamegoldásra való képességeit, valamint az emberi intelligenciához való viszonyát helyezik előtérbe. Így Fekete István, Gregorics Tibor és Nagy Sára szerzők meghatározása szerint a mesterséges intelligencia egyszerre célozza meg magát az embert, illetve ennek tevékenységét helyettesítő rendszerek létrehozását, valamint ezzel együtt az (emberi) intelligencia természetének és sajátosságainak megismerésére is lehetőséget ad;[8] ezzel szemben Elek István emberi módra és logikusan gondolkodó gépeket különböztet meg.[9] Részben hasonló meghatározást ad az Európai Bizottság Európának szóló *Mesterséges intelligencia* című tanulmánya, amely szerint a mesterséges intelligencia olyan rendszereket ölel fel, amelyek konkrét célok elérése érdekében elemzik a környezetüket, és hoznak meg intézkedéseket.[10] A fentiekhez hasonlóan ugyancsak a technológia tanulási képességeire helyezi a hangsúlyt *Magyarország Mesterséges Intelligencia Stratégiájának* meghatározása, amely akként határozza meg a mesterséges intelligenciát „mint a betáplált adatok alapján önmagukat tanítani és javítani képes algoritmikus rendszerek összessége".[11]

A fentiekből is jól látszik, hogy a legtöbb tudományos meghatározás az MI-t egyszerre tekinti logikusan, valamint emberi módra, vagy legalábbis ahhoz hasonlóan gondolkodó rendszernek, amely végső soron – mint emberi alkotás – képes az emberi intelligencia bizonyos fokú reprodukálására. Mindemellett olyan rendszernek is tekinthető, amely képes felmérni a környezetét, és az emberhez hasonlóan a környe-

6 Turing 1950, 433–434.
7 BBC News 2014
8 Fekete–Gregorics–Nagy 1990, 1.
9 Elek 2015, 22–23.
10 Európai Bizottság 2018
11 Innovációs és Technológiai Minisztérium 2020, 6.

zete és az abban lejátszódó változások alapján meghozni döntéseit. Az MI-vel kapcsolatos etikai problémák gyökerét azonban legtöbbször épp a döntési folyamat emberi átláthatóságával kapcsolatos nehézségek adják. Ezt nevezik „fekete doboz" problémának is, amelynek az MI általi adatkezeléseket tekintve különös jelentősége van, mivel az információs önrendelkezési jog egyik legfontosabb biztosítéka nem más, mint az adatkezelés átláthatósága, amely az érintetti oldalon jogként, míg az adatkezelő oldalán kötelezettségként jelentkezik. Erre tekintettel az MI-alapú megoldások általi adatkezelések esetén alapvető kihívásnak minősülnek a megoldás által figyelembe vett főbb szempontok, és ezeknek a rendszer által hozott döntésre gyakorolt hatásának azonosítása, valamint az érintettek erről való megfelelő és átlátható tájékoztatása.

A fentiekkel összhangban leszögezhető, hogy az MI-alapú megoldások alkalmazása esetén az ezekre irányadó etikai szempontokat is figyelembe kell vennie az adatkezelőknek, ellenkező esetben az általuk folytatott adatkezelések tisztességtelennek, és így végső soron adatvédelmi szempontból is jogsértőnek minősülhetnek. Ezzel kapcsolatban az Európai Bizottság *Az emberközpontú mesterséges intelligencia iránti bizalom növelése* című anyaga is meghatároz olyan követelményeket, amelyeknek a megbízható, európai mesterségesintelligencia-rendszereknek meg kell felelnie, kiemelve az alábbi fő követelményeket:

- az emberi cselekvőképesség támogatása és emberi felügyelet;
- műszaki stabilitás és biztonság;
- adatvédelem és adatkezelés;
- átláthatóság;
- sokféleség, megkülönböztetésmentesség és méltányosság;
- társadalmi és környezeti jólét;
- elszámoltathatóság.[12]

A fentiek értelmében tehát e követelményeket valamennyi MI-alapú megoldás tekintetében figyelembe kell venni, összhangban az adatvédelmi alapelvekkel és az érintetti jogok gyakorlása támogatásának, valamint a megfelelő adatbiztonsági szint garantálásának követelményével.

A fentieket követően az Európai Bizottság 2020-ban nyilvánosságra hozta a mesterséges intelligenciáról szóló fehér könyvét, amelyben leszögezte, hogy

> „a mesterséges intelligenciára vonatkozó európai megközelítés célja, hogy előmozdítsa Európa MI-innovációs kapacitását, támogatva az etikus és megbízható mesterséges intelligencia fejlesztését és elterjedését az uniós gazdaságban. A mesterséges intelligenciának az emberek javát és hasznos társadalmi célokat kell szolgálnia."[13]

12 Európai Bizottság 2019
13 Európai Bizottság 2020

Mindezen fenti meglátással pedig az Európai Bizottság világossá tette, hogy az európai MI-szabályozásnak kizárólag az etikus és megbízható MI-alapú megoldások jelentik az elfogadható mértéket, amelyek alkalmazását és elterjedését azonban a kialakuló európai szabályozásnak támogatnia kell.

Megemlítendő azonban, hogy a 2021-ben megjelent, az Európai Mesterséges Intelligenciáról szóló Jogszabály tervezete[14] is széles körben irányoz elő szabályokat az MI-alapú megoldásokra, azokat kockázati kategóriákba sorolva, és ennek megfelelően támasztva velük szemben követelményeket. A fenti tervezet által alkalmazott fogalmak, illetve szabályozás azonban – a személyes adatok kezelésével kapcsolatos jelentősége ellenére – nem áll teljesen összhangban a GDPR-al, amely egyben értelmezési nehézséghez is vezethet. Erre tekintettel többek között a GDPR-al és egyéb adatvédelmi jogszabályokkal való összhang hiányának elkerülését emeli ki az Európai Adatvédelmi Testület és az Európai Adatvédelmi Biztos 5/2021-es Közös Véleménye is.[15] Ennek tükrében kiemelt szempontnak tekinthető az MI-tárgyú európai szabályozás egységes kialakítása és értelmezési köre, amely egyben az egyes piaci szereplők könnyebb eligazodását és az egyes szektorok hatékony önszabályozási megoldásainak kialakítását is segíthetik.

A mesterséges intelligenciával folytatott adatkezelés

Az MI-vel folytatott adatkezelések gyakran jelentős kihívást jelentenek az azokat alkalmazó adatkezelők számára, különös tekintettel a technológiában rejlő kockázatokra, az MI által hozott döntések és következtetések gyakran nehézkes megjósolhatóságára, valamint a vonatkozó folyamatok komplexitására. Az alábbi sorokban azt tekintjük végig, hogy az MI felhasználásával folytatott adatkezeléseknek milyen követelményeknek kell megfelelniük az uniós és az amerikai jog tükrében, valamint ezen adatkezelések kapcsán milyen sajátos szempontok érvényesülhetnek.

Az adatkezelés jogszerűsége az uniós jog tükrében

Az MI által folytatott adatkezelés jogszerűsége[16]

Fontos hangsúlyozni, hogy az adatkezelés alapelvei az MI-alapú megoldások segítségével folytatott adatkezelések esetén is alkalmazandók, figyelemmel a technológia sajátosságaira, valamint az annak segítségével végzett tevékenységek körülményeire. Kiemelendő továbbá, hogy a technológia legfontosabb jellemzőjét képezi a belátha-

14 A Mesterséges Intelligenciáról szóló Jogszabály tervezete

15 Az Európai Adatvédelmi Testület és az Európai Adatvédelmi Biztos 5/2021. sz. közös véleménye a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról szóló európai parlamenti és tanácsi rendeletről, 16.

16 Az MI általi adatkezelés jogszerűsége kapcsán – bár eltérő szempontok kiemelésével – ugyancsak a személyes adatok kezelésére vonatkozó alapelveknek, valamint az adatkezelés jogalapjainak való megfelelést tárgyalja Necz 2020a, 143–150.

tatlan nagyságú adathalmazokra támaszkodás, az érintettek számára gyakran nehézkes átláthatóság, valamint a technológia erős behatása az érintettek magánéletébe (például arcfelismerés útján vagy az érintettek viselkedésének vizsgálatával, egyes jellemzőinek értékelésével), így az ebből eredő kockázatokat az adatkezelő köteles a lehetőség szerint csökkenteni, a fentebb írtakra pedig az érintettek figyelmét felhívni. Tekintettel a fentiekre, különösen ideértve az MI általi adatkezelés sajátosságait, az alábbiakban foglaljuk össze részletesen, hogy az adatkezelés alapelvei a technológia alkalmazása során hogyan is érvényesülhetnek:

- *Jogszerűség, tisztességes eljárás és átláthatóság:* ezen alapelv értelmében az adatkezelés csak jogszerű célból végezhető, valamint tisztességes és az érintettek számára transzparensnek mondható módon. Például, ahogy arra a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) egy 2022-ben hozott döntése egy ügyben rávilágított, az adatkezelő telefonos ügyfélszolgálatával kapcsolatban álló ügyfelek érzelmi állapota MI segítségével folytatott hangelemzés révén, illetve ezen érintettek számára átláthatatlan módon nem ellenőrizhető.[17] Ezen alapelvnek való megfelelés különösen fontos garanciát képez az automatizált döntéshozatal, illetve a profilalkotás területén, amelyek az MI-alapú megoldásoknál gyakorinak mondhatók. Ezen esetekben az alkalmazott megoldás mögötti logikát, valamint az adatkezelés jelentőségére és az érintettre gyakorolt következményekre vonatkozó információkat is meg kell adnia az adatkezelőnek, szerződés teljesítésén vagy hozzájáruláson alapuló adatkezelés esetén pedig – az érintetti autonómia biztosítékaként – lehetővé kell tenni az érintett részére az emberi beavatkozás kérésének, az álláspont kifejezésének, valamint a vonatkozó döntéssel szembeni kifogás megtételének jogát.[18] Kiemelendő azonban, hogy bár e jogok gyakorlása csökkentheti az MI általi diszkriminációt (például adott esetben ideértve a hitelbírálathoz, szociális juttatások iránti kérelem elbírálásához vagy toborzáshoz használt MI-alapú megoldások általi diszkriminációt) lehetőségét, azonban az érintettek jogainak messzemenő védelme érdekében az ilyen algoritmusokat alkalmazó adatkezelőknek különösen jelentős hangsúlyt kell fektetniük ennek kiküszöbölésére,[19] amely magában foglalja az alkalmazott megoldás folyamatos felülvizsgálatát, az esetleges visszaélések és hibák orvoslását, megelőzését is. A fenti kockázatok kiküszöbölését különösen segítheti a technológiai környezet megfelelő kialakítása, továbbá a fenti célból alkalmazott intézkedések és azok tényleges, illetve tervezett hatásainak részletes bemutatása az adatvédelmi hatásvizsgálatban, valamint azok összefoglalása az adatkezelési tájékoztatóban, hogy arra az érintettek is felkészülhessenek. A fenti adatkezelést folytatóktól elvárható továbbá a rendszert alkalmazó és felülvizsgáló személyzet számára belső adatvédelmi szabályzat készítése is,

17 NAIH-85-3/2022. számú határozat, 13, 25.
18 GDPR 22. cikk.
19 Barfield 2018, 29.

amely egyben a diszkrimináció elleni intézkedések körére, a szükséges körű és intenzitású felülvizsgálatra és emberi beavatkozásra is kitér.

- *Célhoz kötöttség:* az adatkezelésnek meghatározott cél érdekében kell történnie, így jogsértőnek tekinthető például, ha az adatkezelő az egészségügyi szolgáltatás nyújtása céljából gyűjtött személyes adatokat valójában gyógyszerekre vagy gyógyászati segédeszközökre vonatkozó reklámtartalmak küldéséhez használja fel.
- *Adattakarékosság:* az MI-alapú megoldás segítségével kezelt személyes adatoknak minden esetben az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük, és azok csak a szükséges mértékben kezelhetők. Mindez azt is jelenti, hogy az adatkezelőknek a konkrét technológiai megoldás és adatkezelési cél együttes értékelésével kell kialakítaniuk, hogy az adott rendszer alkalmazása kapcsán pontosan milyen adatkészletre van szükség, az adatokat milyen forrásból szerzi be, és hogyan használja fel az adott rendszer (például nyers adatok vagy azokból továbbképzett, esetleg más adatokkal való összehasonlítás eredményeként létrehozott adatok), valamint hogy milyen adatkezelési időt is tartanak az adatkezelők szükségesnek az egyes adatok kezelése tekintetében (például mikortól és milyen mértékben elégséges anonimizált vagy konkrét személyekhez nem kapcsolható adatok kezelése). Ezzel kapcsolatban például a spanyol adatvédelmi hatóság mesterséges intelligencia általi adatkezeléseknek az Európai Parlament és a Tanács 2016/679. sz. Általános Adatvédelmi Rendeletének (GDPR) való megfelelésével kapcsolatos tájékoztató anyaga[20] is meghatároz olyan adatminimalizációs technikákat, amelyek hasznosak lehetnek az adatkezelők számára. Így a hatóság kiemeli például az adatgyűjtés első fázisában az adatok további felhasználása előtti tisztítását, amellyel az adatkezelés céljának megvalósulásához felesleges adatok törölhetők, ezáltal pedig az adatkezelés egyes szakaszai is racionálisan és etikusan építhetők fel. Emellett ugyancsak kiemeli az érintettekre vonatkozó, az adatkezelés célja szempontjából szükségtelen következtetések elhagyásának fontosságát, valamint lehetőség szerint titkosított adatok alkalmazását, amelyek az adatok pontosságának és az adatbiztonság megfelelő szintjének elérését is biztosíthatják. Megemlítendő továbbá, hogy a különböző, környezetet mérő szenzorok és ezen eszközök közti kommunikációs hálózatokon (angolul *Internet of Things* vagy IoT) keresztül továbbított adatok esetén különösen fontos lehet továbbá annak adatkezelők általi előzetes felmérése, hogy a szenzorok pontosan milyen adatokat fognak gyűjteni és megosztani további elemzés végzése céljából (például a különböző okosváros-szolgáltatások esetén).[21]
- *Pontosság:* ezen elvből következően az adatkezelőnek biztosítania kell az adatok pontosságát és naprakészségét. Természetesen ez azt is feltételezi, hogy az adat-

20 A spanyol adatvédelmi hatóság (Agencia Española de Protección de Datos) mesterséges intelligencia alkalmazásával végzett adatkezelés GDPR-nak való megfelelésével kapcsolatos anyaga: AEPD 2020, 36–39.

21 Sappa 2019, 135–136.

kezelő csak azon esetekben kezeljen személyes adatokat, amikor az adatkezelés célja másképp nem, vagy nem megfelelő hatékonysággal érhető el (például az MI-alapú megoldás személyre szabott szolgáltatások nyújtásához szükséges). Az MI-alapú megoldások fejlesztése kapcsán azonban számos esetben a hibás következtetések eredményeként létrejött vagy már nem naprakész adatok megőrzése is fontos lehet, hiszen ezek segítségével az adott rendszer alkalmazásával kapcsolatos problémák könnyebben feltárhatók és korrigálhatók. Így amennyiben az adatkezelő ilyen célból őriz meg szükség szerint személyes adatokat, mindez a pontosság elvével összhangban állónak tekinthető, hiszen ezen elvnek való megfelelés csak az adatkezelés céljának viszonylatában értelmezhető.

- *Korlátozott tárolhatóság:* a korlátozott tárolhatóság elvével összhangban az adatokat olyan formában szükséges tárolni, amely az érintettek azonosítását a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. Ez részben technikai, részben szervezési feladat, ugyanis a technikai keretek kialakítása mellett az adatkezelőnek, adott esetben az esetleges adatkezelésbe bevont partnereivel, alvállalkozóival, fel kell mérniük az adatkezelési cél megvalósításához szükséges személyes adatok körét, és – ha ez az adatkezelés tekintetében szükséges és releváns – meghatározni, hogy az adatkezelés mely stádiumaiban elégséges álnevesített vagy anonimizált adatok kezelése.
- *Integritás és bizalmas jelleg:* az integritás és a bizalmas jelleg biztosításához az adatkezelőnek megfelelő technikai és szervezési intézkedéseket kell alkalmaznia az adott technológiai megoldás (például szoftveres viselkedéselemzés vagy kamerás arcfelismerés, rendszámfelismerés) esetén, amely képes kizárni vagy elenyészőre csökkenteni az adatvédelmi incidensek lehetőségét, és az adatbiztonság egy magasnak mondható szintjét garantálja.
- *Elszámoltathatóság:* az adatkezelőnek az adatkezelés teljes folyamata alatt képesnek kell lennie az adatvédelmi alapelveknek megfelelő adatkezelése igazolására, ideértve azt az esetet is, hogyan és miért döntött például anonimizált vagy fiktív adatok helyett – azonosítható természetes személyekre vonatkozó – személyes adatok gyűjtése, illetve további felhasználása mellett, és hogyan gondoskodott az adatok törléséről az adatkezelés céljának megszűnése után.

Ami az adatkezelés jogalapját illeti, az MI általi adatkezelés esetén ugyanúgy számos jogalap releváns lehet, mint az adatkezelés egyéb formái esetén. Amennyiben például kutatási-fejlesztési célból elemeznek arcképeket, úgy erre tekintettel az érintettek hozzájárulása alapján is folytatható az elemzési tevékenység, míg arcfelismerő rendszerek alkalmazása jogos érdeken, illetve elsősorban a közérdek védelmén alapulhat, ha azt az arra jogosult szervek végzik, megfelelő jogszabályi felhatalmazás alapján. Tekintettel azonban arra, hogy a mesterségesintelligencia-alapú megoldások jellemzően jelentős adatmennyiséget dolgoznak fel komplikált elemzések folytatása révén, így a jogalap helyes megválasztása esetén is előfordulhat, hogy az adatkezelés egyéb

szempontokból is jogszerűtlennek tekinthető (például a kezelt adatok köre túlmutat az adatkezelés célja és körülményei által indokolt mértéken).

Hozzájáruláson[22] alapuló adatkezelés esetén kiemelten fontos, hogy az érintett önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását az érintett egyértelmű megerősítő cselekedete (például elektronikus úton tett nyilatkozat) útján adja meg.[23] A hozzájárulás, habár adott esetben MI-alapú adatkezelések esetén is bekérhető papíralapon, megadása jellemzően mégis elektronikusan (például egy alkalmazáson, rendszeren keresztül) történik, amely esetben azonban feltétel, hogy a hozzájárulás formátuma az érintett számára érthető és könnyen hozzáférhető legyen. Így, ha az érintett a hozzájárulását csak egy számára nehézkesen érthető, magas fokú informatikai tudást megkövetelő szoftverkörnyezetben adhatja meg és vonhatja vissza, úgy a hozzájárulása érvénytelen lesz, arra támaszkodva pedig jogszerű adatkezelés nem végezhető. Mindemellett a hozzájárulás nyelvezetének is világosnak és az érintett számára érthetőnek kell lennie, továbbá nem tartalmazhat tisztességtelen feltételeket[24] (például a hozzájárulás kötelező megadásának vagy egyúttal beláthatatlan számú adatkezelő általi direkt marketingüzenetek küldéséhez való hozzájárulás megkövetelése), ezek ugyanis a hozzájárulás önkéntességét jellemzően befolyásolják, az érintettet pedig adott esetben olyan nyilatkozat megtételére késztetik, amelyet más körülmények között nem tett volna meg.

A hozzájáruló nyilatkozat és az ahhoz kapcsolódó adatvédelmi tájékoztató nyelvezete kapcsán kulcskérdésnek tekintendő továbbá az adatkezelés által érintett személyek körének felmérése. Így magyar nyelvű érintettek esetén jellemzően magyar nyelven szükséges megadni a hozzájáruláshoz kapcsolódó tájékoztatást, és rendelkezésre bocsátani az esetleges hozzájárulónyilatkozat-mintát, amennyiben pedig más nyelvet beszélő érintettekre is kiterjed az adatkezelés, úgy elvárható, hogy a külföldi érintettek által jellemzően használt idegen nyelven (például angolul) is elérhető legyen a tájékoztatás és az esetleges nyilatkozatminta szövege. Bármely anyanyelvű érintett esetén elvárható azonban, hogy a tájékoztató és a hozzájáruló nyilatkozat megfogalmazása a számukra érthetően megfogalmazott legyen, így tehát az „érthetőség" követelménye túlmutat pusztán az érintett anyanyelvén írt szövegezésen, és az érintett sajátos körülményeihez, valamint a vele való, elvárható kommunikációhoz igazodik. Így például a gimnáziumi tanulóknak szóló tájékoztatás részévé tehetők az iskolai környezetben ismert, illetve akár diákszavak is, az e csoport által jellemzően nem értett vagy használt kifejezések alkalmazása azonban kerülendő. E logika értelmében a túlságosan általános kifejezések, az adott környezetben nem ismert szakszavak, kevéssé ismert rövidítések alkalmazása az érintettek tájékoztatása során jellemzően nehezen értelmezhető lehet. Egy esetben például a NAIH az érintettek (átlagos fogyasztók) számára értelmezhetetlennek minősítette az „ügyfélszegmentációs szimulációk elvégzése"

22 GDPR 6. cikk (1) *a)* pontja.
23 GDPR (32) preambulum-bekezdés.
24 GDPR (42) preambulum-bekezdés.

kifejezés alkalmazását, felróva azt az adatkezelőnek,[25] de ehhez hasonlóan nem találta megfelelőnek például a reklámiparban gyakran használt „targetálás" kifejezést,[26] vagy az érintettekkel való többféle marketingcsatornán keresztüli kapcsolattartás esetén a „kedvező ajánlatok" küldésének mint adatkezelési célnak az általános megjelölését.[27]

Még érzékenyebb kérdést jelent a megfelelő nyelvezet megválasztása kiszolgáltatottnak tekinthető érintetti csoportok, így különösen gyermekek esetén. Az Adatvédelmi Munkacsoport átláthatósággal kapcsolatos véleménye leszögezi, hogy e személyek nem veszítik el önmagában az adatkezelés átláthatóságához és megismeréséhez fűződő (és így a tájékoztatáshoz való) jogukat azáltal, hogy a hozzájárulás megadására adott esetben nem ők, hanem más személyek (például törvényes képviselő vagy gondnok) jogosultak.[28] Így gyermekek esetén elvárható a részükre a hozzájáruló nyilatkozathoz kapcsolódó, legalább az adatkezelés és jogaik lényegét „gyermeknyelven" is összefoglaló adatvédelmi tájékoztató elkészítése, amennyiben pedig a gyermek személyesen jogosult a hozzájárulást megadni,[29] úgy a nyilatkozatot is hasonló egyszerűséggel kell megfogalmaznia az adatkezelőnek. Érdekes példának tekinthető e körben a Lego vállalat adatvédelemről és sütik alkalmazásáról szóló videója, amely gyermekeknek szánt nyelvezettel igyekszik bemutatni az adatkezelés, valamint a sütik alkalmazásának lényegét.[30]

Természetesen a hozzájárulás visszavonását is éppolyan egyszerű módon kell lehetővé tennie az adatkezelőnek, ahogy a hozzájárulás megadását is lehetővé tette. Így például nem fogadható el, ha az érintett az MI-megoldással végzett viselkedésalapú marketingüzenetek küldéséhez egy applikáción belül adhatja meg a hozzájárulását, azonban a visszavonó nyilatkozatot csak személyesen, illetve papíralapon teheti meg. Ilyen esetben az applikáción belül is lehetővé kell tenni a hozzájárulás visszavonásának lehetőségét, például a vonatkozó funkció felhasználók általi kikapcsolásának biztosításával.[31]

A fentieken túl az MI-alapú adatkezelések jogalapjaként elvileg szerződés teljesítésére is hivatkozhatna helyesen az adatkezelő, amennyiben az adatkezelés olyan szerződés teljesítéséhez lenne szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges. Ez azonban napjainkban a gyakorlatban még kevésbé tekinthető relevánsnak, figyelemmel arra, hogy az MI által támogatott szolgáltatások jelentős részben az azokat üzleti, illetve szervezeti támogatása céljából felhasználó vállalkozásoknak irányulnak, a magánszemélyek, különösen fogyasztók részére irányuló szolgáltatások

25 NAIH/2015/2201/17/H, 15.
26 A NAIH ajánlása az előzetes tájékoztatás adatvédelmi követelményéről, 9.
27 NAIH-2501-10/2022, 14.
28 Adatvédelmi Munkacsoport WP260 rev. 01 véleménye az átláthatóságról, 10.
29 Például ha a hozzájárulás olyan személyes jellegű jognyilatkozatnak minősül, amelynek megtételére a korlátozottan cselekvőképes kiskorút jogszabály feljogosítja [lásd 2013. évi V. törvény 2:12. § (2) *a)* pontja].
30 Lásd például: www.lego.com/hu-hu/cookie-policy
31 Datatilsynet 2018, 28.

pedig javarészt hozzájáruláson alapulnak (ideértve például az egyre népszerűbbé váló chatbot- vagy okosügyintéző szolgáltatásokat is). Ugyancsak kevéssé tekinthetők relevánsnak az MI általi, jogi kötelezettség teljesítéséhez, vagy az érintett vagy másik természetes személy létfontosságú érdekeinek védelme miatt, illetve közérdekből szükséges vagy közhatalmi jogosítvány gyakorlása keretében végzett adatkezelések, tekintettel arra, hogy (napjainkban még) jellemzően sem az adatkezelőkre irányadó jogi kötelezettségek, sem a közérdek vagy a közhatalom gyakorlása nem követeli meg önmagában MI-alapú megoldások alkalmazását, a létfontosságú érdekek védelme érdekében pedig ezek a megoldások egyelőre úgyszintén ritkán játszanak szerepet. Emellett azonban megemlítendő, hogy a gyakorlatban akár közterület megfigyelésére szolgáló kamerarendszerek is társíthatók, illetve felruházhatók különböző arcfelismerő megoldásokkal, képességgel, ezen arcfelismerő rendszerek széles körű, esetleges jogszabályi felhatalmazáson alapuló, valamint közérdekből, illetve közhatalom gyakorlása keretében való alkalmazása azonban a fokozott közbiztonság jelentette várható társadalmi hasznosság mellett legalább olyan széles körben hordozna magában a személyes adatok védelmére, valamint az információs önrendelkezésre jelentett kockázatokat. Hasonló a helyzet az MI jogos érdeken alapuló alkalmazása esetén is, tekintettel arra, hogy az adatkezelői érdek (például az adatkezelő vagyontárgyainak, üzleti érdekeinek védelme, a szolgáltatások fejlesztése) érvényesítése az esetek többségében a magánélet és az érintettek személyes adatainak védelme tekintetében enyhébb behatást jelentő alkalmazásokkal is elérhető, így ezen esetekben az adatkezelő által készítendő vonatkozó érdekmérlegelési teszt érvrendszere kiemelt szerepet kap majd.

Az MI és az adatvédelmi jogok gyakorlása

Az MI-alapú megoldások esetén ezen új technológia alkalmazása jelentős mennyiségű személyes adat kezelésével jár, valamint kiemelt hatással van az érintettek magánéletére és interakcióira, így fontos, hogy az érintetteknek beleszólásuk legyen személyes adataik MI általi kezelésébe, és átláthassák ennek lehetséges hatásait és következményeit.

A tájékoztatás kapcsán a fentebb már említett, a hozzájáruláshoz kapcsolódó tájékoztatásra vonatkozóan írtak irányadók, így e szempontok megismétlésétől eltekintünk. Leszögezendő azonban, hogy az érintettek tájékoztatásának egyéb jogalapú adatkezelések esetén is érvényesülnie kell. Kiemelendő továbbá, hogy az MI alkalmazásán alapuló megoldásokhoz szükséges adatokat jellemzően az érintettektől gyűjtik az adatkezelők, így ilyen esetekben legkésőbb a személyes adatok megszerzésének időpontjában szükséges az adatvédelmi tájékoztatót a rendelkezésükre bocsátani. Például, amennyiben az érintett megnyitja a chatbotalkalmazást, és igénybe veszi annak szolgáltatásait, úgy jó megoldás lehet, ha az érintettek részére a chatbot a beszélgetés megkezdésekor megjeleníti az adatvédelmi tájékoztató közvetlen elérhetőségét. A chatbothoz fűződő szolgáltatások jellege okán (például üzletek elérhetőségének,

nyitvatartási idejének megmutatása helymeghatározási adatok alapján) elképzelhető az is, hogy többféle szolgáltatás igénybevételéhez külön-külön adhat hozzájárulást az érintett, vagy hogy az egyes szolgáltatásokhoz kapcsolódó adatkezelést az adatkezelő eltérő jogalapokra támaszkodva végzi (például „emberi" ügyintéző kapcsolása a chatbotot igénybe vevő ügyfelek részére, ami adott esetben kapcsolódhat az ilyen személyek adatkezelővel kötött szerződésének teljesítéséhez), azonban az adatkezelés menetének és az eltérő jogalapoknak ez esetben is átláthatónak kell lennie az érintettek részére.

Mint az a fenti példán is látszik, az MI-alapú adatkezelések esetén az érintetti jogok gyakorlása alapvetően hasonlóan érvényesül, mint az adatkezelés egyéb formái esetén, azonban a technikai sajátosságok megkövetelik az érintetti jogok gyakorlásának az adatkezelés folyamatába ágyazott különösen hatékony támogatását. Így az MI-alapú megoldásoknál, akár a vonatkozó szoftver kezdeti, kísérleti fázisáról, akár annak piaci alkalmazásáról beszélünk, mindenképpen szükséges a vonatkozó rendszerek és alkalmazások olyan módon való kialakítása, hogy az érintettek adatvédelmi jogaikat a GDPR szerinti határidőben és követelményeknek megfelelően gyakorolhassák.

Így a fentiekre tekintettel az adatkezelőnek biztosítania kell az érintettek hozzáférési jogának gyakorlását is, ideértve az adatkezelés folyamatban létéről történő tájékoztatást, az adatkezelésre vonatkozó információkhoz való hozzáférést, illetve – az adatkezelés körülményeire és a technológia adta lehetőségekre tekintettel – másolatok készítését és kiadását is. Erre tekintettel az adatkezelő felelős azért, hogy a vonatkozó MI-alapú megoldáshoz kapcsolódóan olyan adatbázisokat, illetve rendszereket alkalmazzon, amelyekből akár egy adott érintettre vonatkozó valamennyi személyes adat összegyűjthető és az érintett számára megküldhető, illetve ezen adatokról másolat adható (például egy letölthető fájlban).

A tájékoztatási és hozzáférési jog mellett természetesen a helyesbítéshez fűződő jog gyakorlása is sajátos szempontok szerint történhet, amelynek keretében az érintett a rá vonatkozó pontatlan személyes adatok helyesbítését vagy hiányos személyes adatai – egyebek mellett kiegészítő nyilatkozat útján való – kiegészítését kérheti, azonban e kérelme csakis az adott MI-alapú megoldás keretei között, illetve sajátosságaira tekintettel foghat helyt. Így például okoskamerákkal és hozzájuk kapcsolódó MI-rendszerekkel folytatott adatkezelés esetén az érintett nyilvánvalóan nem kérheti a felvételek tartalmának helyesbítését, azonban az egyes felvételekkel összefüggésben pontatlanul vagy tévesen rögzített adatok (például: a felvételen vagy annak kapcsán megjelenő helytelenül rögzített dátum) helyesbítését már kérheti.[32]

Az érintett jogosult a személyes adatai indokolatlan késedelem nélküli törlését kérni, többek között, amennyiben az adatokra már nincs szükség az eredeti adatkezelési célból, ha az érintett visszavonja a hozzájárulását (ha az adatkezelés hozzájáruláson alapul), ha az érintett tiltakozik az adatkezelés ellen (ha az adatkezelés jogos érdeken alapul), illetve, ha a személyes adatokat az adatkezelőre alkalmazandó uniós

32 A NAIH előzetes tájékoztatás adatvédelmi követelményeiről szóló véleménye, 13.

vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell. Ezen esetek MI-alapú adatkezelések esetén is előfordulhatnak, ideértve például, ha az adatkezelési tájékoztatóban meghatározott és az érintettek számára közölt adatkezelési cél megszűnt. Ez különösen fontos lehet az olyan megoldások esetén, ahol az adatkezelés annak célja szerint is több szakaszra osztható (például kutatási és fejlesztési folyamat, majd a piaci bevezetést követő „éles" alkalmazás). Ezen esetekben az érintettnek át kell látnia az adatkezelés egyes szakaszait, és tisztában kell lennie azzal, hogy az adatkezelő pontosan mely személyes adatait meddig, valamint milyen jogalapon kezeli. Hozzájárulás esetén különösen fontos azon kérdés tisztázása is, hogy a hozzájárulás pontosan meddig terjed; például csak a kutatási és fejlesztési folyamatra vagy az azt követő alkalmazásra is (ideértve későbbi hibák elhárítását, szolgáltatásfejlesztést).

Habár a törléshez való jog kétségkívül kihívás elé állíthatja az MI-alapú megoldásokat alkalmazó adatkezelőket, a GDPR e körben több, ezen adatkezelések vonatkozásában is alkalmazható kivételszabályt említ.[33] Így egészségügyi kutatások (például egy új vakcina kifejlesztése) érdekében végzett adatkezelés esetén például az adatkezelő érvelhet az érintett törlési kérelmével szemben arra hivatkozással, hogy az adatkezelés folytatása népegészségügyi területet érintő közérdekből szükséges.

A fentiekkel is összhangban, a helyesbítéshez és a törléshez való jogok kapcsán hangsúlyozandó, hogy az MI tanulási folyamatok során a „hibás adatok" vagy az érintett személyes adataiból (akár ezek hibás vagy hibátlan jellege esetén) létrehozott további adatok is jelentős tudományos vagy üzleti értéket képezhetnek, lévén, hogy ezek ismerete és az MI-megoldás általi további felhasználása nélkül a szoftveres megoldás nem feltétlenül képes eljutni a tanulási folyamat végére (például elsajátítani a megfelelő képfelismerési képességet), így az ilyen adatok fenti célból való megőrzéséhez az adatkezelőnek jogos (különösen: tudományos vagy üzleti) érdeke fűződik, bizonyos esetekben pedig e körben akár a közérdek is hivatkozható (például gyógyszerkutatásokhoz használt MI-alapú megoldások esetén). A fenti adatok is azonban egy meghatározott célból kezelhetők (ideértve például egy MI-alapú megoldás útján folytatott kutatást). Kiemelendő továbbá, hogy akár eredetileg egyéb célból gyűjtött személyes adatok is felhasználhatók később, például egy tudományos kutatás során, valamint annak érdekében,[34] azonban az ilyen adatkezelési műveleteknek is meg kell felelnie a személyes adatok kezelésére vonatkozó elveknek, így például, ha a kutatás során elegendő anonimizált adatok gyűjtése és feldolgozása, az ennek megfelelő célból konkrét érintetteket azonosító személyes adatok nem kezelhetők jogszerűen.

A fentieken túl az adatkezeléshez fűződő jog korlátozása is sajátos szempontok szerint foghat helyt, figyelembe véve az MI felhasználásával való adatkezelések sajátosságait. Amennyiben például az érintett vitatja az adatok pontosságát, vagy tiltakozik az adatkezelés ellen, úgy az adatkezelőnek képesnek kell lennie arra, hogy korlátozza az adatkezelést azon időtartamra, amely lehetővé teszi számára, hogy ellenőrizze az adatok pontosságát, illetve az adatkezelői jogos indokoknak az érin-

33 GDPR 17. cikk (3) bekezdése.

34 GDPR 5. cikk (1) bekezdés *e)* pontja.

tett jogos indokaival szembeni elsőbbségét. Ez jelentheti például a fenti időtartamokra a vonatkozó adatok migrálását az adott rendszerből egy másik, szűkebb körű hozzáférést engedő rendszerbe, vagy egy biztonságos, zártan kezelt adathordozóra mentést;[35] ha a rendszer működése ezt lehetővé teszi, ezen időtartamra (például amíg tisztázódik, hogy az adott kutatásban részt vevő valóban hozzájárult-e a részvételhez), továbbá a vonatkozó személyes adat egy fiktív adattal is helyettesíthető. Az adatkezelőnek ugyancsak képesnek kell lennie az adatok zárolására, ha az adatkezelés jogellenessége ellenére az érintett azt kéri, vagy ha az adatokra már ugyan nem lenne szükség további adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez. Ilyen eset lehet például, ha egy arcfelismeréssel járó megoldás fejlesztéséhez felhasznált felvételeket jogsértő módon készítették, és az érintett azokat bizonyítékként való felhasználás céljából kéri zárolni a vonatkozó személyiségi jogi perben.

Mint az a fentiekből is látszik, az adatkezelés korlátozásához (zároláshoz) fűződő kérelmek teljesítése számos esetben a szervezési és technikai intézkedések hatékony, együttes alkalmazását várja el az adatkezelőtől, egyben a GDPR jelentős gátat is szab a fenti időtartam során az adatok felhasználásának. Amennyiben tehát az adatkezelés korlátozás alá esik, úgy az adatok tárolhatók, azonban bizonyos kivételekkel (például jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez) más módon nem kezelhetők.[36] Erre tekintettel az adatkezelőnek olyan megoldást kell találnia (például külön adathordozóra mentéssel vagy az adatok adott rendszeren belüli megfelelő megjelölésével), amely biztosítja, hogy a zárolt adatok ne keveredhessenek egyéb adatokkal, és véletlenül se használhassák fel azokat a fenti eseteken kívüli célokból.

Ami az adathordozhatósághoz való jogot illeti, ez az érintettek hozzájárulásán, valamint a közvetlenül velük kötött szerződések teljesítésén alapuló MI-alapú adatkezeléseknél jöhet szóba releváns érintetti jogként, ha az alkalmazott technológia körülményeire tekintettel ez lehetséges. Erre tekintettel az adathordozhatósághoz való jog egyrészt sajátos hozzáférési jogot,[37] másrészt – ha ez technikailag megvalósítható – az adatok adatkezelők közti továbbítását biztosítja az érintett számára. Ez utóbbi jog gyakorlásának biztosítása azonban a gyakorlatban igencsak problémás lehet. Tekintettel ugyanis arra, hogy az MI-alapú megoldások gyakran sajátos logika és elv alapján működnek, így technikai értelemben is csak az azonos vagy egymáshoz igen hasonló megoldásokat használó adatkezelők közti adattovábbítás merülhet fel. Figyelembe kell vennünk azonban azt a tényt is, hogy az adatok továbbítása az adatkezelő saját üzleti titkai vagy szellemi alkotásai védelméhez fűződő érdekeit is jelentős veszélynek teheti ki, például az érintett adatok versenytárs számára való felfedésével. Így az adatkezelőnek ezen esetekben egyrészt mérlegelnie kell az érintetti kérelem

35 A NAIH/2019/363/2. sz. ügyében a NAIH kiemelte, hogy az adatok pontosságának tisztázásáig az adatkezelőnek zárolnia kellett volna az ügyfél telefonszámát.

36 GDPR 18. cikk (2) bekezdés.

37 Az adatkezelő rendelkezésére bocsátott személyes adatok „tagolt, széles körben használt, géppel olvasható formátumban" való rendelkezésre bocsátása [GDPR 20. cikk (1) bekezdés].

megvalósíthatóságát, másrészt saját érdekeinek súlyát az érintett érdekeivel szemben (például az üzleti titoknak minősülő vagy szellemi alkotás részének tekinthető információk kitakarásával).

Tekintettel arra, hogy a közérdekű, illetve közhatalom gyakorlása, vagy jogos érdekből folytatott adatkezelések az MI-alapú megoldások esetén valószínűleg a közeljövőben is meghatározók lesznek, így az adatkezelőknek is különös gondot kell fordítaniuk az érintett tiltakozási jogának elősegítésére. Az érintett jogszerű tiltakozása esetén ugyanis az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.[38] Ennek alátámasztásául szolgál az úgynevezett érdekmérlegelési teszt is, amely azonosítja az adatkezelői és érintetti érdekeket, továbbá tartalmazza azok ellensúlyozását. Ez MI-alapú megoldások esetén tartalmazhatja az MI-megoldás alkalmazásának szükségességére, kiemelt hatékonyságára vonatkozó érveket, valamint annak alátámasztását, hogy az adott megoldás miért nem jelent túlzott sérelmet az érintettek magánéletére, jogaira, valamint érdekeire, és azon intézkedések felsorolását, amelyekkel az adatkezelő az esetleges káros hatásokat enyhíti.

A fentieken túl kiemelendő, hogy amennyiben az adatkezelő által alkalmazott megoldás automatizált döntéshozatalt, illetve profilalkotást is maga után von, úgy az adatkezelőnek biztosítania kell egyéb szempontok érvényesülését, valamint elő kell segítenie az érintett ezzel kapcsolatos, sajátos jogainak gyakorlását. Ennek oka, hogy bár az MI segítségével sok esetben kiküszöbölhetővé válnak az emberi mulasztások, tévedések, az érintettekről alkotott (jellemzően digitális formában, az online térben is elérhető) profilok is igen könnyen nyomon követhetők, vagy további következtetések levonása céljából elemezhetők.[39] Ennek révén pedig az érintett kiszolgáltatottá válhat, az MI segítségével pedig akár még eredményesebben is befolyásolható.

Hangsúlyozandó, hogy a GDPR nem határozza meg ugyan az automatizált döntéshozatal fogalmát, azonban e fogalom alatt olyan esetek értendők, amikor például egy algoritmus hoz meg bizonyos döntéseket, ha a döntésnek kellő súlya, illetve hatása van az érintett vonatkozásában. Ez természetesen nem terjed ki valamennyi MI által hozott döntésre, kizárólag azokra, amelyek az érintettre nézve joghatással járnak, vagy őt hasonlóképpen jelentős mértékben érintik[40] (például, ha egy szerződés érdemi módosításáról határoz MI-alapú megoldás). Az automatizált döntéshozatallal szemben a profilalkotás fogalmát a GDPR már tételesen meghatározza, ez alatt személyes adatok automatizált kezelésének bármely olyan formáját értve,

> „amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesít-

38 Lásd GDPR 21. cikk (1).
39 Buzás 2018, 198.
40 GDPR 22. cikk (1) bekezdés.

> ményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják".[41]

Ezen esetekre például szolgálhatnak az MI segítségével támogatott különböző toborzási célú megoldások, amelyek a jelentkezők adatait, jellemzőit viszonyítják az adott munkakör kapcsán elvárt kvalitásokhoz.

Az automatizált döntéshozatalról és az ahhoz kapcsolódó profilalkotásról egyaránt elmondható, hogy e megoldások – gazdasági és szervezési hatékonyságuk mellett – jelentős beavatkozást jelentenek az érintettek magánszférájába, sok esetben az érintettek személyiségjegyeit és életmódját is felfedve az adatkezelő számára. Például egy helymeghatározási adatokat kezelő ételfutár- vagy étteremkereső applikáció a helymeghatározási adatok elemzése révén felismerheti, hogy az érintett rendszeresen későn jár haza, és erre tekintettel marketing célból felajánlhatja neki a kései órákban is házhoz szállítást vállaló éttermek listáját vagy kuponjait.[42] Az ilyen jellegű adatkezeléseknél az adatkezelőknek különös gondot kell fordítaniuk az adatkezelésük érintett általi átláthatóságára (így a vonatkozó adatkezelési tájékoztatók megfogalmazására), az érintetti jogok elősegítésére és az adatvédelmi alapelvek érvényesülésére (ideértve például az adott esetben gyűjtött adatokon alapuló piackutatási vagy szolgáltatásfejlesztési elemzések elvégzése előtt ezen adatok anonimizálását).

Olyan esetekben, ahol az adatkezelés kizárólag automatizált módon történik (ideértve a profilalkotást is), az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna, vagy őt hasonlóképpen jelentős mértékben érintené.[43] E tilalom alól kivételt jelent, ha a fenti módon hozott döntés az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges, annak meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít, továbbá, ha az az érintett kifejezett hozzájárulásán alapul.

Személyes adatok különleges kategóriái esetén további korlátozást jelent, hogy az adatkezelésre kizárólag akkor kerülhet sor, ha az adatkezeléshez az érintett kifejezett hozzájárulását adta, vagy az adatkezelés jelentős közérdek miatt szükséges, illetve ha a szabályozás által elérni kívánt céllal arányos, megfelelően konkrét védelmet biztosító uniós jog vagy tagállami jog alapján kerül arra sor.[44] A szenzitív adatok elemzésével kapcsolatos veszélyek kapcsán kiemelendő például az elmúlt években jelentős visszhangot kapott Cambridge Analytica elnevezésű analitikai megoldásokkal

41 GDPR 4. cikk 4. pontja.
42 Az Adatvédelmi Munkacsoport WP251rev.01 sz. irányelve az automatizált döntéshozatalról és a profilalkotásról, 11.
43 GDPR 22. cikk (1) bekezdés.
44 GDPR 22. cikk (2), (4) bekezdés.

foglalkozó társaság által folytatott adatgyűjtési gyakorlat, tekintettel arra, hogy a társaság az érintettek számára átláthatatlan módon gyűjtött választási elemzések végzése céljából személyes adatokat a közösségi médián keresztül, amelyeket több jelentős politikai kampány során is felhasználtak.[45] Mint az ezen esetből is következik, a közösségimédia-felületeken végzett politikai vagy piackutatási célú adatkezeléseknek – az érintetti jogok és szabadságok sérelmén túl – jelentős társadalmi vagy gazdasági hatásai is lehetnek, rossz kezekbe kerülve pedig e beláthatatlan méretű adathalmazok akár választási, piaci vagy egyéb társadalmi manipulációhoz is vezethetnek, amelyek elemzését, értékelését az MI fokozott hatékonysággal képes ellátni, adott esetben a káros hatásokat is sokszorosára erősítve. Az egyes online térben elérhető adatokból levonható következtetésekkel kapcsolatos kockázatokat támasztja alá egy amerikai tanulmány is, amely szerint például a Facebookon az egyes tartalmakhoz fűzött felhasználói „kedvelések" (like-ok), valamint pusztán néhány egyéb felhasználói válasz alapján kellő bizonyossággal vonhatók le következtetések a felhasználók szexuális irányultságáról, etnikai hátteréről vagy vallási meggyőződéséről.[46]

A fentiekből eredően tehát joghatással vagy hasonló jelentős megoldással járó, automatizált döntéshozatalt és profilalkotást maguk után vonó MI-alapú megoldások esetén jellemzően hozzájárulás vagy szerződés, illetve speciális – ez idáig még nem jellemző – jogszabályi felhatalmazás alapján folytatható az adatkezelés. Tisztázandó azonban a „joghatás" vagy „ahhoz hasonló hatás" fogalma, tekintve, hogy csak az ilyen hatásokkal járó döntések esetén alkalmazandók a GDPR automatizált döntéshozatalra vonatkozó szabályai. A gyakorlat tükrében joghatásnak tekinthetők a szerződés létesítését, módosítását vagy megszűnését, bizonyos jogosultságok megadását vagy megtagadását maguk után vonó hatások, míg hasonlóan jelentős hatásnak minősülhetnek az érintettek magánéletére és választási szabadságára, diszkriminációra vagy egyéb elhúzódó következményekhez vezető hatások (különösen az érintettek hitelbírálata, egészségügyi, oktatási vagy egyéb szociális szolgáltatásokhoz való hozzájutása). A joghatáshoz hasonló jelentős hatás megléte különösen a viselkedés- vagy egyéb jellemzők értékelésén alapuló marketingtevékenységnél lehet kérdéses, és okozhat fejtörést az adatkezelők számára, tekintettel arra, hogy demográfiai adatok elemzése önmagában nem feltétlenül jár ilyen, az érintett magánéletébe való súlyosabb behatással, azonban egyéb szempontok figyelembevételével e hatás már megvalósulhat. Az adatkezelés sajátosságai (például a kínált szolgáltatások, termékek, a marketingtevékenység által célzott érintettek köre, a promóció fajtája stb.), esetleges intruzív jellege, az érintett eszközeinek követése, az érintett elvárásai és a marketingtartalmak megjelenése, az érintett esetleges sebezhetőségének kihasználása (például gyermekeket célzó vagy gyógyszerreklámok) nyújthatnak tehát támpontot a fenti hatás meglétének megítélésénél.[47]

45 Information Commissioner's Office 2018

46 Kosinski–Stillwell–Graepel 2013, 5802.

47 Az Adatvédelmi Munkacsoport WP251rev.01 sz. irányelve az automatizált döntéshozatalról és a profilalkotásról, 21–22.

Mint az a fentiekből is következik, az érintetti jogok gyakorlásának biztosítása jelentős, ámde az érintetti jogokra és szabadságokra jelentett kockázatok tükrében arányos terheket ró az MI-alapú megoldásokat alkalmazó adatkezelőkre. Erre tekintettel az adatkezelőknek tanácsos már a tényleges megoldás kifejlesztése vagy – szerződéses partner által nyújtott szolgáltatások igénybevétele esetén – a megoldás gyakorlati bevezetése előtt az érintetti jogok biztosíthatóságát felmérni, figyelembe véve, hogy az esetek többségében önmagában egy adott informatikai rendszer hiányosságai vagy sajátos megoldása nem jelentenek mentesítést az adatkezelők számára az érintetti jogok biztosítása és szükség szerinti aktív támogatása alól. Mindez egyúttal azt is jelenti, hogy a jövőben fejlesztendő MI-alapú megoldások nem irányulhatnak az adatvédelmi jogok megsértésére vagy elégtelen biztosítására, az ilyen megoldásokat nyújtó vagy támogató – sok esetben adatfeldolgozónak minősülő – partnerekkel kötendő szerződések esetén javasolt alaposan meghatározni az érintetti jogok gyakorlásának biztosítása tekintetében való együttműködés kereteit, valamint gondosan felmérni a partner által az adott megoldás kapcsán biztosított technikai és szervezési intézkedéseket. Mindezek hiánya ugyanis – adott esetben – adatvédelmi incidenshez, illetve az érintetti jogok megsértéséhez, végső soron pedig az adatkezelő felelősségéhez vezethet.

A mesterséges intelligencia felhasználásával való adatkezelés jogszerűsége az Amerikai Egyesült Államok jogának tükrében

Az elmúlt néhány év óta az Amerikai Egyesült Államokban is jelentősnek mondható szabályozási törekvések figyelhetők meg, amelyek egyrészt a mesterséges intelligencia fejlesztésének támogatását és tudományos vagy társadalmilag hasznos felhasználásának erősítését szolgálják, másrészt igyekeznek annak káros hatásai ellen fellépni, annak lehetőség szerint elejét venni.

A fenti szabályozási törekvést erősíti szövetségi szinten a 2021-ben elfogadott, National Artificial Intelligence Initiative Act,[48] amely egyben elfogadja a nemzeti MI-stratégiát képező National Artificial Intelligence Initiative-et is.[49] E stratégia a fentiek szerint számos kiemelt pillért határoz meg, ahol egyrészt szükségesnek tekinthető az MI alkalmazásának támogatása, valamint számos esetben az érintettek jogainak védelme érdekében az átfogó jellegű, szövetségi szintű szabályozás is. Az e körben meghatározott stratégiai pillérek közé tartozik az innováció, a megbízható MI, az oktatás, az infrastruktúra, egyes szakterületek (ideértve például a mezőgazdaságot, az egészségügyet vagy a szállítást), valamint a nemzetközi együttműködés biztosítása is.

Az MI képességeinek kiaknázása és az innováció támogatása mellett azonban az MI-t bizonyos tekintetben korlátozó, illetve jelentősebb emberi felülvizsgálatot előíró szabályozási törekvések is megfigyelhetők, e körbe értve különösen

48 Lásd: www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210
49 National Artificial Intelligence Initiative: www.ai.gov

az Algorithmic Accountability Act[50] elnevezésű törvénytervezetet, amely elsősorban az MI általi diszkriminációnak igyekszik elejét venni, illetve annak kockázatait csökkenteni, ennek keretén belül pedig az MI-alapú döntéshozatalt alkalmazó társaságoknak hatásvizsgálati dokumentáció elkészítését, az alkalmazott megoldás felülvizsgálatát, valamint egyéb kapcsolódó intézkedések meghozatalát írja elő. Ehhez hasonlóan az általuk alkalmazott algoritmusok kapcsán ír elő hatásvizsgálati kötelezettséget a Data Privacy and Protection Act elnevezésű törvény tervezete a legnagyobb adatokat kezelő szervezetek számára, e körbe értve az olyan szervezeteket, illetve szolgáltatókat, amelyek 250 millió dollár összeget meghaladó bruttó bevétellel rendelkeznek, és több mint 5 millió természetes személy személyes adatait, vagy több mint 200 ezer természetes személy szenzitív adatait gyűjtik, dolgozzák fel vagy továbbítják.[51]

A szövetségi törvényhozás vívmányain túl a tagállami jogban az MI-szabályozás keretén belül kiemelkedőnek tekinthető Kalifornia jogalkotása. Így Kalifornia például két törvénytervezetet is elfogadott korábban a képmás- és hangfelvételekkel való MI általi (úgynevezett deepfake-technológia segítségével) elkövetett visszaélések elleni fellépés, valamint e technológia hatékony szabályozása érdekében.[52] Emellett 2022-ben szintén benyújtották a Facial Recognition Act of 2022 elnevezésű törvénytervezetet,[53] amely átfogó szabályokat vezet be az arcfelismerő rendszerek alkalmazása kapcsán, ideértve többek között e rendszerek hatósági alkalmazásának szabályait, jelentéstétellel, valamint az elfogultság tesztelésével és kiküszöbölésével, az érintettek tájékoztatásával kapcsolatos szabályokat.

Emellett a fogyasztói adatok kezelésével kapcsolatban számos tagállami szabály tartalmaz a profilalkotásra, illetve az automatizált döntéshozatalra vonatkozó szabályokat, ideértve különösen a California Consumer Privacy Act (CCPA) és az azt módosító California Privacy Rights Act (CPRA) értelmében az automatizált döntéshozatallal járó technológiával (e körbe értve a profilalkotást is) kapcsolatos adatkezeléssel való tiltakozásra (úgynevezett opt-out jog), valamint ezen technológiával kapcsolatban alkalmazott logikára, a fogyasztóra kiható eredményekre vonatkozó információkhoz való hozzáféréshez való jogot[54], illetve a Colorado Privacy Act (CPA)[55], a Connecticut Data Privacy Act (CTDPA)[56] és a Virginia Consumer Data Protection Act (VCDPA)[57] értelmében a fogyasztóra joghatással vagy hasonló jelentős hatással bíró adatkezeléssel szembeni tiltakozáshoz való jogot. Mindezen megoldások jelentős részben tükrözik

50 Lásd: www.congress.gov/bill/117th-congress/house-bill/6580/text
51 Lásd: https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf
52 California Legislative Information 2019
53 Lásd: https://lieu.house.gov/sites/lieu.house.gov/files/Lieu%20FRT%20Bill%20FINAL.pdf
54 Lásd: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5,; www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf, 1798.185(16)
55 Lásd: https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf, 6-1-1303(20)
56 Lásd: www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF, Sec. 4.
57 Lásd: https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+SB1392ER+pdf, § 59.1-573. 5.

a GDPR automatizált döntéshozatal, valamint profilalkotás kapcsán előírt egyes rendelkezéseit, különösen a profilalkotás meghatározását,[58] az érintett jogát arra, hogy

> „ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené”;[59]

valamint az automatizált döntéshozatal, illetve a profilalkotás kapcsán alkalmazott logikára és arra vonatkozó tájékoztatást, hogy az ilyen adatkezelés milyen jelentőséggel, illetve az érintettre milyen várható jogkövetkezményekkel bír.[60] Kiemelendő azonban, hogy a 2022-ben elfogadott, és 2023. december 31-én hatályba lépő Utah Consumer Privacy Act (UCPA) kevesebb jogot biztosít a fogyasztóknak a profilalkotás kapcsán, így nem biztosít például e körben tiltakozási jogot.[61] E tekintetben megmutatkozik egyúttal az amerikai tagállami szabályozás széttagoltságából eredő hátránya, amely így az egyes adatvédelmi jogokat eltérő mértékben, illetve tagállamonként sok esetben változóan biztosítja a fogyasztók részére.[62]

Az MI általi adatkezelés területén kibontakozó tagállami szabályozást a kialakuló hatósági kompetenciák is kísérik, e tekintetben pedig Kalifornia állam szintén élenjárónak tekinthető. A CPRA felhatalmazza többek között az újonnan létrehozott kaliforniai adatvédelmi hatóságot (California Privacy Protection Agency) rendeletek kibocsátására a kaliforniai fogyasztók hozzáférési és tiltakozási jogának gyakorlásával kapcsolatban a vállalkozások automatizált döntéshozatali technológia, illetve profilalkotás révén végzett adatkezelései vonatkozásában, ideértve a fentiek szerint, a fenti technológiával kapcsolatban alkalmazott logikára, a fogyasztóra kiható eredményekre vonatkozó információkhoz való hozzáféréshez való jogot is.[63] Mindez pedig széles körben biztosít lehetőséget a hatóság számára arra, hogy a sok esetben kaliforniai székhelyű, világszinten vezető technológiai cégek MI-alapú adatkezeléseit szabályozza Kalifornia tagállam területén, a GDPR-ban lefektetettekhez sok szempontból hasonló követelményeket támasztva.

Hangsúlyozandó azonban, hogy a szövetségi és tagállami szabályozás mellett jelentősnek mondhatók a technológiai szektorban zajló önszabályozási törekvések, valamint a visszaélések megelőzését szolgáló intézkedések. Így a Facebook már korábban bejelentette, hogy a jogosulatlanul megosztott szexuális tartalmak (úgynevezett bosszúpornó)

58 GDPR 4. cikk 4. pont, CCPA 1798.140(z), CPA 6-1-1303(20), CTDPA Section 1(22), VCDPA § 59.1-571. 71.
59 GDPR 22. cikk (1) bek.
60 GDPR 13. cikk (2) bek. *f)* pont, 14. cikk (2) *g)* pont
61 Lásd: https://le.utah.gov/~2022/bills/static/SB0227.html, § 13-61-201(4)
62 Az egyes tagállami fogyasztói adatok kezelésével kapcsolatos jogszabályok és tervezeteik, valamint az adatvédelmi jogok kapcsán lásd: https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf
63 CPRA 1798.185. (16)

felismerésére szolgáló MI-alapú megoldást dolgozott ki.[64] Mindemellett az Egyesült Államokban a bírói gyakorlat is folyamatosan és jelentős mértékben formálja az MI általi adatkezelés lehetőségeit, valamint szabályozói megítélését. Korábban, többek között, az American Civil Liberties Union (ACLU) elnevezésű civil szervezet kezdeményezett pert az arcfelismerő megoldásairól híres Clearview AI elnevezésű társaság ellen, amely az amerikai adatvédelmi jogszabályok megsértésével gyűjtött személyes adatokat (jellemzően: képmásokat), adatbázisát és technológiáját pedig más szervezetek, többek között bűnüldöző hatóságok részére értékesítette.[65] Hangsúlyozandó, hogy a Clearview AI-al szemben több európai adatvédelmi hatóság is bírságot szabott ki a közelmúltban, az európai adatvédelmi jogszabályi rendelkezések megsértése okán, ideértve a francia,[66] az olasz,[67] valamint a görög[68] adatvédelmi hatóságokat, amelyek mind 20 millió euró összegű adatvédelmi bírságot szabtak ki a társaságra.

A fentiek tükrében megállapítható, hogy az Amerikai Egyesült Államok is igyekszik megfelelő szabályozási keretrendszert kialakítani az MI-alapú megoldások és fejlesztések kapcsán, amelynek – a fentiek tükrében – várhatóan a jövőben is a kutatások és a tudományos fejlődés támogatása, valamint az MI visszaélésszerű, valamint diszkriminatív alkalmazása elleni küzdelem lesznek a kulcspontjai.

Szektorális adatvédelmi kérdések

A különböző mesterségesintelligencia-megoldások elterjedtsége számos területen megfigyelhető, amelyek sok esetben sajátos értelmezést követelnek meg. Így más és más szempontok vonatkoznak például az okosirodai vagy okosotthon-megoldásokkal kapcsolatos adatkezelésekre, a viselkedésalapú marketingre vagy egy egészségügyi intézmény által folytatott, MI-alapú megoldással támogatott egészségügyi kutatásra (például egy MI-alapú megoldás fejlesztése bizonyos betegségek könnyebb felismerése céljából). Az alábbi pontokban néhány jellemző szektorális adatkezelési területet mutatok be, ahol a különböző MI-alapú megoldások fokozott elterjedése várható a közeljövőben.

Munkahelyi adatkezelés

Az új kollégák toborzása során, valamint a munkaviszony fennállása alatt alkalmazott különböző MI-alapú megoldások sok esetben képesek a munkáltatói érdekek védelmén és erősítésén túl a munkavállalók számára is előnyöket nyújtani. Az MI mun-

64 Salinas 2019
65 Lásd: www.aclu.org/cases/aclu-v-clearview-ai
66 Lásd: https://edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en
67 Lásd: https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en
68 Lásd: https://edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en

kahelyi alkalmazása körén belül említhetők például a toborzást segítő megoldások, amelyek egyfajta előszűrőt képeznek a társaságok döntéshozói számára, vagy épp támogatják ezek döntéshozatalát az érintettek értékelésével, míg más alkalmazások kifejezetten a munkavállalók képzését vagy ellenőrzésüket segítik elő.

Erre tekintettel egyre elterjedtebbnek mondhatók a munkavállalók munkavégzési hatékonyságának figyelésére szolgáló adatkezelési megoldások, amelyek azonban számos esetben túlzó behatást jelenthetnek az érintettek magánszférájára, sérthetik a jogszerűség, tisztességes eljárás és átláthatóság, valamint az adattakarékosság elvét. Erre tekintettel a munkavállalók megfigyelésére alkalmazható megoldások leginkább az anonimizált adatgyűjtések esetén (például belső munkahelyi hatékonyságot elemző statisztika készítése céljából) vagy – az egyik legenyhébb ellenőrzési eszközként – a munkahelyi hálózathoz kapcsolódó adatforgalom figyelése, és az azzal kapcsolatos rendellenességeknek a fokozatosság elvével összhangban való kivizsgálása esetén játszhatnak szerepet.

Magyarország tekintetében hangsúlyozandó, hogy a munka törvénykönyvéről szóló 2012. évi I. törvény (Mt.) személyiségi jogok védelmével, valamint adatvédelemmel kapcsolatos szakaszai[69] a munkahelyi adatkezelések, valamint a munkavállalói személyiségi jogok korlátozásával járó megoldások esetén többletkövetelményeket támasztanak a munkáltatókkal szemben. Tekintettel arra, hogy a munkahelyi ellenőrzések jellemzően és szükségszerűen a személyiségi jogok korlátozásával járnak, leszögezhető, hogy a korlátozás csak akkor foghat helyt, ha az a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos. Ez esetben pedig a munkáltatónak a munkavállalót a személyiségi jog korlátozásának módjáról, feltételeiről és várható tartamáról, továbbá szükségességét és arányosságát alátámasztó körülményekről előzetesen írásban tájékoztatnia kell.[70] A fentiek kapcsán azonban hangsúlyozandó, hogy a különböző MI-alapú megoldásokkal járó ellenőrzési megoldások jellemzően nem szükségesek a munkavállalók munkahelyi teljesítményének mérésére, és az adatkezelés ez esetben nem is tekinthető arányosnak, mivel a munkavállalói teljesítmény a legtöbb munkakörben ennél jóval enyhébb behatást jelentő ellenőrzési módokkal is vizsgálható.

A fentebb írtakat figyelembe véve leszögezhetjük, hogy a munkahelyen alkalmazott mesterségesintelligencia-megoldások egyik esetben sem működhetnek felügyelet nélkül, és olyan jövőt sem fogadhatunk el, ahol emberek sorsa felett korlátlan hatalmú gépek vagy algoritmusok döntenek. Erre szinte kafkai példát állít egy néhány évvel ezelőtti eset. Egy Los Angeles-i férfi főnöke elfelejtette megújítani a munkaszerződését, amit az irodája adminisztratív feladatait irányító MI-alapú rendszer azonnal észlelt. Elsőként a rendszer érvénytelenítette a férfi belépőkártyáját, majd kizárta az informatikai rendszerek jelentős részéből is, végül pedig értesítette a biztonsági szolgálatot, és kivezettette a férfit az épületből.[71]

69 Mt. 9–11/A. §
70 Mt. 9. § (1)–(2) bekezdés.
71 Wakefield 2018

További kockázatot jelent a munkahelyen alkalmazott MI-alapú rendszerek tekintetében az egyes rendszerek és alkalmazások eredeti célokkal összeegyeztethetetlen további célból való felhasználása, például WiFi-alapú nyomkövető rendszer alkalmazása a munkavállalók mozgásának és magatartásának folyamatos ellenőrzésére.[72] E kockázatok azonban a megfelelően átgondolt és transzparens adatkezelési gyakorlattal minimalizálhatók.

Egészségügyi adatkezelés

A különböző MI által támogatott szoftverek, okoseszközök és egyéb elemzések céljára szolgáló rendszerek az elmúlt években az egészségügyet is forradalmasították. Nem szabad azonban elfelejtenünk, hogy az e körbe tartozó információk az érintettek életének legintimebb szférájába tartoznak, ezeknek az illetéktelenek általi megismerése pedig kiemelt egzisztenciális veszélyt jelenthet az érintettekre nézve,[73] így az egészségügy területén való MI-alkalmazás esetén még jelentősebb hangsúllyal jelennek meg a lehetséges etikai problémák, amelyek teljes körű orvoslására vélhetőleg csak az MI- és egészségügyi szabályozás következő lépcsőfokai jelenthetnek megoldást. E körben különös kihívást jelenthet például az MI alkalmazása egészségügyi kutatások során gyűjtött adatok elemzése érdekében (például a betegek viselkedésének, hangulatának, állapotváltozásának megfigyelése, ezekkel kapcsolatos következtetések levonása), vagy az ápoló vagy szociális robotok elterjedése, az ezekkel való interakciók adatvédelmi megfelelésének biztosítása.

A fentieken túl hangsúlyozandó, hogy az úgynevezett gyenge mesterségesintelligencia-megoldások számára épp az egészségügy lehet az egyik kibontakozási terület. Az e megoldások és a mögöttük rejlő elgondolás lényege, hogy az MI-nek nem feladata, hogy az emberhez mérhető vagy vele konkuráló intelligens létformává váljon, sokkalta inkább az tekinthető az MI feladatának, hogy az embert támogassa, az emberi teljesítőképességet felerősítse, a napi ügyintézést és munkamenetet könnyebbé, hatékonyabbá tegye. Tekintettel arra, hogy az orvoslás és az egészségügyi tanácsadás jellegénél fogva megköveteli a szakember általi felülmérlegelést, így az MI szerepe ezen a területen a jövőben is vélhetőleg inkább segítőfunkciókra korlátozódik majd.[74]

Mindemellett azonban az MI szerepe egyes területeken és feladatkörökben az elkövetkezendő években kiemelkedővé válhat, sőt egyes innovációk már napjainkban is feszegetik az MI kapcsán korábban elképzelt lehetőségeket. Így az amerikai Harvard Medical School és Stanford egyetemek nemrég egy olyan MI-alapú megoldást fejlesztettek ki, amely önmaga képes röntgenképek alapján betegségek jeleit azonosítani.[75]

72 Az Adatvédelmi Munkacsoport 2/2017. számú véleménye a munkahelyi adatkezelésről, 11.
73 Trócsányi 2012, 401.
74 Lőrincz 2019, 3.
75 Kennedy 2022

Reklámcélú és egyéb adatkezelések

Az MI a fentieken túl számos egyéb területen is jelentős hatások kifejtésére lehet képes, amelyek átformálják azokat a szolgáltatásokat vagy jelenségeket, amelyeket az eddigi formájukban megszokhattunk. Néhány éve jelent meg például a Lexus gépjármű egyik újabb modelljét bemutató, első olyan reklám, amelynek forgatókönyvét teljes egészében MI írta. A szoftver több mint egy évtizedre visszamenőleg elemzett reklámfilmeket, és végül így jutott el a kívánt alkotás létrehozásáig.[76] Ilyen és ehhez hasonló alkotások természetesen a jövőben is várhatók; ezekkel kapcsolatban továbbá főként a szellemi tulajdonjogi kihívásoknak lesz majd jelentősége, azonban adatvédelmi szempontok is felmerülhetnek alkalmazásuk kapcsán (például valós embereket ábrázoló fényképek és videófelvételek felhasználása MI által).

Hangsúlyozandó azonban, hogy az MI reklámcélú, illetve ügyfélkapcsolati célú alkalmazása megfelelő szabályozás hiányában kifejezetten káros hatásokkal is járhat. Így például egy, az Ashley Madison nevű kanadai online társkereső szolgáltatóval kapcsolatos perben nyilvánvalóvá vált, hogy az oldal üzemeltetői magukat valós női felhasználóknak kiadó botok (tehát lényegében MI-alapú álprofilok) alkalmazása révén vettek rá jellemzően férfi felhasználókat az oldalon történő előfizetésre, vásárlásra.[77] Mindemellett jelentős sajtóvisszhangot kapott, hogy a Microsoft egy olyan chatbotmegoldást szabadalmaztatott, amelynek segítségével fiktív, történelmi, vagy akár elhunyt személyekkel (például: elhunyt szeretteikkel) is beszélgethetnek a felhasználók.[78] Mindez azonban értelemszerűen jelentős etikai aggályokat is felvethet, tekintettel arra, hogy a megoldás kontrollálatlan alkalmazása korábban soha nem látott, illetve nem ismert emocionális és pszichológiai megterhelést jelenthet a felhasználók számára, amelynek kezelésére hatékony szabályozói megközelítésre is szükség van.

Természetesen nem csak a reklámipar képes az MI robosztus elemzőképességének hasznosítására. Futótűzként terjednek a különböző fénykép-, videó-, valamint szövegelemző megoldások is, amelyek gigantikus mennyiségű adatot képesek rövid idő alatt elemezni és kategorizálni, messze meghaladva az emberi olvasás sebességét és munkabírását. A különböző, főleg forráskutatásra és adatbázisokban való keresésre építő MI-alapú megoldások ráadásul a jogászi munkát is nagymértékben segíthetik, például bírósági döntések keresésével, nagy mennyiségű dokumentumok áttekintésével vagy épp egyszerűbb formanyomtatványok, szerződésminták kitöltésével, automatizálásával. Kiemelendő azonban, hogy az ilyen megoldások sem jelentenek alternatívát sem a jogalkotás, sem a tényleges jogalkalmazás számára, tekintettel arra, hogy e folyamatok olyan komplex, értékalapú döntések meghozatalát követelik meg, amelyre napjainkban csak az ember képes.[79]

76 Griner 2018
77 In re Ashley Madison Customer Data Sec. Breach Litig., 148 F. Supp. 3d 1378, 1380 (JPML 2015)
78 Duffy 2021
79 Pázmándi 2018, 12.

Sajnálatosan az MI alkalmazására számos negatív, kártékonynak mondható példát is találni. Jelentős kockázatot jelenthetnek például az érintettek magánszférájára az úgynevezett „deepfake"-tartalmak. Ezek lényegében MI-alapú megoldások által manipulált videó-, kép-, illetve hangfelvételek. A már napjainkban is elérhető megoldások képesek például olyan mondatokat vagy cselekményeket tulajdonítani egy-egy személynek, amelyet a való életben valószínűleg sohasem mondana vagy tenne, de képesek lehetnek akár több személy vonásait is egyesíteni, fiktív személyeket létrehozni. A fenti megoldásokkal nyilvánvaló, hogy új vagy manipulált személyes adatok jönnek létre, sok esetben az érintettek további azonosíthatósága mellett, valamint személyiségi jogaik csorbítása vagy mások félrevezetése érdekében, így alapelvi szinten szembe menve a személyiségi jogok és a magánszféra védelmével. Ettől azonban sok esetben nehéz elkülöníteni a deepfake-technológia olyan alkalmazását, ahol az például a humor, a politikai szatíra vagy a kritika eszközéül szolgál.

A fentieken túl természetesen megszámlálhatatlan területről beszélhetünk még, ahol az MI-nek az adott iparág forradalmasításán túl a személyes adatok kezelése tekintetében is kiemelt hatása van. Ilyennek mondható például az MI közlekedési célú alkalmazása, de akár a nemzetbiztonság vagy az oktatás területe is. Ez utóbbi különösen azért fontos, mert a digitális analfabetizmus felszámolásáért folytatott küzdelmen túl a munkaképes lakosság digitális kompetenciáinak fejlesztését is segítheti,[80] így az MI pozitív társadalomformáló szerepe e körben különös hangsúlyt nyerhet.

Zárógondolatok

A fentiekre tekintettel megállapítható, hogy a mesterséges intelligencia mint napjaink egyik kiemelkedő technológiai vívmánya, társadalmi, tudományos és gazdasági hatása mellett a személyes adatok kezelésére, valamint a magánélet védelmére is kiemelt hatással van.

Erre tekintettel pedig az MI-alapú megoldásokat alkalmazó adatkezelőknek még az adott megoldás kidolgozása, illetve bevezetése előtt tételesen meg kell tervezniük az adatkezelés menetét és az érintetti jogok gyakorlását támogató megoldásokat, műveleteket, valamint ki kell alakítaniuk az adatok védelmét segítő intézkedések körét. E körbe tartozhat különösen a megfelelő tájékoztatók és belső szabályzatok elkészítése és szükséges körű elérhetővé tétele az érintettek részére, valamint a személyes adatok kezelését végző vagy az adott rendszert, megoldást alkalmazó munkavállalói állomány képzése.

Tekintettel arra, hogy az MI általi adatkezelés az érintettek számára jelentős kockázatokkal járhat, illetve az adatkezelők kezében sok esetben társadalmilag káros túlhatalmat is eredményezhet, így az MI általi adatkezelés kapcsán az adatvédelmi és adatbiztonsági elvárások fokozott hangsúllyal kell hogy érvényesüljenek. Ez pedig különösen igaz a jelentős adattömegek felett rendelkező nagyvállalatok, valamint ál-

80 Czékmann–Ritó 2018, 59.

lami szervek, illetve hatóságok adatkezeléseire, amelyeket vezércsillagként kell hogy vezesse a transzparenciára törekvés, az adatkezelők társadalmi elszámoltathatósága, valamint a közbizalom és a demokratikus társadalom megfelelő működésének védelme. Ennek segítségével ugyanis az MI alkalmazásával, azonban az adatvédelmi tudatosság megőrzése mellett valósítható meg a nagyvállalatok oldaláról a szolgáltatások minőségének javítása, valamint a kutatási és fejlesztési tevékenységek felgyorsítása, az állami szereplők esetében pedig a hatékonyabb ügyintézés, a hatósági ügykezelés és a közbiztonság egy magasabb szintje.[81]

Irodalomjegyzék

Agencia Española de Protección de Datos (2020): *GDPR Compliance of Processings that Embed Artificial Intelligence. An Introduction* (2020. február). Online: www.aepd.es/sites/default/files/2020-07/adecuacion-rgpd-ia-en.pdf

Asimov, Isaac (1942): Runaround. *Astounding Science-Fiction,* 29(1).

Barfield, Woodrow: Towards a Law of Artificial Intelligence. In Woodrow Barfield – Ugo Pagallo: *Research Handbook on the Law of Artificial Intelligence.* Cheltenham (UK) – Northhampton (USA), Edward Elgar, 2018. 2–39. Online: https://doi.org/10.4337/9781786439055.00011

Bradley, Tony (2017): Facebook AI Creates Its Own Language in Creepy Preview of Our Potential Future. *Forbes,* 2017. július 31. Online: https://bit.ly/3CUZahm

Buzás Péter (2018): Az érintett jogai. In Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról.* Budapest, Wolters Kluwer Hungary. 149–206.

Claire Duffy: Microsoft Patented a Chatbot That Would Let You Talk to Dead People. It Was Too Disturbing For Production. *CNN Business*, 2021. január 27. Online: https://edition.cnn.com/2021/01/27/tech/microsoft-chat-bot-patent/index.html

Computer AI Passes Turing Test in 'World First'. *BBC News,* 2014. június 9. Online: www.bbc.com/news/technology-27762088" www.bbc.com/news/technology-27762088

Czékmann Zsolt – Ritó Evelin (2018): Úton az információs társadalom felé – a kormányzati stratégiák tükrében. *Infokommunikáció és Jog,* 2(71), 54–60.

Datatilsynet (2018): *Artificial Intelligence and Privacy.* Report (2018. január). Online: www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

Elek István (2015): *Az intelligencia spontán megjelenése.* Budapest, ELTE Eötvös.

Fekete István – Gregorics Tibor – Nagy Sára (1990): *Bevezetés a mesterséges intelligenciába.* Budapest, LSI Oktatóközpont.

Griner, David (2018): An AI Tried to Write the Perfect Lexus Ad. Here's a Scene-by-Scene Look at What It Was Thinking. *Adweek,* 2018. november 19. Online: www.adweek.com/programmatic/an-ai-tried-to-write-the-perfect-lexus-ad-heres-a-scene-by-scene-look-at-what-it-was-thinking/

Information Commissioner's Office (2018): *Investigation into the Use of Data Analytics in Political Campaigns.* A Report to Parliament. Online: https://bit.ly/3IRRZu9

Innovációs és Technológiai Minisztérium (2020): *Magyarország Mesterséges Intelligencia Stratégiája 2020–2030.* Online: https://ai-hungary.com/api/v1/companies/15/files/137203/view

81 Necz 2020b, 53.

Kennedy, Shania (2022): Harvard, Stanford Develop Self-Supervised AI to Detect Disease Via X-ray. *Health IT Analytics*, 2022. szeptember 19. Online: https://healthitanalytics.com/news/harvard-stanford-develop-self-supervised-ai-to-detect-disease-via-x-ray

Kosinski, Michal – David Stillwell – Thore Graepel (2013): Private Traits and Attributes are Predictable from Digital Records of Human Behaviour. *Proceedings of the National Academy of Sciences of the United States of America,* 110(15), 5802–5805. Online: https://doi.org/10.1073/pnas.1218772110

Lőrincz György (2019): A mesterséges intelligencia alkalmazásával hozott döntés jogi megítélésének egyes kérdései. *Gazdaság és Jog,* 4(27), 1–7.

Necz Dániel (2020a): A mesterséges intelligencia adatvédelmi szempontjai, különös tekintettel a belügyi szervek adatkezelési gyakorlatára. *Rendvédelem,* 9(1), 135–165.

Necz Dániel (2020b): A mesterséges intelligencia belügyi és biztonsági célú alkalmazása. *Scientia et Securitas,* 1(1), 49–53. Online: https://doi.org/10.1556/112.2020.00008

Pázmándi Kinga (2018): Digitalizáció, technológiai fejlődés, jogi paradigmák. *Gazdaság és Jog,* 26(12), 10–14.

Perecz László (2012): Információs forradalom és globalizáció. In Pázmándi Kinga – Verebics János (szerk.): *E-Jog.* Budapest, HVG-ORAC. 17–23.

Salinas, Sara (2019): Facebook Says It Made an A.I. Tool That Can Detect Revenge Porn Before It's Reported. *CNBC,* 2019. március 15. Online: www.cnbc.com/amp/2019/03/15/facebook-ai-tool-detects-revenge-porn-before-its-reported.html

Sappa, Cristiana (2019): How Data Protection Fits with the Algorithmic Society in Two Intellectual Property Rights. A Comparative Analysis. *Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil,* 68(2) 135–144.

Trócsányi Sára (2012): Személyes adatok kezelése az egészségügyben. In Péterfalvi Attila (szerk.): *Adatvédelem és információszabadság a mindennapokban.* Budapest, HVG-ORAC. 401–425.

Turing, Alan M. (1950): Computing Machinery and Intelligence. *Mind,* 59(236), 433–460. Online: https://doi.org/10.1093/mind/LIX.236.433

Wakefield, Jane (2018): The Man Who Was Fired by a Machine. *BBC News,* 2018. június 21. Online: www.bbc.com/news/technology-44561838

Jogforrások

2012. évi I. törvény a munka törvénykönyvéről

2013. évi V. törvény a Polgári Törvénykönyvről

301/2016. (IX. 30.) Korm. rendelet a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről

Az Európai Adatvédelmi Testület és az Európai Adatvédelmi Biztos 5/2021. sz. közös véleménye a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról szóló európai parlamenti és tanácsi rendeletről

Az Európai Parlament és a Tanács (EU) 2016/679. sz. 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; GDPR) Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32016R0679

Az Adatvédelmi Munkacsoport 2/2017. számú véleménye a munkahelyi adatkezelésről. Online: https://ec.europa.eu/newsroom/article29/items/610169

Az Adatvédelmi Munkacsoport WP251rev.01 sz. irányelve az automatizált döntéshozatalról és a profilalkotásról. Online: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Az Adatvédelmi Munkacsoport WP260 rev. 01 véleménye az átláthatóságról. Online: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

California Legislative Information (2019): *AB-730 Elections: Deceptive Audio or Visual Media (2019–2020).* Online: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB730

Európai Bizottság: *A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Az emberközpontú mesterséges intelligencia iránti bizalom növelése.* COM(2019) 168 final. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52019DC0168

Európai Bizottság: *A Bizottság közleménye Mesterséges intelligencia Európa számára.* COM(2018) 237 final/2. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52018DC0237R(01)

Európai Bizottság: *Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése.* Brüsszel, 2020.2.19. COM(2020) 65 final. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:52020DC0065

In re Ashley Madison Customer Data Sec. Breach Litig., 148 F. Supp. 3d 1378, 1380 (JPML 2015)

Javaslat, az Európai Parlament és a Tanács Rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról, Brüsszel, 2021.4.21. COM(2021) 206 final, 2021/0106(COD). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52021PC0206

A NAIH/2015/2201/17/H. sz. határozata

A NAIH/2019/55. sz. határozata

A NAIH/2019/167. sz. határozata

A NAIH/2019/363/2. sz. határozata

A NAIH/2019/2526. sz. határozata

NAIH-85-3/2022. sz. határozata

NAIH-2501-10/2022. sz. határozata

A NAIH ajánlása az előzetes tájékoztatás adatvédelmi követelményeiről. Online: www.naih.hu/files/tajekoztato-ajanlas-v-2015-10-09.pdf

A NAIH tájékoztatója a munkahelyi adatkezelés alapvető követelményeiről. Online: www.naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf